Rapid Recovery 6.2

Guia do usuário

Table of Contents

Introdução ao Rapid Recovery **14**
Core Console **15**
Acesso ao Rapid Recovery Core Console 15
Noções básicas sobre o Guia de início rápido 15
Ocultação do Guia de início rápido 17
Navegar até o Rapid Recovery Core Console 18
Compreensão da área de navegação esquerda 19
Visualização da página Início do Rapid Recovery Core Console 20
Como entender a página Início (visualização de tabelas resumidas) 20
Noções básicas sobre os relatórios do painel do Core 23
Visualização do menu Máquinas protegidas 23
Visualização das informações de resumo de uma máquina protegida 24
Exibindo o painel de resumo 24
Visualização de volumes em uma máquina protegida 25
Exibindo informações de replicação 25
Visualizar o painel de informações do Exchange Server 25
Visualização do painel de informações do SQL Server 25
Visualização das informações de resumo de um host 25
Como ver pontos de recuperação para uma máquina 26
Visualizar eventos de uma máquina protegida 27
Visualização de relatórios para uma máquina protegida 29
Ver máquinas replicadas no menu de navegação 29
Visualizar o menu Apenas pontos de recuperação 30
Visualizar o menu Grupos personalizados 30
Usar a caixa de diálogo Erro 30
Definições do Core **32**
Funções principais das definições do Core 32
Criar cópia de segurança e restaurar definições do Core 33
Reiniciar ou encerrar o serviço Core 34
Definições do Rapid Recovery Core 35
Configurar definições gerais do Core 39
Configuração das definições de atualização 41
Noções básicas sobre trabalhos noturnos 43
Configurar trabalhos noturnos para o Core 46
Modificar definições de fila de transferência 47
Ajustar definições de tempo limite do cliente 47

Noções básicas sobre o cache de deduplicação e locais de armazenamento 48
Configurar definições de cache de deduplicação DVM 50
Configurar as definições do mecanismo Replay 51
Configurar as definições do implantação 52
Configurar definições de conexão de banco de dados 53
Modificar definições de conexão do database local 55
Gerenciar definições do servidor de SMTP 56
Configurar as definições de conexão da conta de nuvem 56
Trabalhar com certificados de gerenciamento do Azure associados ao seu Core 57
Obter o arquivo de configurações de publicação para sua conta do Azure 57
Carregar um certificado de gerenciamento do Azure 58
Atualizar ou excluir certificados de gerenciamento do Azure 59
Gerenciamento de definições de relatórios 59
Gerenciar definições da capacidade de anexação do SQL 60
Noções básicas sobre trabalhos do Core 62
Definições de trabalhos do Core 66
Adição de trabalhos do Core às definições 66
Editar as definições de trabalhos do Core 67
Gerenciar licenças 68
Atualização ou alteração de uma licença 70
Adição de uma licença 71
Contatar o servidor do Portal de licenças do Rapid Recovery 72
Definir as definições do SNMP 72
Definir as configurações do SNMP 73
Fazer o download do arquivo MIB SNMP 74
Configuração das definições do vSphere 75
Gerenciar as configurações de proxy do VMware 76
Configurar as definições do VFogLight 77
Ferramentas de nível do Core 77
Noções básicas sobre as informações do sistema do Core 78
Como visualizar informações do sistema do Core 79
Acessar os logs do Core 79
Como baixar e exibir o arquivo de log do Core 80
Repositórios 81
Noções básicas sobre repositórios 81
Deduplicação no Rapid Recovery 84
Gerenciamento de um repositório de DVM 85
Criar um repositório de DVM 86

Adicionar um local de armazenamento a um repositório de DVM existente..... 89
Sobre como verificar a integridade dos repositórios DVM..... 91
Executar uma verificação de integridade em um repositório DVM..... 92
Sobre a otimização do repositório DVM..... 93
Otimização de um repositório de DVM..... 94
Interromper ou retomar a otimização do repositório DVM..... 94
Gerenciamento de um repositório de camadas..... 95
Criar um repositório de camadas..... 96
Verificar um repositório..... 98
Alteração das configurações do repositório..... 99
Conectar a um repositório existente..... 99
Ver ou modificar detalhes do repositório..... 101
Desconectando um repositório..... 104
Excluir um repositório..... 105
Gerenciar privacidade..... 106
Conformidade com a regulamentação de proteção de dados gerais..... 106
Como o Rapid Recovery usa informações pessoais..... 107
Restrições de chave de licença não telefônica..... 108
Obtenção e uso de licenças de telefone não residencial..... 109
Criptografia..... 111
Noções básicas sobre chaves de criptografia..... 111
Criptografar os dados em transporte em uma rede..... 112
Aplicar ou remover chaves de criptografia..... 112
Associar uma chave de criptografia a uma máquina protegida..... 113
Aplicar uma chave de criptografia a partir da página Máquinas protegidas..... 114
Desassociar uma chave de criptografia de uma máquina protegida..... 115
Gerenciar chaves de criptografia..... 116
Adicionar uma chave de criptografia..... 118
Importar uma chave de criptografia..... 119
Desbloquear uma chave de criptografia..... 119
Bloquear uma chave de criptografia..... 120
Editar uma chave de criptografia..... 121
Alterar a frase de acesso de uma chave de criptografia..... 122
Exportar uma chave de criptografia..... 122
Remover uma chave de criptografia..... 123
Como alterar tipos de chave de criptografia..... 123
Protegendo máquinas..... 125
Sobre como proteger máquinas com Rapid Recovery..... 125

Fatores ao escolher proteção com base em agente ou sem agente..... 126
Sobre como proteger as máquinas Linux com o Rapid Recovery..... 128
Sobre a proteção de servidores de banco de dados Oracle..... 128
Inserir ou editar credenciais de bancos de dados Oracle..... 130
Ativar modo de log de arquivo e adicionar o gravador VSS para bancos de dados Oracle protegidos..... 132
Sobre o truncamento de logs do Oracle..... 133
Truncamento manual de logs de banco de dados Oracle..... 133
Gerenciamento de servidores de aplicativos protegidos no Rapid Recovery Core..... 134
Sobre a proteção de clusters do servidor..... 135
Noções básicas sobre Rapid Snap for Virtual..... 135
Benefícios de instalar as ferramentas do hipervisor para proteção sem agente..... 140
Entendendo backups consistentes de falhas e consistentes de aplicativo..... 141
Noções básicas do instalador de software do agente Rapid Recovery..... 141
Como baixar o Rapid Recovery Agent Installer..... 142
Implantação do agente em várias máquinas simultaneamente a partir do Core Console..... 142
Como usar o assistente de implantação do software do agente para implantar em uma ou mais máquinas..... 143
Implantar em máquinas de um domínio Active Directory..... 144
Implantar em máquinas em um host virtual VMware vCenter/ESXi..... 145
Aplicar um upgrade do Software do agente Rapid Recovery em máquinas protegidas..... 146
Implantar nas máquinas manualmente..... 147
Verificar a implantação em várias máquinas..... 147
Modificar definições de implantação..... 148
Noções básicas sobre programações de proteção..... 149
Proteção de uma máquina..... 150
Proteger um cluster..... 155
Proteger nós em um cluster..... 160
Criar programações de proteção personalizada no Modo Simples..... 161
Criar vários períodos de programação de proteção no Modo Avançado..... 162
Pausar e retomar a proteção..... 164
Sobre como proteger diversas máquinas..... 166
Como proteger diversas máquinas em um domínio Active Directory..... 167
Proteger diversas máquinas em um host virtual VMware vCenter/ESXi..... 171
Proteger máquinas virtuais vCenter/ESXi usando a proteção sem agente..... 176
Proteger diversas máquinas em um host virtual Hyper-V..... 181
Proteger máquinas virtuais Hyper-V usando a proteção sem agente..... 186
Como proteger diversas máquinas manualmente..... 191
Monitorar a proteção de várias máquinas..... 196

Ativar o suporte a aplicativos..... 196
Definições e funções para servidores protegidos do Exchange..... 197
Definir credenciais para uma máquina do Exchange Server..... 198
Forçar o truncamento de log para uma máquina Exchange..... 199
Sobre verificações de montabilidade do banco de dados no Exchange..... 199
Forçar uma verificação de capacidade de montagem de um banco de dados do Exchange.....200
Forçar uma verificação de soma de verificação dos arquivos do banco de dados do Exchange.....200
Definições e funções para servidores SQL protegidos.....201
Definir credenciais para uma máquina SQL Server.....202
Forçar truncamento de log para uma máquina SQL.....202
Sobre a capacidade de anexação do SQL..... 203
Forçar uma verificação de capacidade de anexação do SQL Server..... 204
Gerenciar máquinas protegidas..... 205
Sobre o gerenciamento de máquinas protegidas..... 205
Visualizar máquinas protegidas.....205
Visualizar informações de resumo de cluster.....206
Configurar as definições da máquina.....206
Visualização e modificação das definições de máquina protegida..... 207
Alterar as configurações para um host ou nó Hyper-V..... 211
Alterar as configurações para uma máquina virtual protegida Hyper-V..... 212
Alterar as configurações do vSphere para uma máquina virtual protegida VMware..... 213
Sobre a modificação das definições da transferência.....214
Estrangulamento da velocidade de transferência.....215
Personalizar trabalhos noturnos para uma máquina protegida.....216
Visualização das informações do sistema de uma máquina protegida.....217
Gerenciar máquinas.....218
Remover uma máquina..... 218
Remover um cluster da proteção..... 218
Remover nós de cluster da proteção..... 219
Remover todos os nós de um cluster da proteção.....219
Visualizar informações de licença em uma máquina..... 219
Download e visualização do arquivo de log de uma máquina protegida..... 220
Converter um nó de cluster protegido em uma máquina protegida..... 220
Noções básicas sobre grupos personalizados.....221
Criar grupos personalizados.....221
Modificar nomes de grupos personalizados.....222
Remover grupos personalizados..... 223

Realizar ações de grupo....223
Visualizar todas as máquinas de um grupo personalizado em uma página.... 224
Instantâneos e pontos de recuperação.... 225
Gerenciar snapshots e pontos de recuperação.... 225
Ver a página de pontos de recuperação de uma máquina protegida....225
Noções básicas sobre os indicadores de status do ponto de recuperação.... 227
Montar um ponto de recuperação....228
Desmontar pontos de recuperação....229
Trabalhar com pontos de recuperação do Linux.... 230
Montar um volume de ponto de recuperação em máquina Linux....230
Desmontar um ponto de recuperação em uma máquina Linux.... 232
Forçar um snapshot....232
Remover pontos de recuperação....233
Excluir uma cadeia de pontos de recuperação órfãos....234
Como migrar pontos de recuperação para um repositório diferente....234
Replicação.... 236
Replicação com Rapid Recovery.... 236
Cadeias de pontos de recuperação e órfãos....240
Quando a replicação começar.... 241
Determinar suas necessidades e sua estratégia de seeding.... 241
Considerações sobre desempenho para transferência de dados replicados.... 243
Sobre replicação e pontos de recuperação criptografados....245
Sobre políticas de retenção para replicação....245
Ver a replicação de entrada e saída....245
Configurar a replicação.... 247
Replicar para um Core de destino autogerenciado.... 248
Replicar para um Core de destino de terceiros....252
Enviar uma solicitação de replicação para um provedor de serviços terceirizado.... 252
Revisar uma solicitação de replicação de um cliente.... 255
Aprovar uma solicitação de replicação....256
Negar uma solicitação de replicação.... 256
Ignorar uma solicitação de replicação de um cliente....257
Adicionar uma máquina a uma replicação existente.... 257
Consumo da unidade de propagação em um Core de destino.... 260
Abandonar uma unidade de propagação....261
Gerenciar definições de replicação....262
Programar a replicação.... 262
Usar a função Copiar para criar uma unidade de propagação....263

Monitorar a replicação..... 265
Pausar e retomar a replicação..... 267
Forçar a replicação..... 268
Gerenciar definições para replicação de saída..... 268
Alterar configurações de Core de destino..... 269
Definir a prioridade de replicação de uma máquina protegida..... 270
Remover replicação de saída do Core de origem..... 270
Remover replicação de entrada do Core de destino..... 271
Recuperar dados replicados..... 272
Eventos..... 273
Como exibir eventos usando tarefas, alertas e páginas de diário..... 273
Visualizar tarefas..... 274
Ver as tarefas em execução de qualquer página do Core Console..... 276
Suspender ou retomar tarefas agendadas..... 276
Visualizar alertas..... 277
Ver um diário de todos os eventos registrados..... 278
Navegar entre tarefas, alertas e diário de eventos..... 279
Noções básicas sobre as notificações de eventos no Rapid Recovery..... 280
Configurar grupos de notificação..... 282
Noções básicas sobre notificações por e-mail..... 285
Configurar um servidor de e-mail..... 285
Configurar um modelo de e-mail de notificação..... 287
Definir as configurações de evento..... 289
Sobre redução de repetição..... 290
Configurar redução de repetição..... 290
Configurar retenção de eventos..... 290
Relatório..... 292
Sobre os relatórios do Rapid Recovery..... 292
Gerar um relatório no Core Console..... 294
Gerar um relatório de Core sob demanda..... 294
Gerar um relatório de máquina protegida sob demanda..... 297
Gerenciar relatórios programados no Core Console..... 298
Programar um relatório..... 299
Modificar a programação de um relatório..... 302
Interromper, retomar ou excluir um relatório programado..... 302
Usar o menu de relatórios..... 303
Usar a barra de ferramentas Relatórios..... 304
Noções básicas sobre o relatório do trabalho..... 305

Noções básicas sobre o relatório de resumo dos trabalhos....306
Noções básicas sobre o relatório de falhas....307
Noções básicas sobre o relatório resumido....307
Noções básicas sobre o relatório do Repositório....308
Noções básicas sobre o relatório de resumo clássico....309
Exportação da VM....310
Exportação para máquinas virtuais usando o Rapid Recovery....310
Exportar dados para uma máquina virtual ESXi....312
Realizar uma exportação única para ESXi....312
Configurar a exportação contínua para ESXi....314
Exportar dados para uma máquina virtual VMWare Workstation....315
Realizar uma exportação única para VMware Workstation....316
Configurar a exportação contínua para VMware Workstation....317
Exportar dados para uma máquina virtual Hyper-V....319
Realizar uma exportação única de Hyper-V....320
Configurar a exportação contínua para Hyper-V....321
Exportar dados para uma máquina virtual VirtualBox....323
Realizar uma exportação única de VirtualBox....324
Configurar a exportação contínua para VirtualBox....325
Exportar dados para uma máquina virtual Azure....326
Trabalhar com o Microsoft Azure....327
Aviso de isenção de responsabilidade da interface do Azure....327
Criar um contêiner na conta de armazenamento do Azure....327
Documentação do Microsoft Azure....328
Antes da exportação virtual para o Azure....329
Exportar e implantar VMs para Azure....329
Realizar uma exportação única para o Azure....330
Configurar a exportação contínua para Azure....334
Implantar uma máquina virtual no Azure....336
Gerenciar exportações....338
Restaurar dados....341
Sobre como restaurar dados com o Rapid Recovery....341
Noções básicas sobre Live Recovery....341
Restaurar dados de pontos de recuperação....342
Sobre o recurso de pesquisa e restauração de arquivo....343
Localizar e restaurar um arquivo....344
Sobre restauração de volumes a partir de um ponto de recuperação....346
Restaurar volumes a partir de um ponto de recuperação....347

Restaurar um diretório ou arquivo usando o Windows Explorer..... 350
Restaurar um diretório ou arquivo e preservar as permissões usando o Windows Explorer..... 350
Restaurar clusters e nós de cluster..... 351
Restauração a partir de um arquivo anexado..... 351
Restauração de e-mail no Rapid Recovery..... 352
Pré-requisitos de restauração de e-mail..... 353
Abrir um banco de dados do Exchange no Rapid Recovery..... 353
Restaurar um item de e-mail no Rapid Recovery..... 354
Bare metal restore..... 358
Restauração sem sistema operacional para máquinas Windows..... 358
Realizar uma restauração sem sistema operacional para máquinas Windows..... 359
Pré-requisitos para realizar uma restauração sem sistema operacional para uma máquina Windows..... 360
Realizar um bare metal restore usando o Assistente de restauração de máquina..... 361
Entender a criação do CD de inicialização para máquinas Windows..... 365
Entender a injeção de drivers em um CD de inicialização..... 365
Criar uma imagem ISO do CD de inicialização..... 366
Como transferir a imagem ISO do CD de inicialização para a mídia..... 367
Como carregar o CD de inicialização e iniciar o computador de destino..... 368
Como usar o Universal Recovery Console para uma BMR..... 368
Sobre as ferramentas do Universal Recovery Console..... 369
Carregar drivers usando o Universal Recovery Console..... 369
Carregar drivers no Universal Recovery Console usando mídia portátil..... 370
Como carregar um driver no URC usando o Chromium..... 371
Como selecionar um ponto de recuperação e iniciar uma BMR..... 371
Sobre como mapear volumes para uma restauração sem sistema operacional..... 372
Como mapear manualmente discos para uma BMR..... 373
Mapear manualmente discos para obter uma BMR..... 373
Como realizar uma BMR com base em um arquivo..... 374
Carregar os drivers no sistema operacional..... 377
Realizar uma bare metal restore em máquinas Linux..... 377
Pré-requisitos para realizar uma bare metal restore em máquinas Linux..... 379
Gerenciar uma imagem de inicialização do Linux..... 379
Sobre a imagem ISO de inicialização para Linux..... 380
Salvar a imagem ISO do Live DVD em mídia..... 381
Carregar o Live DVD e iniciar o computador de destino..... 381
Conectar-se ao destino BMR a partir do Rapid Recovery Core..... 381
Como gerenciar partições do Linux..... 382

Criar partições na unidade de destino....382
Formatar partições na unidade de destino....383
Montar partições a partir da linha de comando....383
Iniciar uma restauração sem sistema operacional para Linux....384
Iniciar o utilitário Screen....385
Realizar uma bare metal restore em uma máquina Linux usando a linha de comando....385
Restaurar volumes em uma máquina Linux usando a linha de comando....387
Confirmar uma bare metal restore....388
Visualizar o progresso da recuperação....389
Iniciar um servidor de destino restaurado....389
Como solucionar problemas de conexão com o Universal Recovery Console....389
Como reparar problemas de inicialização....390
Confirmar a restauração sem sistema operacional na linha de comando....390
Realizar uma verificação do sistema de arquivos no volume restaurado....390
Como usar a linha de comando para tornar uma máquina Linux restaurada inicializável....391
Como gerenciar dados de classificação por vencimento....393
Retenção de dados, enfileiramento para armazenamento secundário e arquivamento....393
Gerenciar políticas de retenção....394
Configurar as definições da política de retenção padrão do Core....394
Personalizar as definições de política de retenção de uma máquina protegida....397
Forçar rollup para uma máquina protegida....399
Arquivamento....401
Noções básicas sobre arquivos....401
Opções de criação e armazenamento de arquivo....401
Opções de armazenamento e arquivamento da Amazon....402
Opções de cadeia de pontos de recuperação para arquivos....403
Métodos para acessar um arquivo....404
Usos para arquivos....404
Criar um arquivo....404
Arquivar na nuvem....408
Editar um arquivo programado....409
Pausar ou retomar um arquivo programado....411
Forçar um trabalho de arquivo....411
Verificar um arquivo....412
Anexar um arquivo....413
Importação de um arquivo....414
Contas de nuvem....417

Sobre contas de nuvem..... 417
Considerando opções de armazenamento na nuvem..... 418
Adicionar uma conta de nuvem..... 419
Editar uma conta de nuvem..... 422
Remover uma conta de nuvem..... 422
O Local Mount Utility..... 423
Sobre o Local Mount Utility..... 423
Trabalhar com máquinas Rapid Recovery Core no Utilitário de montagem local..... 423
Adicionar uma máquina Core ao Local Mount Utility..... 424
Alterar as opções do Local Mount Utility..... 425
Como editar definições de conexão do Core no Local Mount Utility..... 426
Reconectar a um Core..... 427
Como remover uma máquina Rapid Recovery Core do Local Mount Utility..... 427
Trabalhar com máquinas protegidas no Local Mount Utility..... 427
Montar um ponto de recuperação usando o Local Mount Utility..... 427
Usar o Local Mount Utility para explorar um ponto de recuperação montado..... 428
Atualizar pontos de recuperação..... 429
Desmontar pontos de recuperação no Local Mount Utility..... 429
Referências do Core Console..... 430
Como ver a interface do usuário do Core Console..... 430
Visualizar máquinas protegidas..... 438
Visualizar eventos de uma máquina protegida..... 439
Visualizar o menu Mais de uma máquina protegida..... 441
Third-party contributions..... 442
Apache 2.0..... 448
Chromium BSD License N/A..... 450
Code Project Open License (CPOL) 1.02..... 451
Far Manager BSD License N/A..... 454
GNU AFFERO GENERAL PUBLIC LICENSE..... 454
GPL (GNU General Public License) 2.0..... 462
LGPL (GNU Lesser General Public License) 2.1..... 466
OpenSSL 1.0..... 471
Sobre nós..... 474

Copyright © 2018 Quest Software Inc.

TODOS OS DIREITOS RESERVADOS.

Este guia contém informações proprietárias protegidas por direitos autorais. O software descrito neste guia é fornecido com uma licença de software ou um acordo de não divulgação. Este software pode ser usado ou copiado somente segundo os termos do acordo aplicável. Nenhuma parte deste guia pode ser reproduzida ou transmitida de qualquer forma ou por qualquer meio, eletrônico ou mecânico, incluindo fotocópias e gravações para qualquer outro fim que não o uso pessoal do comprador sem permissão por escrito da Quest Software Inc.

As informações contidas neste documento são fornecidas em conjunto com os produtos da Quest Software. Nenhuma licença, expressa ou implícita, por preclusão ou de outra forma, a quaisquer direitos de propriedade intelectual é concedida por este documento ou em conexão com a venda dos produtos da Quest Software. EXCETO CONFORME DEFINIDO NOS TERMOS E CONDIÇÕES ESPECIFICADOS NO ACORDO DE LICENÇA DESTE PRODUTO, A QUEST SOFTWARE NÃO ASSUME NENHUMA RESPONSABILIDADE E RENUNCIA QUALQUER GARANTIA EXPRESSA, IMPLÍCITA OU ESTABELECIDA POR LEI RELACIONADA A SEUS PRODUTOS INCLUINDO, MAS NÃO LIMITADO A, GARANTIA IMPLÍCITA DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UMA FINALIDADE ESPECÍFICA OU NÃO VIOLAÇÃO. EM NENHUMA CIRSCUSTÂNCIA A QUEST SOFTWARE SERÁ RESPONSÁVEL POR QUAISQUER DANOS DIRETOS, INDIRETOS, CONSEQUENCIAIS, PUNITIVOS, ESPECIAIS OU INCIDENTAIS (INCLUINDO, SEM LIMITAÇÃO, DANOS POR PERDA DE LUCROS, INTERRUPÇÃO DE NEGÓCIOS OU PERDA DE INFORMAÇÕES) RESULTANTES DO USO OU DA INCAPACIDADE DE USAR ESTE DOCUMENTO, MESMO SE A QUEST SOFTWARE TIVER SIDO NOTIFICADA A RESPEITO DA POSSIBILIDADE DE TAIS DANOS. A Quest Software não faz representações ou garantias com relação à precisão ou integridade do conteúdo deste documento e se reserva o direito de fazer alterações em especificações e descrições de produtos a qualquer momento e sem aviso. A Quest Software não faz nenhum compromisso em atualizar as informações contidas neste documento.

Se você tem quaisquer dúvidas ou perguntas sobre seu potencial uso deste material, entre em contato com:

Quest Software Inc., Attn: LEGAL Dept., 4 Polaris Way, Alisa Viejo, CA 92656.

Consulte o nosso website (https://www.quest.com) para obter informações de contato de escritórios regionais e internacionais

Patentes

Nós, da Quest Software, temos orgulho da nossa tecnologia avançada. Patentes em vigor e pendentes podem se aplicar a este produto. Para informações atualizadas sobre as patentes aplicáveis a este produto, acesse https://www.quest.com/legal.

Marcas registradas

Quest, o logotipo Quest e Join the Innovation são marcas comerciais e marcas registradas da Quest Software Inc. Para a lista completa de marcas da Quest, acesse https://www.quest.com/legal/trademark-information.aspx. Todas as outras marcas comerciais e registradas são de propriedade dos seus respectivos proprietários.

Legenda



WARNING: um ícone de ADVERTÊNCIA indica um potencial de danos à propriedade, risco de lesões corporais ou mesmo de risco de vida.

CAUTION: Um ícone de CUIDADO indica a possibilidade de danos ao hardware ou perda de dados caso as instruções não sejam seguidas.



IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: Um ícone de informações indica informações de suporte.

Introdução ao Rapid Recovery

O Rapid Recovery é uma solução de backup, replicação e recuperação que oferece objetivos de tempo de recuperação e de ponto de recuperação quase zero. O Rapid Recovery oferece proteção de dados, recuperação de desastres, migração e gerenciamento de dados. Você tem a flexibilidade de executar uma bare metal restore (para hardware similar ou não) e pode restaurar os backups em máquinas virtuais ou físicas, independentemente da origem. O Rapid Recovery também pode arquivar na nuvem, em um appliance de backup e recuperação da série DL ou em um sistema suportado de sua escolha. Com o Rapid Recovery, você pode replicar para um ou mais destinos para mais redundância e segurança.

O Rapid Recovery oferece:

- **Flexibilidade**. Você pode executar universal recovery para várias plataformas, incluindo a restauração de físico para virtual, virtual para físico, virtual para virtual, e física para físico.
- **Integração da nuvem**. Você pode exportar uma VM, arquivar e replicar para a nuvem e executar uma restauração sem sistema operacional dos arquivos na nuvem. Os serviços de nuvem compatíveis incluem Microsoft Azure, Amazon Web Services (AWS), qualquer provedor baseado em OpenStack (incluindo o Rackspace) e Google Cloud. As plataformas específicas do governo dos EUA incluem AWS GovCloud (US) e Azure Government.
- **Deduplicação inteligente**. Você pode reduzir os requisitos de armazenamento armazenando dados uma vez, e fazendo referência a eles daí para frente (uma vez por repositório ou domínio de criptografia).
- **Recuperação Imediata**. Nosso recurso Live Recovery permite que você acesse dados críticos em primeiro lugar, enquanto as operações de restauração restantes são concluídas em paralelo.
- **Recuperação em nível de arquivos**. Você pode recuperar os dados em nível de arquivo nas instalações, a partir de um local remoto ou a partir da nuvem.
- **Pesquisa em nível de arquivos**. Usando critérios especificados por você, é possível pesquisar um ou mais arquivos em um intervalo de pontos de recuperação. Dos resultados da pesquisa, você pode, então, selecionar e restaurar os arquivos que você deseja para a máquina do núcleo local diretamente do Core Console.
- **Suporte virtual**. O Rapid Recovery é compatível com exportação virtual única, permitindo gerar uma VM inicializável a partir de um ponto de recuperação e espera virtual, na qual a VM inicializável que você gera é continuamente atualizada após cada backup. Você pode até mesmo realizar uma exportação virtual para os volumes compartilhados de cluster do Microsoft Hyper-V.
- **Suporte a Rapid Snap for Virtual**. O suporte avançado para virtualização inclui proteção sem agente para VMs vCenter/ESXi e VMs Hyper-V. O Rapid Snap for Virtual inclui a proteção e a descoberta automática para o VMware ESXi 5.5 e superiores sem nenhum software de agente instalado. A proteção baseada em host é compatível somente com o Rapid Recovery Agent em um host Microsoft Hyper-V, permitindo a proteção sem agente de todas as VMs convidadas.
- **Suporte a aplicativos**. O Rapid Recovery Agent é integrado com suporte a aplicativos para Microsoft Exchange, SQL Server e Oracle. Quando você protege esses servidores de aplicativos no Core, os instantâneos de backup reconhecem automaticamente os aplicativos; transações abertas e logs de transação contínua são concluídos e caches são alinhados antes da criação do instantâneo. Recursos de aplicativos específicos são suportados, inclusive a capacidade de anexação do SQL (para SQL Server) e as verificações DBVERIFY de integridade do banco de dados (para Oracle). O reconhecimento de aplicativos também se estende para a proteção sem agente para SQL Server e Exchange Server.

Consulte os seguintes recursos para obter mais informações sobre o Rapid Recovery.

- O site de suporte do produto Rapid Recovery encontra-se em https://support.quest.com/rapid-recovery/.
- O site de documentação encontra-se em https://support.quest.com/rapid-recovery/technical-documents/.

Core Console

Esta seção descreve os diferentes elementos da interface de usuário do Rapid Recovery Core Console.

Acesso ao Rapid Recovery Core Console

Conclua as etapas a seguir para acessar o Rapid Recovery Core Console.

- Execute um dos seguintes para acessar o Rapid Recovery Core Console:
    1. Faça login localmente no servidor do Rapid Recovery Core e, em seguida, clique duas vezes no ícone do Core Console.
    2. Ou digite uma das seguintes URLs no seu navegador da Web:
    - https://<yourCoreServerName>:8006/apprecovery/admin/ ou
    - https://<yourCoreServerIPaddress>:8006/apprecovery/admin/

> **NOTE:** Como a interface do usuário do Rapid Recovery Core Console é dependente do JavaScript, o navegador da Web usado para acessar o Core Console deve ter o JavaScript ativado.
>
> **NOTE:** Se você alterou a porta padrão do serviço Rapid Recovery, atualize a porta conforme necessário na URL acima.

Noções básicas sobre o Guia de início rápido

O Guia de Início Rápido é um recurso que oferece a você um fluxo guiado de tarefas sugeridas para configuração e uso do Rapid Recovery Core.

O Guia de início rápido é exibido automaticamente na primeira vez que você atualiza ou instala o Rapid Recovery Core e navega até o Core Console. Clique em **Guia de Inicialização** na página **Bem-Vindo** do guia para ver as várias tarefas de configuração sugeridas. Navegue pelo guia usando as opções **Ignorar etapa** e **Voltar**. Quando tiver visto a última tarefa sugerida, clique em **Concluir** para fechar o guia.

Você pode abrir o Guia de Início Rápido novamente a qualquer momento a partir do menu Ajuda no Core Console. Também é possível ocultar a página **Bem-Vindo** do Guia de início rápido.

A menos que você o oculte, o Guia de início rápido reaparecerá toda vez que você efetuar login no Rapid Recovery Core Console e acessar a página **Início**. Para obter mais informações, consulte Ocultação do Guia de início rápido.

Você não é obrigado a realizar as etapas sugeridas pelo guia. É possível simplesmente visualizar as tarefas sugeridas e navegar por elas usando as opções **Ignorar etapa** e **Voltar**. Opcionalmente, para ocultar o guia para qualquer ponto, clique em **Sair do Guia**.

Se você optar por executar alguma tarefa de configuração sugerida pelo Guia de início rápido, siga os prompts indicados em qualquer etapa do guia e aparecerá o assistente apropriado ou a área relevante da interface do usuário. Os procedimentos para executar cada tarefa sugerida pelo guia estão descritos neste documento, como indicado na tabela abaixo.

NOTE: Nem todas as tarefas de configuração sugeridas pelo Guia de início rápido são obrigatórias para todos os usuários. É preciso entender que tarefas deseja realizar para suas necessidades específicas.

O Guia de início rápido aborda as seguintes tarefas de configuração:

Tabela 1. Tarefas de configuração do Guia de início rápido

Função	Descrição resumida	Resultado da seleção da tarefa/link para o procedimento
Proteção	Proteção de uma única máquina, um cluster de servers ou várias máquinas usando a proteção em massa	Clique em Proteger ou selecione **Proteger máquina** no menu suspenso para abrir o Assistente de proteção de máquina. Para obter informações sobre como executar o Assistente de proteção de máquina, consulte Proteção de uma máquina. Selecione **Proteger cluster** no menu suspenso para abrir a caixa de diálogo Conectar ao cluster. Para obter mais informações sobre como proteger um cluster, consulte Proteger um cluster. Selecione **Proteção em massa** no menu suspenso para abrir o Assistente para proteger várias máquinas. Para obter informações sobre como executar o Assistente de proteção de diversas máquinas, consulte Sobre como proteger diversas máquinas.
Replicação	Configuração da replicação de um Core principal (origem) para um secundário (de destino)	Clique em **Replicação** para abrir a página Replicação. É solicitado que um Core de destino seja adicionado usando o Assistente de replicação. Para obter informações sobre o uso do Assistente de replicação para configurar a replicação em um Core autogerenciado, consulte Replicar para um Core de destino autogerenciado. Para obter informações gerais sobre replicação, consulte Configurar a replicação.
Exportação virtual	Realização de uma exportação única ou estabelecimento de exportação contínua de uma máquina protegida para uma máquina virtual	Clique em **Exportar** para exportar dados da máquina protegida para uma máquina virtual. É possível realizar uma exportação única ou configurar o standby virtual para exportação contínua para uma VM. Para obter informações sobre exportações virtuais, consulte Exportação para máquinas virtuais usando o Rapid Recovery.
Gerenciar e configurar	Permite definir configurações adicionais do Rapid Recovery Core	Clique em **Mais** para ver funções adicionais que você pode gerenciar ou configurar. Funções inclui arquivos, montagens, CDs de inicialização, repositórios, chaves de criptografia, contas na nuvem, pesquisa de arquivo, políticas de retenção, notificações, relatórios, logs e mais.
Configurar a criptografia	Como adicionar ou importar chaves de criptografia que você pode usar para uma ou mais máquinas protegidas	Clique em **Chaves de criptografia** para gerenciar a segurança de dados protegidos com a adição ou a importação de chaves de criptografia. Você pode aplicar chaves de criptografia a uma ou mais máquinas protegidas. A criptografia é descrita no tópico Criptografia.
Configurar as notificações	Configuração de notificações de eventos, avisos e alertas	Clique em **Eventos** para especificar os grupos de notificação de eventos, avisos e alertas. Para enviar estas

Função	Descrição resumida	Resultado da seleção da tarefa/link para o procedimento
		informações por e-mail, você também deve estabelecer as definições do server de SMTP. Para obter informações sobre o gerenciamento de eventos, consulte o tópico Eventos, incluindo os tópicos Configurar grupos de notificação e Configurar um servidor de e-mail.
Gerenciar a retenção	Visualização ou alteração da política de retenção padrão do Core	Clique em **Política de retenção** para abrir a página Política de retenção do Core. Aqui você pode definir por quanto tempo manter um ponto de recuperação antes de implantá-lo. Para obter informações conceituais sobre políticas de retenção, consulte o tópico Como gerenciar dados de classificação por vencimento. Para obter informações de procedimento, consulte Gerenciar políticas de retenção.
Restaurar	Restauração de dados de um ponto de recuperação do Core	Clique em **Restaurar** para abrir o Assistente de restauração de máquinas. Para obter mais informações sobre como restaurar dados, consulte o tópico Sobre restauração de volumes a partir de um ponto de recuperação.

Ocultação do Guia de início rápido

O Guia de início rápido é exibido automaticamente na primeira vez que você atualiza ou instala o Rapid Recovery Core.

Também aparece quando o Guia de início rápido é selecionado no menu suspenso de Ajuda e toda vez que for acessada a página principal do Core Console.

Use o procedimento abaixo para ocultar o Guia de início rápido.

- No Rapid Recovery Core Console, se a página **Bem-Vindo** do Guia de início rápido estiver aberta, faça o seguinte:
  - Se desejar ocultar a página **Bem-Vindo** do Guia de início rápido, selecione **Não exibir novamente**.

    NOTE: Essa opção ocultará a página **Bem-Vindo** na próxima vez em que o Guia de início rápido for aberto e em todas as ocasiões subsequentes até que o Rapid Recovery Core seja atualizado.

    NOTE: Se você optar por ocultar essa página e quiser acessar as opções avançadas no futuro, selecione **Voltar** no assistente para ver essa página oculta.
  - Se desejar ocultar o Guia de início rápido nesta sessão, clique em **Fechar**.

    O Guia de início rápido é fechado. Da próxima vez em que for acessada a página principal no Core Console, o Guia de início rápido será exibido.
    Também é possível abrir o Guia de início rápido no menu Ajuda.
- Em qualquer página do Guia de início rápido, clique em **Sair do guia.**

  O Guia de início rápido é fechado. Se essa opção for selecionada, ainda será possível abrir o Guia de início rápido no menu Ajuda.

Navegar até o Rapid Recovery Core Console.

Ao efetuar o login no Core Console, e ao clicar a qualquer momento no ícone **Início**, a página **Início** aparecerá. A página **Início** mostra uma visualização do Rapid Recovery Core, com duas opções. Na área de visualização principal, o conteúdo padrão é o novo painel do Core, que apresenta um conjunto de relatórios em tempo real do seu sistema. Os relatórios padrão do painel incluem status de trabalho de transferência recente, transferência por máquina, uma visão geral do repositório e o estado de conectividade de máquinas protegidas, replicadas e "apenas pontos de recuperação". Ou você pode alternar para a visualização Tabelas resumidas clássica. Nessa visualização, o título da página mostra o nome de exibição do seu Rapid Recovery Core e você pode ver tabelas de resumo que mostram máquinas protegidas, repositórios e alertas recentes. Para obter mais informações, consulte Como entender a página Início (visualização de tabelas resumidas) e Noções básicas sobre os relatórios do painel do Core, respectivamente.

Na página **Início** (e em todas as páginas do Core Console), a área de navegação à esquerda mostra os itens protegidos no seu Core. Você pode navegar para outras páginas da interface com um dos procedimentos a seguir:

- Clicando no ícone correspondente da barra de ícones na área de navegação à esquerda. As opções acessíveis na barra de ícones incluem Replicar, Espera Virtual, Eventos, Configurações e Mais.
- Expandir o menu (Mais) na barra de ícones e selecionando um destino.
- Clicando em um botão ou opção de menu da barra de botões. Os botões incluem Proteger, Restaurar, Arquivamento e Replicação.

Quando você seleciona um item da área de navegação à esquerda, o foco do Core Console muda para exibir as informações de resumo sobre esse item. Por exemplo, se você clicar no nome de uma máquina protegida, o Core Console mostra informações sobre essa máquina apenas, em vez de todo o Core. Nesse exemplo, o nome de exibição da máquina protegida aparece como o título da página. Um submenu é mostrado à direita, permitindo que você visualize informações específicas sobre a máquina protegida. As opções do menu incluem: Resumo, Pontos de recuperação, Eventos, Configurações, Relatórios e muito mais.

Para voltar a visualizar informações sobre o Core, incluindo relatórios de painel ou uma exibição resumida de várias máquinas protegidas ou replicadas, clique no ícone **Início** no canto superior esquerdo da UI. Na página **Início**, você pode alternar entre a visualização do painel e a da página de resumo clicando no link vermelho na parte superior direita da página.

O título na parte superior do Core Console oferece contexto para as informações que você está vendo no Core. Por exemplo:

- A qualquer momento que você vir o nome de exibição ou endereço IP do Core como título da página, você estará vendo as informações de resumo sobre o Core.
- Se o título for "Painel", você estará vendo o painel do Core.
- Se você vir o nome de exibição ou o endereço IP de uma máquina protegida ou um painel Resumo na parte superior da página, você estará vendo informações sobre uma única máquina protegida pelo ou replicada no Core.
- Se você vir o título "Máquinas protegidas", você estará vendo informações sobre todas as máquinas protegidas no Rapid Recovery Core.
- Se você vir o título "Máquinas replicadas de…", você estará vendo informações sobre todas as máquinas replicadas no Rapid Recovery Core.
- Se você vir o título "Apenas pontos de recuperação", você estará vendo informações sobre todas as máquinas "apenas pontos de recuperação" nesse Core.

Para obter informações sobre os recursos e funções disponíveis em cada página, consulte a seção apropriada a seguir.

Para obter mais informações sobre a visualização de máquinas protegidas, consulte Visualização do menu Máquinas protegidas. Para obter mais informações sobre o gerenciamento de máquinas protegidas, consulte Gerenciar máquinas protegidas.

Para obter mais informações sobre a visualização de máquinas replicadas, consulte Ver a replicação de entrada e saída.

Para obter mais informações sobre a visualização de máquinas "apenas pontos de recuperação", consulte Visualizar o menu Apenas pontos de recuperação.

Compreensão da área de navegação esquerda

A área de navegação esquerda do Console do Core é exibida no lado esquerdo daquela interface de usuário. O conteúdo deste área de navegação pode variar de acordo com o tipo de objetos protegidos no seu Rapid Recovery Core.

A área de navegação esquerda sempre contém o seguinte:

- **Barra de ícones.** Para navegação entre as principais páginas do Console do Core.
- **Filtro de texto.** O filtro de texto é um campo de texto que permite filtrar os itens exibidos nos vários menus que aparecem abaixo dele. Quando você clicar na seta à direita do filtro de texto, cada um dos menus que aparecem abaixo dele se expandirá ou será minimizado.

Seguindo esses elementos, a área de navegação esquerda tipicamente exibe menus para ajudá-lo a navegar, filtrar e visualizar os objetos protegidos em seu Core. Isso inclui máquinas protegidas, máquinas replicadas e assim por diante.

Cada menu é sensível ao contexto; ou seja, cada menu só aparece no Console do Core se ele for relevante. Por exemplo, se você proteger pelo menos uma máquina, o menu de máquinas protegidas será exibido e assim por diante.

Para obter mais informações, consulte as tabelas da área de navegação à esquerda em Como ver a interface do usuário do Core Console.

See also: Visualização das informações de resumo de uma máquina protegida
See also: Visualização das informações de resumo de um host
See also: Replicação
See also: Noções básicas sobre grupos personalizados

Visualização da página Início do Rapid Recovery Core Console

Sempre que você fizer login no Rapid Recovery Core Console ou sempre que você clicar no ícone **Início**  na barra de ícones, a página **Início** será exibida. A página **Início** oferece uma visualização de **painel** e a visualização familiar de **tabelas de resumo**. As tabelas de resumo são a exibição padrão.

Você pode alternar entre visualizações na página **Início** clicando no ícone de alternância de painel na parte superior direita da página **Início**.

Da página **Início**, e de todas as outras páginas do Core Console, você pode navegar para as funções desejadas usando a área de navegação à esquerda.

Para obter mais informações, consulte os seguintes tópicos:

- Compreensão da área de navegação esquerda
- Noções básicas sobre os relatórios do painel do Core
- Como entender a página Início (visualização de tabelas resumidas)
- Como ver a interface do usuário do Core Console

Como entender a página Início (visualização de tabelas resumidas)

A página **Início** aplica-se apenas ao Core. Na visualização de painel, ela mostra relatórios gráficos em tempo real. Ao alternar para a visualização de tabelas resumidas, a página **Início** exibe todas as máquinas que o Core protege ou replica, os repositórios associados ao seu Core e alertas de máquinas nesse Core.

A visualização de cada painel na página **Início** pode ser expandida ou contraída. Por exemplo, se você clicar no ícone  (contrair visualização) no lado superior direito do painel Máquinas protegidas, a visualização de máquinas protegidas é contraída e apenas o nome do painel fica visível. Para expandir a exibição para ver todas as máquinas protegidas novamente, clique no ícone  (expandir visualização).

A tabela a seguir descreve os vários elementos da página **Início** na visualização de tabelas resumidas.

Tabela 2. Opções da página Início

Elemento de UI	Descrição
Máquinas protegidas	O painel Máquinas protegidas mostra uma lista das máquinas que este Core protege. Esse painel é exibido independentemente de haver alguma máquina adicionada ao Core para proteção.

Elemento de UI	Descrição
	Essa seção inclui as seguintes informações sobre cada máquina protegida: • **Tipo de máquina.** Um ícone indica se a máquina é uma máquina física, virtual ou um cluster protegido. • **Status.** Círculos coloridos na coluna Status indicam se a máquina protegida está acessível, em pausa ou offline e inalcançável. • **Nome de exibição.** O nome de exibição ou endereço IP da máquina protegida. • **Nome do repositório.** O nome do repositório onde os pontos de recuperação da máquina estão armazenados. • **Último snapshot.** A data e a hora em que o Rapid Recovery criou o instantâneo de ponto de recuperação mais recente para essa máquina. • **Pontos de recuperação.** O número de pontos de recuperação armazenados no repositório e o uso de espaço para cada máquina protegida. • **Versão**. A versão do software do agente Rapid Recovery instalada na máquina. Se você clicar no nome de uma máquina específica mostrada nesse painel, uma página Resumo é exibida com as informações de resumo da máquina selecionada. Para obter mais informações sobre o que você pode realizar na página Resumo, consulte Visualização das informações de resumo de uma máquina protegida.
Máquinas replicadas	O painel Máquinas replicadas lista as máquinas que este Core replicou de outro Core. Esse painel não é mostrado a menos que seu Core replique máquinas de outro Core. Essa seção inclui as seguintes informações sobre cada máquina replicada: • **Tipo de máquina.** Um ícone indica se a máquina é uma máquina física, virtual ou um cluster protegido. • **Status.** Círculos coloridos na coluna Status indicam se a máquina replicada está acessível, em pausa ou offline e inalcançável. • **Nome de exibição.** O nome de exibição ou endereço IP da máquina replicada. • **Nome da replicação.** O nome de exibição do Core de origem de qualquer máquina replicada neste Core de destino. Você pode definir esse nome ao configurar a replicação. • **Nome do repositório.** O nome do repositório onde os pontos de recuperação da máquina estão armazenados. • **Último snapshot replicado.** A data e a hora em que o Rapid Recovery criou a réplica mais recente da máquina protegida original. • **Pontos de recuperação.** O número de pontos de recuperação armazenados no repositório e o uso de espaço para cada máquina replicada. • **Versão**. A versão do software Rapid Recovery Agent instalada na máquina. Se você clicar no nome de uma máquina específica mostrada nesse painel, a página Resumo é exibida com as informações de resumo da máquina replicada.
Máquinas "apenas pontos de recuperação"	O painel Máquinas "apenas pontos de recuperação" lista das máquinas removidos da proteção ou replicação, se os pontos de recuperação forem mantidos. Essas máquinas podem ser usadas para recuperação em nível de arquivo, mas não para bare metal restore, restauração de volumes inteiros ou adição de dados de snapshot. Esse painel não é mostrado, a menos que você tenha alguma máquinas que atenda essa definição.

Elemento de UI	Descrição
	A seção inclui as seguintes informações sobre cada máquina apenas com pontos de recuperação: • **Tipo de máquina.** Um ícone indica se a máquina é uma máquina física, virtual ou um cluster protegido. • **Status.** Círculos coloridos na coluna Status indicam se a máquina "apenas pontos de recuperação" está acessível, em pausa ou offline e inalcançável. • **Nome de exibição.** O nome de exibição ou endereço IP da máquina cujos pontos de recuperação você manteve. • **Nome do repositório.** O nome do repositório onde os pontos de recuperação restantes da máquina estão armazenados. • **Pontos de recuperação.** O número de pontos de recuperação armazenados no repositório e o uso de espaço para cada máquina "apenas pontos de recuperação". Se você clicar no nome de uma máquina específica mostrada nesse painel, a página Resumo aparece para essa máquina "apenas pontos de recuperação".
Repositórios DVM	Esse painel é exibido para DL1000, independentemente se algum repositório DVM (Deduplication Volume Manager) foi criado. Esse painel não é mostrado a menos que seu Core tenha um ou mais repositórios DVM. São incluídas as seguintes informações sobre cada Repositório de DVM: • **Tipo.** Um ícone retrata um repositório. • **Status.** Círculos coloridos na coluna Status mostram se o repositório está montado e se pode aceitar transferências de pontos de recuperação, ou se está inalcançável ou em estado de erro. • **Nome do repositório.** O nome de exibição do repositório. • **Uso de espaço.** A quantidade total de espaço usado no repositório e o tamanho ou extensão do volume de armazenamento. • **Dados protegidos.** A quantidade de espaço usado no repositório. • **Máquinas.** O número de máquinas cujos pontos de recuperação o repositório armazena. • **Pontos de recuperação.** O número de pontos de recuperação armazenados no repositório. • **Taxa de compactação.** A taxa com que o repositório comprime os dados protegidos para economizar espaço. Para obter mais informações, consulte Noções básicas sobre repositórios.
Alertas	Esta seção mostra os alertas importantes do Core e de todas as máquinas que ele protege. A seção inclui as seguintes informações: • **Ícones.** A coluna de ícones indica a natureza do alerta. Eles incluem mensagens informativas, erros • **Data.** Exibe a data e a hora em que o Rapid Recovery gerou o alerta. • **Mensagem.** Descreve o alerta. Você também pode ver esses detalhes na página Eventos do Core. Para obter mais informações, consulte Como exibir eventos usando tarefas, alertas e páginas de diário.

Noções básicas sobre os relatórios do painel do Core

O painel do Core exibe um conjunto de relatórios gráficos em tempo real de dados relevantes para o Core, as máquinas protegidas e os instantâneos salvos em seu repositório. Os relatórios do painel incluem:

- Relatórios do sistema Core
  - **Monitor de problemas**. Esse relatório mostra atividade do trabalho, conexões com o portal de licenças e atividade de transferência para detectar um problema logo no sistema. Clique no widget do relógio para limpar todos os eventos novos de monitor e monitorados da atividade.
  - **Repositório**. Esse relatório mostra os repositórios associados ao Core. Ele mostra o número de repositórios, quantas máquinas estão protegidas, o número de pontos de recuperação e a porcentagem de compressão ou deduplicação. Esse relatório é atualizado a cada minuto.
- Relatórios da máquina
  - **Conectividade da máquina**. Esse relatório mostra o estado de conectividade de máquinas protegidas e replicadas no Core. Ele também mostra a conectividade de dados em uma .
- Relatórios de instantâneos
  - **Trabalho de transferência**. Esse relatório mostra todas as transferências de dados do snapshot (inclusive imagem de base e snapshots incrementais) concluídas nas últimas 24 horas. Entre os snapshots estão imagem de base e snapshots incrementais. Esse relatório de painel é exibido como um gráfico de círculo.
  - **Trabalho de transferência por máquina**. Esse trabalho mostra, por máquina protegida, o número de trabalhos de transferência com falha e bem-sucedidos nas últimas 24 horas. Esse relatório de painel é exibido como um gráfico de linha.

Na parte superior do painel, você pode clicar no widget  (Expandir) para exibir uma lista de relatórios exibidos no painel, nas três categorias descritas acima. Cada categoria de relatório e relatório tem uma caixa de seleção. Se a caixa estiver selecionada, o relatório ou a categoria aparecerá no painel. Se você desmarcar a opção, o relatório não será exibido. Dessa forma, você pode alterar facilmente a exibição dos relatórios no painel.

Se você clicar em  (Contrair), o menu desaparecerá.

Você também pode recolher ou expandir a visualização de todos os relatórios no painel clicando na seta para cima ou para baixo no cabeçalho do relatório. Alguns relatórios de painel (conectividade da máquina e repositório) têm um sinal de adição próximo à seta, em que você pode adicionar outra máquina protegida ou outro repositório, respectivamente.

Você também pode arrastar e soltar para mover o local de um dos relatórios em outro lugar no relatório para ordenar os relatórios de uma maneira mais efetiva para o uso.

Visualização do menu Máquinas protegidas

Na interface de usuário do Rapid Recovery, um menu Máquinas protegidas aparece na área de navegação esquerda. Assim como todos os rótulos de menu na área de navegação, o rótulo desse menu é exibido em letras maiúsculas. Por padrão, esse menu está totalmente expandido e mostra uma lista de máquinas protegidas por esse Core. Se houver clusters do servidor protegidos, eles são incluídos nessa lista.

Para expandir ou retrair a exibição de máquinas protegidas e clusters do servidor no Core, clique na seta no lado esquerdo desse menu.

O menu Máquinas protegidas inclui um menu suspenso no lado direito relacionando as funções que podem ser realizadas em todas as máquinas protegidas. Clique na seta à direita de **Máquinas protegidas** para ver o menu.

Cada máquina relacionada no menu Máquinas protegidas também tem um menu suspenso que controla as funções apenas daquela máquina.

Se você estiver gerenciando clusters do servidor no Rapid Recovery Core, o cluster também aparecerá no menu de navegação esquerdo. No menu suspenso de qualquer cluster, você pode também navegar para a página **Nós protegidos** do cluster selecionado.

Se você clicar na seta à esquerda do menu Máquinas protegidas, será exibida a lista de contratos de máquinas protegidas e clusters do servidor, e não a de máquinas. Clicar novamente nessa seta faz com que a lista de máquinas seja expandida novamente.

Clique no nome de qualquer máquina do menu Máquinas protegidas para abrir a página Resumo dessa máquina. Para obter mais informações sobre o que você pode realizar na página Resumo, consulte Visualização das informações de resumo de uma máquina protegida.

Por fim, clicar diretamente no menu **Máquinas protegidas** faz com que a página **Máquinas protegidas** seja mostrada na área de conteúdo principal, com um único painel mostrando máquinas protegidas desse Core. Para obter mais informações sobre o que você pode realizar no painel **Máquinas protegidas** da página Máquinas protegidas, consulte .

NOTE: Na página **Máquinas protegidas**, você pode voltar a uma visualização da perspectiva do Core clicando no ícone **Início** da barra de ícones.

Visualização das informações de resumo de uma máquina protegida

Quando você clica no nome de uma máquina protegida do Core Console, a página **Resumo** é mostrada. Ela contém, no mínimo, um painel de Resumo e um painel de Volumes. Se uma máquina for adicionada a replicação, um painel Replicação também é mostrado.

Se você tiver um ou mais servers Exchange protegidos, você também verá um painel de Informações do Exchange Server que contém informações sobre seu server Exchange protegido.

Se você tiver um ou mais servers SQL protegidos, você também verá um painel de Informações do SQL Server que contém informações sobre seu server SQL protegido.

No topo desta página há um menu de ações que você pode realizar na máquina protegida. Abaixo dela há, no mínimo, um painel de Resumo e um painel de Volumes. Se uma máquina for adicionada a replicação, um painel Replicação também é mostrado.

Ao mostrar informações sobre uma máquina protegida — na página de Resumo e todas as outras visualizações — há um menu na parte superior da página com funções que você pode executar. Esse menu é exibido imediatamente abaixo do nome da máquina protegida.

See also: Exibindo o painel de resumo
See also: Visualização de volumes em uma máquina protegida
See also: Exibindo informações de replicação
See also: Visualizar o painel de informações do Exchange Server
See also: Visualização do painel de informações do SQL Server
c_Viewing_summary_information_for_a_host.xml

Exibindo o painel de resumo

O painel **Resumo** contém informações resumidas sobre a máquina protegida, incluindo o nome do host, a data e a hora do último snapshot, a data e a hora do próximo snapshot agendado, as informações sobre a chave de

criptografia e as informações de versão do software do agente Rapid Recovery. Há também um link para uma página Informações do sistema detalhada para a máquina.

Visualização de volumes em uma máquina protegida

Para qualquer máquina protegida, na página Resumo, no painel Volumes, é possível realizar as seguintes ações para qualquer um dos volumes listados:

- Definir uma programação de proteção para um volume selecionado. As programações de proteção são normalmente estabelecidas quando você protege uma máquina pela primeira vez. Para obter mais informações sobre a modificação de programações de proteção, consulte Criar programações de proteção personalizada no Modo Simples.
- Forçar imagem de base ou instantâneo. Os instantâneos normalmente ocorrem na programação de proteção. No entanto, a qualquer momento, você poderá forçar uma imagem de base ou um instantâneo incremental para volumes selecionados. Para obter mais informações, consulte Forçar um snapshot.

Exibindo informações de replicação

O painel **Replicação** contém informações de resumo sobre a máquina replicada, inclusive o nome da replicação, o estado da replicação, o progresso e o espaço disponível.

Visualizar o painel de informações do Exchange Server

O painel **Informações do Exchange Server** aparece somente para as máquinas protegidas que forem Exchange Servers.

Esse painel contém informações resumidas sobre o Exchange Server protegido, incluindo a versão instalada do Microsoft Exchange, o caminho no qual o Exchange está instalado e o caminho definido para os dados da caixa de correio do Exchange.

A grade Armazenamentos de e-mail mostra o nome do Exchange Database (EDB), o caminho do arquivo do EDB, o caminho no qual os arquivos de log estão armazenados, o prefixo do log, o caminho do sistema, o Grupo de Disponibilidade do Bancos de Dados (DAG) e o tipo de armazenamento de e-mail.

Visualização do painel de informações do SQL Server

O painel **Informações do SQL Server** é exibido somente para máquinas protegidas que são SQL servers.

Este painel contém informações de resumo sobre os SQL servers protegidos. Você pode expandir as informações do database para ver detalhes para cada tabela no database. Você também pode ver o database ou o nome da tabela e o caminho do banco de dados.

Visualização das informações de resumo de um host

Quando você clica no nome de uma máquina host de um hipervisor ou cluster no Core Console, a página **Resumo** é mostrada. Ela contém, no mínimo, uma barra de ações de funções, um painel de Resumo e um painel de Processadores. As barra de ações é exibida na parte superior de todas as páginas para o host. O painel de Resumo inclui informações como o nome do host e o software de virtualização. Os painel de Processadores inclui uma tabela que lista a arquitetura, o número de Cores, o número de threads, a velocidade de clock e a descrição de cada processador.

Dependendo do tipo de host da máquina, os seguintes painéis também podem aparecer:

- **Servidores SMB.** Se um host do Hyper-V usar um ou mais servidores SMB, esta seção listará o nome do host de cada servidor SMB.
- **Nós.** A página de **Resumo** de um host de cluster inclui a seção para listar o nome do host e o número da versão do Rapid Recovery para cada nó.
- **Volumes.** Ao usar a proteção sem agente, a página **Resumo** de um host do Hyper-V inclui esta seção para listar o nome, o sistema de arquivos, o uso do espaço, a programação atual e o próximo instantâneo de cada volume protegido.
- **Discos compartilhados.** Se um host do Hyper-V que usa a proteção sem agente tiver um ou mais VHDXs compartilhados, esta seção listará o nome e o caminho de cada disco rígido virtual.

Para obter mais informações sobre clusters CSV, consulte "Suporte para Volumes Compartilhados Clusterizados" no *Guia de requisitos do sistema do Rapid Recovery*. Para obter informações sobre outros tópicos relacionados, consulte os links a seguir:

- Visualização das informações de resumo de uma máquina protegida
- Noções básicas sobre Rapid Snap for Virtual

Como ver pontos de recuperação para uma máquina

A página Pontos de recuperação mostra uma lista dos pontos de recuperação coletados para essa máquina protegida, além de dados pertinentes sobre a máquina e o repositório. Nessa página, você pode montar, exportar e restaurar pontos de recuperação específicos ou excluir pontos de recuperação.

A página é dividida em dois painéis: Resumo dos pontos de recuperação e Pontos de recuperação. O painel Resumo não contém links de ações. Ele exibe os dados relacionados a seguir sobre a máquina.

Tabela 3. Dados do painel Resumo dos pontos de recuperação

Elemento de UI	Descrição
Total de pontos de recuperação	O número de pontos de recuperação coletados para essa máquina protegida específica.
Total de dados protegidos	A quantidade de dados da máquina protegida armazenados no repositório.
Repositório	O nome do repositório no qual o Rapid Recovery armazena os pontos de recuperação dessa máquina protegida.
Status do repositório	A barra de progresso exibe a porcentagem do espaço total usada no repositório. A quantidade de dados usada e o tamanho total do repositório aparecem abaixo da barra de progresso.

Para obter mais informações, consulte .

Visualizar eventos de uma máquina protegida

Na página **Eventos**, você pode visualizar os trabalhos que ocorreram ou estão em progresso na máquina protegida selecionada. Os botões na parte superior da página permitem navegar para listas de trabalhos em cada uma das três categorias de atividades:

- **Tarefas.** Um trabalho que deve ser realizado pelo Rapid Recovery para que funcione corretamente.
- **Alertas.**Ama notificação relacionada a uma tarefa ou evento que inclui erros e aviso.
- **Registro.**Uma combinação de todas as tarefas e alertas de máquinas protegidas.

A tabela a seguir contém descrições de cada elemento da página **Eventos**.

Tabela 4. Elementos da página Eventos

Elemento de UI	Descrição
Pesquisar palavra-chave	Permite pesquisar um item específico dentro de cada categoria. Disponível somente para tarefas.
De	Para restringir os resultados, você pode inserir uma data de início da pesquisa. Disponível somente para tarefas.
Para	Para restringir os resultados, você pode inserir uma data de término da pesquisa. Disponível somente para tarefas.
Ícones de status	Cada ícone representa um status diferente do trabalho. Para alertas e tarefas, clicar em um dos ícones permite filtrar a lista por esse status, gerando, essencialmente, um relatório. Quando você clica no ícone uma segunda vez, o filtro desse status é removido. Você pode filtrar por mais de um status. Os status são: • **Ativo.**Um trabalho em progresso. • **Enfileirado.** Um trabalho que está aguardando a conclusão de outro trabalho para poder começar. • **Aguardando.**Um trabalho que está aguardando sua aprovação ou conclusão, como uma unidade de propagação. (Para obter mais informações sobre unidades de propagação, consulte Replicação.) • **Concluído.**Um trabalho que foi concluído com êxito. • **Com falha.** Um trabalho que teve uma falha e não foi concluído.
Ícone de serviço	Este botão adiciona trabalhos de serviços à lista de trabalhos. Quando você clica nesse ícone, um ícone de serviço menor aparece em cada ícone de status, permitindo filtrar por trabalhos de serviço que possuam esses status (se houver). Exemplos de trabalhos de serviços são a exclusão de arquivos de índice ou a remoção de uma máquina da proteção.

Elemento de UI	Descrição
Lista suspensa Tipo de exportação	A lista suspensa inclui os formatos para os quais você pode exportar o relatório de eventos. Disponível somente para tarefas. Ela inclui os seguintes formatos: • PDF • HTML • CSV • XLS • XLSX
(ícone Exportar)	Converte o relatório de eventos para o formato selecionado. Disponível somente para tarefas.
Seleção de página	Os relatórios de eventos podem incluir vários trabalhos em múltiplas páginas. Os números e as setas na parte inferior da página **Eventos** permitem navegar pelas páginas adicionais do relatório.

O página **Eventos** exibe todos os eventos em uma tabela. A seguinte tabela lista as informações exibidas para cada item.

Tabela 5. Informações detalhadas da tabela de resumo de eventos

Elemento de UI	Descrição
Status	Exibe o status da tarefa, alerta ou item de registro. Disponível para alertas ou itens de registro, clique no cabeçalho para filtrar os resultados por status.
Nome	Nome está disponível somente para tarefas. Esse campo de texto lista o tipo de tarefa que foi concluída nessa máquina protegida. Os exemplos incluem transferência de volumes, manutenção de repositório, execução, realização de verificação de capacidade de montagem, realização de verificação de soma de verificação e assim por diante.
Hora inicial	Disponível para tarefas, alertas e itens de registro. Exibe a data e a hora de início do trabalho ou da tarefa.
Hora final	Disponível somente para tarefas. Exibe a data e a hora de conclusão do trabalho ou da tarefa.
Detalhes do trabalho	Disponível somente para tarefas. Abra a caixa de diálogo **Monitorar tarefa ativa** de maneira que você possa visualizar os detalhes do trabalho ou da tarefa específico(a). Esses detalhes incluem um ID do trabalho, taxa de transferência de dados do core (se relevante), tempo decorrido para conclusão do trabalho, trabalho total em quantidade de gigabytes e tarefas subordinadas associadas ao trabalho.
Mensagem	Disponível para alertas e itens de registro. Esse campo de texto fornece uma mensagem descritiva do alerta ou do item de registro.

Visualização de relatórios para uma máquina protegida

O menu suspenso **Relatórios** permite gerar relatórios sob demanda para a máquina protegida selecionada.

- O relatório do trabalho fornece um relatório sobre o status d e trabalhos bem-sucedidos e trabalhos com falha para a máquina selecionada. Os trabalhos com falha podem ainda ser vistos com mais detalhes em um Relatório de falhas. Para obter mais informações sobre esse tipo de relatório, consulte Noções básicas sobre o relatório do trabalho.
- O relatório de falhas fornece informações sobre trabalhos de Core com falha e cancelados para a máquina especificada. Para obter mais informações sobre esse tipo de relatório, consulte Noções básicas sobre o relatório de falhas.

Para obter informações sobre como gerar esses relatórios, consulte Gerar um relatório de Core sob demanda.

Ver máquinas replicadas no menu de navegação

Se o seu Core replica máquinas de outro Rapid Recovery Core, o nome de exibição do Core de origem aparece como um menu minimizado na navegação à esquerda do Console do Core. Assim como acontece com todos os rótulos de menu na área de navegação, esse nome de menu das máquinas replicadas aparece com todas as letras maiúsculas, abaixo do menu de Máquinas Protegidas. Por padrão, o menu de máquinas replicadas é totalmente expandido, e mostra a lista de todas as máquinas provenientes do Core de origem que são replicadas em seu Core de destino.

Para expandir ou minimizar a exibição de máquinas replicadas a partir do Core de origem, clique na seta no lado esquerdo desse menu.

Cada menu de máquinas replicadas inclui um menu suspenso no lado direito relacionando as funções que podem ser realizadas simultaneamente em todas as máquinas replicadas a partir daquele Core. Clique na seta à direita do menu de máquinas replicadas para ver uma lista suspensa de funções que você pode executar. Essas ações incluem:

- Pausar replicação. Se a replicação estiver atualmente ativa, para a ação até você retomá-la.
- Retomar replicação. Se a replicação tiver sido pausada, ela será iniciada novamente.
- Forçar replicação. Replica sob demanda, em vez de em um momento agendado.
- Remover a replicação. Remove a relação de replicação entre o core de origem e seu core de destino. Opcionalmente, você pode apagar os pontos de recuperação armazenados neste Core. Para obter mais informações, consulte Remover replicação de saída do Core de origem ou Remover replicação de entrada do Core de destino.

Clicar diretamente no nome do Core de origem no menu de navegação faz com que a página **Máquinas replicadas de [Nome do Core de Origem]** seja exibida na área de conteúdo principal. Para obter mais informações sobre o que você pode realizar nesta página, consulte Ver a replicação de entrada e saída.

Pausar e retomar a replicação
Forçar a replicação
Remover replicação de saída do Core de origem
Remover replicação de entrada do Core de destino

Visualizar o menu Apenas pontos de recuperação

O menu Apenas pontos de recuperação é exibido na área de navegação à esquerda se uma das seguintes condições for verdadeira:

- Se o seu Rapid Recovery Core mantém alguns pontos de recuperação de uma máquina que estava anteriormente protegida.
- Se você removeu a replicação, mas manteve os pontos de recuperação.

Assim como todos os rótulos de menu na área de navegação, o rótulo desse menu é exibido em letras maiúsculas.

Para expandir ou retrair a exibição de máquinas apenas com pontos de recuperação, clique na seta à esquerda desse menu.

O menu inclui um menu suspenso no lado direito relacionando as funções que podem ser realizadas simultaneamente em todas as máquinas apenas com ponto de recuperação. Nesse caso, a única função que você pode realizar é remover os pontos de recuperação do Core.

CAUTION: Essa ação remove todas as máquinas apenas com pontos de recuperação em seu Rapid Recovery **Core, excluindo-os permanentemente e impedindo a restauração das informações desses pontos de recuperação a partir desse Core.**

Visualizar o menu Grupos personalizados

O menu Grupos personalizados aparecerá na área de navegação esquerda apenas se você tiver definido um ou mais grupos personalizados. Assim como todos os rótulos de menu na área de navegação, o rótulo desse menu é exibido em letras maiúsculas.

Para expandir ou retrair a exibição dos itens desse menu, clique na seta à sua esquerda.

O menu Grupos personalizados inclui um menu suspenso no lado direito relacionando as funções que podem ser realizadas simultaneamente em todos os itens semelhantes desse grupo.

Para obter mais informações, consulte Noções básicas sobre grupos personalizados.

Usar a caixa de diálogo Erro

Quando um erro ocorre na interface de usuário do Rapid RecoveryRapid Recovery Core Console, como a tentativa de inserir um parâmetro inválido, uma caixa de diálogo Erro aparece. A caixa de diálogo geralmente indica a causa do erro, fornece alguns links para informações adicionais sobre o erro e inclui um botão Fechar. Você precisa fechar a caixa de diálogo Erro para continuar, mas talvez queira visualizar mais informações sobre o erro.

Na caixa de diálogo Erro, escolha entre as opções a seguir:

Os erros da interface de usuário que causam o aparecimento da caixa de diálogo Erro não são rastreados na página Eventos do Rapid Recovery, pois são apenas erros de validação ou inserção de dados. No entanto, quando você clica na opção Pesquisar base de conhecimento referente a algum erro, a URL do link fornecido

é registrada no arquivo AppRecovery.log do Core. Você pode pesquisar a cadeia de caracteres de texto "KB article url generated" no log para ver a URL de cada erro que foi visualizado em um navegador. Para obter mais informações sobre download ou visualização de logs de erros do Core, consulte os tópicos Como baixar e exibir o arquivo de log do Core ou Acessar os logs do Core, respectivamente.

Definições do Core

Esta seção descreve como gerenciar e alterar as definições do Rapid Recovery Core e descreve os principais botões de função e as ferramentas disponíveis no Core Console.

Por padrão, o Rapid Recovery Core tem definições ajustáveis que são configuradas por padrão para proporcionar um desempenho ideal para a maioria dos usuários. Essas definições afetam as informações exibidas no Core Console ou o desempenho do Rapid Recovery Core. Na barra de ícones, clique em (Definições) para acessar as configurações do Core.

Um conjunto de funções principais são mostradas como botões na parte superior da página na horizontal. Para acessar uma dessas funções, clique no botão correspondente. Para obter mais informações sobre esses botões, consulte Funções principais das definições do Core.

Abaixo dos botões de função principais estão definições configuráveis do Core. Para ver todas as opções de configuração para qualquer uma das definições, clique em um link de atalho no lado esquerdo do painel de definições ou role a tela para baixo no lado direito da página. Para obter mais informações sobre o conjunto completo des definições do Core, consulte Definições do Rapid Recovery Core.

Você pode também acessar as ferramentas do Core, como ver um resumo das informações do sistema ou fazer download dos arquivos de log do Core. Para obter mais informações, consulte Ferramentas de nível do Core.

Funções principais das definições do Core

Um conjunto de funções principais são mostradas como botões organizados horizontalmente na parte superior da página (Definições). Para acessar uma dessas funções, clique no botão correspondente.

Os botões de função acessíveis na página Definições são descritos na tabela a seguir.

Tabela 6. Funções principais das definições do Core

Botão de função principal	Descrição
Definições da cópia de segurança	Faz backup das definições de configuração do Core em um arquivo XML indicado por você. Especifique um local do caminho totalmente qualificado para o servidor Core.
Definições de restauração	Se você tiver um arquivo XML de backup das definições do Core, essa opção permitirá especificar o nome e o caminho local do arquivo, do qual você pode restaurar as definições do Core. Utilize essa função para restaurar as definições do Core ou para migrar de outro Core. Opcionalmente, você também pode restaurar repositórios.
Reiniciar serviço do Core	Essa opção encerra e depois inicia serviço do Core normalmente.
Encerrar serviço do Core	Essa opção encerra normalmente o serviço do Core.

Para obter mais informações sobre a criação de backup e a restauração das definições do Core, consulte Criar cópia de segurança e restaurar definições do Core.

Para obter mais informações sobre como encerrar e reiniciar o serviço do Core, consulte Reiniciar ou encerrar o serviço Core.

Criar cópia de segurança e restaurar definições do Core

Você pode criar uma cópia de segurança em arquivo das informações de definição e, posteriormente, restaurar essas definições caso haja problemas com a máquina Core você queira migrar essas definições para uma máquina diferente. As informações incluídas na cópia de segurança incluem os metadados do repositório (como o nome do repositório, o caminho de dados e o caminho de metadados); as máquinas protegidas no Core; os relacionamentos de replicação (destinos e origens); quais máquinas estão configuradas para standby virtual; e informações sobre chaves de criptografia.

Esse processo restaura apenas as definições de configuração, não os dados. Informações de segurança (como credenciais de autenticação) não são armazenadas no arquivo de configuração. Salvar um arquivo de configuração de Core não acarreta riscos de segurança.

NOTE: Você deve primeiramente criar uma cópia de segurança das informações de definição do Core para poder usar esse processo para restaurar as definições.

Use este procedimento para criar uma cópia de segurança das definições do Core e restaurá-las.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Configurações).

   A página **Configuration** (Configuração) aparece. Na parte superior do painel de Configurações, acima das categorias de definições, você verá opções para **Fazer backup das configurações** ou para **Restaurar configurações**.
3. Caso queira criar uma cópia de segurança das definições do Core, vá para a Etapa 4. Caso queira restaurar definições do Core, vá para a Etapa 6.
4. Para fazer uma cópia de segurança das definições atuais em um arquivo XML, na parte superior da página **Definições**, clique em **Definições da cópia de segurança**.

   Aparece a caixa de diálogo Configuração da cópia de segurança do Core.
5. Na caixa de texto Caminho local, digite o caminho de um diretório acessível localmente à máquina Core no qual você deseja armazenar as definições do Core em um arquivo XML e clique em **Cópia de segurança**.

   Por exemplo, digite `C:\Users\Your_User_Name\Documents\RRCoreSettings` e clique em **Back Up** (Fazer backup).

   Um arquivo chamado AppRecoveryCoreConfigurationBackup.xml é salvo no destino local que você especificou.
6. Para restaurar as definições do Core a partir de um arquivo XML de cópia de segurança salvo anteriormente usando esse método, execute as etapas a seguir.

   NOTE: Quando você restaura as definições de configuração do Core, o serviço Rapid Recovery Core é reiniciado.

   a. Na parte superior da página **Settings** (Configurações), clique em **Restore Settings** (Restaurar configurações).

   A caixa de diálogo **Configuração da restauração do núcleo** é mostrada.

   b. Na caixa de texto **Caminho local**, digite o caminho local onde você armazenou as definições de configuração do Core.

   Por exemplo, digite `C:\Users\Your_User_Name\Documents\RRCoreSettings`.

c. Caso não queira restaurar as informações de repositório, vá para a Etapa g.

d. Opcionalmente, caso queira restaurar as informações de repositório para a configuração do arquivo de cópia de segurança, selecione **Restaurar repositórios** e clique em **Restaurar**.

A caixa de diálogo **Restaurar repositórios** é exibida.

Se você optar por restaurar as informações de repositório a partir da cópia de segurança dos dados de configuração, os repositórios configurados quando as definições do Core foram salvas serão exibidos para confirmação. Por padrão, todos os repositórios existentes estão selecionados.

e. Confirme as informações de repositório que você deseja restaurar. Se vários repositórios aparecerem nas listas para confirmação e você quiser restaurar as informações de apenas alguns deles, desmarque a seleção dos repositórios que não deseja restaurar.

f. Quando você estiver satisfeito com a seleção de repositórios que deseja restaurar, clique em **Salvar**.

A caixa de diálogo **Restaurar repositórios** é fechada.

g. Na caixa de diálogo **Restaurar repositórios**, clique em **Restaurar**.

A caixa de diálogo **Restaurar repositórios** é fechada e o processo de restauração é iniciado. Um alerta aparece, indicando que a configuração do serviço de repositório foi alterada.

h. Caso não tenha sido possível restaurar alguma definição de configuração, uma mensagem de erro será exibida. Confira os detalhes do erro para ver se há alguma ação necessária da sua parte. Para obter mais informações, consulte Como exibir eventos usando tarefas, alertas e páginas de diário. Para continuar, clique em **Fechar** para limpar a caixa de diálogo de erro.

i. Depois de restaurar a configuração, verifique o seguinte:

- Desbloqueie todas as chaves de criptografia. Para obter mais informações, consulte Desbloquear uma chave de criptografia.
- Se o standby virtual estiver configurado para atualizar continuamente uma VM para um destino de rede, você precisa especificar as credenciais da rede nas definições do standby virtual antes de uma sincronização bem-sucedida. Para obter mais informações, consulte Exportação da VM.
- Se o arquivamento programado estiver configurado para arquivar em uma conta de nuvem, você precisa especificar as credenciais para que o Core possa se conectar à conta de nuvem. Para obter mais informações sobre a conexão do Core com uma conta de nuvem, consulte Adicionar uma conta de nuvem.
- Se a replicação estiver configurada e você quiser restaurar para um Core de destino, confirme as definições do Core de destino (particularmente do host) no Core de origem. Para obter mais informações, se você estiver gerenciando seu próprio Core, consulte Replicar para um Core de destino autogerenciado. Se estiver replicando para um núcleo gerenciado por terceiros, consulte Replicar para um Core de destino de terceiros.
- Se a verificação de capacidade de anexação do SQL estiver configurada e a instância do SQL Server estiver realizando as verificações na máquina do Core, especifique as credenciais do SQL nas definições de Capacidade de anexação. Para obter mais informações, consulte Gerenciar definições da capacidade de anexação do SQL.

Verifique se a configuração do mecanismo de reprodução foi restaurada e atualize as definições se elas não garantirem uma comunicação eficaz. Para obter mais informações, consulte Configurar as definições do mecanismo Replay.

Reiniciar ou encerrar o serviço Core

Invariavelmente, uma máquina em que o Rapid Recovery Core está em execução é encerrada ou precisa ser reiniciada. No versão 6.2, o Rapid Recovery Core foi aprimorado para melhorar sua capacidade de encerrar e reiniciar os serviços do Core.

Agora a interface do usuário do Core oferece recursos para reiniciar ou encerrar o serviço do Core com um clique. Esse recurso é útil quando a manutenção planejada do servidor Core (incluindo a reinicialização) é

necessária. Os usuários recebem uma notificação quando os serviços correspondentes são encerrados. Esses recursos são acessados na parte superior da página Definições do Core.

NOTE: Outro recurso útil que suporta o encerramento normal é a capacidade para impedir que o Core agende tarefas futuras. Para obter mais informações, consulte o tópico Suspender ou retomar tarefas agendadas.

Use este procedimento para reiniciar ou encerrar o serviço do Core.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Configurações).

   A página **Settings** (Configurações) será exibida. Na parte superior do painel de Configurações, acima das categorias de definições, você verá opções para **Reiniciar serviço do Core** ou para **Encerrar serviço do Core**.
3. Se você quiser reiniciar o serviço do Core, na parte superior do painel de Configurações, clique em **Restart Core Service** (Reiniciar serviço do Core).

   Uma lista de cada tarefa que deve ser concluída antes da reinicialização será exibida, incluindo uma exibição do progresso da tarefa.
4. Opcionalmente, você pode seguir uma destas opções:
   a. Para forçar a reinicialização (um processo menos comum em que as tarefas são explicitamente interrompidas antes da conclusão), clique em **Force Restart** (Forçar reinicialização).
   b. Para cancelar a reinicialização do serviço do Core, clique em **Cancel** (Cancelar).
5. Se você quiser encerrar o serviço do Core sem reiniciá-lo imediatamente, na parte superior do painel de Configurações, clique em **Shut Down Core Service** (Encerrar serviço do Core).
6. Opcionalmente, você pode seguir uma destas opções:
   a. Para forçar o encerramento (um processo menos comum em que as tarefas são explicitamente interrompidas antes da conclusão), clique em **Force Shutdown** (Forçar encerramento).
   b. Para cancelar a reinicialização do serviço do Core, clique em **Cancel** (Cancelar).

Tarefas relacionadas

See also: Suspender ou retomar tarefas agendadas

Definições do Rapid Recovery Core

O painel de Definições contém uma coluna de navegação no lado esquerdo, listando cada definição do Core. Clique em qualquer link nesta lista ou role a tela para baixo no lado direito da página para ver todas as opções de configuração para cada definição do Core.

Quando você clica em uma configuração que deseja alterar, essa configuração se torna um controle editável. Execute um dos seguintes:

- Quando o controle for um menu suspenso, clique na seta para baixo para listar as opções e selecione a opção desejada no menu.
- Quando o controle for um campo de texto, digite um valor.
- Quando a opção exibe Sim ou Não, clique no valor, o qual será substituído por uma caixa de seleção. Para uma configuração de Sim, marque a caixa de seleção. Para um valor Não, desmarque a caixa de seleção.
- Quando a opção exibe um valor temporal (por exemplo, mostrando horas, minutos e segundos), você pode clicar em cada componente e digitar um novo valor ou usar as setas para cima e para baixo para selecionar novos valores.

Para cada definição, quando estiver satisfeito com suas alterações, clique na para confirmar e salvar a alteração e sair do modo de edição, ou clique em para sair do modo de edição sem salvar.

As definições do Rapid Recovery Core que você pode configurar estão descritas na tabela a seguir. Cada definição tem um link para um tópico relevante com mais informações.

Tabela 7. Definições configuráveis do Rapid Recovery Core

Definição de configuração	Descrição
Geral	As definições gerais incluem opções de configuração que se aplicam geralmente ao Rapid Recovery, incluindo opções de exibição e portas do servidor da Web e do serviço Rapid Recovery Core. Para obter mais informações sobre as definições gerais do Rapid Recovery Core, incluindo como configurá-las, consulte Configurar definições gerais do Core.
Atualizações	As definições de atualização controlam os aspectos relacionados ao recurso de atualização automática, que verifica se há versões atualizadas do software Rapid Recovery. Para obter mais informações sobre as definições de atualização do Rapid Recovery Core, incluindo como configurá-las, consulte Configuração das definições de atualização.
Trabalhos noturnos	As definições de trabalhos noturnos referem-se às tarefas automatizadas que o Core realiza diariamente. Você pode configurar o horário de início e quais trabalhos são executados. A Quest recomenda programar os trabalhos fora do horário de expediente normal para reduzir a carga no sistema quando a demanda por recursos está alta. Para obter mais informações, consulte Noções básicas sobre trabalhos noturnos, Configurar trabalhos noturnos para o Core e Personalizar trabalhos noturnos para uma máquina protegida.
Fila de transferência	As definições de fila de transferência controlam o número de tentativas de transferência quando os trabalhos falham devido à indisponibilidade de recursos. Você pode estabelecer o número máximo de transferências simultâneas e o número máximo de tentativas de transferência de dados. Para obter mais informações sobre as definições da fila de transferência, consulte Modificar definições de fila de transferência.
Tempo limite do cliente	As definições de tempo limite do cliente determinam por quanto tempo serão realizadas tentativas de solicitações de conexão específicas ou de operações de leitura e gravação. Para obter mais informações sobre as definições de tempo limite do cliente, consulte Ajustar definições de tempo limite do cliente.
Cache de deduplicação DVM	A deduplicação garante que cada bloco de informações seja armazenado apenas uma vez no repositório, criando referências para blocos de dados repetidos. As referências são armazenadas em um cache de deduplicação. Quando chaves de criptografia são usadas, a deduplicação ocorre dentro de cada domínio de criptografia. As definições do cache de deduplicação do DVM permitem configurar o tamanho e especificar os locais dos caches primário e secundário, bem como do cache de metadados. Para obter mais informações sobre cache de deduplicação, consulte Noções básicas sobre o cache de deduplicação e locais de armazenamento. Para obter informações sobre como ajustar as definições, consulte Configurar definições de cache de deduplicação DVM.
Mecanismo Replay	As configurações do mecanismo Replay controlam as informações referentes ao canal de comunicação do mecanismo Replay, tais como endereços IP e configurações de

Definição de configuração	Descrição
	tempo limite, para ajudar a ajustar o desempenho específico às suas necessidades de rede. Para obter mais informações sobre as configurações do mecanismo para o Rapid Recovery, consulte Configurar as definições do mecanismo Replay.
Implantar	As definições de implantação permitem definir opções para implantar o software Rapid Recovery Agent de seu Core nas máquinas que você deseja proteger. Para obter mais informações sobre a configuração de definições de implantação, consulte Configurar as definições do implantação.
Conexão do banco de dados	O Rapid Recovery armazena as informações transacionais em um banco de dados de serviço MongoDB que, por padrão, é instalado localmente na máquina do Core. Você pode configurar essas definições para alterar o tempo de retenção de informações no banco de dados ou o tamanho do pool de conexões para permitir mais ou menos conexões simultâneas. Para obter mais informações sobre a configuração ou modificação de definições de conexão do banco de dados de serviço, consulte Configurar definições de conexão de banco de dados.
Definições do banco de dados local	O Rapid Recovery exibe informações sobre tarefas, eventos e alertas do Core na página Eventos. O Rapid Recovery armazena essas informações transacionais em um banco de dados de serviço MongoDB, que é instalado localmente na mesma máquina do Rapid Recovery Core. Você pode configurar informações de credencial (nome de usuário e senha) para o banco de dados de serviço Mongo local usando as definições de Banco de dados local. Para obter mais informações sobre como ajustar as definições do banco de dados local, consulte Modificar definições de conexão do database local.
Servidor SMTP	Configure as definições do servidor do protocolo SMTP para o Core enviar informações de eventos do Core por e-mail. Para obter mais informações sobre como configurar um server de SMTP para e-mail, consulte Configurar um servidor de e-mail. **NOTE:** Para enviar informações sobre eventos por e-mail, você também deve configurar as definições de grupo de notificação. Para obter mais informações sobre especificação de eventos para receber alertas por e-mail, consulte Configurar grupos de notificação.
Contas de nuvem	As definições contas de nuvem permitem que você especifique as definições de configuração das contas de nuvem suportadas. Essas definições não criam contas de nuvem. Em vez disso, eles associam contas existentes de armazenamento em nuvem externa ou de provedor de serviços de nuvem ao Rapid Recovery Core para facilitar ações como arquivamento de informações do Rapid Recovery. Para obter informações sobre como configurar as definições de tempo limite para contas de nuvem, consulte Configurar as definições de conexão da conta de nuvem. Para obter mais informações sobre como gerenciar contas de nuvem no Rapid Recovery Core Console, consulte Contas de nuvem.
Certificados de gerenciamento do Azure	Para obter informações sobre como tornar suas assinaturas do Azure acessíveis ao Core Console, carregue um certificado de gerenciamento do Azure para associá-lo ao seu Core. No Core Console, você pode carregar novos certificados, atualizar a visualização dos certificados atualmente associados ao seu Core ou excluir um certificado atualmente associado ao seu Core.

Definição de configuração	Descrição
	Para obter mais informações sobre como usar certificados de gerenciamento do Azure com o Core, consulte Trabalhar com certificados de gerenciamento do Azure associados ao seu Core.
Relatórios	As definições de relatório incluem parâmetros de configuração que permitem selecionar a fonte usada quando um relatório é gerado no Rapid Recovery Core. Você também pode definir o tamanho do papel e a orientação da página para relatórios. Para obter mais informações sobre como alterar as definições de relatórios, consulte Gerenciamento de definições de relatórios.
Capacidade de anexação	As definições de Capacidade de anexação permitem especificar se você deseja realizar Verificação de capacidade de anexação do SQL na máquina protegida ou se a instância do SQL Server deve ser usada no Core. Se você especificar SQL no Core, é preciso fornecer as informações de credencial. Para obter mais informações sobre como gerenciar as definições de capacidade de anexação do SQL para o Core, consulte Gerenciar definições da capacidade de anexação do SQL.
Trabalhos	Os trabalhos do Core são criados automaticamente quando você inicia operações, como replicação. Você pode especificar as definições de cada trabalho usando as configurações do Core para Trabalhos. Você pode configurar o número de trabalhos executados simultaneamente. Caso um erro de rede ou outro erro de comunicação impeça que o trabalho seja bem-sucedido de início, você pode definir o número de novas tentativas a serem feitas usando a definição de Contagem de tentativas. Para obter mais informações sobre trabalhos do Core, quais trabalhos estão disponíveis e como configurá-los, consulte Definições de trabalhos do Core.
Aplicação de licença	No Core Console, o Rapid Recovery permite alterar a licença associada ao Core, limitar o número de instantâneos diários, visualizar informações sobre o pool de licenças e contatar o servidor de licenças. Para obter mais informações sobre o gerenciamento de licenças no Core, consulte Gerenciar licenças. Para obter mais informações sobre o gerenciamento de licenças, consulte *Guia do usuário do portal de licenças do Rapid Recovery*. **NOTE:** O Portal de licenças do Rapid Recovery tem um ciclo de lançamento diferente do software Rapid Recovery. Para acessar a documentação mais recente do produto, consulte o site de documentação técnica da Quest.
Configuração do SNMP	O Protocolo Simples de Gerenciamento de Rede (SNMP) é um protocolo para gerenciar dispositivos em uma rede IP. Você pode configurar o Rapid Recovery Core como um agente SNMP. Assim o Core pode enviar informações como alertas, status do repositório e máquinas protegidas. Para obter mais informações sobre como usar SNMP com o Rapid Recovery, consulte Definir as definições do SNMP.
vSphere	As definições do vSphere Core são aplicadas somente aos usuários com proteção sem agentes em máquinas virtuais. Se você estiver usando um host vSphere, essas definições incluem configurações que se aplicam às VMs. Para obter mais informações sobre as definições do vSphere para a proteção sem agentes VMware ou ESXi, consulte Configuração das definições do vSphere.

Definição de configuração	Descrição
Proxy VMware	Um serviço de proxy VMware instalado com o Core permite que os usuários definam tempos limites de serviço associados ao armazenamento em disco VMware. Para obter mais informações sobre essas configurações, consulte Gerenciar as configurações de proxy do VMware.
Portal de proteção de dados	Se você estiver gerenciando dois ou mais Cores, pode integrar o servidor do Core ao Portal de proteção de dados Quest. Esse recurso, particularmente útil para provedores de serviços gerenciados, permite gerenciar vários Cores; acessar um painel de onde você pode monitorar tarefas e eventos, exibir o status do repositório e verificar a integridade do sistema; gerar relatórios e criar uma lista crescente de outras funções a partir de uma única interface de usuário baseada na web. Para ativar ou desativar o acesso ao portal, utilize esta configuração.
vFoglight	O Quest Foglight for Virtualization (vFoglight) ajuda os administradores a monitorar, analisar e otimizar hipervisores em ambientes VMware, Hyper-V e OpenStack. Para clientes que gerenciam VMs usando o vFoglight e os protegem em um Rapid Recovery Console, essa configuração do Core permite integrar a navegação para os dois produtos. Depois de especificar as configurações do vFoglight com sucesso, ao clicar no URL do vFoglight na página **Summary** (Resumo) da VM no Core Console, os usuários navegam para a página correspondente dessa máquina virtual no vFoglight. Para obter mais informações sobre as configurações do Core para o vFoglight, consulte Configurar as definições do VFogLight. Para obter mais informações sobre o vFoglight, consulte a página do produto vFoglight no site do Quest.

Você pode também acessar as ferramentas do Core, como ver um resumo das informações do sistema ou fazer download dos arquivos de log do Core. Para obter mais informações, consulte Ferramentas de nível do Core.

Configurar definições gerais do Core

As definições gerais do Rapid Recovery Core incluem ID do Core, nome de exibição do Core, porta do servidor da web, porta de serviço, localidade (o idioma de exibição do Core Console) e o tema de cor da exibição.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de Definições do Core, no lado esquerdo da página de Definições, clique em **Geral**.
   - Role a tela para baixo no lado direito da página de Definições até que consiga ver o cabeçalho "Geral".
3. Clique na definição geral que deseja alterar.

   A definições selecionada se tornará editável, como um campo de texto ou um menu suspenso.
4. Insira as informações de configuração conforme descrito na tabela a seguir.

Tabela 8. Informações sobre as definições gerais

Caixa de texto	Descrição
ID do Core	Cada Core tem uma ID exclusiva. Essa ID é utilizada, por exemplo, para integrar o Core ao portal do Portal de proteção de dados para fornecer relatórios ou gerenciamento de dois ou mais Cores. Agora a ID do Core é listada nas Definições gerais. **NOTE:** Esse campo não é configurável.

Caixa de texto	Descrição
Nome de exibição	Insira um novo nome de exibição para o Core. Esse é o nome que será exibido no Rapid Recovery Core Console e (se habilitado) no Portal de proteção de dados. Você pode inserir até 64 caracteres.
Porta do servidor da Web	Insira um número de porta para o servidor da Web. A porta padrão é 8006. **NOTE:** A Quest recomenda usar a porta padrão.
Porta de serviço	Insira um número de porta para o serviço Rapid Recovery Core. A porta padrão é 8006. **NOTE:** A Quest recomenda usar a porta padrão.
Localidade	Na lista suspensa **Localidade**, selecione o idioma que você deseja usar. Você pode escolher entre inglês, francês, alemão, japonês, coreano, português, chinês simplificado e espanhol. **NOTE:** Se você alterar o idioma, confirme a mensagem indicando que o serviço Rapid Recovery Core deve ser reiniciado para que o idioma atualizado possa ser exibido no Core Console. Você pode reiniciar este serviço usando o botão **Reiniciar serviço do Core** na parte superior da página Configurações do Core.
Tema	Na lista suspensa **Temas**, selecione o estilo que você deseja aplicar ao Core Console. Três temas estão disponíveis: • **Escuro**. Esse tema tem um plano de fundo cinza escuro sólido em toda a interface (menu de navegação à esquerda, barra de botões superior e painel principal). Os elementos de texto e botões de texto aparecem em off-white quando não estão em foco e em branco quando estão em foco. Os links clicáveis aparecem em um azul médio. Os botões ocasionais têm texto branco sobre um fundo azul médio. • **Híbrido**. Esse tema tem o plano de fundo cinza escuro familiar para menu de navegação à esquerda e a barra de botões na parte superior do Core Console. Os elementos de texto nessas áreas são brancos. O painel principal tem um fundo branco com realces em off-white, com elementos de texto e os botões de texto em preto. Os links clicáveis aparecem em um azul escuro. Os botões ocasionais têm texto branco sobre um fundo azul. • **Claro**. Esse tema tem um plano de fundo branco em toda a interface (menu de navegação à esquerda, barra de botões superior e painel principal). O logotipo da Quest e alguns elementos de design são exibidos em laranja. Os elementos de texto ficam em cinza escuro, com títulos em preto. Os links clicáveis aparecem em azul médio com a passagem do mouse. Os botões ocasionais têm texto branco sobre um fundo azul médio.
Concordar em usar dados pessoais	Para alterar a configuração que permite ao aplicativo usar informações pessoais, na lista suspensa **Concordar com o uso de dados pessoais**, selecione **Sim** ou **Não**, conforme apropriado. Na caixa de diálogo resultante, selecione e registre o arquivo de licença apropriado. Ao atualizar ou instalar o Rapid Recovery Core, você terá a opção de definir o compartilhamento de informações pessoais. Se você concordar em compartilhar informações com a Quest, você poderá usar recursos como a atualização automática e o Portal de proteção de dados (que é habilitado por padrão).

Caixa de texto	Descrição
	Se durante a instalação você recusar compartilhar informações com a Quest, será solicitado registrar uma licença de telefone não residencial. Você deve ter acesso à licença de telefone não residencial para salvar e confirmar a alteração. Independentemente da opção selecionada durante a instalação, você pode alterar a configuração **Concordar com o uso de dados pessoais** nas configurações gerais do Core. Certifique-se de ter acesso à licença de telefone não residencial, pois essa ação solicita que você carregue a licença de telefone não residencial. Na versão 6.2, ao alterar essa configuração de "Sim" para "Não", o seguinte se aplica: a. Será solicitado carregar o arquivo de licença de telefone não residencial. b. Depois de confirmar a licença de telefone não residencial, as configurações de atualizações para o Core se ajustam automaticamente para nunca verificar ou instalar atualizações do Core. c. A configuração do Portal de proteção de dados "Habilitar a conexão para o portal de proteção de dados" é definida como "Não". No entanto, o inverso não é verdadeiro. Ao alterar essa configuração de "Não" para "Sim", você concede permissão ao Core de compartilhar suas informações; no entanto, nenhuma informação será compartilhada até que você altere explicitamente a licença para o modo de telefone residencial e atualize o Core apropriado. Por exemplo: a. A chave de telefone não residencial permanece registrada até você carregar explicitamente uma chave de telefone residencial padrão (que você pode obter através do portal de licenças). b. Para usar a opção de atualizações automáticas, altere a opção "Verificar se há novas atualizações" de "Nunca" para "Diariamente", "Semanalmente" ou "Mensalmente". Opcionalmente, altere a opção "Instalar atualizações" para notificá-lo ou para instalar as atualizações automaticamente. c. Para compartilhar informações com o Portal de proteção de dados, defina "Habilitar a conexão para portal de proteção de dados" para "Sim". **NOTE:** Se você configurar essa opção primeiro, você será solicitado a carregar uma licença de telefone residencial. Para entender o efeito de compartilhamento de informações pessoais, consulte Gerenciar privacidade, incluindo o tópico Como o Rapid Recovery usa informações pessoais. Para obter mais informações sobre as funções que você não pode executar ao usar o modo de telefone não residencial, consulte o tópico Restrições de chave de licença não telefônica. Para solicitar uma licença para o **modo de telefone não residencial**, consulte Obtenção e uso de licenças de telefone não residencial.

5. Para cada definição, quando estiver satisfeito com suas alterações, clique na ✓ para salvar a alteração e sair do modo de edição, ou clique em ✕ para sair do modo de edição sem salvar.

Configuração das definições de atualização

O Rapid Recovery inclui o recurso de atualização automática. Ao instalar o Rapid Recovery Core, é possível optar por atualizar automaticamente o software Rapid Recovery Core quando houver novas atualizações disponíveis e a frequência com que o sistema deve verificar se há atualizações.

NOTE: O recurso de atualização automática exige uma licença usando o modo de telefone residencial padrão. Se estiver usando uma licença de software no modo de telefone não residencial, o Core não tem permissão para se comunicar com o Portal de licenças do Rapid Recovery e não é possível atualizar o Core ou notificar você sobre as atualizações disponíveis. Para obter mais informações, consulte Gerenciar privacidade.

Os números de versão do Rapid Recovery normalmente incluem quatro blocos de informações, separados por pontos decimais: o número da versão principal, o número da versão secundária, a revisão e número da compilação. Por exemplo, a primeira versão remarcada do Rapid Recovery foi a 6.0.1.609. A versão seguinte foi a 6.0.2.142.

O recurso de atualização automática faz uma comparação entre todos os dígitos de um número de versão. Se você ativar a atualização automática, o software Core é apenas atualizado sem intervenção quando os números de versão principal e secundário são idênticos. Por exemplo, uma atualização automática ocorreria da versão de Core 6.0.1.609 para 6.0.2.142 (as duas versões começam com 6.0). Na mesma máquina, o Core não atualizaria automaticamente de 6.0.2.142 para 6.1.1.XXX, pois os dígitos após o primeiro decimal não são iguais. Em vez disso, você será notificado (através de um banner no topo do Core Console) de que há uma atualização para o software Core disponível. Esta notificação dá a você uma oportunidade para rever as notas de versão e determinar se atualizar para a versão mais recente do Core é adequado às suas necessidades.

NOTE: Para obter informações sobre como instalar o software Guia de instalação e atualização do Rapid Recovery Core, consulte o *Rapid Recovery*.

É possível visualizar e alterar as definições que o sistema utiliza para verificar se há atualizações a qualquer momento.

CAUTION: Ao usar replicação, a configuração do sistema para instalar atualizações automaticamente pode fazer com que o Core de origem seja atualizado antes do Core de destino, o que pode acarretar falha de replicação ou impedir o estabelecimento de uma nova replicação entre os Cores. Para usuários de replicação, a Quest **recomenda que os administradores apliquem atualizações automáticas apenas ao Core de destino, depois atualizem manualmente o Core de origem e, por fim, atualizem as máquinas protegidas.**

Execute as etapas deste procedimento para configurar as definições de atualização.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página **Definições**, clique em **Atualizações**.
   - Role a tela para baixo no lado direito da página **Definições** até ver o cabeçalho Atualizações.
3. Clique na definição que você deseja alterar.

   A definição selecionada se torna editável.
4. Insira as informações de configuração conforme descrito na tabela a seguir.

Tabela 9. Informações das definições de atualização

Caixa de texto	Descrição
Verificar se há novas atualizações	Selecione a frequência com que o Rapid Recovery deve procurar e instalar as atualizações. Você pode selecionar dentre as seguintes opções: • Nunca • Diariamente • Semanalmente • Mensalmente

Caixa de texto	Descrição
	Se você optar por atualizações automáticas, depois que o limite de tempo selecionado passar, se uma atualização estiver disponível ela é instalada depois que os trabalhos noturnos forem concluídos.
Instalar atualizações	Especifique como as atualizações disponíveis serão tratadas escolhendo uma das seguintes opções: • Nunca procurar por atualizações • Notificar-me sobre atualizações, mas não instalá-las automaticamente • Instalar atualizações automaticamente
Status	O estado indica se há novas atualizações disponíveis.
Última verificação	O campo Última verificação indica a data e a hora em que o sistema verificou se há novas atualizações pela última vez. Clique em**Verificar agora** para verificar imediatamente se há alguma atualização de software disponível. Esta verificação ocorre independentemente da frequência definida.

5. Para cada definição, quando estiver satisfeito com suas alterações, clique na ✓ para salvar a alteração e sair do modo de edição, ou clique em ✕ para sair do modo de edição sem salvar.

Noções básicas sobre trabalhos noturnos

Trabalhos noturnos são tarefas diárias automatizadas que ocorrem em horários predeterminados, fora do horário de expediente normal. Como demandam muita memória e incluem várias verificações de integridade e tarefas de consolidação de dados, esses trabalhos devem ser executados preferivelmente quando o Rapid Recovery Core está menos ativo.

Todos os trabalhos noturnos e o escopo a que se aplicam são descritos na tabela a seguir. Os trabalhos noturnos podem ser gerenciados do nível do Core (aplicado a todas as máquinas protegidas no Core). Esses trabalhos noturnos também podem ser aplicado a uma lista de máquinas protegidas específicas do escopo como "Máquina protegida."

Tabela 10. Informações sobre trabalhos noturnos

Nome do trabalho	Escopo	Descrição
Alterar	N/A	Esse comando abre a caixa de diálogo **Trabalhos noturnos**, onde você pode habilitar, desabilitar ou alterar as definições de cada trabalho noturno.
Hora de trabalhos noturnos	Todos	Essa definição representa a hora em que a execução dos trabalhos noturnos começa, de acordo com a programação. A Quest recomenda configurar seu Core para executar trabalhos noturnos durante um período de baixa atividade. A hora padrão é 00:00.
Verificar a capacidade de anexação dos bancos de dados SQL	Máquina protegida	Verifica a integridade de pontos de recuperação que contêm bancos de dados SQL. Para obter mais informações, consulte Gerenciar definições da capacidade de anexação do SQL.

Nome do trabalho	Escopo	Descrição
Verificar a soma de verificação dos bancos de dados do Exchange	Máquina protegida	Verifica a integridade dos pontos de recuperação que contêm arquivos de Banco de dados do Exchange (EDB). **NOTE:** Esta opção aparece apenas quando há um Exchange Server sendo protegido no Core.
Verificar integridade dos bancos de dados da Oracle	Core ou máquina protegida	Verifica a integridade dos bancos de dados Oracle usando o utilitário DBVERIFY. Processo: • Montar o último ponto de recuperação de cada grupo de proteção. • Enumerar os arquivos e pastas de cada volume. • Examina os pontos de recuperação para garantir que os arquivos de dados sejam válidos e os blocos de dados não estejam corrompidos. • Desmontar o ponto de recuperação.
Verificar a integridade dos pontos de recuperação	Core ou máquina protegida	Verifica a integridade dos pontos de recuperação de cada máquina protegida. Por padrão, a opção `Check integrity of recovery points` não está habilitada. Processo: • Montar o último ponto de recuperação de cada grupo de proteção. • Enumerar os arquivos e pastas de cada volume. • Examinar os pontos de recuperação para garantir sua validade. • Desmontar o ponto de recuperação.
Limpar as chaves de registro órfãs em agentes do Hyper-V		Para hosts do Hyper-V que usam a proteção sem agente do Rapid Recovery versão 6.1.X, esse trabalho noturno limpa chaves órfãs criadas no Registro do Windows para cada operação de anexar e desanexar. As entradas do Registro são inofensivas, mas com o passar do tempo podem se acumular, diminuindo o desempenho. **NOTE:** A partir do versão 6.2 Rapid Recovery, uma abordagem melhorada para obter metadados de armazenamento a proteção sem agente do Hyper-V impede a criação de entradas do Registro.
Consolidar snapshots do VMware para máquinas virtuais protegidas	Core ou máquina protegida	Esse trabalho noturno é relevante se você usar APIs VMware nativas para proteger máquinas sem o software do agente Rapid Recovery. Você deve consolidar os snapshots do VMware periodicamente. A ativação desse trabalho noturno permite realizar essas consolidações diariamente. Esse trabalho noturno contém um parâmetro, "Máximo de consolidações simultâneas", que precisa ser definido como um número entre 1 e 100.
Exclusão deferida	Core	Essa configuração permite adiar a remoção de pontos de recuperação do repositório até o período especificado no Core para executar trabalhos noturnos. Quando ativado, após a execução de outros trabalhos noturnos, o processamento do Core é dedicado para executar o trabalho "Excluir registros anteriormente sinalizados para exclusão". Esse trabalho remove pontos de recuperação marcados do repositório até que todos tenham sido removidos ou até que se passem quatro horas do horário de execução dos

Nome do trabalho	Escopo	Descrição
		trabalhos noturnos. Então, os trabalhos noturnos são finalizados e outros trabalhos na fila são retomados. Todas as exclusões restantes ocorrem em segundo plano, simultaneamente com outras tarefas, até a execução dos trabalhos noturnos do dia seguinte. Por padrão, a opção `Deferred Delete` não está habilitada. A Quest recomenda deixar esse trabalho noturno desativado, a menos que você esteja tendo problemas de desempenho de transferência relacionados às exclusões de pontos de recuperação salvos em backup. Se ativar essa opção, a Quest recomenda revisar os trabalhos do Core para garantir que a maioria dos pontos de recuperação marcados para exclusão seja removida do repositório dentro de uma semana. Essa abordagem ajuda a equilibrar o desempenho de transferência máxima com máxima recuperação de espaço no repositório.
Excluir eventos e trabalhos antigos	Core	Mantém a escala do banco de dados de eventos removendo os eventos antigos. O número de dias pode ser alterado, sendo 30 o padrão.
Registrar truncamento do Exchange	Máquina protegida	Mantém o tamanho dos logs do Exchange truncando o log de transações de banco de dados do Exchange para corresponder ao último ponto de recuperação. **NOTE:** Esta opção aparece apenas quando há um Exchange Server sendo protegido no Core.
Registrar truncamento da Oracle	Máquina protegida	Controla o truncamento de logs do Oracle. A menos que esteja desativado, o truncamento ocorre uma vez por dia, quando os trabalhos noturnos são executados. • Você pode seguir a política de exclusão **Automática** do Core (ativada por padrão), que trunca todos os logs do Oracle armazenados localmente quando os trabalhos noturnos são executados. Os logs do dia atual ainda persistem nos instantâneos de backup antes da execução dos trabalhos noturnos. • Você pode selecionar uma política de exclusão personalizada para um servidor Oracle protegido específico. A política **Manter mais recentes** permite especificar a duração que antecede o truncamento de logs do Oracle, e a política **Manter número especificado** permite manter um número especificado de arquivos de log antes de truncar os mais antigos. • Você pode desativar o trabalho noturno, que resulta em um acúmulo substancial de arquivos de log. Nesses casos, os usuários também podem truncar os arquivos de log manualmente, como descrito no tópico Truncamento manual de logs de banco de dados Oracle.
Registrar truncamento do SQL	Máquina protegida	Mantém o tamanho dos logs do SQL Server truncando o log de transações de banco de dados para corresponder ao último ponto de recuperação. **NOTE:** Esta opção aparece apenas quando há um SQL Server sendo protegido no Core.

Nome do trabalho	Escopo	Descrição
Rollup	Core ou máquina protegida	Aplica a política de retenção aos seus dados de backup com a combinação de pontos de recuperação "em execução" na programação definida pela política. Você pode personalizar a política no Core, que, por padrão, se aplica em todas as máquinas protegidas. Por padrão, o trabalho de rollup é executado para o Core inteiro. Ou clique em [Expandir] para expandir a visualização das máquinas protegidas. Depois, você pode definir o conjunto de máquinas protegidas em que deseja fazer rollup usando a política do Core. Para obter mais informações sobre como usar uma política de retenção em uma máquina protegida que difere da política padrão definida no Core, consulte Personalizar as definições de política de retenção de uma máquina protegida.

Configurar trabalhos noturnos para o Core

Quando qualquer opção de trabalho noturno é ativada no Rapid Recovery Core, o trabalho selecionado é executado uma vez por dia, no horário especificado, com todas as máquinas protegidas pelo Core. Da mesma forma, se você desabilita algum trabalho noturno no nível do Core, o trabalho especificado deixa de ser executado em todas as máquinas protegidas pelo Core.

NOTE: Se o escopo de um trabalho noturno, conforme descrito no tópico Noções básicas sobre trabalhos noturnos, inclui máquinas protegidas, você pode configurar esse trabalho para ser aplicado apenas a uma ou mais máquinas protegidas individualmente. Para obter mais informações sobre como aplicar definições de trabalhos noturnos específicas a uma máquina protegida, consulte Personalizar trabalhos noturnos para uma máquina protegida.

Como os trabalhos noturnos usam muita memória, a Quest recomenda configurar o Core para executá-los durante um período de baixa atividade. Por padrão, os trabalhos noturnos são programados para serem executados à meia-noite. Se outro horário for mais adequado, altere essa definição no campo Horário dos trabalhos noturnos usando este procedimento.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página **Definições**, clique em **Trabalhos noturnos**.
   - Role a tela para baixo no lado direito da página **Definições** até ver o cabeçalho Trabalhos noturnos.
3. Para alterar qualquer trabalho noturno ou alterar a hora em que trabalhos noturnos começam a ser executados, clique em **Change** (Alterar).

   A caixa de diálogo **Trabalhos noturnos** é exibida.
4. Para alterar o horário em que os trabalhos noturnos são executados, insira um novo horário no campo **Horário dos trabalhos noturnos**.
5. Na primeira coluna, clique para selecionar cada opção de trabalhos noturnos que você deseja definir para o Core. Clique em qualquer opção selecionada para desmarcá-la.
6. Clique em **OK**.

   A caixa de diálogo **Trabalhos noturnos** é fechada e suas definições de trabalho noturno do Core são salvas.

Modificar definições de fila de transferência

As definições da fila de transferência são no nível do Core e estabelecem o número máximo de transferências simultâneas e de novas tentativas de transferência de dados.

Execute as etapas deste procedimento para modificar as definições da fila.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página Definições, clique em **Fila de transferência**.
   - Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Fila de transferência.
3. Clique na definição que você deseja alterar.

   A definição selecionada se torna editável.
4. Insira as informações de configuração conforme descrito na tabela a seguir.

Tabela 11. Informações das definições de fila de transferência

Caixa de texto	Descrição
Máximo de transferências simultâneas	Digite um valor para atualizar o número de transferências simultâneas. Defina um número de 1 a 60. Quanto menor for o número, menor a carga sobre a rede e outros recursos do sistema. Conforme o número de agentes processados aumenta, a carga sobre o sistema também aumenta.
Máximo de novas tentativas	Digite um valor para definir o número máximo de tentativas antes de cancelar a operação de transferência. Defina um número de 1 a 60.

5. Para cada definição, quando estiver satisfeito com suas alterações, clique na para salvar a alteração e sair do modo de edição, ou clique em para sair do modo de edição sem salvar.

Ajustar definições de tempo limite do cliente

As definições de tempo limite do cliente controlam por quanto tempo diferentes operações serão tentadas antes que o tempo se esgote.

NOTE: A Quest recomenda manter as definições padrão de tempo limite, a menos que você tenha problemas específicos em seu ambiente e um representante do Quest Support recomende a modificação das definições.

Execute as etapas deste procedimento para ajustar as definições de tempo limite do cliente.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página Definições, clique em **Tempo limite do cliente**.
   - Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Tempo limite do cliente.
3. Clique na definição que você deseja alterar.

A definição selecionada se torna editável.

4. Insira as informações de configuração conforme descrito na tabela a seguir.
5.

Tabela 12. Informações das definições de tempo limite do cliente

Configuração	Descrição
Tempo limite de conexão	Controla o tempo limite da conexão entre o Core e as máquinas protegidas ao enviar dados usando o protocolo de transferência de hipertexto (HTTP). Insira a quantidade de tempo que deve passar antes que um tempo limite de conexão ocorra. Usa o formato HH:MM:SS. **NOTE:** A definição padrão é 0:05:00 ou cinco minutos.
Tempo limite de leitura/gravação	Controla o tempo limite da conexão entre o Core e as máquinas protegidas ao ler ou gravar dados de fluxo através por HTTP. Um exemplo é o recebimento pelo Core de blocos de dados alterados de uma máquina protegida para criar um snapshot incremental. Insira a quantidade de tempo que deve passar antes que um tempo limite ocorra durante um evento de leitura/gravação. Usa o formato HH:MM:SS. **NOTE:** A definição padrão é 0:05:00 ou cinco minutos.
Tempo limite da UI de conexão	Controla o tempo limite da conexão entre a interface gráfica de usuário e o serviço Rapid Recovery Core por HTTP. Insira a quantidade de tempo que deve passar antes que um tempo limite de UI de conexão ocorra. Usa o formato HH:MM:SS. **NOTE:** A definição padrão é 0:05:00 ou cinco minutos.
Tempo limite da UI de leitura/gravação	Controla o tempo limite da conexão para leitura e gravação de fluxos de dados entre a interface gráfica de usuário e o serviço Rapid Recovery Core por HTTP. Insira a quantidade de tempo que deve passar antes que um tempo limite ocorra durante eventos de leitura ou gravação. Usa o formato HH:MM:SS. **NOTE:** A definição padrão é 0:05:00 ou cinco minutos.

6. Para cada definição, quando estiver satisfeito com suas alterações, clique na ✓ para salvar a alteração e sair do modo de edição, ou clique em ✕ para sair do modo de edição sem salvar.

Noções básicas sobre o cache de deduplicação e locais de armazenamento

A deduplicação global reduz a quantidade de espaço de armazenamento em disco necessário para os dados salvos em cópias de segurança pelo Core. Cada repositório é deduplicado, armazenando cada bloco único uma vez fisicamente em disco, e utilizando referências virtuais ou indicadores a esses blocos em cópias de segurança subsequentes. Para identificar blocos duplicados, o Rapid Recovery inclui um cache de deduplicação em repositórios de gerenciador de volume de deduplicação (DVM). O cache mantém referências a blocos exclusivos.

Por padrão, para repositórios de DVM, essa cache de deduplicação é de 1,5 GB. Esse tamanho é suficiente para vários repositórios. Até esse cache ser excedido, seus dados são deduplicados em todo o repositório. Quando a quantidade de informações redundantes for tão grande que o cache de deduplicação fique cheio, seu repositório não poderá mais tirar total vantagem de deduplicação adicional para dados recém-adicionados. A quantidade de dados salvos em seu repositório antes que o cache de deduplicação encha varia por tipo de dados salvos em cópias de segurança e é diferente para cada usuário.

É possível aumentar o tamanho do cache de deduplicação DVM alterando as definições do cache de deduplicação no Rapid Recovery Core. Para obter mais informações sobre como aumentar o tamanho do cache, consulte o tópico Configurar definições de cache de deduplicação DVM.

Quando você aumentar o tamanho do cache de deduplicação DVM, há dois fatores a considerar: espaço em disco e uso de RAM.

Espaço em disco. Duas cópias do cache de deduplicação DVM são armazenadas em disco: um cache primário, e um cache secundário, que é uma cópia paralela. Portanto, se você estiver usando o tamanho de cache padrão 1,5 GB para um repositório de DVM, 3 GB de armazenamento em disco são usados no seu sistema. À medida que você aumenta o tamanho do cache, a quantidade de espaço em disco utilizado continua proporcionalmente o dobro do tamanho do cache. Para garantir o desempenho adequado e resistente a erros, o Core altera de forma dinâmica a prioridade desses caches. Ambos são necessários, a única diferença é que o cache designado como principal é salvo primeiro.

Uso de RAM. Quando o Rapid Recovery Core inicia, ele carrega o cache de deduplicação para a memória RAM. O tamanho do cache, portanto, afeta o uso de memória do seu sistema. A quantidade total de memória RAM usada pelo Core depende de muitos fatores. Esses fatores incluem quais operações estão em execução, o número de usuários, o número de máquinas protegidas e o tamanho do cache de deduplicação. Toda operação realizada pelo Core (transferência, replicação, rollup e assim por diante) consome mais RAM. Depois que uma operação é concluída, o consumo de memória diminui cada vez mais. Contudo, os administradores devem considerar o requisito mais alto do carregamento de RAM para obterem operações eficientes.

As definições padrão do Rapid Recovery Core colocam o cache principal, o cache secundário e o cache de metadados de repositórios de DVM no diretório AppRecovery. Essa pasta é instalada na máquina do Core.

NOTE: Dependendo de suas configurações, o diretório do AppRecovery pode não estar visível no Rapid Recovery Core. Para ver esse diretório, você pode precisar alterar as Opções de pasta no painel de controle para exibir arquivos, pastas e unidades ocultas.

Supondo que o Rapid Recovery Core esteja instalado na unidade C, esses locais são normalmente os seguintes:

Tabela 13. Os locais de armazenamento padrão para configurações do cache de deduplicação DVM

Configuração	Local de armazenamento padrão
Local do cache principal	C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache
Local do cache secundário	C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache
Local do cache de metadados	C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata

Você pode alterar o local de armazenamento desses caches. Por exemplo, para aumentar a tolerância a erros, é possível alterar o local do seu cache secundário para uma unidade física diferente do cache principal, supondo que o Rapid Recovery Core tenha acesso ao local.

Para obter mais informações sobre como alterar os locais de armazenamento para qualquer dessas definições, consulte o tópico Configurar definições de cache de deduplicação DVM.

A Quest recomenda que você planeje o armazenamento da deduplicação separadamente. A deduplicação ocorre apenas em um único repositório (não em vários repositórios). Se você estiver usando criptografia baseada em

Core, a deduplicação é limitada aos dados protegidos por uma única chave, visto que, por motivos de segurança, cada chave funciona para um único domínio de criptografia.

Para obter mais informações sobre deduplicação, consulte Deduplicação no Rapid Recovery.

Configurar definições de cache de deduplicação DVM

Execute as etapas deste procedimento para configurar as definições de cache de deduplicação de repositórios de DVM.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página Definições, clique em **Cache de deduplicação DVM**. Essa definição é mostrada apenas se o seu Core tiver um ou mais repositórios de DVM.
   - Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Cache de deduplicação DVM.
3. Se você quiser restaurar as definições do cache de deduplicação DVM para o padrão a qualquer momento, faça o seguinte:
   a. Na parte superior da área de definições do cache de deduplicação, clique em **Restore Default** (Restaurar padrão).

   A caixa de diálogo Restaurar padrão é exibida

   b. Clique em **Sim** para confirmar a restauração.
4. Clique na definição que você deseja alterar.

   A definição selecionada se torna editável.
5. Para alterar definições individuais de cache de deduplicação, digite as informações de definição conforme descritas na tabela a seguir.

Tabela 14. Informações de definição do cache de deduplicação DVM

Configuração	Descrição
Restaurar padrão	Esse controle redefine os locais de cache de DVM para os locais padrão do sistema, que são descritos para cada definição.
Local do cache principal	Se você desejar alterar o local do cache primário para repositórios de DVM, na caixa de texto Local de cache primário, insira o caminho para um local de armazenamento acessível ao Core. O local padrão é: `C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache` Uma vez que o cache principal e o secundário têm o mesmo tamanho, o armazenamento coletivo para esses dois caches exige duas vezes a quantidade de espaço da quantidade alocada para o tamanho do cache de deduplicação. Por exemplo, se você especificar a quantidade padrão de 1,5 GB para o tamanho do cache de deduplicação, garanta que cada um dos dois locais de armazenamento tenha, pelo menos, 1,5 GB. Em particular, se os dois locais pertencem à mesma unidade (por exemplo, na unidade C), deverá haver pelo menos 3 GB de espaço livre em disco.
Local do cache secundário	Se você desejar alterar o local do cache secundário para repositórios de DVM, na caixa de texto Local de cache secundário, insira o caminho para um local de armazenamento acessível ao Core. O local padrão é:

Configuração	Descrição
	`C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache`
Local de metadados de cache	Se você desejar alterar o local de metadados de cache para repositórios de DVM, na caixa de texto Local de metadados de cache, insira o caminho para um local de armazenamento acessível ao Core. O local padrão é: `C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata`
Tamanho do cache de deduplicação (GB)	Se você quiser alterar o tamanho do cache para deduplicação de repositórios de DVM, na caixa de texto Tamanho do cache de deduplicação, digite um novo valor (em GB). O local padrão é: `C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache` A configuração do tamanho mínimo do cache é de 1,5 GB. Além disso, o tamanho do cache não pode exceder 50 por cento da RAM instalada.

6. Para cada definição, quando estiver satisfeito com suas alterações, clique na ✓ para salvar a alteração e sair do modo de edição, ou clique em ✕ para sair do modo de edição sem salvar.

Configurar as definições do mecanismo Replay

Você pode configurar as informações relacionadas ao mecanismo Replay, que é o canal de comunicação do Rapid Recovery. Esses parâmetros determinam as definições do Core para proporcionar uma comunicação eficaz.

Em geral, a Quest recomenda usar as definições padrão. Em alguns casos, o Quest Support pode solicitar que você modifique essas definições para ajustar o desempenho às suas necessidades de rede.

Conclua as etapas deste procedimento para configurar as definições do mecanismo Replay.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em ⚙ (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página Definições, clique em **Replay Engine**.
   - Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Replay Engine.
3. Clique na definição que você deseja alterar.

   A definição selecionada se torna editável.
4. Insira as informações de configuração conforme descrito na tabela a seguir.

Tabela 15. Informações de definições do mecanismo Replay

Caixa de texto	Descrição
Endereço IP	O Core usa esse endereço IP para montar e restaurar um ponto de recuperação, para permitir o feedback entre máquinas protegidas e o Core. O endereço IP do mecanismo Replay é preenchido automaticamente com o endereço IP da máquina do Core. Se você inserir manualmente o endereço IP do servidor, esse valor é utilizado nos casos em que a máquina protegida não pode resolver automaticamente o endereço IP fornecido.

Caixa de texto	Descrição
	Você não precisará definir esse valor manualmente, a menos que tenha problemas com a conexão entre máquinas protegidas e o Core.
Porta preferencial	Insira um número de porta ou aceite a definição padrão. A porta padrão é 8007. A porta é usada para especificar o canal de comunicação do mecanismo Replay.
Porta em uso	Representa a porta em uso para a configuração do mecanismo Replay.
Permitir atribuição automática de porta	Clique para permitir a atribuição automática de porta TCP.
Grupo de administradores	Insira um novo nome para o grupo de administração. O nome padrão é BUILTIN \Administrators.
Comprimento mínimo de I/O assíncrono	Insira um valor ou escolha a definição padrão. Descreve o comprimento mínimo assíncrono de entrada/saída. A definição padrão é 65536.
Tempo limite de leitura	Insira um valor de tempo limite de leitura ou escolha a definição padrão. A definição padrão é 00:05:00.
Tempo limite de gravação	Insira um valor de tempo limite de gravação ou escolha a definição padrão. A definição padrão é 00:05:00.
Tamanho do buffer de recebimento	Insira um tamanho de memória intermediária de entrada ou aceite a definição padrão. A definição padrão é 8192.
Tamanho do buffer de envio	Insira um tamanho de memória intermediária de saída ou aceite a definição padrão. A definição padrão é 8192.
Sem atraso	Recomendamos deixar essa caixa de seleção desmarcada visto que, se isso não for feito, a eficiência da rede poderá ser afetada. Se for determinado que é preciso modificar essa configuração, entre em contato com o Suporte da Quest para obter orientações de como fazer isso.

5. Para cada definição, quando estiver satisfeito com suas alterações, clique na ✓ para salvar a alteração e sair do modo de edição, ou clique em ✕ para sair do modo de edição sem salvar.

Configurar as definições do implantação

O Rapid Recovery permite baixar instaladores do Rapid Recovery para as máquinas que você deseja proteger.

Você pode configurar definições relacionadas à implantação do software Rapid Recovery Agent do seu Core para as máquinas que deseja proteger.

Execute as etapas deste procedimento para configurar as definições de implantação.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página Definições, clique em **Implantar**.
   - Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Implantar.
3. Clique na definição que você deseja alterar.

   A definição selecionada se torna editável.
4. Insira as informações de configuração conforme descrito na tabela a seguir.

Tabela 16. Informações das definições de implantação

Caixa de texto	Descrição
Nome do instalador do Agent	O nome de arquivo padrão é Agent-Web.exe. Se você quiser alterar esse nome de arquivo por qualquer motivo, você pode usar essa definição para especificar um novo nome para o arquivo executável do Core Web Installer. Esse arquivo gera um fluxo de download da versão mais recente do Rapid Recovery Core Installer, que é executada diretamente da Web e permite pausar e retomar o processo conforme necessário.
Endereço do Core	Digite o endereço de servidor do Core. Isso normalmente consiste no protocolo, no nome do seu servidor do Core e porta, e no diretório onde os arquivos do Core residem. Por exemplo, se seu servidor for Sample, essa configuração será https://sample:8006/apprecovery/admin/Core
Tempo limite para falha de recebimento	Especifica por quanto tempo a implantação do software Agent deve ser tentada antes de atingir o tempo limite. A definição padrão é 00:25:00 ou vinte e cinco minutos. Se você quiser alterar essa definição, digite o intervalo de tempo em que você quer que o sistema tente implantar o software do agente antes que um tempo limite ocorra durante eventos de leitura ou gravação. Usa o formato HH:MM:SS.
Máximo de instalações paralelas	Essa configuração controla o número máximo de implantações do software Agent para o Core tentar de uma vez. A definição padrão é 100.

5. Para cada definição, quando estiver satisfeito com suas alterações, clique na para salvar a alteração e sair do modo de edição, ou clique em para sair do modo de edição sem salvar.

Configurar definições de conexão de banco de dados

O Rapid Recovery exibe informações sobre tarefas, eventos e alertas do Core na página Eventos. O Rapid Recovery armazena essas informações transacionais em um banco de dados de serviço MongoDB que, por padrão, é instalado localmente na máquina do Core. Você pode configurar essas definições para alterar o tempo de retenção de informações no banco de dados ou o tamanho do pool de conexões para permitir mais ou menos conexões simultâneas.

Se estiver usando um segundo Rapid Recovery Core, você pode configurar as definições de conexão de banco de dados no primeiro Core para apontar para a segunda máquina do Core. Dessa maneira, os dados de eventos dos dois Cores serão armazenados no MongoDB do segundo Core.

Você também pode configurar as definições de conexão de banco de dados do Core para apontar para outra máquina que possua um MongoDB instalado separadamente e esteja acessível ao Rapid Recovery Core pela rede. Nesse caso, os dados de transação de evento do seu Core são salvos nesse banco de dados de serviço e não localmente. Para obter mais informações sobre a configuração ou modificação de definições de conexão do banco de dados de serviço, consulte Configurar definições de conexão de banco de dados.

NOTE: Para obter mais informações sobre como visualizar informações de eventos do Rapid Recovery Core, consulte Como exibir eventos usando tarefas, alertas e páginas de diário.

Os clientes podem optar por especificar a instalação do banco de dados de serviço MongoDB em outra máquina que seja acessível ao Rapid Recovery Core na rede. Se o banco de dados de serviço do Rapid Recovery Core estiver instalado em uma máquina diferente daquela que hospeda o Rapid Recovery Core, você deverá fornecer credenciais de banco de dados (nome de usuário e senha) nessas definições.

Conclua as etapas deste procedimento para modificar as definições de conexão do banco de dados de serviço usado pelo Rapid Recovery Core.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página Definições, clique em **Conexão do banco de dados**.
   - Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Conexão do banco de dados.
3. Na parte superior da área de definições de Conexão do banco de dados, você pode fazer o seguinte:
   - Clique em **Testar conexão** para confirmar as definições.

     É recomendável testar a conexão se você alterar qualquer uma das definições da conexão do banco de dados.
   - Clique em **Restaurar padrão** para restaurar todas as definições padrão de conexão do banco de dados.

     Você será solicitado a confirmar esta ação, o que resulta em abandonar qualquer definição personalizada de conexão do banco de dados.
4. Clique na definição que você deseja alterar.

   A definição selecionada se torna editável.
5. Insira as informações de configuração conforme descrito na tabela a seguir.

Tabela 17. Informações das definições de conexão do banco de dados

Descrições das configurações de conexão disponíveis na página Configurações do Rapid Recovery Core.

Caixa de texto	Descrição
Nome do host	Insira um nome de host para a conexão de banco de dados. **NOTE:** Quando localhost é o parâmetro especificado como host, o MongoDB é instalado localmente na máquina que hospeda o Core.
Porta	Insira o número da porta para a conexão do banco de dados. **NOTE:** A definição padrão é 27017.
Nome de usuário	Insira o nome de um usuário com privilégios administrativos para o banco de dados de serviço MongoDB.

Caixa de texto	Descrição
	NOTE: Se o parâmetro do nome do host é localhost, esse campo não é necessário.
Senha	Insira a senha associada ao nome de usuário que você especificou. **NOTE:** Se o parâmetro do nome do host é localhost, esse campo não é necessário.
Período de retenção (dia)	Insira o número de dias de retenção do histórico de eventos e trabalhos no banco de dados de serviço.
Tamanho máximo do pool de conexão	Define o número máximo de conexões de banco de dados em cache para permitir a reutilização dinâmica. **NOTE:** A definição padrão é 100.
Tamanho mínimo do pool de conexão	Define o número mínimo de conexões de banco de dados em cache para permitir a reutilização dinâmica. **NOTE:** A definição padrão é 0.

6. Para cada definição, quando estiver satisfeito com suas alterações, clique na ✓ para salvar a alteração e sair do modo de edição, ou clique em ✕ para sair do modo de edição sem salvar.

Modificar definições de conexão do database local

Você pode ver eventos do sistema relacionados ao Rapid Recovery Core na página Eventos. O Rapid Recovery Core armazena essas informações transacionais em um banco de dados de serviço MongoDB. Por padrão, esse banco de dados é instalado localmente na máquina do Core e o nome do host nas definições de conexão do banco de dados é padronizado como localhost. Nessa situação, a interface loopback ignora o hardware de interface de rede local e as credenciais do banco de dados não são necessárias.

Opcionalmente, para aumentar a segurança, você pode especificar as credenciais do banco de dados explicitamente (um nome de usuário e senha) para o banco de dados MongoDB usado pelo Rapid Recovery Core.

NOTE: Para obter mais informações sobre como visualizar informações de eventos do Rapid Recovery Core, consulte Como exibir eventos usando tarefas, alertas e páginas de diário. Para obter informações sobre as definições de conexão do banco de dados, consulte Configurar definições de conexão de banco de dados.

Execute as etapas deste procedimento para modificar as definições de conexão do banco de dados local para especificar as credenciais do banco de dados.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página Definições, clique em **Definições do banco de dados local**.
   - Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Definições do banco de dados local.
3. Clique na definição que você deseja alterar.

   A definição selecionada se torna editável.
4. Digite as credenciais adequadas para se conectar ao banco de dados do serviço, conforme descrito na tabela a seguir.

Tabela 18. Informações das definições do banco de dados local

Caixa de texto	Descrição
Nome de usuário	Insira o nome de um usuário com privilégios administrativos para o banco de dados de serviço MongoDB.
Senha	Insira a senha associada ao nome de usuário que você especificou.

5. Para cada definição, quando estiver satisfeito com suas alterações, clique na para salvar a alteração e sair do modo de edição, ou clique em para sair do modo de edição sem salvar.

Gerenciar definições do servidor de SMTP

Se você configurar as definições do servidor de SMTP (simple mail transfer protocol) no Core, poderá enviar notificações de tarefas, eventos e alertas por e-mail.

As informações sobre a configuração de um servidor de e-mails SMTP são descritas no tópico Configurar um servidor de e-mail.

NOTE: Para enviar informações sobre eventos por e-mail, você também deve configurar as definições de grupo de notificação. Para obter mais informações sobre especificação de eventos para recepção de alertas de e-mail, consulte Configurar grupos de notificação.

Configurar as definições de conexão da conta de nuvem

As definições de conexão da conta de nuvem permitem determinar o tempo que deve ser decorrido entre as tentativas do Rapid Recovery de se conectar à sua conta de nuvem antes que o tempo de operação expire. Execute as etapas do procedimento a seguir para configurar as definições da conexão para sua conta em nuvem.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em **Configurações**.

A pagina Definições é exibida.

3. No menu à esquerda, clique em **Contas de nuvem**.
4. Na tabela Contas de nuvem, clique no menu suspenso ⋯ ao lado da conta de nuvem que você deseja configurar e siga uma destas ações:
   - Para retornar qualquer configuração de nuvem personalizada para o seguinte padrão, clique em **Redefinir**.
     - **Solicitar tempo limite** 01:30 (minutos e segundos)
     - **Tamanho do buffer de gravação** 8388608 (bytes)
     - **Tamanho do buffer de leitura** 8388608 (bytes)
   - Para alterar as configurações de conexão da conta de nuvem, clique em **Editar**, e na caixa de diálogo **Configuração da nuvem**, execute uma das seguintes ações:
     - Para **Solicitar tempo limite**, utilize as setas para cima e para baixo para determinar o período, em minutos e segundos, a ser utilizado pelo Rapid Recovery sobre uma tentativa única de se conectar à conta de nuvem quando houver um atraso. As tentativas de conexão irão parar depois da quantidade de tempo inserida.
     - Para **Tamanho do buffer de gravação**, insira o tamanho do buffer que deseja reservar para gravar dados arquivados na nuvem.
     - Para **Tamanho do buffer de leitura**, insira o tamanho do bloco que deseja reservar para ler dados arquivados da nuvem.

Trabalhar com certificados de gerenciamento do Azure associados ao seu Core

Nas configurações do Rapid Recovery Core, você pode associar certificados de gerenciamento do Azure ao Core. Esse processo permite que o Core acesse informações sobre suas assinaturas do Azure, disponibilizando essas informações no Core Console.

Por exemplo, quando você executa uma exportação virtual para o Azure, depois de carregar as informações do certificado, você pode selecionar a assinatura do Azure apropriada em uma caixa suspensa. Os objetos associados a essa assinatura também se tornarão acessíveis a outros controles na interface do usuário do Core Console, como contas de armazenamento, contêineres e assim por diante.

As informações do certificado de gerenciamento do Azure são armazenadas em um arquivo de configurações de publicação gerado no Microsoft Azure. Você pode adicionar um ou mais certificados de gerenciamento ao Core. O Core armazena as credenciais em cache com segurança.

Trabalhar com certificados de gerenciamento do Azure nas configurações do Core inclui as seguintes tarefas:

- Obter o arquivo de configurações de publicação para sua conta do Azure
- Carregar um certificado de gerenciamento do Azure
- Atualizar ou excluir certificados de gerenciamento do Azure

Obter o arquivo de configurações de publicação para sua conta do Azure

Para executar esta tarefa, você deve usar uma máquina Windows com o PowerShell ativado. Você também deve ter acesso a uma conta do Azure com a função de administrador de serviços ou coadministrador de serviços.

O arquivo de configurações de publicação é um documento XML gerado no Azure. O arquivo contém a definição da API AzureServiceManagement e informações sobre a assinatura do Azure, incluindo credenciais codificadas

seguras, o tipo de assinatura e um certificado de gerenciamento do Azure. Esse arquivo contém a extensão `.publishsettings`, da qual a descrição é derivada. Sem o arquivo de configurações de publicação, não é possível conectar o Core a uma conta do Azure.

Você pode obter uma cópia do arquivo de configurações de publicação de uma máquina Windows conectada em sua conta do Azure.

CAUTION: Como o arquivo de configurações de publicação contém suas credenciais e informações sobre sua conta do Azure, a Microsoft recomenda armazená-lo em um local seguro. Uma vez carregado o certificado, você pode excluir o arquivo do seu sistema local.

A Microsoft impõe um limite de 100 certificados de gerenciamento por assinatura, com um limite adicional máximo de 100 certificados de gerenciamento para todas as assinaturas sob a ID de usuário de um administrador de serviços específico. Se precisar acessar a mesma conta do Azure de vários Cores, você pode gerar o arquivo de configurações de publicação uma vez e reutilizar o mesmo arquivo para carregar o certificado de gerenciamento em vários Cores. Dessa forma, você pode evitar exceder o limite de geração de certificados.

NOTE: Para obter mais informações sobre esse limite, consulte a seção “Limitações” do artigo da Base de Dados de Conhecimento da Microsoft “Visão geral sobre certificados para os Serviços de Nuvem do Azure” em https://docs.microsoft.com/pt-br/azure/cloud-services/cloud-services-certs-create.

Conclua as etapas deste procedimento para obter o arquivo de configurações de publicação.

1. Em uma máquina Windows, faça login no painel do Azure.
2. Enquanto estiver conectado no Azure, abra outra janela do navegador.
3. Execute um script do PowerShell para baixar o arquivo digitando o seguinte endereço no URL do navegador: `https://manage.windowsazure.com/publishsettings/index?client=powershell`.

   Quando bem-sucedido, o arquivo de configurações de publicação será salvo no diretório de download padrão.
4. Mova este arquivo para uma máquina acessível ao Core Console.

Para associar as informações de assinatura do Azure ao seu Rapid Recovery Core, consulte o tópico do *Guia do usuário do Rapid Recovery* “Carregar um certificado de gerenciamento do Azure”.

Carregar um certificado de gerenciamento do Azure

Para executar esta tarefa, é necessário ter um arquivo de configurações de publicação na conta do Azure apropriada. Para obter informações sobre como acessar esse arquivo, consulte Obter o arquivo de configurações de publicação para sua conta do Azure.

Ao carregar um certificado de gerenciamento do Azure no Core, você dá ao Core Console acesso a informações de assinatura da sua conta do Azure. Você pode ver objetos associados à sua assinatura do Azure no Core Console.

Conclua as etapas deste procedimento para carregar um certificado de gerenciamento do Azure no Core.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página Definições, clique em **Certificados de gerenciamento do Azure**.
   - Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Certificados de gerenciamento do Azure.
3. Abaixo do cabeçalho Certificados de gerenciamento do Azure, clique em **+Carregar certificado**.

   A caixa de diálogo **Carregar certificado** será exibida.
4. Na caixa de diálogo **Carregar certificado**, clique em **Procurar**.

A janela **Carregar arquivo** será exibida.

5. Navegue até o local onde o arquivo de configurações de publicação está localizado, selecione o arquivo e clique em **Abrir**.

   A janela **Carregar arquivo** se fechará e o certificado de gerenciamento será carregado no Core Console.

Atualizar ou excluir certificados de gerenciamento do Azure

Para excluir um certificado de gerenciamento do Azure do Core Console, um certificado deve ser carregado no e associado ao Core. Para obter mais informações sobre como associar certificados ao Core, consulte Carregar um certificado de gerenciamento do Azure.

Conclua as etapas deste procedimento para atualizar a exibição dos certificados de gerenciamento do Azure ao Core ou para excluir um certificado do Core.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página Definições, clique em **Certificados de gerenciamento do Azure**.
   - Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Certificados de gerenciamento do Azure.
3. Para atualizar a exibição dos certificados disponíveis no Core Console, abaixo do cabeçalho Certificados de gerenciamento do Azure, clique em **Atualizar**.

   A página **Definições do Core** será atualizada, mostrando informações atualizadas sobre os certificados associados ao Core.
4. Para excluir um certificado do Core, para o certificado adequado, clique em e selecione **Excluir**.
5. Na caixa de diálogo de confirmação, clique para confirmar a exclusão do certificado.

   A caixa de diálogo será fechada, e o certificado de gerenciamento do Azure selecionado será excluído do Core.

Gerenciamento de definições de relatórios

Você pode gerar relatórios para o Rapid Recovery Core ou para máquinas protegidas. Para obter informações sobre os relatórios que você pode gerar, consulte Relatório.

Execute as etapas deste procedimento para gerenciar as definições de relatórios do Core.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página Definições, clique em **Relatórios**.
   - Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Relatórios.

     As definições de **Relatórios** do Core são mostradas. As Definições de relatórios são descritas na tabela a seguir.

Opção	Descrição
Restaurar padrão	Esta opção restaura todas as definições de relatório com as definições padrão. Os padrões de cada definição são listados abaixo.

Opção	Descrição
Fonte	Esta opção controla a fonte padrão usada nos relatórios. A fonte tipográfica padrão é Trebuchet MS. Você pode alterar essa definição para qualquer fonte tipográfica disponível em seu sistema.
Tamanho do papel	Esta opção controla o tamanho de papel padrão para a impressão de relatórios. O padrão é carta. Você pode selecionar dentre os seguintes tamanhos de papel: • A3 • A4 • B4 • Executivo • Ledger • Ofício • Carta • Tabloide
Orientação da página	Esta opção controla a orientação da página para relatórios exportados. A orientação padrão é Paisagem. Você pode selecionar dentre as seguintes opções de layout: • Paisagem • Retrato

3. Para alterar qualquer uma das definições para os Relatórios, clique no campo da definição apropriada.

   O campo da definição é mostrado como um menu suspenso configurável.
4. Clique no menu suspenso e selecione um dos valores disponíveis.

   Por exemplo, no campo Fonte, clique em **Times New Roman**.
5. Para cada definição, quando estiver satisfeito com suas alterações, clique na ✓ para salvar a alteração e sair do modo de edição, ou clique em ✕ para sair do modo de edição sem salvar.

   A opção selecionada agora aparece como a nova definição do parâmetro selecionado dos Relatórios.

Gerenciar definições da capacidade de anexação do SQL

As verificações de capacidade de anexação do SQL ocorrem como parte dos trabalhos noturnos do Rapid Recovery. Para reduzir os custos de licenciamento, o Rapid Recovery oferece duas opções para executar verificações de capacidade de anexação: usando uma instância licenciada do SQL Server instalada na máquina do Rapid Recovery Core ou usando a instância do SQL Server já instalada na sua máquina protegida. Esta segunda opção agora é a definição padrão. No entanto, se sua máquina protegida já estiver ativa quando os trabalhos noturnos ocorrerem, considere realizar das verificações com uma instância do SQL Server no Core.

A capacidade de executar verificações de capacidade de anexação utilizando a instância do SQL Server em uma máquina protegida é uma função do software Rapid Recovery Agent. Esse recurso não funcionará se

o SQL Server estiver protegido sem agente. Portanto, se estiver usando proteção sem agente na máquina SQL, configure essa definição do Core para **Usar o SQL Server no core**, como mostrado na Etapa 3 deste procedimento.

No resumo, o processo de gerenciamento das configurações de capacidade de anexação do SQL do Core envolve as seguintes tarefas:

- Montar o último ponto de recuperação de grupos de proteção que contêm bancos de dados.
- Conectar ao banco de dados a partir do SQL Server.
- Abrir o banco de dados.
- Fechar o banco de dados.
- Desmontar o ponto de recuperação.

  Para ativar essa verificação noturna, especifique uma instância do SQL Server a ser usada para realizar verificações de capacidade de anexação de bancos de dados SQL Server em máquinas protegidas.

  NOTE: Esta opção aparece apenas quando há um SQL Server sendo protegido no Core.

Para configurar o Core para executar as verificações de capacidade de anexação do SQL como parte dos trabalhos noturnos, siga as seguintes etapas.

NOTE: Se você selecionar a opção padrão para usar a instância do SQL Server instalada na máquina protegida, essa instância do SQL Server gerenciará a capacidade de anexação de SQL em todas as máquinas SQL protegidas. Se você não quiser que essa configuração se aplique a todas as máquinas SQL protegidas, selecione Usar o SQL Server no core. Para realizar verificações de capacidade de anexação no Core, você precisa instalar ou usar uma versão licenciada do SQL Server na máquina do Core.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página Definições, clique em **Capacidade de anexação**.
   - Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Capacidade de anexação.
3. Para usar a instância do SQL Server instalada na máquina SQL Server protegida, selecione **Usar o SQL Server na máquina protegida**. Essa é a opção padrão.
4. Para usar a instância do SQL Server instalada no Rapid Recovery Core, selecione **Usar o SQL Server no core** e insira as informações de autenticação, conforme descrito na tabela a seguir.

Tabela 19. Informações de credenciais do SQL Server

Descrições das informações necessárias para autenticar uma conexão com o SQL Server.

Caixa de texto	Descrição
SQL Server	No menu suspenso do SQL Server, selecione a instância adequada do SQL Server no servidor do Core.
Tipo de credencial	Selecione o método de autenticação adequado para suas credenciais entre as opções a seguir: • Windows • SQL
Nome de usuário	Especifique um nome de usuário para acessar o SQL Server no Core com base no tipo de credencial selecionado.

Caixa de texto	Descrição
Senha	Especifique uma senha para acessar o SQL Server no Core com base no tipo de credencial selecionado.

5. Clique em **Testar conexão**.

   NOTE: Se as credenciais forem inseridas de forma incorreta, será exibida uma mensagem para alertá-lo de que as credenciais falharam. Corrija as informações de credenciais e teste novamente a conexão.

6. Quando estiver satisfeito com as alterações, clique em **Aplicar**.

Noções básicas sobre trabalhos do Core

Trabalhos do Core são processos que o Rapid Recovery Core executa para dar suporte às suas operações, incluindo backup para pontos de recuperação, replicação de dados, arquivamento de dados, exportação de dados para VMs, manutenção de repositórios, etc. Os trabalhos do Core são iniciados automaticamente para algumas operações, como replicação ou arquivamento, de acordo com a programação estabelecida. Você também pode chamar alguns trabalhos sob demanda de vários elementos do Core Console.

- Quando visualizar ou editar as definições de trabalhos do Core, cada trabalho do Core terá dois parâmetros: Máximo de trabalhos simultâneos e Contagem de tentativas.
  - O parâmetro Máximo de trabalhos simultâneos determina quantos trabalhos desse tipo podem ser executados ao mesmo tempo.
  - O parâmetro Contagem de tentativas determina quantas vezes o trabalho deve ser tentado antes de ser abandonado, caso erros de rede ou outros erros evitem a conclusão na primeira vez.
- Na tabela Trabalhos do Core, a coluna Definições indica se o trabalho listado está incluído nas definições de trabalho do Core por padrão ou precisa ser explicitamente adicionado.

A tabela a seguir descreve os principais trabalhos do Core disponíveis e suas funções.

Tabela 20. Trabalhos do Core

Nome do trabalho	Descrição	Máximo de trabalhos simultâneos	Contagem de tentativas	Definições
Verificar a capacidade de anexação de bancos de dados SQL em snapshots	Permite que o Core verifique a consistência dos bancos de dados SQL e garante que todos os arquivos de apoio MDF (dados) e LDF (log) estejam disponíveis no snapshot de backup. Processo: • Montar o último ponto de recuperação de grupos de proteção que contêm bancos de dados SQL. • Montar o banco de dados. Se você estiver realizando a capacidade de anexação do servidor SQL	1	0	Padrão

Nome do trabalho	Descrição	Máximo de trabalhos simultâneos	Contagem de tentativas	Definições
	protegido, monte usando o caminho de UNC. • Conectar ao banco de dados a partir do SQL Server. • Realizar a verificação de capacidade de anexação. • Realizar operações limpeza. • Fechar o banco de dados. • Desmontar o banco de dados. • Desmontar o ponto de recuperação.			
Verificar a soma de verificação dos bancos de dados do Exchange	Verifica a integridade de pontos de recuperação que contêm bancos de dados do Exchange. Processo: • Montar o último ponto de recuperação de grupos de proteção que contêm bancos de dados SQL. • Conectar ao banco de dados a partir do SQL Server. • Abrir o banco de dados. • Fechar o banco de dados. • Desmontar o ponto de recuperação.	1	0	Padrão
Verificar a montabilidade de bancos de dados do Exchange	Verifica se os bancos de dados do Exchange são montáveis.	1	0	Padrão
Replicar dados de máquinas protegidas a partir da origem remota	Transfere uma cópia dos pontos de recuperação para uma máquina protegida de um Core de origem para um Core de destino. Este trabalho é executado no Core de destino que recebe os pontos de recuperação replicados de entrada.	3	0	Padrão
Replicar dados de máquinas protegidas no destino remoto	Transfere uma cópia dos pontos de recuperação para uma máquina protegida de um Core de origem (no qual foram salvos originalmente) para um Core de destino. Este trabalho é executado no Core de origem e controla a replicação de saída.	1	3	Padrão

Nome do trabalho	Descrição	Máximo de trabalhos simultâneos	Contagem de tentativas	Definições
Realizar rollup dos pontos de recuperação	Aplica a política de retenção aos seus dados de backup com a combinação de pontos de recuperação "em execução" na programação definida pela política de retenção.	1	0	Padrão
Verificar pontos de recuperação	Verifica a integridade dos pontos de recuperação.	1	0	Adicionar
Excluir todos os pontos de recuperação	Exclui todo o conjunto de pontos de recuperação em uma máquina protegida.	1	0	Adicionar
Excluir cadeia de pontos de recuperação	Exclui toda uma cadeia de pontos de recuperação em uma máquina protegida.	1	0	Adicionar
Excluir intervalo de pontos de recuperação	Exclui um conjunto de pontos de recuperação em uma máquina protegida, por identificação do ponto de recuperação ou período.	1	0	Adicionar
Implementar software do agente em máquinas	Implanta o software do agente Rapid Recovery na máquina ou nas máquinas especificadas.	1	0	Adicionar
Baixar bibliotecas do Exchange	Baixa as bibliotecas do Microsoft Exchange da máquina protegida para a máquina do Core no caminho `C:\ProgramData\AppRecovery\ExchangeLibraries`.	1	0	Adicionar
Exportar para arquivo	Cria um backup no caminho especificado com um arquivamento dos pontos de recuperação selecionados. Processo: • Montar pontos de recuperação. • Gravar dados nos backups. • Desmontar o ponto de recuperação.	1	0	Adicionar
Exportar para máquina virtual	Exporta dados do ponto de recuperação especificado da máquina protegida para o caminho de destino como uma máquina virtual. Processo: • Montar ponto de recuperação. • Criar máquina virtual a partir dos dados do ponto de recuperação no caminho de destino. • Desmontar o ponto de recuperação.	1	0	Adicionar

Nome do trabalho	Descrição	Máximo de trabalhos simultâneos	Contagem de tentativas	Definições
Importar arquivos	Importa o ponto de recuperação a partir do backup especificado em um arquivamento do Core criado anteriormente.	1	0	Adicionar
Manter repositório	Realiza uma verificação do repositório. Processo: • Verificar o sistema de arquivos do repositório. • Montar ponto de recuperação. • Recalcular cache de deduplicação do repositório. • Carregar pontos de recuperação do repositório.	1	0	Adicionar
Montar snapshots de pontos de recuperação	Realiza a montagem do ponto de recuperação para o caminho especificado.	1	0	Adicionar
Proteger máquinas virtuais ESX®	Adiciona todas as máquinas virtuais especificadas a uma proteção sem agentes. O trabalho é realizado imediatamente depois de adicionar a proteção sem agentes de uma ou mais VMs ao Core usando o Assistente de proteção de diversas máquinas. O trabalho define um número de identificação para cada VM especificada, grava informações sobre o Core em um arquivo de configuração e recupera metadados a partir do arquivo.	1	0	Adicionar
Restaurar do ponto de recuperação	Realiza uma restauração a partir de um ponto de recuperação para uma máquina de destino especificada. Processo: • Montar ponto de recuperação. • Gravar todos os dados do ponto de recuperação na máquina especificada. • Desmontar o ponto de recuperação.	1	0	Adicionar
Carregar logs	Carrega logs no servidor especificado.	1	0	Adicionar

Alguns trabalhos do Core estão incluídos em Definições. As Definições de trabalhos permitem que você especifique quantos trabalhos simultâneos do mesmo tipo o Core pode realizar e quantas novas tentativas devem ser realizadas se a primeira tentativa falhar.

Para obter mais informações sobre essas Definições, consulte Definições de trabalhos do Core.

Para obter informações sobre como adicionar trabalhos às Definições do Core, consulte Adição de trabalhos do Core às definições.

Para obter informações sobre como editar as definições de trabalhos na lista Definições, consulte Editar as definições de trabalhos do Core.

Definições de trabalhos do Core

Ao selecionar (Definições) na barra de ícones, você pode acessar as definições de alguns trabalhos do Core. A área **Trabalhos** da página de definições do Core permite que você determine duas definições para cada tipo de trabalho listado:

1. O número máximo de trabalhos desse tipo que o Core deve tentar por vez. O valor deve ser definido entre 1 e 50.
2. O número de vezes que um trabalho deve ser tentado se um erro de rede ou outro erro de comunicação impedir a conclusão do trabalho na primeira vez. O valor deve ser definido entre 0 e 10.

Vários trabalhos são incluídos automaticamente nas definições do Core. Esses trabalhos incluem um valor de "Padrão" na coluna Definições (conforme mostrado no tópico Noções básicas sobre trabalhos do Core).

Você pode adicionar alguns outros trabalhos às definições se quiser configurar essas definições para controlar o número máximo de trabalhos ou novas tentativas para essas funções. Esses trabalhos incluem um valor de "Adicionar" na coluna Definições. Para obter informações sobre como adicionar esses trabalhos para à tabela Definições, consulte Adição de trabalhos do Core às definições.

Não é possível definir esses dois parâmetros em trabalhos do Core indisponíveis nas Definições.

No caso de trabalhos mostrados nas definições, você pode editar as definições existentes. Isso permite que você personalize os dois parâmetros, exclua um tipo de trabalho da lista Definições de trabalho ou restaure as definições padrão. Para obter informações mais detalhadas, consulte o tópico Editar as definições de trabalhos do Core.

Adição de trabalhos do Core às definições

As definições de trabalhos do Core permitem definir, para cada tipo de trabalho, o número máximo de trabalhos que o Core deve tentar de cada vez e quantas vezes o trabalho deve ser repetido se a primeira tentativa falhar.

Cada tipo de trabalho do Core tem valores padrão para esses dois parâmetros, conforme descrito no tópico Definições de trabalhos do Core. Esta lista também indica que tipos de trabalho são incluídos por padrão nas definições do Core.

A adição de um trabalho do Core às definições permite alterar esses parâmetros para o tipo de trabalho adicionado.

Execute as etapas do procedimento a seguir para adicionar um trabalho às definições do Core.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página Definições, clique em **Trabalhos**.
   - Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Trabalhos.

     As definições de Trabalhos do Core são mostradas.
3. Na página de Definições do Core, em Trabalhos, clique em **Add** (Adicionar).

   A caixa de diálogo Definições de trabalho é exibida.
4. Na caixa de diálogo **Definições de trabalho**, no campo **Trabalhos**, selecione o nome de um trabalho que você deseja adicionar às definições do Core.

Esses trabalhos são descritos no tópico Definições de trabalhos do Core.

5. Para definir o número máximo de trabalhos que o Core pode realizar ao mesmo tempo, na caixa de texto **Máximo de trabalhos simultâneos**, insira um novo valor entre 1 e 50.
6. Para definir o número de tentativas que o Core deve fazer antes de abandonar o trabalho, na caixa de texto **Contagem de tentativas**, insira um novo valor entre 0 e 10.
7. Clique em **Salvar**.

   A caixa de diálogo Definições de trabalho é fechada e, em seguida, as novas definições de trabalho são aplicados.

Editar as definições de trabalhos do Core

As definições de trabalhos do Core permitem definir, para cada tipo de trabalho, o número máximo de trabalhos que o Core deve tentar de cada vez e quantas vezes o trabalho deve ser repetido se a primeira tentativa falhar.

Cada tipo de trabalho do Core tem valores padrão para esses dois parâmetros, conforme descrito no tópico Noções básicas sobre trabalhos do Core. Esta lista também indica que tipos de trabalho são incluídos por padrão nas definições do Core. Ao editar as definições de trabalhos do Core, você pode fazer o seguinte:

- Você pode personalizar as definições de cada tipo de trabalho do Core.
- Você pode excluir um tipo de trabalho da lista de definições do Core. Esse recurso não está disponível se o tipo de trabalho estiver incluído nas definições por padrão.

  NOTE: Excluir um trabalho das definições do Core simplesmente remove o tipo de trabalho dessa lista. Para editar as definições do Core para esse tipo de trabalho novamente no futuro, você pode adicioná-lo à lista como descrito no tópico Adição de trabalhos do Core às definições.

- Você pode restaurar as definições de qualquer tipo de trabalho para as definições padrão.

  NOTE: Embora você possa usar esse recurso apenas para os tipos de trabalho incluídos por padrão nas definições do Core, você pode definir outros tipos de trabalho nos padrões removendo da lista e adicionando novamente.

Execute as etapas no procedimento a seguir para editar as definições de um trabalho.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página **Definições**, clique em **Trabalhos**.
   - Role a tela para baixo no lado direito da página **Definições** até ver o cabeçalho Trabalhos.

     As definições de Trabalhos do Core são mostradas.
3. Na grade Trabalho, selecione um trabalho que você deseja remover da lista. No menu suspenso do trabalho, selecione **Excluir**.

   O trabalho é removido da lista.
4. Na grade Trabalho, selecione um trabalho na lista para o qual você quer redefinir as configurações. No menu suspenso do trabalho, selecione **Restaurar padrões**.

As definições desse trabalho são redefinidas com as definições padrão.

5. Na grade Trabalho, selecione o trabalho que você deseja alterar. No menu suspenso do trabalho, selecione **Editar**.
6. A caixa de diálogo Definições de trabalho: [NomedoTrabalho] é aberta.
7. Para alterar o número máximo de trabalhos que o Core pode realizar ao mesmo tempo, na caixa de texto Máximo de trabalhos simultâneos, insira um novo valor entre 1 e 50.
8. Para alterar a definição relativa ao número de tentativas adicionais que o Core deve fazer antes de abandonar o trabalho, na caixa de texto Contagem de tentativas, insira um novo valor entre 0 e 10.
9. Clique em **Salvar**.

   A caixa de diálogo Definições de trabalho é fechada e, em seguida, as novas definições de trabalho são aplicados.

Gerenciar licenças

Existem três tipos de licenças de software para o Rapid Recovery:

- **Avaliação**, que para de capturar instantâneos depois de 14 dias,
- **Assinatura**, que tem uma data de validade, e
- **Perpétua**, que não tem data de validade.

Muitos usuários do Rapid Recovery Core começam com uma licença de avaliação, que tem recursos limitados. Após os 14 dias, se a circunstância exigir, um administrador do grupo poderá estender a licença de avaliação por 28 dias. Caso contrário, você poderá comprar e registrar licenças de assinatura ou perpétuas.

NOTE: Para obter informações sobre como inserir uma chave de licença ou as informações do arquivo (por exemplo, atualizar ou alterar uma licença de teste para uma licença válida de longo prazo), consulte Atualização ou alteração de uma licença.

O Rapid Recovery fornece licenças em um arquivo. Um arquivo de licença do Rapid Recovery contém um pool de licenças que você pode distribuir às máquinas que deseja proteger. Esse pool é refletido no Portal de licenças do Rapid Recovery. Para cada tipo de licença anteriormente listado, há dois tipos de pools de licenças:

- **Empresarial.** Cada licença nesse pool pode ser aplicado a uma instalação do Rapid Recovery Agent ou um soquete em um host do hipervisor usando a proteção sem agente, independentemente do espaço usado.
- **Capacidade.** Essas licenças são aplicadas à quantidade de dados que você planeja proteger, medida em terabytes (TB), independentemente do número de Rapid Recovery Agents instalados ou soquetes que você possui. Caso você exceda a quantidade de espaço alocado à licença adquirida, deverá adquirir outra licença. Para o licenciamento de capacidade:
  - Os DL Appliances usam um modelo de licença de capacidade de back-end, no qual a capacidade especificada na licença limita o tamanho do repositório (em TB) que você pode usar na solução.
  - As instalações de software usam um modelo de licença de capacidade de front-end, no qual a capacidade especificada na licença limita a quantidade de dados (em TB) das máquinas que você deseja proteger que você pode salvar em seu repositório. A capacidade de front-end é medida antes da compactação e eliminação de duplicação.

Na versão 6.2, um Core pode usar somente um tipo de pool de licenças. Por exemplo, se o Core usa um pool de licenças baseado em capacidade, ele não poderá também usar um pool de licenças Enterprise. O inverso também é verdadeiro.

Os tipos de pools de licenças não podem ser combinados em um único arquivo de licença. Por exemplo, você não pode incluir um pool de licenças Empresariais e um pool de licenças de Capacidade sob as mesma licença perpétua.

Arquivos de licença são arquivos de texto que terminam com a extensão de arquivo `.lic` . A seguir, são apresentados exemplos de arquivos de licença:

- Os arquivos de licença podem aparecer com comprimento de 9 caracteres, que consistem de três grupos de números separados por um hífen, por exemplo: `123-456-789.lic`.
- Licenças baseadas em software podem aparecer no formato Software-<nome do grupo>.lic, com o nome do grupo após o nome do cliente ou conta, por exemplo: `Software-YourCompany.lic`.
- Licenças de soluções da série DL podem aparecer no formato <Série do dispositivo>-<nome do grupo>.lic, com o nome do grupo após a conta do nome do cliente, por exemplo: `DL4X00 Series-YourCompany.lic`.

O Rapid Recovery suporta estes tipos de licenças em dois modos: o modo padrão de telefone residencial e o modo de telefone não residencial, que tem diversas limitações. As licenças de assinatura são executadas apenas no modo de telefone residencial. A licença perpétua e a licença de avaliação pode usar licenças de telefone residencial ou de telefone não residencial. Para ver como esse modo afeta a utilização dos dados pessoais no Rapid Recovery, consulte o tópico "Gerenciar privacidade". Para ver informações sobre restrições nas licenças de telefone não residenciais, ou informações sobre como obter uma licença usando esse modo, consulte "Como obter e usar licenças de telefone não residenciais". Estes tópicos estão no *Guia do usuário do Rapid Recovery*.

O Rapid Recovery gerenciar licenças ou entrar em contato com o servidor de licenças diretamente a partir do Core Console selecionando (Definições) na barra de ícones e clicando em **Licenciamento**.

As definições de Aplicação de licença incluem as seguintes informações:

Detalhes da licença:

- **Alterar licença**. Permite a você alterar uma licença existente associada ao Core carregando um arquivo de licença ou inserindo uma chave de licença.
- **Adicionar licença**. Esta opção está disponível somente para soluções de backup da série DL e permite que você carregue um arquivo de licença ou insira uma chave de licença.
- **Grupo do portal de licenças**. Esta opção abre o portal de licenças para gerenciamento do grupo.
- **Tipo de licença**. Os tipos de licenças incluem Avaliação, Assinatura ou Empresarial. Para obter mais informações, consulte o tópico Noções básicas dos tipos de licenças de software no *Guia do usuário do portal de licenças do Rapid Recovery*.
- **Status da licença**. Indica o status da licença. Um status ativo garante que os instantâneos possam continuar conforme programado. Se a licença estiver bloqueada ou vencida, ou se o Core não conseguir se comunicar com o Portal de licenças do Rapid Recovery após o período de carência, os instantâneos serão pausados até que o status da licença seja corrigido.
- **A chave da licença expira em**. Esta opção está disponível somente quando se usa uma licença de assinatura e mostra o tempo que falta para a assinatura expirar, em dias.

Limitações de licença:

- **Número máximo de snapshots por dia**. Indica o número de backups limitados pela licença específica.

Conjunto de licenças:

- **Tamanho do conjunto**. O pool de licenças é o número de licenças de não avaliação disponíveis para alocação entre grupos e subgrupos no Portal de licenças do Rapid Recovery. O tamanho do pool determina quantas licenças podem ser alocadas. Para obter mais informações, consulte o tópico Noções básicas dos pools de licenças no *Guia do usuário do portal de licenças do Rapid Recovery*.
- **Usadas por este Core**. Indica o número de máquinas do pool de licenças protegidas por esse Core.
- **Total usado no grupo**. Indica o número total de máquinas protegidas no mesmo grupo de licenças desse Core.
- **Tecla home de telefone desabilitada**. Se estiver visível, esse status indica que o Core não se comunica com o Portal de licenças do Rapid Recovery ou com o Portal de proteção de dados. A atualização

automática está desativada, e nenhuma informação pessoal é comunicada entre o Core e a Quest Software Inc. ou qualquer outra entidade, em conformidade com as políticas de GDPR.

Servidor de licenças. Essas configurações se aplicam a licenças padrão (telefônicas). Essas configurações não são aplicáveis às soluções e outras licenças não telefônicas:

- **Endereço do servidor de licenças**. Exibe um URL ativo do servidor de licenças associado a esse Core.
- **Última resposta do servidor de licenças**. Indica se a última tentativa de comunicação com o portal do servidor de licenças foi bem-sucedida.
- **Último contato com o servidor de aplicação de licença**. Exibe a data e a hora do último contato bem-sucedido com o servidor de licenciamento.
- **Próxima tentativa de entrar em contato com o servidor de licenciamento**. Indica a próxima data e hora agendada para tentar a comunicação com o servidor de licenciamento.
- **Entrar em contato agora**. Este botão entra em contato com o servidor de licenças sob demanda. Use esta opção após fazer alterações em sua configuração de licenças para registrá-las imediatamente em vez de aguardar a próxima tentativa programada.

Para obter mais informações sobre licenças, consulte o *Guia do usuário do portal de licenças do Rapid Recovery*.

Para obter mais informações sobre como atualizar ou alterar uma chave ou arquivo de licença, consulte Atualização ou alteração de uma licença.

Os usuários de soluções de backup da série DL também podem adicionar licenças ao Core, se necessário. Para obter mais informações, consulte Adição de uma licença.

Para obter mais informações sobre como entrar em contato com o servidor do portal de licenças, consulte Contatar o servidor do Portal de licenças do Rapid Recovery.

Você também pode ver informações de licenciamento de uma única máquina protegida. Para obter mais informações, consulte Visualizar informações de licença em uma máquina.

Atualização ou alteração de uma licença

Depois de ou comprar uma licença de longo prazo do Rapid Recovery, você receberá por e-mail um arquivo de licença ou uma chave de licença.

Execute as etapas descritas neste procedimento para atualizar sua licença de teste ou alterar sua licença existente e associá-la ao Rapid Recovery Core Console.

NOTE: Os usuários de soluções de backup da série DL também podem adicionar licenças ao Core, se necessário. Para obter mais informações, consulte Adição de uma licença.

NOTE: Para obter informações sobre como adquirir uma chave de licença ou obter mais detalhes sobre como usar o portal de licenças para fazer baixar software, registrar soluções, gerenciar assinaturas e grupos de licença e gerar relatórios do portal de licenças, consulte o *Guia do usuário do portal de licenças do Rapid Recovery*.

Se você tiver acabado de instalar um novo Core e estiver vendo uma mensagem no Core Console solicitando que você escolha um arquivo ou uma chave de licença, vá para a Etapa 5.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Configurações).
3. Role a tela para baixo no lado direito da página **Definições** até ver o cabeçalho **Servidor de licenças**.

   As definições de aplicação de licença do Core são exibidas.
4. Para atualizar ou alterar a licença existente associada ao Core, na parte superior da área de definições de detalhes da licença do Core, clique em **Alterar licença**.

   A caixa de diálogo **Change License** (Alterar licença) será mostrada.
5. Se quiser inserir manualmente a chave de licença, vá para a etapa 6. Se desejar carregar um arquivo de licença, faça o seguinte:

a. Para carregar um arquivo de licença, no campo **Escolha um arquivo de licença ou insira a chave de licença**, clique em **Selecionar arquivo**.

Na caixa de diálogo **Carregamento de arquivo**, navegue pelo sistema de arquivos e localize o novo arquivo de licença que você quer usar. Por exemplo, localize `Software-YourCompany.lic`.

b. Clique no arquivo de licença e em **Abrir**.

A caixa de diálogo **Carregamento de arquivo** é fechada. O arquivo de licença selecionado aparecerá no campo de texto da licença.

c. Na caixa de diálogo **Alterar licença**, clique em **Continuar**.

O arquivo de licença que você selecionou será autenticado e essa licença será associada ao Core.

d. Pule para a etapa 7.

6. Para inserir manualmente a chave de licença, no campo de texto **Escolha o arquivo de licença ou insira a chave de licença**, insira a chave de licença e clique em **Continuar**.

   A caixa de diálogo será fechada, o arquivo de licença que você selecionou será autenticado e essa licença será associada ao Core.

7. Se você vir a página de boas-vindas do **Guia de início rápido**, você poderá iniciar o guia ou fechar essa ferramenta. Esta é a última etapa necessária para este procedimento.

   NOTE: Para obter mais informações sobre o Guia de Início Rápido, consulte "Noções básicas sobre o Guia de Início Rápido" no *Guia do usuário do Rapid Recovery*.

8. Se estiver executando estas etapas na página de **Definições** do Core, role a tela para baixo no lado direito da página de **Definições** até poder ver o cabeçalho do Servidor de licenças.
9. Na área Servidor de licenças, clique em **Entrar em contato agora**.

   Assim que a licença é aplicada ao servidor de licenças, todas as máquinas protegidas associadas são atualizadas automaticamente com a nova licença.

Se aparecerem mensagens de erro na parte superior do Rapid Recovery Core Console (como os serviços específicos não foram iniciados), siga as orientações na mensagem de erro para resolver esses erros.

Adição de uma licença

Os proprietários de soluções de backup da série DL podem adicionar uma ou mais licenças ao Rapid Recovery Core Console.

Assim que você tiver atualizado ou adquirido sua licença do Rapid Recovery, você receberá um arquivo de licença ou uma chave de licença por e-mail.

Você também pode atualizar ou alterar uma licença existente no Core Console. Para obter mais informações, consulte Atualização ou alteração de uma licença.

NOTE: Somente usuários de soluções de backup da série DL podem ver o botão **Adicionar solução**.

NOTE: Para obter informações sobre como obter uma chave de licença, consulte o *Guia do usuário do portal de licenças do Rapid Recovery*.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Configurações).
3. Role a tela para baixo no lado direito da página **Definições** até ver o cabeçalho Aplicação de licença.

   As definições de aplicação de licença do Core são exibidas.

4. Para adicionar uma licença e associá-la ao Core, na parte superior da área de definições Detalhes da licença do Core, clique em **Adicionar licença**. Na caixa de diálogo resultante, realize um dos procedimentos a seguir:

   a. Se você quiser inserir manualmente a chave de licença, digite a chave com cuidado e clique em **Continuar**.

A caixa de diálogo é fechada, o arquivo de licença que você selecionou é autenticado e essa licença é associada ao Core.

b. Se deseja carregar um arquivo de licença, clique em **Escolher arquivo**.

Na caixa de diálogo **Carregamento de arquivo** , navegue pelo sistema de arquivos e localize o novo arquivo de licença que você quer usar. Por exemplo, localize `Software-YourCompany.lic`.

c. Clique no arquivo de licença e em **Abrir**.

A caixa de diálogo Carregamento de arquivo é fechada. O arquivo de licença selecionado aparece na caixa de diálogo atual.

d. Na caixa de diálogo, clique em **Continuar**.

A caixa de diálogo é fechada, o arquivo de licença que você selecionou é autenticado e essa licença é associada ao Core.

5. Role a tela para baixo no lado direito da página **Definições** até ver o cabeçalho Servidor de licenças.

   As definições de Aplicação de licença do Core são mostradas.

6. Na área Servidor de licenças, clique em **Entrar em contato agora**.

   Assim que a licença é aplicada ao servidor de licenças, todas as máquinas protegidas associadas são atualizadas automaticamente com a nova licença.

Contatar o servidor do Portal de licenças do Rapid Recovery

O Rapid Recovery Core Console com frequência acessa o servidor do Portal de licenças do Rapid Recovery para se manter atualizado com as alterações feitas no portal de licenças.

No caso de licenças que não são de teste, o Rapid Recovery Core entra em contato com o portal de licenças a cada hora. Se não consegue se conectar ao portal de licenças após o período de avaliação de 10 dias, o Core para de criar snapshots.

Normalmente, a comunicação com o server do portal de licenças ocorre automaticamente em intervalos designados. No entanto, é possível iniciar a comunicação sob demanda.

Execute as etapas deste procedimento para entrar em contato com o server do portal de licenças.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em **Definições** e role a tela para baixo no lado direito da página **Definições** até ver o cabeçalho Servidor de licenças.
3. Na área Server de licenças, clique em **Entrar em contato agora**.

Definir as definições do SNMP

O Protocolo Simples de Gerenciamento de Rede (SNMP) é um protocolo para gerenciar dispositivos em uma rede IP. O SNMP é usado principalmente para monitorar dispositivos em uma rede a fim de detectar condições que exijam atenção. Esse protocolo usa componentes de software (agentes) para relatar informações para computadores administrativos (gerentes). Um agente SNMP processa as solicitações do gerente para obter ou definir determinados parâmetros. O agente SNMP pode enviar interceptações (notificações sobre eventos específicos) ao gerente.

Os objetos de dados gerenciados por agentes SNMP são organizados em um arquivo de Base de Informações de Gerenciamento (MIB) que contém Identificadores de Objeto (OIDs). Cada OID identifica uma variável que pode ser lida ou definida usando o SNMP.

O Rapid Recovery inclui suporte para SNMP versão 1.0.

Você pode configurar o Rapid Recovery Core como um agente SNMP. Assim o Core pode enviar informações como alertas, status do repositório e máquinas protegidas. Um host SNMP pode ler essas informações usando

um aplicativo independente conhecido como navegador de SNMP. Você pode instalar o navegador de SNMP em qualquer máquina que o Rapid Recovery Core possa acessar pela rede.

Para certificar-se de que as notificações de eventos de SNMP do Core podem ser recebidas pelo navegador de SNMP, verifique se as opções de notificação de um grupo de notificação estão corretamente configuradas para notificar por interceptação SNMP.

NOTE: Você pode usar o grupo padrão ou criar um grupo de notificação personalizado. O processo é idêntico.

Abra o grupo de notificação, selecione a guia **Opções de notificação** e certifique-se de que a opção **Notificar por interceptação SNMP** está ativada. O grupo de notificação especifica a interceptação número 1 por padrão. Se necessário, você pode alterar o número da interceptação para garantir que ele coincide com a definição esperada pelo navegador de SNMP.

Para obter mais informações e detalhes específicos sobre como configurar as opções de notificação, consulte Configurar grupos de notificação.

Como alternativa, você pode baixar um arquivo MIB do Rapid Recovery Core. Um navegador de SNMP pode ler esse arquivo de forma mais acessível ao usuário que os dados recebidos diretamente do Core.

Esta seção inclui os seguintes tópicos:

- Definir as configurações do SNMP
- Fazer o download do arquivo MIB SNMP

Definir as configurações do SNMP

Use as configurações do SNMP para controlar a comunicação, como alertas, entre um Rapid Recovery Core e outro navegador SNMP. As configurações disponíveis incluem a porta SNMP, a porta do receptor de interceptação e o nome do host do receptor de interceptação.

NOTE: As compilações do Rapid Recovery anteriores à versão 6.1 não incluem a capacidade de alterar a configuração de **Community string** (String da comunidade).

Use este procedimento para configurar as definições do SNMP no Core.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página Definições, clique em **Configuração do SNMP**.
   - Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Configuração do SNMP.

     As definições de configuração do SNMP serão exibidas.
3. Modifique as definições do SNMP conforme descrito na tabela a seguir.

Tabela 21. Informações das definições de conexão do SNMP

Caixa de texto	Descrição
Processar solicitação recebida	Para permitir que o Core reconheça protocolos SNMP recebidos, selecione essa opção. Para bloquear protocolos SNMP recebidos, desmarque a opção. **NOTE:** Selecionar a opção para processar solicitações recebidas permite editar a configuração da string da comunidade.
String da comunidade	Digite um nome para a comunidade.

Caixa de texto	Descrição
	NOTE: Você pode alterar essa configuração somente se **Processar solicitação recebida** for definido para **Sim**.
Porta de entrada	Insira um número de porta para a conexão do SNMP. **NOTE:** A definição padrão é 8161.
Enviar interceptação	Para permitir que alertas (interceptações) sejam enviados usando o protocolo SNMP, selecione essa opção. Para bloquear alertas, desmarque a opção.
Porta do receptor do trap	Insira um número de porta para o alerta recebido. A definição padrão é 162.
Nome do host do receptor do trap	Insira um nome de host para a conexão do SNMP. **NOTE:** O nome de host padrão é localhost.

4. Para cada definição, quando estiver satisfeito com suas alterações, clique na ✓ para salvar a alteração e sair do modo de edição, ou clique em ✕ para sair do modo de edição sem salvar.

Fazer o download do arquivo MIB SNMP

O SNMP (Simple Network Management Protocol) é usado para monitorar dispositivos em uma rede a fim de detectar condições que exigem atenção. Quando o Rapid Recovery Core está definido como um agente SNMP, o Core relata informações como alertas, status de repositório e máquinas protegidas. Um host SNMP pode ler essas informações usando um aplicativo independente, conhecido como navegador de SNMP.

Os objetos de dados gerenciados por agentes SNMP são organizados em um arquivo Base de Informações de Gerenciamento (MIB) que contém Identificadores de Objeto (OIDs). Cada OID identifica uma variável que pode ser lida ou definida usando o SNMP.

Você pode baixar um arquivo MIB do Rapid Recovery Core. Um navegador de SNMP pode ler esse arquivo, denominado quest-rapid-recovery-core.mib, de forma mais acessível ao usuário que os dados recebidos diretamente do Core.

Use esse procedimento para baixar o arquivo MIB SNMP do Rapid Recovery Core.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em ••• (Mais) e clique em **Downloads**.

   A página **Downloads** aparece.
3. Role para baixo até o painel Outros arquivos.
4. Para baixar o arquivo MIB, clique no link de download do **Arquivo MIB SNMP**.

   As definições de Configuração do SNMP são exibidas.
5. Na caixa de diálogo **Abrir quest-rapid-recovery-core.mib**, realize um dos procedimentos a seguir:
   - Para abrir o arquivo de log, selecione **Abrir com**, selecione um navegador de SNMP para visualizar o arquivo MIB baseado em texto e, por último, clique em **OK**.

     O arquivo MIB é aberto no aplicativo selecionado.
   - Para salvar o arquivo localmente, selecione **Salvar arquivo** e clique em **OK**.

O arquivo quest-rapid-recovery-core.mib é salvo na sua pasta Downloads. Ele pode ser aberto usando um navegador de SNMP ou um editor de texto.

Configuração das definições do vSphere

VMware vSphere é um conjunto de software de virtualização com o qual você pode gerenciar máquinas virtuais ESXi ou vCenter Server. Se você estiver usando vSphere, não é necessário carregar o software do agente do Rapid Recovery em VMs individuais para protegê-las. Esse recurso é chamado de proteção sem agentes, que se aplica somente a máquinas virtuais.

Use este procedimento para configurar as definições do vSphere no Core.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página Definições, clique em **vSphere**.
   - Role a tela para baixo no lado direito da página Definições até ver o cabeçalho vSphere.
3. Modifique as definições do vSphere conforme descrito na tabela a seguir.

Tabela 22. Informações das definições do vSphere Core

Elemento de UI	UI Type	Descrição
Duração da conexão	Caixa de número	Estabelece o tempo antes do qual ocorre um tempo limite da conexão com o ESXi Server. Usa o formato HH:MM:SS. **NOTE:** A definição padrão é 00:10:00 ou dez minutos.
Máximo de consolidações simultâneas	Campo de texto	Define o número máximo de consolidações simultâneas para máquinas virtuais protegidas. **NOTE:** A definição padrão é 0.
Máximo de novas tentativas	Campo de texto	Define o número máximo de tentativas de conexão com um disco virtual ou de operações de leitura e gravação antes do tempo limite. **NOTE:** A definição padrão é 10.
Permitir restauração paralela	Booleano (caixa de seleção)	Quando esta opção está marcada, ela permite a restauração paralela de uma máquina virtual sem agentes. Quando esta opção está desmarcada, a função está desabilitada. **NOTE:** A definição padrão é Não (desmarcada).

4. Para cada definição, quando estiver satisfeito com suas alterações, clique na para salvar a alteração e sair do modo de edição, ou clique em para sair do modo de edição sem salvar.

Gerenciar as configurações de proxy do VMware

As configurações de proxy do VMware são destinadas para as máquinas VMware ESXi protegidas que precisam de APIs do Kit de desenvolvimento de disco virtual (VDDK) para acessar o armazenamento em disco do VMware. O Rapid Recovery endereça este acesso e possíveis tempos limites associados a ele usando um processo chamado de proxy do VMware. Este serviço é instalado automaticamente com o Rapid Recovery Core e é executado apenas quando ele é necessário. A página Configurações do Core permite que você ajuste as configurações de tempo limite do serviço da maneira que você achar adequada.

1. Na barra de ícones do Rapid Recovery Core Console, clique em (Configurações) e, em seguida, faça o seguinte:
   - Na lista de configurações do Core no lado esquerdo da página Configurações, clique em **Proxy do VMware**.
   - Role para baixo no lado direito da página Configurações até visualizar o cabeçalho **Proxy do VMware**.
2. Em **Proxy do VMware**, modifique as configurações de tempo limite descritas na tabela a seguir.

Tabela 23. Informações das definições de proxy do VMware

Elemento de UI	Descrição
Tempo limite de conexão	O tempo máximo que deve passar para o proxy do VMware parar de tentar se conectar ao armazenamento em disco do VMware, designado por hh:mm:ss. **NOTE:** A definição padrão é 5 minutos (00:05:00).
Tempo limite de leitura/gravação	O tempo máximo que deve passar para o proxy do VMware parar de tentar ler ou gravar no armazenamento em disco do VMware, designado por hh:mm:ss. **NOTE:** A definição padrão é 5 minutos (00:05:00).
Tempo limite de início do serviço	O tempo máximo que deve passar para o Rapid Recovery parar de tentar iniciar o serviço de proxy do VMware, designado por hh:mm:ss. **NOTE:** A definição padrão é 5 minutos (00:05:00).
Tempo limite de interrupção do serviço	O tempo máximo que deve passar para o Rapid Recovery parar de tentar interromper o serviço de proxy do VMware, designado por hh:mm:ss. **NOTE:** A definição padrão é 1 minuto (00:01:00).

3. Para cada definição, quando estiver satisfeito com suas alterações, clique na marca de seleção para salvar a alteração e sair do modo de edição, ou clique em **X** para sair do modo de edição sem salvar.

Configurar as definições do VFogLight

Se você fornecer informações do vFoglight nas configurações do Core, o Core Console exibirá o URL do vFoglight para cada VM protegida em sua página de resumo. Clicar nesse URL abre as informações sobre a VM no vFoglight.

Conclua as seguintes etapas para integrar o servidor vFoglight ao seu servidor do Rapid Recovery Core.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página Definições, clique em **Configuração do vFoglight**.
   - Role a tela para baixo no lado direito da página Definições até ver o cabeçalho vFoglight.

     As definições de configuração do vFoglight são exibidas.
3. Modifique as definições do vFoglight conforme descrito na tabela a seguir.

Tabela 24. Informações das definições de conexão do vFoglight

Caixa de texto	Descrição
Usar https	Ativa ou desativa o protocolo S-HTTP. HTTPS seguro é o valor padrão.
Host	Insira um nome de host ou endereço IP do server vFoglight. Consulte o administrador do servidor vFoglight para obter detalhes.
Porta	Especifique a porta apropriada. A porta padrão é 32896. Consulte o administrador do servidor vFoglight para obter detalhes.
Token de autenticação	Forneça a autenticação adequada para permitir que o Core se comunique com o servidor vFoglight. Consulte o administrador do servidor vFoglight para obter detalhes.

4. Para cada definição, quando estiver satisfeito com suas alterações, clique em para salvar a alteração e sair do modo de edição, ou clique em para sair do modo de edição sem salvar.

Ferramentas de nível do Core

Além de configurar as definições do Core, você também pode usar as ferramentas do nível do Core descritas na tabela a seguir.

Tabela 25. Outras ferramentas do nível do Core

Elemento de UI	Descrição
Informações do sistema	O Rapid Recovery permite visualizar informações sobre o Rapid Recovery Core, incluindo informações do sistema, volumes locais e montados e conexões do mecanismo de reprodução. Para obter mais informações sobre as informações mostradas da página Informações do sistema, consulte Noções básicas sobre as informações do sistema do Core. Para obter mais informações sobre como visualizar as Informações do sistema, consulte Como visualizar informações do sistema do Core.

Elemento de UI	Descrição
Download dos arquivos de log do Core	Informações sobre várias atividades do Rapid Recovery Core são salvas no arquivo de log do Core. Para diagnosticar possíveis problemas, você pode baixar e visualizar logs do Rapid Recovery Core. Para obter mais informações sobre como acessar e visualizar os logs do Core, consulte Acessar os logs do Core. Cada máquina protegida também salva um log de atividade. Esse log pode ser carregado para o Core se você selecionar o trabalho noturno chamado Baixando os logs das máquinas protegidas. Para obter mais informações sobre trabalhos noturnos, consulte Noções básicas sobre trabalhos noturnos. Para obter mais informações sobre como configurar as definições de trabalho noturno do Core, consulte Configurar trabalhos noturnos para o Core. Para obter mais informações sobre a configuração de trabalhos noturnos para máquinas protegidas específicas, consulte Personalizar trabalhos noturnos para uma máquina protegida.

Noções básicas sobre as informações do sistema do Core

O Rapid Recovery permite que você visualize informações sobre o Rapid Recovery Core. Você pode visualizar informações gerais, informações sobre volumes locais e informações sobre volumes montados.

No painel **Geral**, você pode ver as informações descritas na tabela a seguir.

Tabela 26. Informações do sistema

Elemento de UI	Descrição
Nome do host	O nome da máquina do Rapid Recovery Core.
Versão do SO	A versão do sistema operacional instalado no Rapid Recovery Core.
Arquitetura do SO	Relaciona a estrutura subjacente e o design da máquina que hospeda o Rapid Recovery Core. Inclui potencialmente o chipset e lista o sistema de 64 bits. O Rapid Recovery Core dá suporte apenas a sistemas de 64 bits.
Memória (física)	Lista a quantidade de memória de acesso aleatório instalada na máquina do Core.
Nome de exibição	Mostra o nome de exibição do Core, que pode é configurável (consulte Configurar definições gerais do Core).
Nome de domínio totalmente qualificado	Mostra o nome de domínio totalmente qualificado da máquina do Core.
Local do cache de metadados	Mostra o caminho do local do cache de metadados. Para obter mais informações, consulte Noções básicas sobre o cache de deduplicação e locais de armazenamento.
Local do cache principal	Mostra o caminho do local do cache de deduplicação principal. Para obter mais informações, consulte Noções básicas sobre o cache de deduplicação e locais de armazenamento.

Elemento de UI	Descrição
Local do cache secundário	Mostra o caminho do local do cache de deduplicação secundário. Para obter mais informações, consulte Noções básicas sobre o cache de deduplicação e locais de armazenamento.

O painel **Volumes**, contém as seguintes informações sobre os volumes de armazenamento da máquina Core: Nome, ID do dispositivo, sistema de arquivos, capacidade bruta, capacidade formatada, capacidade utilizada e pontos de montagem.

O painel **Conexões do mecanismo de reprodução** exibe informações detalhadas sobre os pontos de recuperação montados atualmente. Essas informações incluem ponto final local, ponto final remoto, ID de agente de imagem montada, ID da imagem montada e nome de exibição da imagem montada. Você pode ver se a montagem é gravável, ver o usuário autenticado, os bytes lidos e os bytes gravados.

Você pode desmontar pontos de recuperação montados localmente em um Core a partir da página Montagens. Para obter mais informações sobre desmontagem de pontos de recuperação, consulte Desmontar pontos de recuperação.

Para obter mais informações, consulte Como visualizar informações do sistema do Core.

Como visualizar informações do sistema do Core

As informações do sistema do Core incluem informações gerais, informações sobre volumes locais e informações sobre volumes montados do Core. Para obter uma descrição detalhada das informações disponíveis nessa página, consulte Noções básicas sobre as informações do sistema do Core.

Conclua as etapas nesse procedimento para exibir informações do sistema do Core.

NOTE: Você também pode ver informações do sistema de uma máquina protegida específica. Para obter mais informações, consulte Visualização das informações do sistema de uma máquina protegida.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Mais) e, em seguida, clique em **Informações do sistema**.

   A página **Informações do sistema** é exibida.

Acessar os logs do Core

Informações sobre várias atividades do Rapid Recovery Core são salvas no arquivo de log do Core. Esse arquivo, **AppRecovery.log**, é armazenado por padrão no caminho `C:\ProgramData\AppRecovery\logs`.

NOTE: Dependendo de suas configurações, o diretório do AppRecovery pode não estar visível no Rapid Recovery Core. Para ver esse diretório, você pode precisar alterar as Opções de pasta no painel de controle para exibir arquivos, pastas e unidades ocultas. Se essas definições incluírem a opção de ocultar as extensões dos tipos de arquivo conhecidos, o arquivo de log do Core pode ser mostrado como AppRecovery sem extensão `.log`.

O log do Core inclui informações sobre trabalhos do Core concluídos, falhas de conexão, resultados de tentativas do Core em entrar em contato com o Portal de licenças e outras informações. Cada declaração armazenada no arquivo de log do Core é precedida por um de quatro qualificadores: INFO, DEBUG, ERROR e WARN. Esses qualificadores ajudam classificar a natureza das informações armazenadas no log ao diagnosticar um problema.

NOTE: Da mesma forma, um arquivo de log também é armazenado em cada máquina protegida que contém informações relacionadas às tentativas de comunicação com o Core. Para obter mais informações sobre logs de máquina, consulte Download e visualização do arquivo de log de uma máquina protegida.

A capacidade de acessar logs pode ser útil para solucionar um problema ou trabalhar com o suporte do Quest Rapid Recovery. Para acessar os logs, consulte os procedimentos a seguir:

See also: Como baixar e exibir o arquivo de log do Core
See also: Download e visualização do arquivo de log de uma máquina protegida

Como baixar e exibir o arquivo de log do Core

Caso encontre algum erro no Core, você pode baixar os logs de Core para exibi-los ou compartilhá-los com o representante do Quest Support.

1. Na barra de ícones do Rapid Recovery Core Console, clique em (Mais) e, em seguida, clique em **Core Log** (Log do core).
2. Na página **Baixar log do Core**, clique em **Clique aqui para começar o download**.
3. Caso precise abrir ou salvar o arquivo `Core AppRecovery.log`, clique em **Save** (Salvar).
4. Caso você veja a caixa de diálogo **Abrindo Core AppRecovery.log**, faça o seguinte:
   - Para abrir o arquivo de log, selecione **Abrir com** e um aplicativo (como Bloco de Notas) para visualizar o arquivo de log com base em texto e, por fim, clique em **OK**.

     O arquivo **Core AppRecovery.log** é aberto no aplicativo selecionado.
   - Para salvar o arquivo localmente, selecione **Salvar arquivo** e clique em **OK**.

     O arquivo **Core AppRecovery.log** é salvo na sua pasta **Downloads**. Ele pode ser aberto usando-se qualquer editor de texto.

See also: Como baixar e exibir o arquivo de log do Core
See also: Download e visualização do arquivo de log de uma máquina protegida

Repositórios

Essa seção descreve como trabalhar com os repositórios suportados pelo Rapid Recovery. Aborda os recursos e os atributos do tipo de repositório principal (Deduplication Volume Manager ou DVM) e do tipo secundário (um repositório de camadas). Ela descreve tipos de deduplicação usados no Rapid Recovery e como a deduplicação é usada em todo o aplicativo. Em seguida, esta seção descreve como gerenciar o DVM e os repositórios de camadas, incluindo a criação de um repositório, a exibição e a edição de seus detalhes, e a exclusão de um repositório. Você também pode aprender a abrir um repositório de um Core em outro Core.

Os tópicos são:

- Noções básicas sobre repositórios
- Deduplicação no Rapid Recovery
- Gerenciamento de um repositório de DVM
- Gerenciamento de um repositório de camadas
- Verificar um repositório
- Alteração das configurações do repositório
- Conectar a um repositório existente
- Ver ou modificar detalhes do repositório
- Excluir um repositório

Noções básicas sobre repositórios

Um repositório é uma estrutura de dados usada para armazenar e gerenciar dados do Rapid Recovery. Os instantâneos de backup são salvos em um repositório na forma de pontos de recuperação. Antes de proteger máquinas, replicar ou restaurar dados no Rapid Recovery, você precisa de pelo menos um repositório.

Um administrador do Rapid Recovery cria explicitamente um repositório dentro de um local de armazenamento (um volume de disco) associado a um Core específico. Pode-se criar um repositório a partir da interface do usuário ou a partir da linha de comando. No Rapid Recovery Core Console, você pode criar um novo repositório DVM principal ou um repositório de camadas secundário. Ao proteger uma máquina, você também pode definir um repositório DVM como uma etapa avançada no fluxo de trabalho do assistente.

A partir da página **Repositórios** do Rapid Recovery Core Console, você pode criar um novo repositório ou conectar o Core a um repositório existente (atualmente utilizado por outro Core). Em geral, é possível ver detalhes de um repositório, ver as configurações do repositório, verificar um repositório ou excluir um repositório. Os repositórios DVM permitem adicionar um local de armazenamento ou otimizar um repositório. Os repositórios de camadas permitem que você desconecte-se da máquina que hospeda o repositório. Para obter mais informações sobre como gerenciar um tipo de repositório específico, consulte Gerenciamento de um repositório de DVM ou Gerenciamento de um repositório de camadas, respectivamente.

Um repositório pode residir em diferentes tecnologias de armazenamento, incluindo DAS (Armazenamento por Conexão Direta), SAN (Rede de Área de Armazenamento) ou NAS (Armazenamento Conectado à Rede).

NOTE: Armazene repositórios do Rapid Recovery em dispositivos de armazenamento primário. A velocidade do volume de armazenamento é o fator mais crítico. Dispositivos de armazenamento de arquivamento como Domínio de dados não são suportados devido a limitações de desempenho. De forma semelhante, não armazene repositórios em arquivadores NAS organizados em níveis na nuvem, pois esses dispositivos tendem a ter limitações de desempenho quando usados como armazenamento primário.

DAS oferece a largura de banda de dados mais alta e a taxa de acesso mais rápida, sendo de fácil implementação. Para obter melhores resultados, utilize DAS com armazenamento de RAID (Reduntant Array of Independent Disks [matriz redundante de discos independentes]) 6. Para obter mais informações, consulte o artigo 118153 da Base de conhecimento da Quest, Opções de repositório: Armazenamento por conexão direta, Rede de área de armazenamento ou Armazenamento conectado à rede.

O local de armazenamento para um repositório DVM primário deve ser sempre em um único subdiretório especificado por você (por exemplo, `E:\Repository`), nunca na raiz de um volume (por exemplo, `E:\`). Ao criar um repositório de camadas, não é possível especificar um diretório, mas você pode especificar um contêiner. Você pode selecionar o contêiner padrão ou criar um novo.

Os repositórios DVM são usados para armazenamento primário, onde os pontos de recuperação são salvos pelo Core diretamente nos dispositivos de armazenamento especificados.

Os repositórios de camadas são usados para armazenamento secundário. Nesse modelo, os pontos de recuperação são relocados de um repositório DVM primário para um volume de armazenamento secundário que você especificar. Depois de copiados e verificados, os pontos de recuperação são removidos da repositório primário, liberando espaço para mais dados de backup.

NOTE: No versão 6.2, os repositórios de camadas são suportados apenas em soluções de backup e eliminação de duplicação da série Quest DR.

Você pode ter qualquer combinação de repositórios DVM e de camadas definidos para um único Core. Se os dois tipos de repositório forem adicionados ao Core, a página **Repositórios** mostrará um painel à parte listando cada tipo separadamente. Os repositórios principais são listados primeiro, seguidos pelos repositórios de camadas (secundários).

A seção a seguir descreve os recursos de cada tipo de repositório suportado pelo Rapid Recovery.

Repositório DVM. Este formato de repositório utiliza o Deduplication Volume Manager (DVM).

- DVM é uma tecnologia de repositório primário usada para armazenar pontos de recuperação.
- Os repositórios DVM são criados e gerenciados no Rapid Recovery Core Console.
- Os repositórios DVM oferecem suporte a vários volumes, até 255 repositórios em um único Core.
- Você pode especificar o tamanho de um repositório de DVM após a criação e pode adicionar extensões posteriormente.
- Você pode criar repositórios DVM somente em máquinas com sistemas operacionais Windows.
- O volume do repositório DVM pode ser local (no armazenamento conectado ao servidor do Core) ou em um local de armazenamento em um local compartilhado CIFS.
- Você pode utilizar esse tipo de repositório ao atualizar as instalações existentes do Rapid Recovery e ao utilizar novas instalações do AppAssure.
- Os repositórios DVM podem se estender a tecnologias de armazenamento diferentes.
- Os tipos de armazenamento suportados incluem Rede de área de armazenamento (SAN), Armazenamento por conexão direta (DAS) ou Armazenamento conectado à rede (NAS)
- Requer 8 GB de RAM, de preferência, memória ECC (Error Checking and Correction [checagem e correção de erros])
- Requer processador quad core na máquina do Core
- Suporta múltiplos repositórios DVM por host
- Não há serviços adicionais necessários; o repositório de DVM utiliza serviços de Core original para comunicação com o Core e para monitoramento de eventos
- Cada repositório de DVM suporta até 4096 extensões de repositório (também chamadas de locais de armazenamento)
- Tamanho fixo; o repositório de DVM exige a especificação do tamanho do repositório sobre um volume. O tamanho que você especificar não pode exceder o tamanho do volume. Cada volume definido como um local de armazenamento deve apresentar um mínimo de 1 GB de espaço livre disponível.
- O local de armazenamento do repositório pode ser um disco simples ou dinâmico, com a velocidade sendo o fator mais importante
- Pode utilizar chaves de criptografia padrão criadas e gerenciadas no Core Console (criptografia com base em Core)
- Deduplica os dados em todo o repositório (ou nos domínios de criptografia dentro de cada repositório, se as chaves de criptografia forem utilizadas)
- Utiliza um cache de deduplicação DVM exclusivo e redimensionável, com um local de armazenamento configurável nas configurações do Core
- Otimizado para gravar dados, armazenar dados de snapshot em um repositório local ao Core, com todos os dados processados através do Core
- Não pode ser renomeado depois da criação
- Novos repositórios desse tipo podem ser criados utilizando APIs REST, Utilitário de gerenciamento de linha de comando (cmdutil.exe) do Rapid Recovery ou cmdlet do Windows PowerShell

Ao criar um repositório DVM, o Rapid Recovery Core pré-aloca o espaço de armazenamento necessário para os dados e metadados no local especificado. O tamanho mínimo do repositório DVM é 1 GB, que, para fins práticos, é muito pequeno (exceto para teste).

Uma vez que a deduplicação DVM exige um cache principal e um cache secundário, certifique-se de que o espaço de armazenamento reservado apresente o dobro do tamanho de seu cache de deduplicação. Por exemplo, se você tiver 1,5 GB reservados nas configurações de cache de deduplicação DVM no Core, reserve

3 GB no volume do cache. O caminho de instalação padrão para o cache está na unidade C. Para obter mais informações, consulte Noções básicas sobre o cache de deduplicação e locais de armazenamento.

Repositório de camadas. O repositório de camadas foi introduzido no Rapid Recovery versão 6.1.

- A tecnologia de repositório de camadas é usada apenas para armazenamento secundário.
- Os pontos de recuperação existentes (de 1 semana ou mais) que ainda não foram designados para arquivamento podem ser relocados do repositório DVM primário do Rapid Recovery. Esse recurso é ativado por meio do período de retenção.
- Os repositórios de camadas são criados e gerenciados no Rapid Recovery Core Console.
- Atualmente, os repositórios de camadas são suportados apenas na solução de backup e eliminação de duplicação da série Quest DR versão 4.0.
- Os pontos de recuperação de camadas para o armazenamento secundário continuam sendo protegidos por criptografia e estão sujeitos a rollup. A política de retenção e rollup continua a ser gerenciada pelo Core no novo local.
- Conforme o rollup continua a cada noite, os novos pontos de recuperação são constantemente organizados em camadas. Ao visualizar os pontos de recuperação protegidos por máquina, esses pontos de recuperação que estão em camadas são designados por um ícone dourado de banco de dados .

Quanto à interoperabilidade, os pontos de recuperação salvos em repositórios DVM primários podem ser organizados em camadas em um repositório secundário. Como as soluções DR que suportam a organização em camadas usam um sistema operacional CentOS, os repositórios DVM não são suportados nessas soluções.

Usando soluções virtuais e físicas para armazenamento de repositórios

Se estiver usando o Rapid Recovery em uma solução de recuperação e backup Quest DL4300, você pode criar repositórios DVM e de camadas. Na versão 6.2, o repositório de camadas deve ser armazenado em uma solução de backup e eliminação de duplicação DR executando o sistema operacional 4.0.

Os repositórios de camadas gerenciados na DL usam licenças de capacidade. Portanto, embora seja possível organizar em camadas os nível pontos de recuperação do repositório DVM associado a uma solução DL no armazenamento secundário em uma solução DR, o espaço consumido por esses pontos de recuperação é desvantajoso para a capacidade da solução DL. Portanto, é mais econômico arquivar pontos de recuperação de uma solução DL e armazenar os arquivos no DR.

Nenhuma outra solução de armazenamento, backup, recuperação ou deduplicação foi testado explicitamente para o uso com o Rapid Recovery. Continue por sua conta e risco.

O Virtual DR2000v pode ser usado para um repositório de camadas, desde que ele tenha os serviços RDS corretos instalados e execute o sistema operacional 4.0. Outras soluções virtuais ainda não são suportadas no Rapid Recovery Core versão 6.2.

See also: Gerenciamento de um repositório de DVM
See also: Gerenciamento de um repositório de camadas

Deduplicação no Rapid Recovery

A deduplicação é uma técnica de compactação de dados que reduz os requisitos de armazenamento e a carga da rede. O processo envolve armazenar fisicamente blocos de dados exclusivos no disco somente uma vez. No Rapid Recovery, quando qualquer bloco de dados exclusivo ocorre uma segunda vez dentro de um repositório, em vez de armazenar os dados novamente, uma referência virtual dos dados é armazenada.

A desduplicação ocorre nos snapshots de backup capturados pelo Rapid Recovery Core.

- As informações de backup são deduplicadas dentro de um único repositório. Elas não podem ser desduplicadas em múltiplos repositórios .
- Os repositórios DVM usam criptografia com base em destino. Para fins de segurança, a criptografia é realizada antes da eliminação de duplicação. A eliminação de duplicação ainda é limitada aos dados protegidos dentro de uma única chave de criptografia.

Se o cache de eliminação de duplicação fica cheio, a eliminação de duplicação torna-se abaixo do ideal. Neste caso, a eliminação de duplicação pode ser executada como um processo posterior (também conhecido como reclamação de bloco). Depois de aumentar o tamanho do cache de eliminação de duplicação, execute o trabalho de otimização do repositório. A partir daí, o núcleo irá recuperar blocos, oferecendo mais espaço em seu repositório.

Para obter mais informações sobre o trabalho de otimização do repositório, consulte Sobre a otimização do repositório DVM. Para obter mais informações sobre como executar essa tarefa, consulte Otimização de um repositório de DVM.

Assim, o Rapid Recovery tira proveito de todos os tipos de eliminação de duplicação descritos aqui: eliminação de duplicação baseada em destino, eliminação de duplicação em linha e eliminação de duplicação de pós-processamento.

Para obter mais informações sobre o local em que as referências para os blocos exclusivos estão armazenadas para os repositórios de DVM, consulte Noções básicas sobre o cache de deduplicação e locais de armazenamento. Para obter informações sobre como ajustar as configurações do cache de deduplicação DVM, consulte Configurar definições de cache de deduplicação DVM.

Gerenciamento de um repositório de DVM

O gerenciamento de um repositório de DVM envolve as seguintes operações:

1. **Criação de um repositório de DVM**. Antes de criar um repositório, considere o tipo de tecnologia adequada.

   Para obter informações sobre os diferentes tipos de repositório, consulte Noções básicas sobre repositórios.
   Para obter mais informações sobre a criação de um repositório DVM, consulte Criar um repositório de DVM.
2. **Conectar a um repositório**. Para obter mais informações sobre como conectar a um repositório existente gerenciado atualmente por outro Core, consulte Conectar a um repositório existente.
3. **Adicionando um novo local de armazenamento**. Para obter mais informações sobre a adição de um novo local de armazenamento em um repositório de DVM, consulte Adicionar um local de armazenamento a um repositório de DVM existente.
4. **Verificando um repositório**. Para obter mais informações sobre a verificação de repositório de DVM, consulte Verificar um repositório.
5. **Modificando as definições do repositório**. Para obter mais informações sobre como ver os detalhes do repositório ou modificar as definições de um repositório, consulte Ver ou modificar detalhes do repositório
6. **Executar a otimização do repositório DVM**. Para obter mais informações sobre o trabalho de otimização do repositório, consulte Sobre a otimização do repositório DVM. Para as etapas de otimização de um repositório de DVM existente, consulte Otimização de um repositório de DVM.
7. **Excluindo um repositório**. Para obter mais informações sobre a exclusão de um repositório, consulte Excluir um repositório.

Para obter informações sobre como gerenciar um repositório de camadas, consulte Gerenciamento de um repositório de camadas.

Criar um repositório de DVM

Este processo descreve como criar um repositório no seu Core usando a tecnologia de repositório de Gerenciador de volume de deduplicação (DVM).

- Você precisa ter acesso de administrador da máquina para a qual você quer criar um repositório de DVM.
- Esse tipo de repositório exige, pelo menos, 1 GB de espaço de armazenamento disponível no volume que você definir como local de armazenamento.
- O local de armazenamento para um repositório de DVM precisa estar em uma unidade local conectada ao servidor Core ou em um compartilhamento CIFS.
- O servidor Core pode ser qualquer dispositivo de série DL (incluindo o DL1000) ou pode ser qualquer servidor Windows com base em software que preencha os requisitos do sistema.

NOTE: Os repositórios DVM não são suportados nem soluções de backup de disco e deduplicação da série DR. As soluções DR usam a própria deduplicação. Essa deduplicação é incompatível com a deduplicação que o Rapid Recovery Core aplica a um repositório DVM.

Se você quiser criar um repositório de camadas para armazenamento secundário de pontos de recuperação originalmente salvos no repositório DVM, consulte o tópico Criar um repositório de camadas.

Execute as seguintes etapas para criar um repositório de DVM.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Repositórios**.

   A página **Repositórios** aparece.
3. Na parte superior da página, sob o titulo da página Repositórios, clique na seta suspensa ao lado de **Create** (Criar) e selecione **DVM Repository** (Repositório DVM).

   A caixa de diálogo **Add New Repository** (Adicionar novo repositório) será exibida.
4. Insira as informações conforme descrito na tabela a seguir.

Tabela 27. Definições de Adicionar novo repositório

Caixa de texto	Descrição
Nome do repositório	Insira o nome de exibição do repositório. Por padrão, essa caixa de texto consiste na palavra Repositório e um número, que corresponde ao número de repositórios neste Core. Por exemplo, se este for o primeiro repositório, o nome padrão é Repositório 1. Altere o nome conforme a necessidade. Nomes de repositório devem conter entre 1 e 40 caracteres alfanuméricos, incluindo espaços. Não use ou .
Operações simultâneas	Defina o número de solicitações simultâneas que você deseja que o repositório suporte. Por padrão, o valor é 64.
Comentários	Como opção, insira uma nota descritiva sobre esse repositório. Você pode inserir até 254 caracteres. Por exemplo, digite **Repositório de DVM 2**.

5. Clique em **Adicionar local de armazenamento** para definir o local de armazenamento ou o volume específico desse repositório. Use uma unidade de armazenamento primário rápido com espaço de armazenamento suficiente. O local de armazenamento de um repositório DVM pode ser local (no armazenamento anexado ao servidor do Core) ou em um local de rede compartilhada CIFS. Não é possível especificar ambos para um único local de armazenamento.

CAUTION: Defina uma pasta dedicada na raiz do local de armazenamento do seu repositório. Não especifique o local da raiz. Por exemplo, use `E:\Repository\`, e não `E:\`. Se o repositório que você está criando nessa etapa for removido mais tarde, todos os arquivos no local de armazenamento do seu repositório serão excluídos. Se você definir o local de armazenamento na raiz, todos os outros arquivos no volume (por exemplo: `E:\`) são excluídos, o que poderia resultar em uma perda de dados catastrófica.

A caixa de diálogo **Adicionar local de armazenamento** é exibida.

6. Clique em **Adicionar local de armazenamento** para definir o local de armazenamento ou o volume específico do repositório. Esse volume deve ser um local de armazenamento principal.
7. Na área **Local de armazenamento**, especifique a forma de adicionar o arquivo ao local de armazenamento. Você pode escolher adicionar um volume de armazenamento conectado localmente (como um armazenamento por conexão direta, uma rede de área de armazenamento ou um armazenamento conectado à rede). Você também pode especificar um volume de armazenamento em um local compartilhado CIFS.
   - Selecione **Adicionar arquivo no disco local** para especificar uma máquina local e, depois, insira as informações conforme descrito na tabela a seguir.

Tabela 28. Definições de disco local

Caixa de texto	Descrição
Caminho de dados	Insira o local para armazenar os dados protegidos. Por exemplo, digite `X:\Repository\Data`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Caminho de metadados	Insira o local para armazenar os metadados protegidos. Por exemplo, digite `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

   - Ou selecione **Adicionar arquivo no compartilhamento de CIFS** para especificar um local de compartilhamento de rede e, depois, insira as informações conforme descrito na tabela a seguir.

Tabela 29. Credenciais de compartilhamento de CIFS

Caixa de texto	Descrição
Caminho de UNC	Insira o caminho para o local de compartilhamento de rede. Se esse local estiver na raiz, defina um nome de pasta dedicada (por exemplo, `Repository`). O caminho precisa começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Especifique um nome de usuário para acessar o local de compartilhamento de rede.

Caixa de texto	Descrição
Senha	Especifique a senha para acessar o local de compartilhamento de rede.

8. Na área **Configuração de armazenamento**, clique em **Mais detalhes** e insira os detalhes do local de armazenamento, como descrito na tabela a seguir.

Tabela 30. Detalhes da Configuração de armazenamento

Caixa de texto	Descrição
Tamanho	Defina o tamanho ou capacidade do local de armazenamento. O tamanho mínimo é 1 GB. O padrão é 250 GB. Você pode selecionar dentre os seguintes: • GB • TB **NOTE:** O tamanho que você especificar não pode exceder o tamanho do volume. Se o local de armazenamento for um volume NTFS (Sistema de arquivos de nova tecnologia) usando o Windows 8 ou Windows 2012 ou superior, o limite de tamanho do arquivo é 256 TB. **NOTE:** Para que o Rapid Recovery valide o sistema operacional, a Instrumentação de gerenciamento do Microsoft Windows (WMI) deve estar instalada no local de armazenamento pretendido.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Em • Desligar • Sincronizar Se definido como Ligado, que é o padrão, o Windows controla o armazenamento em cache. Isso é apropriado para o Windows 10 e para versões do Windows Server 2012 e posterior. **NOTE:** Definir a política de cache de gravação como Ligado pode resultar em desempenho mais rápido. Se você estiver utilizando o Windows Server 2008 SP2 ou Windows Server 2008 R2 SP2, a recomendação de configuração será Desligado. Se configurado como Desativado, o Rapid Recovery controla o armazenamento em cache. Se definido como Sincronizar, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é 512.
Média de bytes por registro	Especifique a média de bytes por registro. O valor padrão é 8192.

9. Clique em **Salvar**.

A caixa de diálogo **Adicionar local de armazenamento** é fechada e suas configurações são salvas. A caixa de diálogo **Adicionar novo Repositório** exibe o seu novo local de armazenamento.

10. Como opção, repita as etapas 6 a etapa 9 para adicionar mais locais de armazenamento ao repositório.
11. Quando todos os sobre os locais de armazenamento que você deseja criar para o repositório neste momento forem definidos, na caixa de diálogo **Adicionar novo repositório**, clique em **Criar**.

    A caixa de diálogo **Adicionar novo repositório** é fechada e suas configurações são salvas. A página **Repositórios** é exibida, mostrando seu repositório DVM adicionado recentemente na tabela de resumo.

Adicionar um local de armazenamento a um repositório de DVM existente

Um repositório DVM deve existir no repositório para executar este procedimento.

Adicionar um local de armazenamento a um repositório de DVM permite definir onde você deseja que o repositório ou o volume seja armazenado.

Execute as etapas do procedimento a seguir para especificar o local de armazenamento do repositório ou do volume.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Repositórios**.

   A página **Repositórios** aparece.

   A página Repositórios de DVM é exibida.
3. Na tabela de resumo de repositórios, na linha que representa o repositório DVM ao qual você deseja adicionar um local de armazenamento, clique no menu suspenso (Mais opções) e selecione **Adicionar local de armazenamento**.

   A caixa de diálogo **Adicionar local de armazenamento** é exibida.
4. Especifique a forma de adicionar o arquivo ao local de armazenamento. Você pode selecionar adicionar o arquivo no disco local ou no compartilhamento de CIFS.
   - Selecione **Adicionar arquivo no disco local** para especificar uma máquina local e, depois, insira as informações conforme descrito na tabela a seguir.

Tabela 31. Definições de disco local

Caixa de texto	Descrição
Caminho de dados	Insira o local para armazenar os dados protegidos. Por exemplo, digite `X:\Repository\Data`. As mesmas limitações do caminho se aplicam; use somente caracteres alfanuméricos, hífen ou ponto, sem espaços ou caracteres especiais.
Caminho de metadados	Insira o local para armazenar os metadados protegidos. Por exemplo, digite `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

   - Ou selecione **Adicionar arquivo no compartilhamento de CIFS** para especificar um local de compartilhamento de rede e, depois, insira as informações conforme descrito na tabela a seguir.

Tabela 32. Credenciais de compartilhamento de CIFS

Caixa de texto	Descrição
Caminho de UNC	Insira o caminho para o local de compartilhamento de rede. Se esse local estiver na raiz, defina um nome de pasta dedicada (por exemplo, `Repository`). O caminho precisa começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Especifique um nome de usuário para acessar o local de compartilhamento de rede.
Senha	Especifique a senha para acessar o local de compartilhamento de rede.

5. No painel Configuração de armazenamento, clique em **Mais detalhes** e insira os detalhes do local de armazenamento, como descrito na tabela a seguir.

Tabela 33. Detalhes do local de armazenamento

Caixa de texto	Descrição
Tamanho	Defina o tamanho ou capacidade do local de armazenamento. O tamanho padrão é 250 GB. Você pode selecionar dentre os seguintes: • GB • TB **NOTE:** O tamanho mínimo é 1 GB. O tamanho que você especificar não pode exceder o tamanho do volume. Se o local de armazenamento for um volume NTFS usando o Windows 8, Windows 8.1 ou Windows Server 2012, 2012 R2 ou 2016, o limite de tamanho do arquivo é 256 TB. **NOTE:** Para que o Rapid Recovery valide o sistema operacional, a Instrumentação de gerenciamento do Microsoft Windows (WMI) deve estar instalada no local de armazenamento pretendido.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Em • Desligar • Sincronizar Se definido como Ligado, que é o padrão, o Windows controla o armazenamento em cache. Isso é apropriado para o Windows 10 e para versões do Windows Server 2012 e posterior. **NOTE:** Definir a política de cache de gravação como Ligado pode resultar em desempenho mais rápido. Se você estiver utilizando o Windows Server 2008 SP2 ou Windows Server 2008 R2 SP2, a recomendação de configuração será Desligado.

Caixa de texto	Descrição
	Se configurado como Desativado, o Rapid Recovery controla o armazenamento em cache. Se definido como Sincronizar, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é 512.
Média de bytes por registro	Especifique a média de bytes por registro. O valor padrão é 8192.

6. Opcionalmente, se desejar executar o trabalho de otimização do repositório para o repositório selecionado, selecione **Executar trabalho de otimização do repositório para [Nome do repositório]**.

   A Quest recomenda a execução do Trabalho de otimização do repositório ao adicionar locais de armazenamento a um repositório existente. Esse trabalho otimiza o espaço livre ao aplicar a deduplicação dos dados armazenados no repositório.

   Com base em fatores como tamanho do repositório, quantidade de dados no repositório, largura da banda de rede disponível e carga local na entrada e na saída do sistema, a execução de um Trabalho de otimização do repositório poderá demorar e utilizar grande quantidade da largura da banda de seu ambiente.

   Para obter mais informações sobre o trabalho de otimização do repositório, consulte Sobre a otimização do repositório DVM.

7. Clique em **Salvar**.

   A caixa de diálogo é fechada e o local de armazenamento, salvo. Na tabela de resumo de repositórios, o local de armazenamento criado será visível ao expandir os detalhes do repositório.

Sobre como verificar a integridade dos repositórios DVM

No AppAssure versão 5.3.6 e versões anteriores, a replicação incluía o processo de copiar pontos de recuperação do Core de origem para o Core de destino. O rollup dos pontos de recuperação do envelhecimento ocorreram somente no Core de origem. Os pontos de recuperação mais antigos combinados foram sincronizados diariamente durante a execução do trabalho noturno.

A partir do Rapid Recovery Core versão 5.4.1 e versões atuais do AppAssure, os usuários podem definir diferentes políticas de retenção entre os Cores de origem e de destino. Para que a replicação funcione adequadamente com diferentes políticas de retenção, o Core de destino deve ter a mesma versão do software (ou mais recente) que tem o Core de origem.

Os administradores podem agora configurar o rollup em um Core de destino a uma taxa diferente do Core de origem. Da mesma forma, você pode agora definir uma política de retenção personalizada para qualquer máquina replicada. Por exemplo, você pode executar o processo de rollup de pontos de recuperação no Core de destino a um ritmo mais rápido e com menos granularidade do que no Core de origem, economizando espaço. Ou, você pode realizar o processo de rollup dos pontos de recuperação para qualquer máquina replicada selecionada a uma taxa mais lenta no Core de destino e manter mais granulosidade que pode ser útil para fins de conformidade. Para obter mais informações sobre como usar uma política de retenção que difere do padrão no Core, consulte Personalizar as definições de política de retenção de uma máquina protegida.

Alguns clientes experimentaram inconsistências nos pontos de recuperação que foram replicadas para um Core de destino antes do AppAssure versão 5.3.6. Para resolver este problema, o AppAssure versão 5.4.1 e posterior incluem um trabalho de Core a ser executado em repositório de DVM. A Quest recomenda executar o trabalho de verificação de integridade uma única vez em cada repositório DVM em um Core de destino replicado se o repositório foi criado antes da versão 5.4.x (se ele foi criado na versão 5.3.x ou anterior).

Para obter instruções sobre como executar esta verificação, consulte o procedimentoExecutar uma verificação de integridade em um repositório DVM.

O trabalho de verificação de integridade **não** estará disponível:

- Em um novo repositório DVM no Core de destino criado na versão 5.4.1 ou posterior do Rapid Recovery ou criado no AppAssure.
- Em um Core de origem.
- Se você já tiver executado o trabalho de verificação de integridade (ou Trabalho de verificar o repositório) neste repositório.
- Se você não tiver usado a replicação.

Se o seu Core tiver sido atualizado em qualquer ponto do AppAssure 5.3.x e você usou replicação, você deve executar este trabalho antes de poder configurar diferentes políticas de retenção entre o Core de origem e o Core de destino, ou configurar uma política de retenção personalizada em uma máquina replicada.

Você não verá ou será capaz de executar este trabalho, a menos que você tenha um ou mais repositórios que se qualifiquem (criados antes de 5.4.x e ainda não executados).

A execução desse trabalho verifica a integridade de todos os dados armazenados no repositório especificado, garantindo que seja possível recuperar os dados de cada snapshot ou imagem de base. Se a verificação de integridade detectar algum problema com os dados em seu repositório, o trabalho para imediatamente. Os detalhes do evento para aquele trabalho no Core solicitam que você entre em contato com o Suporte de proteção de dados da Quest, de forma que é possível marcar o horário para trabalhar com um representante de suporte a fim realizar procedimentos adicionais de identificação e correção de inconsistências de dados.

CAUTION: A execução deste trabalho deve levar um longo tempo. A extensão de tempo varia dependendo da quantidade e tipo de dados em seu repositório e no sistema de armazenamento subjacente. Enquanto o trabalho está em execução, nenhuma outra transação pode ser executada naquele repositório, incluindo transferências (cópias de segurança do Snapshot e da imagem de base, e replicação), trabalhos noturnos e assim por diante.

É possível executar outras operações em outros repositórios enquanto este trabalho está em execução.

NOTE: Este trabalho verifica a integridade de todo o conteúdo dentro do repositório. Para obter informações sobre o trabalho `Checking repository`, que pode ser usado para verificar se um repositório está em condições de ser montado e usado, consulte Verificar um repositório.

Executar uma verificação de integridade em um repositório DVM

Uma verificação de integridade está disponível para repositórios DVM. A finalidade deste procedimento é verificar a integridade de um repositório DVM inteiro. Ele é recomendado para cores de destino replicados durante o upgrade do AppAssure 5.3.x para a versão 5.4. Durante a execução da verificação de integridade, que pode ser prolongada, nenhuma outra ação pode ser executada no repositório.

Se você tiver vários repositórios de DVM para um Core de destino, execute este processo uma vez para cada repositório.

NOTE: Se você tiver outro repositório DVM no Core de destino para o qual o trabalho de verificação de repositório já foi concluído ou se criou um novo repositório adicional para este core de destino, você poderá executar operações em um repositório secundário enquanto o trabalho de verificação de repositório está sendo executado no repositório DVM que você especificou.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Repositórios**.

A página **Repositories** (Repositórios) será exibida.

3. Na tabela de resumo dos repositórios DVM, na linha que representa o repositório DVM que você quer verificar, clique em ••• (Mais opções) e, no menu suspenso, selecione **Verificação de integridade**.

   É exibida uma mensagem de confirmação.

   > **CAUTION: Antes de confirmar que deseja realizar o trabalho, você deve pensar bem sobre o tempo de duração necessário. Enquanto o trabalho está em execução, nenhuma outra transação pode ser executada naquele repositório, incluindo transferências (cópias de segurança do Snapshot e da imagem de base, e replicação), trabalhos noturnos e assim por diante.**

4. Na caixa de diálogo **Check Repository** (Verificar repositório), para realizar a verificação de integridade, clique em **Yes** (Sim).

   A caixa de diálogo é fechada. Todos os trabalhos enfileirados em andamento são cancelados e começa o trabalho de verificação da integridade.

5. Para monitorar o andamento do trabalho de verificação de um repositório, incluindo a determinação das etapas adicionais necessárias depois da verificação, na barra de ícones, clique em (Eventos).

6. Na página **Tarefas**, clique em **Detalhes do trabalho** para ver mais informações sobre o status do trabalho.

   - Se você vir um erro em alguma tarefa subordinada desse trabalho, anote o erro e forneça as informações para o representante do suporte técnico da Quest.
   - Se o trabalho de verificação do repositório concluir todas as tarefas subordinadas com sucesso, você poderá estabelecer uma política de retenção personalizada para esse repositório.

Sobre a otimização do repositório DVM

Durante o uso de um repositório de DVM, os dados capturados em cada snapshot são deduplicados. Essa deduplicação ocorre de maneira incremental, desde que os snapshots sejam salvos no repositório. Uma ocorrência de cada string de informações é salva no repositório. Quando uma string de informações é duplicada, uma referência para a string original no cache de deduplicação é usada, economizando espaço de armazenamento no repositório.

Caso o cache de deduplicação DVM esteja cheio, somente dados de snapshot já referenciados no cache são deduplicados. À medida que ocorre deduplicação, o cache continua sendo atualizado com valores exclusivos, substituindo os valores mais antigos no cache. Isso resulta em uma deduplicação inferior à ideal.

Para obter mais informações sobre deduplicação, consulte Noções básicas sobre o cache de deduplicação e locais de armazenamento.

Você pode escolher aumentar o cache de deduplicação DVM antes que ele esteja cheio, o que garante a deduplicação ideal continuada dos dados nesse repositório. Para obter mais informações, consulte Configurar definições de cache de deduplicação DVM.

Você também pode aumentar o cache de deduplicação depois de estar cheio. Caso queira recuperar espaço no repositório depois de aumentar o cache, você pode otimizar o repositório. Essa ação força uma comparação dos dados nos snapshots com as informações no cache de deduplicação. Caso alguma string repetida seja encontrada no repositório, esses dados são substituídos por referências aos dados, o que economiza espaço de armazenamento no repositório. Às vezes, isso é conhecido como deduplicação off-line, pois esse processo de deduplicação ocorre mediante a solicitação, e não de maneira incremental à medida que os dados do snapshot são transferidos.

O processo de otimização utiliza muito o processador. O tempo necessário para executar esse trabalho depende de vários fatores. Entre esses fatores estão o tamanho do repositório, a quantidade de dados no repositório, a largura da banda da rede disponível e a carga existente na entrada e na saída do sistema. Quanto mais dados houver no repositório, por mais tempo esse trabalho será executado.

As ações a seguir são substituídas ou canceladas quando o trabalho de otimização do repositório ocorre.

- Trabalho de excluir todos os pontos de recuperação
- Trabalho de cadeia excluir pontos de recuperação
- Trabalho de manter o repositório
- Base do trabalho de excluir pontos de recuperação
- Trabalho de otimizar o repositório

Para etapas sobre como otimizar um repositório de DVM existente, consulte Otimização de um repositório de DVM.

Você pode interromper o trabalho de otimizar o repositório por um período limitado, caso necessário. Para obter mais informações, consulte Interromper ou retomar a otimização do repositório DVM.

Otimização de um repositório de DVM

Você precisa ter um repositório de DVM no seu Core para executar este procedimento.

Você pode executar a deduplicação offline de dados salvos em um repositório de DVM existente. Isso é realizado com a abertura do Trabalho de otimização do repositório.

NOTE: A Quest recomenda executar o trabalho de otimização de repositório apenas depois de ter aumentado o tamanho do cache de deduplicação. Essa ação permite que você recupere o espaço do repositório e use mais efetivamente o cache de deduplicação do DVM.

Execute as etapas deste procedimento para otimizar um repositório de DVM.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Repositories** (Repositórios).

   A página **Repositórios** aparece.
3. No painel Repositórios de DVM, na linha que representa o repositório que você deseja otimizar, clique em (Mais opções) e selecione **Optimize** (Otimizar).

   Um prompt de aviso é exibido pedindo que você confirme a otimização.
4. Clique para confirmar a otimização.

   O trabalho de otimização tem precedência sobre a maioria dos outros trabalhos. Se necessário, você pode interromper um trabalho otimização em andamento. Para obter mais informações sobre a interrupção ou a retomada este trabalho, consulte Interromper ou retomar a otimização do repositório DVM.

Interromper ou retomar a otimização do repositório DVM

Essa tarefa requer que um repositório DVM exista em seu Core, com um trabalho de otimização de repositório em execução.

Ao iniciar o Trabalho de otimização do repositório, o repositório de DVM selecionado é deduplicado. Essa otimização de deduplicação é um trabalho que exige muito do processador e tem a finalidade de economizar espaço no repositório. Para obter mais informações, consulte Sobre a otimização do repositório DVM.

Assim que esse trabalho for iniciado, você poderá interromper o trabalho utilizando o seguinte procedimento. Isso pausa a deduplicação. Se você já tiver interrompido uma otimização, você poderá retomar o processo utilizando esse procedimento.

NOTE: Esse procedimento é aplicável somente a repositórios de DVM e somente quando o trabalho de otimização do repositório tiver sido iniciado.

Complete as etapas desse procedimento para interromper ou retomar um trabalho de otimização do repositório.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Mais) e selecione **Repositories** (Repositórios).

   A página **Repositórios** aparece.

   A página Repositórios de DVM é exibida.
3. Se desejar interromper um trabalho de otimização, faça o seguinte:
   a. Na tabela de resumo de repositórios, na linha que representa o repositório apropriado, clique em (Mais opções) e selecione **Interrupt Optimization Job** (Interromper trabalho de otimização).

   Um prompt de aviso aparece, solicitando a confirmação da interrupção.

   b. Clique para confirmar a interrupção.
4. Se desejar retomar um trabalho de otimização interrompido, faça o seguinte:
   a. Na tabela de resumo de repositórios, na linha representando o repositório apropriado, clique em (Mais opções) e selecione **Optimize** (Otimizar).

   Um prompt de aviso é exibido pedindo que você confirme a otimização.

   b. Na caixa de diálogo, selecione a opção **Continuar o trabalho a partir do ponto da interrupção,** e clique em **Sim**.

   A caixa de diálogo é fechada, e o trabalho de otimização do repositório é retomado a partir do ponto em que ele foi interrompido pela última vez.

Gerenciamento de um repositório de camadas

Um repositório de camadas é um repositório secundário definido no Core no qual pontos de recuperação podem ser relocados de um repositório DVM primário.

Uma vez movidos, os pontos de recuperação são excluídos do repositório DVM primário. O Core continua a gerenciar os pontos de recuperação relocados até serem acumulados e excluídos.

Para organizar os dados de backup em camadas, você deve definir a idade que os pontos de recuperação no repositório DVM devem atingir para começarem a ser organizados em camadas. Isso é feito na página do período de retenção.

Para poder relocar os pontos de recuperação para um repositório de camadas, você deve criar o repositório secundário no Rapid Recovery Core.

O gerenciamento de um repositório de camadas envolve as seguintes operações:

1. **Criar um repositório de camadas**. Para organizar seus pontos de recuperação antigos em camadas no armazenamento secundário, é necessário definir primeiro o repositório de camadas no Rapid Recovery Core Console. No versão 6.2, a organização em camadas é suportada apenas em soluções de deduplicação da série DR que estejam executando o SO 4.0. O repositório requer serviços RDS nativos na solução DR. Para obter mais informações, consulte Noções básicas sobre repositórios. Para obter mais informações sobre a criação de um repositório de camadas, consulte Criar um repositório de camadas.
2. **Conectar a um repositório**. Para obter mais informações sobre como conectar a um repositório de camadas existente, consulte Conectar a um repositório existente.
3. **Definir período de retenção.** Depois de adicionar um repositório de camadas ao Core, defina no período de retenção a idade dos pontos de recuperação que devem ser organizados em camadas do repositório DVM para o repositório de camadas. Você deve configurar a organização em camadas usando uma política de retenção personalizada para máquinas protegidas específicas. Para obter informações sobre

como definir a política de retenção para os pontos de recuperação em camadaspara máquinas protegidas especificas, consulte Personalizar as definições de política de retenção de uma máquina protegida.

4. **Modificando as definições do repositório**. Para obter mais informações sobre como modificar as configurações de um repositório de camadas, consulte Ver ou modificar detalhes do repositório.
5. **Verificando um repositório**. Para obter mais informações sobre a verificação de um repositório, consulte Verificar um repositório.
6. **Excluindo um repositório**. Para obter mais informações sobre a exclusão de um repositório, consulte Excluir um repositório.

Para obter informações sobre como gerenciar um repositório de DVM, consulte Gerenciamento de um repositório de DVM.

Criar um repositório de camadas

Este processo descreve como criar um repositório de camadas no Rapid Recovery Core Console, que pode ser usado como armazenamento secundário apenas para backups de máquinas protegidas no seu Core.

NOTE: No versão 6.2, o único local físico suportado para repositórios de camadas é uma solução de deduplicação da série DR com o SO 4.0 instalado. Definindo sua política de retenção para camada, você pode especificar um período após o qual os pontos de recuperação são relocados do repositório DVM para o repositório de camadas na solução DR. A solução DR inclui serviços RDS (Armazenamento rápido de dados).

Se desejar criar um repositório DVM primário, consulte o tópico Criar um repositório de DVM.

- Para fins de planejamento, 128 GB do volume de armazenamento são reservados por padrão para o dicionário de deduplicação.
- O servidor do Core pode ser um servidor Windows baseado em software devidamente dimensionado que esteja de acordo com os requisitos de sistema operacional e sistema de arquivos do Rapid Recovery. Também pode ser qualquer solução de backup DL diferente do modelo DL1000 ou DL4000. Esses modelos de solução atualmente suportam apenas repositórios DVM.

  NOTE: Para obter informações sobre os requisitos do sistema, consulte o *Guia de requisitos do sistema do Rapid Recovery*.
- Você precisa ter acesso de administrador do dispositivo DR para a qual você quer criar o repositório de camadas.
- Você precisa especificar o nome do host do dispositivo DR.

Em um volume de armazenamento aprovisionado de modo dinâmico, o repositório volume exibe a quantidade de espaço consumido pelo sistema operacional. Um volume aprovisionado de modo tradicional pode exibir todo o conteúdo da unidade que será consumida com dados. Você pode monitorar seus repositórios regularmente usando o relatório do repositório. Isso ajuda você a não ocupar totalmente um volume do repositório. Para obter informações sobre como gerar um relatório do repositório manualmente, consulte Gerar um relatório de Core sob demanda. Para obter informações sobre como automatizar a geração de relatórios de forma permanente, consulte Programar um relatório.

Execute as etapas deste procedimento para criar um repositório de camadas.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Repositórios**.

   A página **Repositórios** aparece.
3. Na parte superior da página, sob o titulo da página Repositórios, clique na seta suspensa ao lado de **Create** (Criar) e selecione **Tiering Repository** (Repositório de camadas).

O **Assistente de criação de repositório** é exibido.

4. Na página **Connection** (Conexão), no campo de texto do Servidor, digite o endereço IP ou o nome do servidor de rede da máquina em que você deseja conectar e adicionar um repositório. Depois, clique em **Avançar**.

   Os serviços RDS são pré-instalados nas soluções DR. Se a máquina contiver um servidor RDS e executar o sistema operacional 4.0, você se conectará a ele. Do contrário, entre em contato com o administrador da solução DR para obter assistência, faça upgrade para a versão correta do servidor RDS e retorne a esta etapa.

5. Na página **Configuração**, digite as informações de configuração do repositório conforme descrito na tabela a seguir e em **Avançar**.

Tabela 34. Configurações da página Configuração

Descrições das configurações disponíveis para configurar o repositório.

Caixa de texto	Descrição
Nome	Insira um nome de exibição para seu repositório. Por padrão, essa caixa de texto consiste na palavra Repositório e um número. Para este core, o nome sugerido corresponde ao atual número de repositórios. Por exemplo, para o primeiro repositório, o nome sugerido é Repositório 1, para o segundo repositório o nome sugerido é Repositório 2, e assim por diante. Se estiver usando repositórios de mais de um tipo de tecnologia, você pode incluir o tipo no nome, como `TieringRepository1`. Nomes de repositório devem conter entre 1 e 40 caracteres alfanuméricos, incluindo espaços. Não use ou .
Comentários	Estas informações são opcionais. Você pode usá-la para descrever o tipo de informações que você salva neste repositório. Por exemplo, "Esse repositório mantém pontos de recuperação obsoletos para todos os servidores Exchange e SQL no domínio da conta". Essas informações podem ser modificadas a qualquer momento.
Grupo de armazenamento e opções de contêiner	Selecione as opções para seu repositório de camadas como segue: • Selecione **Use default storage group and container** (Usar grupo de armazenamento e contêiner padrão) para criar a estrutura para seu repositório em locais padrão. A maioria dos usuários pode selecionar essa opção padrão. • Selecione **Choose an existing storage group and container** (Escolher um grupo de armazenamento e contêiner existentes) se você quiser especificar a estrutura para seu repositório de camadas e selecione os objetos apropriados. Essa opção deve ser usada por usuários avançados que conhecem as opções de grupo de armazenamento e contêiner.

6. Na página **Opções de segurança**, realize um dos procedimentos a seguir:

   • Para restringir o acesso para o Core que você está criando e impedir que outros usuários da rede acessem informações desse repositório, selecione **Proteger este repositório com a sua licença exclusiva**. Depois, clique em **Concluir**.

   Essa etapa é uma precaução opcional. Seu repositório já está protegido, no entanto, o acesso ao Rapid Recovery Core exige autenticação. Essas opções de segurança são aplicadas quando um usuário tenta

abrir esse repositório em um Rapid Recovery Core diferente. Para obter segurança adicional, você pode também aplicar chaves de criptografia no nível do Core para backups em qualquer máquina protegida.

- Para completar o processo de criação de um repositório de camadas sem proteger o repositório com sua licença, desmarque a opção **Proteger esse repositório com sua licença exclusiva**, clique em **Concluir** e, na caixa de diálogo **Aviso de repositório não protegido**, clique em **Sim**.

O **Assistente de criação de repositório** é fechado. As informações do repositório que você especificou geram um trabalho de Criação de repositório, que é iniciado imediatamente. Esse trabalho e a criação do repositório resultante leva alguns minutos para terminar. Quando o trabalho for concluído, um painel de **Repositórios de camadas** aparece na parte inferior da página **Repositório**, mostrando o novo repositório de camadas que você acabou de adicionar.

7. Como opção, você pode monitorar o andamento da tarefa de criação do repositório de camadas. Para obter mais informações, consulte Visualizar tarefas.

Verificar um repositório

O Rapid Recovery permite que você execute uma verificação de diagnóstico de um volume de repositório quando ocorrem erros no Core. Os erros podem ser o resultado do encerramento indevido do Core, da falha de montagem ou desmontagem de um repositório, de uma falha de hardware ou de outros fatores ambientais na pilha IP inferior que podem ser expostos à funcionalidade do Rapid Recovery.

Para todos os tipos de tecnologia de repositório, a verificação executa as seguintes tarefas:

- Verificar repositório
- Montagem do repositório
- Carregamento dos pontos de recuperação do repositório

Somente para os repositórios DVM, a verificação também executa a tarefa "Recalcular cache de deduplicação do repositório".

NOTE: Este procedimento deve ser executado somente para fins de diagnóstico. Por exemplo, execute essa verificação no caso de falha de hardware, desligamento inapropriado do Core ou falha de importação de um repositório.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Repositories** (Repositórios).

   A página **Repositórios** aparece.
3. Para verificar um repositório, em qualquer linha de tabela de resumo para qualquer tipo de tecnologia de repositório, clique em (Mais opções) e selecione **Check** (Verificar).

   A caixa de diálogo **Verificar repositório** é exibida.
4. Na caixa de diálogo **Verificar repositório**, confirme que você entendeu que todas as tarefas ativas associadas a esse repositório serão canceladas e que você deseja prosseguir.

   Os trabalhos ativos são cancelados e o trabalho de verificação do repositório é iniciado.
5. Opcionalmente, para monitorar o status do trabalho, clique no menu suspenso **Running tasks** (Tarefas em execução) na barra de botões e, em seguida, clique no trabalho de manutenção do repositório.

Alteração das configurações do repositório

Este procedimento presume que seu Core tem umrepositório de camadas em funcionamento. Para exibir ou alterar as configurações do repositório para um repositório DVM, consulte Ver ou modificar detalhes do repositório.

Nas configurações do repositório, você pode alterar o nome de exibição, comentários e opção de segurança.

1. No Rapid Recovery Core Console, na barra de ícones, clique em (Mais) e, em seguida, selecione **Repositórios**.
2. Na página **Repositórios**, role a tela até o painel de **Repositórios de camadas**.
3. Na linha que representa o repositório que você deseja atualizar, clique no (Mais opções) e selecione **Definições**.

   O assistente **Editar definições do repositório** será exibido.
4. Na página **Configuração**, você pode alterar as definições descritas na tabela a seguir.

Opção	Descrição
Nome	O nome de exibição do repositório. Por exemplo, Repositório 1.
Comentários	Notas ou uma descrição que você deseja associar a esse repositório.

5. Clique em **Avançar**.
6. Na página **Security Options** (Opções de segurança), para estabelecer a segurança de forma que apenas um Core com o mesmo número de licença desse Core seja permitido se comunicar com o repositório, selecione **Secure this repository with your unique license** (Proteger este repositório com sua licença exclusiva).

   NOTE: Essa etapa é uma precaução opcional. Seu repositório já está protegido, no entanto, o acesso ao Rapid Recovery Core exige autenticação. Essas opções de segurança são aplicadas quando um usuário tenta abrir esse repositório em um Rapid Recovery Core diferente. Para obter segurança adicional, você pode também aplicar chaves de criptografia no nível do Core para backups em qualquer máquina protegida.
7. Clique em **Concluir**.

   As alterações serão aplicadas ao repositório.
8. Se você optou por não adicionar segurança ao seu repositório na etapa anterior, a caixa de diálogo **Unsecure Repository Warning** (Aviso de repositório não protegido) será exibida. Clique em **Yes** (Sim) para confirmar que você não quer proteger o repositório com uma chave de licença.

   O assistente **Editar definições do repositório** será fechado. As alterações feitas nas configurações do repositório serão aplicadas imediatamente.

Conectar a um repositório existente

Para executar este procedimento, você deve ter as credenciais apropriadas do Core original, o local ou caminho de rede, o endereço IP ou o nome do servidor.

CAUTION: Execute este procedimento somente para repositórios e dados para os quais você tem permissão legal para acessar.

Se estiver se conectando a um repositório de camadas, esse repositório deverá estar desconectado do Core que o utilizou anteriormente. Para obter mais informações sobre como desconectar um repositório, consulte o tópico Desconectando um repositório.

Se estiver conectando a um repositório DVM que não está associado a outro Core, nenhum outro pré-requisito se aplica.

Se estiver conectando a um repositório DVM que pertence atualmente a outro Core em funcionamento, prepare-se primeiro para a transferência iminente de propriedade. Os seguintes pré-requisitos se aplicam:

- Se o Core original que contém o repositório estiver funcionando, interrompa temporariamente a proteção das máquinas nesse Core.
- Em seguida, interrompa o serviço do original Core enquanto estiver transferindo a propriedade.
- Depois de conectar o repositório ao novo Core conforme descrito neste procedimento, volte ao Core original. Certifique-se de que todas as máquinas que você continua a proteger tenham um repositório associado a elas.
- Em seguida, reinicie o serviços do Core no Core original.

Para obter mais informações sobre como pausar a proteção, consulte Pausar e retomar a proteção. Para obter mais informações sobre como encerrar e reiniciar o serviço do Core, consulte Reiniciar ou encerrar o serviço Core.

No Rapid Recovery Core Console, é possível conectar a um repositório existente que é atualmente gerenciado em outro Core. Concluir esta conexão altera a propriedade do repositório do Core original para o Core atual. Depois de conectar ao repositório, as informações ficam acessíveis somente para o segundo Core, e não no Core original. O repositório ao qual você conectar deve ser acessível em um local de rede compartilhado ou em um dispositivo de armazenamento acessível para o segundo Core.

Esse processo é útil quando o Core original está inativo e você quer acionar um Core substituto. Se, posteriormente, você quiser alterar a propriedade novamente do segundo Core para um terceiro Core (ou para o original), poderá fazê-lo. As mesmas regras se aplicam.

O Core original que perder o repositório não deve estar em uso. Por exemplo, a máquina deve estar desligada, estar inacessível a uma rede ou os serviços do Core devem ser interrompidos.

Os repositórios de camadas podem ser protegidos com uma licença exclusiva. A seleção dessa configuração de segurança adicional impede que os indivíduos não autorizados consigam transferir o controle do seu repositório para outro repositório. Se você proteger seu repositório com sua licença exclusiva, apenas os administradores com acesso à sua chave de licença poderão conectar ao seu repositório. Para obter mais informações sobre como atualizar as configurações do repositório, consulte o procedimento Alteração das configurações do repositório.

Execute o procedimento a seguir para conectar a um repositório existente.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Mais) e selecione **Repositórios**.

   A página **Repositories** (Repositórios) será exibida.
3. Para conectar a um repositório DVM existente, clique no menu suspenso menu ao lado de **Conectar a existente** e selecione **Repositório DVM**.

   A caixa de diálogo **Connect Existing DVM Repository** (Conectar repositório DVM existente) será exibida.
4. Vá para a etapa 6.
5. Para conectar a um repositório de camadas existente, clique no menu suspenso menu ao lado de **Conectar a existente** e selecione **Repositório de camadas**. Vá para a etapa 7.
6. Na caixa de diálogo **Connect Existing DVM Repository** (Conectar repositório DVM existente), digite as seguintes informações sobre o repositório que deseja abrir e clique em **Connect** (Conectar).

Tabela 35. Opções para abrir o repositório DVM existente

Caixa de texto	Descrição
Caminho	O caminho do repositório (por exemplo, `D:\work\machine` para um caminho local ou `\\10.10.99.155\repositories` para endereço IP ou \\servername\sharename para um caminho de rede).
Nome de usuário	Se o repositório tiver um caminho de rede, insira o nome de usuário para efetuar login no compartilhamento de rede.
Senha	Se o repositório tiver um caminho de rede, insira a senha para efetuar login no compartilhamento de rede.

A caixa de diálogo é fechada e o repositório selecionado é adicionado ao seu Core atual.

7. No **Connect Repository Wizard** (Assistente para conectar repositório), na página **Connection** (Conexão), digite o nome ou endereço IP do servidor da máquina que hospeda o repositório que você deseja conectar a esse Core e clique em **Next** (Avançar).
8. Na página **Cores** do assistente, clique para selecionar o Core apropriado e depois clique em **Next** (Avançar).
9. Na página **Details** (Detalhes) do assistente, revise os detalhes para garantir que o Core selecionado seja apropriado. Para conectar ao Core selecionado, clique em **Finish** (Concluir).

   Se você vir um erro indicando que o repositório selecionado está em uso, faça login no Core e prepare-o para transferir a propriedade de seu repositório para o Core. Pause qualquer proteção existente; pause qualquer replicação existente; aguarde a conclusão dos trabalhos em fila ou cancele-os. Encerre os serviços do Core ou desligue o servidor do Core normalmente e repita este procedimento. Para obter mais informações sobre como pausar a proteção, consulte Pausar e retomar a proteção. Para obter mais informações sobre como pausar a replicação, consulte Pausar e retomar a replicação. Para obter mais informações sobre como encerrar e reiniciar o serviço do Core, consulte Reiniciar ou encerrar o serviço Core.

Ver ou modificar detalhes do repositório

Para ver os detalhes do repositório, o Core deve conter um repositório primeiro. Para obter informações sobre a criação de um repositório DVM ou de camadas, consulte Criar um repositório de DVM ou Criar um repositório de camadas, respectivamente.

No painel **DVM Repositories** (Repositórios DVM), cada repositório DVM adicionado ao Core é exibido.

- Se você clicar em (Expandir), as linhas filho exibem os locais dos dados e metadados do repositório DVM.
- Também é possível (contrair) a visualização.

No painel **Repositórios de camadas**, pelo menos três linhas de dados são usadas para representar cada repositório existente:

- A linha superior é o servidor RDS . Você pode conectar a no máximo três servidores RDS por Core.
- A segunda linha mostra o grupo de armazenamento . Cada servidor RDS pode incluir no máximo cinco grupos de armazenamento.
- A terceira linha lista o repositório de camadas.

Você pode (Expandir) e (Contrair) a exibição nospainéis **Repositórios de camadas** para economizar espaço.

Os detalhes do repositório variam de acordo com o tipo de tecnologia do repositório. Para ver ou modificar detalhes do repositório, use o seguinte procedimento:

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Repositórios**.

   A página **Repositories** (Repositórios) será exibida.
3. As seguintes ações gerais estão disponíveis:

Opção	Descrição
+ Criar	No menu suspenso, selecione o tipo de repositório apropriado para criar um repositório. Você pode selecionar dentre: • Repositório de DVM • Repositório de camadas
Conectar a existente	No menu suspenso, selecione o tipo de repositório para abrir um repositório de outro Core. Este processo altera a propriedade do repositório para o Core. Você pode selecionar dentre: • Repositório de DVM • Repositório de camadas Para obter mais informações, consulte Conectar a um repositório existente.
Atualizar	Atualiza a lista de repositórios mostrados na página.

4. No painel **DVM Repositories** (Repositórios DVM), no menu suspenso (Mais opções) para qualquer repositório DVM , você pode executar as seguintes ações:

Opção	Descrição
Adicionar local de armazenamento	Estenda o repositório existente adicionando um local de armazenamento

Opção	Descrição
	NOTE: Quando estender o volume de um repositório DVM, primeiro pause a proteção. Em seguida estenda o volume e, por fim, retome a proteção. Essa ação impede um erro raro, que pode ocorrer apenas ao estender um volume simultaneamente a uma fase de transferência específica.
Verificar	Executar uma verificação do repositório.
Definições	Visualizar ou modificar as definições do repositório. Essas definições incluem: • Visualizar o nome do repositório • Visualizar ou alterar o máximo de operações simultâneas • Visualizar ou alterar uma descrição do repositório • Ativar ou desativar a desduplicação • Ativar ou desativar a compressão dos dados armazenados no repositório
Otimizar	Executar um trabalho de otimização do repositório. Para obter mais informações, consulte Sobre a otimização do repositório DVM.
Excluir	Excluir um repositório. **CAUTION: Essa opção excluirá completamente o repositório DVM selecionado e todos os dados nele armazenados.**

5. No painel **Tiering Repositories** (Repositórios de camadas), no menu suspenso (Mais opções) para qualquer serviço RDS , você pode executar as seguintes ações:

Opção	Descrição
Alterar credenciais	Permite que você altere a senha associada ao host atualmente selecionado. Esta ação é útil ao alterar a propriedade de um repositório para manter a segurança. **NOTE:** Confirme a nova senha e clique em **Save** (Salvar) para atualizar suas credenciais.

6. Nenhuma ação está disponível para grupos de armazenamento.
7. Nopainel **Repositórios de camadas**, no menu suspenso (Mais opções) para qualquer repositório de camadas, você poderá executar as seguintes ações:

Opção	Descrição
Definições	Abre o Assistente para editar configurações do repositório, onde você pode ver ou modificar as

Opção	Descrição
	configurações do repositório. Essas definições incluem: • Visualizar o servidor ou host • Visualizar ou alterar o nome do repositório • Visualizar ou alterar os comentários do repositório
Verificar	Cancela todas as tarefas ativas do repositório selecionado e, em seguida, executa uma verificação do repositório.
Desconectar	Desmonta o repositório selecionado. **NOTE:** Depois que você se desconectar, poderá se conectar ao repositório novamente mais tarde usando o recurso **Connect to Existing** (Conectar a existente) na parte superior da página de repositórios.
Excluir	Excluir um repositório. **CAUTION: Essa opção excluirá completamente o repositório selecionado e todos os dados nele armazenados.**

Desconectando um repositório

Este procedimento presume que seu Core tem um repositório de camadas em funcionamento.

Na página **Repositórios**, você pode desconectar um repositório já existente. Esse processo não excluir dados do repositório. Ele simplesmente desmonta a conexão atual com o repositório e o respectivo conteúdo. Isso é útil, por exemplo, em uma situação na qual você deseja se conectar ao repositório de outro Core.

Execute este procedimento para desconectar um repositório de camadas em funcionamento.

1. Na barra de ícones do Rapid Recovery Core Console, clique no (Mais) e, em seguida, clique no **Repositórios**.
2. Na página **Repositórios**, na linha que representa o repositório que você deseja desconectar, clique no (Mais opções) e selecione **Desconectar**.

   A caixa de diálogo **Desconectar repositório** será aberta.
3. Clique para confirmar a ação para desconectar o repositório existente.

   O repositório será desconectado, e a página **Repositórios** será atualizada. O repositório não aparecerá mais na lista de repositórios atualmente disponíveis.

Para reconectar ao repositório, consulte o procedimento Conectar a um repositório existente.

Excluir um repositório

Execute as etapas deste procedimento para excluir um repositório.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Repositories** (Repositórios).

   A página **Repositories** (Repositórios) será exibida.
3. Na tabela de resumo dos repositórios, na linha que representa o repositório que você deseja excluir, clique em (Mais opções) para expandir o menu suspenso e selecione **Delete** (Excluir).

   Aparece uma mensagem de aviso pedindo para confirmar a exclusão.

   CAUTION: Quando um repositório é excluído, os dados contidos nele são descartados e não podem ser recuperados.
4. Clique em **Sim** para confirmar a exclusão do repositório.

Gerenciar privacidade

Esta seção descreve as informações pessoais que o Rapid Recovery pode coletar, para que essas informações são usadas e como você pode controlar a privacidade dos dados.

Os tópicos são:

- Conformidade com a regulamentação de proteção de dados gerais
- Como o Rapid Recovery usa informações pessoais
- Restrições de chave de licença não telefônica
- Obtenção e uso de licenças de telefone não residencial

Conformidade com a regulamentação de proteção de dados gerais

A regulamentação geral de proteção de dados (GDPR) é uma legislação criada para fortalecer e unificar a proteção de dados para todos os indivíduos dentro da União Europeia (UE). Também aborda a exportação de dados pessoais para fora da UE, o que a torna relevante para fabricantes de software nos EUA e em outros países. Atualiza as regras que regem o tratamento de dados pessoais do indivíduo. A GDPR é amplamente adotada em todo o setor de software.

Para estar em conformidade com a GDPR, a coleta de informações de identificação pessoal (PII) pelo Rapid Recovery Core foi considerada com atenção. A coleta de dados foi simplificada e as informações coletadas estão claramente documentadas.

Ao instalar o Rapid Recovery Core, executar o utilitário de recuperação e atualização (RUU) ou executar a ferramenta de coleta de informações, você fornece uma descrição das informações que o Rapid Recovery coleta e dos nossos objetivos para a coleta de informações.

Se você aceitar o uso declarado de dados pessoais, você pode associar uma licença (em execução no modo "telefone residencial" padrão) ao seu Core. Se você optar por recusar a utilização dos dados pessoais descritos na política de privacidade, você deve solicitar uma licença especial "telefone não residencial". Depois de receber essa licença e associá-la com seus núcleos, suas informações de identificação pessoal não serão usadas e determinadas funções (atualização automática e permissão de integração entre o núcleo e o Portal de proteção de dados) são desativadas.

Independentemente da opção de privacidade que você selecionou durante a instalação, da configuração geral do Core **Concordar com uso de dados pessoais**, você pode alterar essa configuração. Para alternar entre os modos de telefone residencial e não-residencial, em qualquer sentido, você deve ter acesso à licença apropriada.

Para obter mais informações sobre a GDPR, consulte o site da Regulamentação geral de proteção de dados da UE, em http://www.eugdpr.org/eugdpr.org.html.

Para obter mais informações sobre como gerenciar sua privacidade, consulte os seguintes tópicos no *Guia do usuário do Rapid Recovery*:

- Determinadas regras de negócio se aplicam quando se alterna entre o modo de telefone residencial e o modo de telefone não residencial usando a configuração geral de **Concordar com o uso de dados pessoais**. Para obter mais informações, consulte o tópico "Configurar definições gerais do Core".
- Para ver quais informações que o Rapid Recovery coleta, em que circunstâncias e por que as informações são coletadas, consulte "Como o Rapid Recovery usa as informações pessoais".
- Para ver quais funções você pode executar ao utilizar uma licença de telefone não residencial, consulte o tópico "Restrições da licença de telefone não residencial".
- Para baixar uma licença de telefone não residencial, faça login no Portal de licenças do Rapid Recovery. Clique em **Licenciamento** no menu de navegação e selecione **Chave de licença** no menu suspenso no canto superior direito.
- Para obter mais informações sobre como obter uma licença em modo de telefone não residencial, consulte o tópico "Obtenção e uso de chaves de telefone não residencial."

Como o Rapid Recovery usa informações pessoais

Conforme descrito em Gerenciar licenças, o Rapid Recovery usa três tipos de licenças de software: assinatura, permanente e licenças de avaliação.

Existem dois modos em que as licenças podem ser usadas:

- **Modo de telefone residencial.** Todas as licenças são emitidas de modo de telefone residencial, a menos que solicitado de outra forma. Se você registrar uma licença de telefone residencial com o Portal de licenças do Rapid Recovery, o Rapid Recovery coleta algumas informações de identificação pessoal (PII). As informações coletadas e como elas são usadas são descritas abaixo.
- **Modo de telefone não residencial.** Mesmo quando conectado à Internet, se você obter e registrar uma licença telefônica não residencial, o Rapid Recovery não compartilhará suas informações de identificação pessoal (PII). O uso desse modo impede que sejam executadas determinadas funções, como descrito no tópico Obtenção e uso de licenças de telefone não residencial.

As licenças de assinatura só podem ser usadas no modo de telefone residencial. A licença perpétua e a licença de avaliação podem ser usadas no modo de telefone residencial ou no modo não residencial.

Se você registrar uma licença de telefone residencial, você dá à Rapid Recovery permissão para coletar as seguintes informações de identificação pessoal PII:

- Os endereços IP e nomes de hosts em que ele funciona ou interage com o Rapid Recovery Core e Agent.
- Os endereços de e-mail associados às licenças do Rapid Recovery; e
- O consumo de licenças em comparação com a quantidade de licenças no grupo de licenças.

Essa informação é enviada à Quest Software Inc. com as seguintes finalidades:

- Para aplicar devidamente os termos da licença apropriada no produto;
- Para fornecer suporte ao cliente; por exemplo, quando você executar a Ferramenta de coleta de informações, os logs e os dados de diagnóstico que você especificar serão reunidos em uma pasta local

para serem enviados à Quest, ou podem ser carregados para o Amazon, acessível apenas para o Suporte de proteção de dados da Quest.

- Para notificar os usuários das atualizações disponíveis (se as configurações de atualização no Core especificarem uma opção diferente de **Nunca verificar as atualizações**); e
- Para permitir a comunicação entre o Core e o Portal de proteção de dados. Essa comunicação pode ser habilitada ou desabilitada usando as configurações do **Portal de proteção de dados** no Core. Esse portal permite aos usuários licenciados com um contrato de suporte atual monitorar a integridade dos Cores e das máquinas protegidas, gerenciar vários Cores e gerar relatórios sob demanda para os Cores e máquinas protegidas relevantes.

Você tem o direito de escolher se quer ou não compartilhar essas informações com a Quest. Em primeiro lugar, ao instalar ou atualizar o Rapid Recovery Core, você pode optar por compartilhar essa informação na página **Política de privacidade** do instalador. Além disso, se você decidir não compartilhar informações com a Quest, você pode alterar a configuração geral do Core **Aceitar o uso de dados pessoais**. Ao alterar essa configuração, será solicitado que você insira uma licença. Se você inserir uma licença de telefone não residencial, a atualização automática será desabilitada, assim como a sua conexão com o Portal de proteção de dados.

Para obter mais recursos sobre esse tópico, consulte os seguintes links relacionados.

- Para obter mais informações sobre as funções que você não pode executar quando usar o modo de telefone não residencial, consulte o tópico Restrições de chave de licença não telefônica.
- Para obter mais informações sobre a obtenção de uma licença que usa o modo de telefone não residencial, entre em contato com a equipe de licenciamento da Quest pelo formulário da web, conforme descrito no tópico Obtenção e uso de licenças de telefone não residencial.
- Para obter mais informações sobre como alterar as configurações gerais, incluindo o compartilhamento de informações de identificação pessoal, consulte o tópico Configurar definições gerais do Core.
- Para obter mais informações sobre a exibição de informações de licenças para uma única máquina protegida, consulte Visualizar informações de licença em uma máquina.
- Para obter mais informações sobre como inserir a chave de licença ou informações do arquivo (por exemplo, para atualizar uma licença perpétua de telefone residencial para uma licença perpétua de telefone não residencial, consulte Atualização ou alteração de uma licença.
- Para obter mais informações sobre os tipos de licenças disponíveis, consulte Gerenciar licenças.
- Para obter mais informações sobre como entrar em contato com o servidor do portal de licenças, consulte Contatar o servidor do Portal de licenças do Rapid Recovery.
- Para obter mais tópicos sobre o gerenciamento de licenças, consulte o *Guia do usuário do portal de licenças do Rapid Recovery*.

Restrições de chave de licença não telefônica

Registrar uma licença do Rapid Recovery no modo de telefone residencial impede o Core de compartilhar suas informações pessoais. Isso inclui o endereço de e-mail, endereços IP e informações de consumo da licença.

Depois de registrar uma licença de telefone não residencial, não será possível:

- Exibir as informações do servidor de licenças na página **Configurações** do Core Console (pois o Core não está autorizado a se comunicar com o Portal de licenças do Rapid Recovery).
- Gerenciar o consumo de licenças do Core Console.
- Enviar informações ao Suporte de proteção de dados da Quest a partir da ferramenta de coleta de informações do Rapid Recovery.
- Monitorar a integridade dos Cores e das máquinas protegidas, gerenciar vários Cores e gerar relatórios sob demanda para as máquinas relevantes em vários Cores do Portal de proteção de dados.
- Usar o recurso de atualização automática para atualizar uma nova versão do Rapid Recovery Core (seu núcleo não é notificado que novas versões estão disponíveis).
- Usar o recurso de atualização automática para atualizar diretamente máquinas Linux protegidas usando gerenciadores de pacotes, como yum, zypper ou apt (você ainda pode fazer download de um pacote de instalação de uma máquina Linux acessível pela Internet e mover arquivos de instalação para o computador seguro manualmente).

Obtenção e uso de licenças de telefone não residencial

Se você tiver obtido a licença de telefone não residencial antes de atualizar ou instalar o Rapid Recovery Core versão 6.2, transfira a licença para o servidor do Core. Ao executar o instalador, na página **Política de privacidade**, selecione a opção de recusar o compartilhamento de dados e, quando solicitado, registre a licença de telefone não residencial.

Se o Rapid Recovery Core versão 6.2 já estiver registrado com uma chave de telefone residencial, acesse as configurações gerais no Core, selecione a opção de recusar o compartilhamento de dados e, quando solicitado, registre a chave de telefone não residencial.

Para obter mais informações ou instruções passo a passo sobre como alterar as configurações gerais de seu Core, consulte o tópico Configurar definições gerais do Core.

Para obter mais informações sobre o gerenciamento de licenças do Rapid Recovery Core, consulte Gerenciar licenças.

Conclua as etapas neste procedimento para entrar em contato com a equipe de licenças da Quest a fim de obter uma licença de telefone não residencial.

1. Em um navegador da web, navegue até o site de assistência de licenças da Quest em https://support.quest.com/contact-us/licensing.
2. No menu suspenso **Como podemos ajudá-lo**, selecione **Obter uma licença para o meu produto**.
3. No menu suspenso **Selecionar produtos**, selecione **Rapid Recovery**.
4. No menu suspenso **Versão do produto**, selecione a opção adequada.

   Por exemplo, selecione **6.2**.
5. Na seção Informações de contato do formulário, adicione as informações conforme descrito na tabela a seguir.

Nome do campo	Descrição	Campo obrigatório
E-mail comercial	Digite o endereço de e-mail para o qual você deseja que a equipe de licenças da Quest responda. Se você tiver acesso à conta de e-mail	Sim

Nome do campo	Descrição	Campo obrigatório
	associada à sua licença do Rapid Recovery, use esse endereço para uma resposta mais rápida.	
Nome do contato	Digite o seu nome	Sim
Sobrenome do contato	Digite o seu sobrenome	Sim
Nome da empresa	Digite o nome da empresa associada a sua licença do Rapid Recovery	
Federal dos EUA	Selecione se a licença está relacionada a uma organização federal dos EUA.	Não
País	Selecione o seu país.	Sim
Número de telefone	Digite seu número de telefone, incluindo o código de área. Se estiver fora dos EUA, inclua o código de país.	Sim
Número da licença (se disponível)		Não
Chave de licença (se disponível)	Chaves de licença foram usadas até o AppAssure 5.4.1. Isso geralmente é uma cadeia de 30 caracteres (6 grupos de 5 números e letras alfabéticas maiúsculas, separadas por hífens).	Não
ID do computador	O nome do computador Core registrado.	Não
Etiqueta de serviço (se disponível)	Digite a etiqueta de serviço, se disponível.	Não
Detalhes da solicitação de licença	Indique neste campo que, pela GDPR, você deseja uma licença de telefone não residencial para substituir sua licença de telefone residencial com o objetivo de proteger suas informações de identificação pessoal (PII). **NOTE:** Ao fazer essa solicitação, você concorda que irá excluir a chave de licença de telefone residencial ao receber e registrar a chave de telefone não residencial. Você também concorda que não irá compartilhar essa chave.	Sim
Arquivo de licença	Se você tiver uma licença de telefone residencial, você pode anexar o arquivo de licença.	Não

6. Para validar a solicitação e enviar o formulário, selecione**Não sou um robô** e, em seguida, clique em **Avançar**.

   O formulário é enviado e você receberá uma mensagem de e-mail com um número de solicitação de serviço (SR).

Ao receber um arquivo de licença de telefone não residencial, carregue-o no servidor do Core para registrar a licença. Para obter mais informações, consulte Atualização ou alteração de uma licença.

Criptografia

Esta seção descreve o processo de proteger dados no seu ambiente usando chaves de criptografia e configurações de criptografia de instantâneo no nível do computador.

Noções básicas sobre chaves de criptografia

O Rapid Recovery pode criptografar dados de snapshot de todos os volumes em qualquer repositório usando chaves de criptografia que você define e gerencia a partir do Core Console.

Em vez de criptografar todo o repositório, o Rapid Recovery permite especificar uma chave de criptografia para uma ou mais máquinas protegidas em um único Rapid Recovery Core. Cada chave de criptografia ativa cria um domínio de criptografia. Não há limite para o número de chaves de criptografia que podem ser criadas no Core.

Em um ambiente multilocatário (quando um único Core hospeda vários domínios de criptografia), os dados são particionados e deduplicados dentro de cada domínio de criptografia. Por isso, a Quest recomenda usar uma única chave de criptografia para várias máquinas protegidas se você deseja maximizar os benefícios da deduplicação entre um conjunto de máquinas protegidas.

Você também pode compartilhar chaves de criptografia entre Cores usando um de três métodos. Um método é exportar uma chave de criptografia como um arquivo a partir de um Rapid Recovery Core e importá-la para outro Core. Um segundo método é arquivar dados protegidos com uma chave de criptografia e importar esses dados arquivados para outro Rapid Recovery Core. O terceiro método é replicar os pontos de recuperação de uma máquina protegida usando uma chave de criptografia. Depois que você replica máquinas protegidas, as chaves de criptografia usadas no Core de origem aparecem como chaves de criptografia replicadas no Core de destino.

Em todos os casos, depois de importada, qualquer chave de criptografia aparece no Core com o estado Bloqueado. Para acessar dados de uma chave de criptografia bloqueada, é necessário desbloqueá-la. Para obter informações sobre importação, exportação, bloqueio ou desbloqueio de chaves de criptografia, consulte o tópico Gerenciar chaves de criptografia.

Os principais conceitos e considerações sobre segurança incluem:

- A criptografia é feita usando o padrão AES (Advanced Encryption Standard) de 256 bits no modo CBC (Cipher Block Chaining), que é compatível com SHA-3.
- A deduplicação opera dentro de um domínio de criptografia para garantir a privacidade.
- A criptografia é realizada sem impacto no desempenho.
- Você pode aplicar uma única chave de criptografia a qualquer número de máquinas protegidas, mas uma máquina protegida só pode ter apenas uma chave de criptografia aplicada a qualquer momento.
- Você pode adicionar, remover, importar, exportar, modificar e excluir chaves de criptografia que estão configuradas no Rapid Recovery Core.

> **CAUTION: O** Rapid Recovery **obtém um novo snapshot sempre que você aplicar uma chave de criptografia a uma máquina protegida. Um novo snapshot também é acionado quando você desassocia uma chave de criptografia de uma máquina protegida.**

As chaves de criptografia geradas a partir do Rapid Recovery Core são arquivos de texto que contêm quatro parâmetros, descritos na tabela a seguir:

Tabela 36. Componentes de uma chave de criptografia

Componente	Descrição
Nome	Este valor é equivalente ao nome atribuído ao adicionar uma chave no Rapid Recovery Core Console.
Chave	Este parâmetro consiste em 107 caracteres do alfabeto inglês, numéricos e matemáticos gerados aleatoriamente.
ID	O ID da chave consiste em 26 caracteres do alfabeto inglês, maiúsculos e minúsculos, gerados aleatoriamente.
Comentários	O comentário contém o texto da descrição da chave inserido quando a chave foi criada.

Criptografar os dados em transporte em uma rede

O Rapid Recovery Coreversão 6.2 inclui um novo recurso de criptografia: agora é possível criptografar todos os dados em transporte por uma rede intermediária, a Quest recomenda a ativação desta configuração de criptografia quando os dados entre o Core e as máquinas protegidas (ou entre dois núcleos, como para replicação) devem trafegar por redes públicas ou não confiáveis, como a Internet.

Embora haja apenas um pequeno custo envolvido na ativação desta criptografia, se os seus Cores e as máquinas protegidas estiverem dentro dos limites de uma rede local (LAN), você pode desabilitar essa opção com segurança.

Leia as seguintes informações e ajuste o seu ambiente de acordo.

Por padrão, ao proteger uma máquina usando o Assistente de proteção de máquina ou o Assistente de proteção de diversas máquinas, a criptografia dos dados em transporte por uma rede é habilitada. Se você selecionar opções avançadas para o assistente, você poderá visualizar as opções de criptografia. Na página de criptografia do assistente, se preferir, você pode desmarcar a opção **Criptografar os dados em transporte por uma rede**.

NOTE: Se você não selecionar as opções avançadas no assistente, a criptografia de dados em transporte é ativada mesmo assim.

Depois de concluir o assistente de proteção relevante, você sempre poderá ativar ou desativar a criptografia para dados de instantâneo, alterando as configurações de transferência no nível da máquina. Selecione a máquina protegida, clique em **Configurações** e, em Configurações de transferência, para a configuração **Criptografar os dados de instantâneo**, selecione **Sim** para habilitar a criptografia ou **Não** para desativar a criptografia durante o transporte. Para obter detalhes específicos, consulte Visualização e modificação das definições de máquina protegida no *Guia do usuário do Rapid Recovery*.

Aplicar ou remover chaves de criptografia

Você pode proteger os dados protegidos no seu Core a qualquer momento definindo uma chave de criptografia e aplicando-a a uma ou mais máquinas protegidas no seu repositório. Você pode aplicar uma única chave de

criptografia a qualquer número de máquinas protegidas, mas uma máquina protegida só pode usar uma única chave de criptografia a qualquer momento.

O escopo da deduplicação no Rapid Recovery é limitado às máquinas protegidas que usam o mesmo repositório e a mesma chave de criptografia. Por isso, para maximizar o valor da deduplicação, a Quest recomenda aplicar uma única chave de criptografia a tantas máquinas protegidas quanto seja viável. No entanto, não há limite para o número de chaves de criptografia que podem ser criadas no Core. Portanto, se a conformidade legal, as regras de segurança, as políticas de privacidade ou outras circunstâncias o exigirem, você pode adicionar e gerenciar qualquer número de chaves de criptografia. Nesse caso, você pode aplicar cada chave a apenas uma máquina protegida ou a qualquer conjunto de máquinas no seu repositório.

Quando você aplica uma chave de criptografia a uma máquina protegida ou separa uma chave de criptografia de uma máquina protegida, o Rapid Recovery cria uma nova imagem de base para aquela máquina no próximo snapshot programado ou forçado. Os dados armazenados nessa imagem de base (e em todos os snapshots incrementais subsequentes criados enquanto a chave de criptografia está aplicada) são protegidos por um padrão de criptografia avançado de 256 bits. Não existem métodos conhecidos para violar esse método de criptografia.

Se você alterar o nome ou a frase de acesso para uma chave de criptografia existente atualmente utilizada para uma máquina protegida, no próximo snapshot programado ou forçado, o Rapid Recovery Core captura e reflete as propriedades atualizadas da chave. Os dados armazenados nessa imagem (e em todos os snapshots incrementais subsequentes criados enquanto a chave de criptografia está aplicada) são protegidos por um padrão de criptografia avançado de 256 bits. Não existem métodos conhecidos para violar esse método de criptografia.

Depois que uma chave de criptografia é criada e aplicada a uma máquina protegida, há dois conceitos envolvidos na remoção dessa criptografia. O primeiro é desassociar a chave da máquina protegida. Opcionalmente, depois que a chave de criptografia é desassociada de todas as máquinas protegidas, é possível excluí-la do Rapid Recovery Core.

Esta seção inclui os seguintes tópicos:

- Associar uma chave de criptografia a uma máquina protegida
- Aplicar uma chave de criptografia a partir da página Máquinas protegidas
- Desassociar uma chave de criptografia de uma máquina protegida

Associar uma chave de criptografia a uma máquina protegida

Você pode aplicar uma chave de criptografia a uma máquina protegida usando um dos dois métodos:

- **Como parte da proteção de uma máquina.** Ao usar esse método, você pode aplicar a criptografia a uma ou várias máquinas simultaneamente. Esse método permite adicionar uma nova chave de criptografia, ou aplicar uma chave existente às máquinas selecionadas.

  Para usar a criptografia ao definir a proteção para uma máquina pela primeira vez, você deve selecionar as opções avançadas no Assistente de proteção de máquinas relevante. Essa seleção adiciona uma página de criptografia ao fluxo de trabalho do assistente. Nessa página, selecione **Enable encryption** (Ativar criptografia) e, em seguida, selecione uma chave de criptografia existente ou especifique parâmetros para uma nova chave. Para obter mais informações, consulte Proteção de uma máquina ou Sobre como proteger diversas máquinas, respectivamente.

- **Modificando as definições de configuração de uma máquina.** Esse método aplica uma chave de criptografia a uma máquina protegida de cada vez. Há duas abordagens para modificar as definições de configuração de uma máquina na UI do Rapid Recovery:

  - Modificar os parâmetros de configuração de uma máquina protegida específica. A chave de criptografia que você quer usar para essa abordagem já precisa existir no Rapid Recovery Core, ser um tipo de chave universal e precisa estar no estado desbloqueado. A criptografia é parte das

Definições gerais. Para obter mais informações, consulte Visualização e modificação das definições de máquina protegida.

- Clique no ícone  **Não criptografado** na página Máquinas protegidas. Usando esta abordagem, você pode criar e aplicar uma nova chave de criptografia ou atribuir uma chave universal desbloqueada existente à máquina protegida especificada. Para obter mais informações, consulte Aplicar uma chave de criptografia a partir da página Máquinas protegidas.

Aplicar uma chave de criptografia a partir da página Máquinas protegidas

Assim que uma chave de criptografia for adicionada a um Rapid Recovery Core, ela poderá ser utilizada para qualquer número de máquinas protegidas.

Se você selecionar uma chave de criptografia durante a proteção inicial de uma ou mais máquinas, a chave será automaticamente aplicada às máquinas que você proteger usando esse assistente. Nesses casos, este procedimento não é necessário.

Execute esse procedimento:

- Se desejar aplicar uma chave de criptografia desbloqueada universal existente a qualquer máquina protegida em seu Core.
- Se tiver acabado de adicionar uma nova chave de criptografia utilizando o processo descrito no tópico Adicionar uma chave de criptografia e desejar aplicar essa chave a uma máquina protegida.
- Se a criptografia já tiver sido aplicada a uma máquina protegida em seu Core, mas você desejar alterar a chave para uma chave desbloqueada universal diferente disponível em seu Core.

CAUTION: Depois de aplicar uma chave de criptografia a uma máquina protegida, o Rapid Recovery **obtém uma nova imagem de base para essa máquina no próximo snapshot programado ou forçado.**

1. Navegue até o Rapid Recovery Core e clique em **Máquinas protegidas**.

   A página **Máquinas protegidas** é exibida, listando todas as máquinas protegidas por esse Core. Um cadeado aberto  aparece para as máquinas que não têm uma chave de criptografia aplicada. Um cadeado fechado  indica que a máquina protegida está com a criptografia aplicada.

2. No painel Máquinas protegidas, clique no ícone de cadeado da máquina protegida que deseja configurar.

   A caixa de diálogo **Configuração de criptografia** é exibida.

3. Execute um dos seguintes:

   - Se desejar aplicar uma chave de criptografia existente a essa máquina, selecione **Criptografar dados utilizando criptografia com base no Core com uma chave existente** e selecione a chave apropriada no menu suspenso. Clique em **OK** para confirmar.
   - Se desejar alterar uma chave de criptografia existente para uma chave desbloqueada universal diferente, selecione **Criptografar dados utilizando criptografia com base no Core com uma nova chave** e selecione a chave apropriada no menu suspenso. Clique em **OK** para confirmar.
   - Se deseja criar uma nova chave de criptografia e aplicá-la a essa máquina protegida, selecione **Criptografar dados utilizando criptografia com base no Core com uma nova chave**. Em seguida, insira os detalhes da chave, como descrito na tabela a seguir.

Tabela 37. Detalhes de nova chave de criptografia

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia. Os nomes de chaves de criptografia devem ter entre 1 e 64 caracteres alfanuméricos. Não use caracteres proibidos ou frases proibidas.
Descrição	Insira um comentário descritivo para a chave de criptografia. Essas informações aparecem no campo Descrição ao visualizar uma lista de chaves de criptografia no Rapid Recovery Core Console. As descrições podem conter até 254 caracteres. A melhor prática é evitar o uso de caracteres proibidos e frases proibidas.
Senha	Insira a frase de acesso usada para controlar o acesso. A melhor prática é evitar o uso de caracteres proibidos. Armazene a frase de acesso em um local seguro. O Quest Support não consegue recuperar uma frase de acesso. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais máquinas protegidas, você não poderá recuperar os dados caso perca a frase de acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso. Usado para confirmar a entrada da frase de acesso.

4. Clique em **OK**.

   A caixa de diálogo é fechada. A chave de criptografia que você especificou será aplicada às cópias de segurança futuras dessa máquina protegida e o cadeado agora aparece fechado.

   Opcionalmente, se quiser que a chave de criptografia seja aplicada imediatamente, force um snapshot. Para obter mais informações, consulte Forçar um snapshot.

> **CAUTION: O** Rapid Recovery **usa a criptografia AES de 256 bits no modo encadeamento de blocos de codificação (CBC) com chaves de 256 bits. Embora o uso de criptografia seja opcional, a** Quest **recomenda que você estabeleça uma chave de criptografia e que proteja a frase de acesso definida. Armazene a frase de acesso em um local seguro, pois ela é essencial para a recuperação dos dados. Sem a frase de acesso, não é possível executar a recuperação dos dados.**

Desassociar uma chave de criptografia de uma máquina protegida

Depois que uma chave de criptografia é aplicada a uma máquina protegida, todos os dados de snapshot subsequentes armazenados no Rapid Recovery Core são criptografados.

Você pode desassociar uma chave de criptografia de uma máquina protegida. Essa ação não descriptografa as cópias de segurança existentes, mas gera uma nova imagem de base da máquina no momento do próximo snapshot programado ou forçado.

> **NOTE:** Se desejar remover uma chave de criptografia do Core, conforme descrito no tópico Remover uma chave de criptografia, deverá primeiramente desassociar essa chave de criptografia de todas as máquinas protegidas.

Realize este procedimento para desassociar uma chave de criptografia de uma máquina protegida específica.

1. Navegue até o Rapid Recovery Core e clique em **Máquinas protegidas**.

A página Máquinas protegidas é exibida, listando todas as máquinas protegidas por esse Core. Um cadeado aberto aparece para as máquinas que não têm uma chave de criptografia aplicada. Um cadeado fechado indica que a máquina protegida está com a criptografia aplicada.

2. No painel Máquinas protegidas, clique no ícone **Encrypted** (Criptografado) da máquina protegida que deseja configurar.

   A caixa de diálogo **Configuração de criptografia** é exibida.

3. Selecione **Criptografar dados usando criptografia baseada em Core com uma chave existente** e, no menu suspenso, selecione **(Nenhum)** e clique em **OK**.
4. Se desejar remover a chave de criptografia do Rapid Recovery Core, repita este procedimento em todas as máquinas protegidas que usam essa chave. Em seguida, execute o procedimento descrito no tópico Remover uma chave de criptografia.

Gerenciar chaves de criptografia

Para gerenciar chaves de criptografia do Rapid Recovery Core, na barra de ícones, clique em (Mais) e selecione **Chaves de criptografia**. A página **Chaves de criptografia** é exibida. Para cada chave de criptografia adicionada ao Rapid Recovery Core (caso alguma já tenha sido definida), você vê as informações descritas na tabela a seguir.

Tabela 38. Informações sobre cada chave de criptografia

Elemento de UI	Descrição
Selecione um item	Para cada chave de criptografia, você pode marcar a caixa de seleção para realizar ações na lista de opções do menu acima da tabela.
Nome	O nome associado à chave de criptografia.
Impressão digital	Esse parâmetro é uma cadeia de 26 caracteres alfabéticos de letras maiúsculas e minúsculas em inglês geradas aleatoriamente que ajuda a identificar exclusivamente cada chave de criptografia.
Tipo	Tipo descreve o ponto de origem de uma chave de criptografia e a possibilidade de ser aplicada. Uma chave de criptografia conter um de dois tipos possíveis: **Universal**. O tipo Universal é a condição padrão quando você cria uma chave de criptografia. Uma chave com um tipo Universal, combinada com um estado Desbloqueado, indica que a chave pode ser aplicada a uma máquina protegida. Você não pode bloquear manualmente um tipo de chave universal; em vez disso, você deve primeiro alterar o tipo conforme descrito no procedimento Como alterar tipos de chave de criptografia. **Replicação**. Quando uma máquina protegida em um Core de origem tem criptografia ativada e os pontos de recuperação dessa máquina são replicados em um Core de destino, qualquer chave de criptografia usada na origem é exibida automaticamente no Core de destino com um tipo de Replicação. O estado padrão após o recebimento de uma chave replicada é bloqueado. Você pode desbloquear uma chave de criptografia com um tipo de Replicação fornecendo a frase de acesso. Caso uma chave tenha um tipo Desbloqueado, você pode bloqueá-la manualmente. Para obter mais informações, consulte o tópico Desbloquear uma chave de criptografia.

Elemento de UI	Descrição
Estado	O estado indica se uma chave de criptografia pode ser usada. Dois estados possíveis incluem: • **Desbloqueado**. Um estado Desbloqueado indica que a chave pode ser usada imediatamente. Por exemplo, você pode criptografar instantâneos para uma máquina protegida ou realizar a recuperação de dados de um ponto de recuperação replicado no Core de destino. • **Bloqueado**. Um estado Bloqueado indica que a chave não pode ser usada até que seja desbloqueada, fornecendo a palavra-chave. Bloqueado é o estado padrão para uma chave de criptografia importada ou replicada recentemente. Quando o estado de uma chave de criptografia é bloqueado, ela deve ser desbloqueada para ser usada. Caso você tenha desbloqueado anteriormente uma chave de criptografia bloqueada e a duração de desbloqueio tenha expirado, o estado muda de desbloqueado para bloqueado. Depois que a chave é bloqueada automaticamente, você deve desbloquear a chave novamente para poder usá-la. Para obter mais informações, consulte o tópico Desbloquear uma chave de criptografia.
Descrição	A descrição é um campo opcional que é recomendado para fornecer informações úteis sobre a chave de criptografia como seu uso pretendido ou uma dica de senha.

No nível superior do painel Chaves de criptografia, você pode adicionar uma chave de criptografia ou importar uma chave usando um arquivo exportado de outro Rapid Recovery Core. Você também pode excluir chaves selecionadas na tabela de resumo.

Desde que haja uma chave de criptografia para um Core, você pode gerenciar as chaves existentes editando as propriedades de nome ou descrição, alterando a frase de acesso, desbloqueando uma chave de criptografia bloqueada ou removendo a chave do Rapid Recovery Core. Você também pode exportar uma chave para um arquivo, que pode ser importado para outro Rapid Recovery Core.

Quando você adiciona uma chave de criptografia na página **Chaves de criptografia**, a chave é exibida na lista de chave de criptografia, mas não é aplicada a uma máquina protegida específica. Para obter informações sobre como aplicar uma chave de criptografia criada no painel **Chaves de criptografia** ou para excluir uma chave por completo do Rapid Recovery Core, consulte Aplicar ou remover chaves de criptografia.

No painel **Chaves de criptografia**, você pode gerenciar a segurança dos dados de backup no Core de qualquer máquina protegida no repositório fazendo o seguinte:

- Adicionar uma chave de criptografia
- Importar uma chave de criptografia
- Desbloquear uma chave de criptografia
- Editar uma chave de criptografia
- Alterar a frase de acesso de uma chave de criptografia
- Exportar uma chave de criptografia
- Remover uma chave de criptografia
- Como alterar tipos de chave de criptografia

Adicionar uma chave de criptografia

O Rapid Recovery usa a criptografia AES de 256 bits no modo encadeamento de blocos de codificação (CBC) com chaves de 256 bits. Embora o uso de criptografia seja opcional, a Quest recomenda que você estabeleça uma chave de criptografia e que proteja a frase de acesso definida.

CAUTION: Armazene a frase de acesso em um local seguro. Sem uma frase de acesso, não é possível recuperar os dados dos pontos de recuperação criptografados.

Depois de definir uma chave de criptografia, você pode usá-la para proteger seus dados. As chaves de criptografia podem ser usadas em qualquer número de máquinas protegidas.

Esta etapa descreve como adicionar uma chave de criptografia no Console do Rapid Recovery Core. Esse processo não aplica a chave a nenhuma máquina que esteja sendo protegida atualmente no Core. Você também pode adicionar uma chave de criptografia durante o processo de proteção de uma máquina. Para obter mais informações sobre como adicionar criptografia como parte da proteção de uma máquina, consulte Proteção de uma máquina. Para obter mais informações sobre como adicionar criptografia a duas ou mais máquinas ao protegê-las inicialmente, consulte Sobre como proteger diversas máquinas.

Execute as etapas deste procedimento para adicionar uma chave de criptografia.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Chaves de criptografia**.

   A página **Chaves de criptografia** é exibida.
3. Clique em **Adicionar chave de criptografia**.

   A caixa de diálogo **Criar chave de criptografia** será exibida.
4. Na caixa de diálogo **Criar chave de criptografia**, insira os detalhes da chave, como descrito na tabela a seguir.

Tabela 39. Criar detalhes da chave de criptografia.

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia. Os nomes de chaves de criptografia devem ter entre 1 e 64 caracteres alfanuméricos. Não use caracteres proibidos ou frases proibidas.
Descrição	Insira um comentário para a chave de criptografia. Essas informações aparecem no campo Descrição ao visualizar as chaves de criptografia no Core Console. Você pode inserir até 254 caracteres. A melhor prática é evitar o uso de caracteres proibidos e frases proibidas.
Senha	Insira a frase de acesso usada para controlar o acesso. A melhor prática é evitar o uso de caracteres proibidos. **CAUTION: Armazene a frase de acesso em um local seguro.O suporte Quest não pode recuperar uma frase de acesso. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais máquinas protegidas, você não poderá recuperar os dados caso perca a frase de acesso.**
Confirmar frase de acesso	Insira novamente a frase de acesso. Usado para confirmar a entrada da frase de acesso.

5. Clique em **OK**.

A caixa de diálogo é fechada e a chave de criptografia criada fica visível na página Chaves de criptografia.

6. Para aplicar uma chave de criptografia a uma máquina protegida, consulte Aplicar uma chave de criptografia a partir da página Máquinas protegidas.

Importar uma chave de criptografia

Você pode importar uma chave de criptografia de outro Rapid Recovery Core e usar essa chave para criptografar dados para uma máquina protegida no Core. Para importar a chave, é necessário que ela possa ser acessada pela máquina Core, localmente ou através da rede. Você também deve saber a frase de acesso da chave de criptografia.

Execute as etapas deste procedimento para importar uma chave de criptografia.

NOTE: Este procedimento não aplica a chave a nenhuma máquina protegida. Para obter mais informações sobre como aplicar a chave, consulte Aplicar uma chave de criptografia a partir da página Máquinas protegidas.

1. Navegar para o Rapid Recovery Core.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Chaves de criptografia**.

   A página **Chaves de criptografia** é exibida.
3. Clique em **Importar**.

   A caixa de diálogo **Upload de arquivo** é exibida.
4. Na caixa de diálogo**Upload de arquivo**, navegue para a rede ou o diretório local contendo a chave de criptografia que você deseja importar.

   Por exemplo, navegue para a pasta **Downloads** do usuário conectado.

   O nome de arquivo da chave começa com "EncryptionKey-", seguido do ID da chave e terminando com a extensão .key. Um exemplo de nome de chave de criptografia é EncryptionKey-RandomAlphabeticCharacters.key.
5. Selecione a chave que você deseja importar e clique em **Abrir**.
6. Na caixa de diálogo **Importar chave**, clique em **OK**.

   A caixa de diálogo é fechada e a chave de criptografia importada permanece visível na página **Chaves de criptografia**. Se a chave de criptografia foi usada para proteger um volume antes de ser exportada, o estado da chave é Bloqueado.

Desbloquear uma chave de criptografia

Chaves de criptografia podem estar em estado bloqueado ou desbloqueado. Uma chave de criptografia desbloqueada pode ser aplicada a uma máquina protegida para proteger os dados de cópia de segurança dessa máquina salvos no repositório. Em um Rapid Recovery Core, usando uma chave de criptografia desbloqueada, você também pode recuperar dados de um ponto de recuperação.

Quando você importa uma chave de criptografia para um Rapid Recovery Core, o estado padrão é Bloqueado. Isso é válido quer você tenha importado a chave de criptografia explicitamente, quer ela tenha sido adicionada ao Rapid Recovery Core pela replicação de máquinas protegidas criptografadas ou pela importação de um arquivo de pontos de recuperação criptografados.

No caso de chaves de criptografia adicionadas ao Rapid Recovery Core somente por replicação, ao desbloquear uma chave, você pode especificar um período de tempo (em horas, dias ou meses) durante o qual ela continuará desbloqueada. Cada dia é baseado em um período de 24 horas começando no momento em que a solicitação de desbloqueio é salva no Rapid Recovery Core. Por exemplo, se a chave for desbloqueada às 11h24 na terça-

feira e a duração selecionada for de dois dias, a chave será bloqueada outra vez, automaticamente, às 11h24 de quinta-feira.

NOTE: Não é possível usar uma chave de criptografia bloqueada para recuperar dados nem aplicá-la a uma máquina protegida. Você deve primeiro fornecer a frase de acesso, desbloqueando assim a chave.

Você também pode bloquear uma chave de criptografia desbloqueada, garantindo que ela não possa ser aplicada a uma máquina protegida até ser desbloqueada. Para bloquear uma chave de criptografia com o estado Universal, primeiramente, é necessário alterar o tipo para Replicado.

Se uma chave de criptografia desbloqueada está sendo usada atualmente para proteger uma máquina no Core, é preciso primeiro desassociá-la da máquina protegida para poder bloqueá-la.

Conclua as etapas deste procedimento para desbloquear uma chave de criptografia bloqueada.

1. Navegar para o Rapid Recovery Core.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Chaves de criptografia**.

   A página **Chaves de criptografia** é exibida. A coluna Estado indica quais chaves de criptografia estão bloqueadas.
3. Localize a chave de criptografia que você deseja desbloquear, clique no menu suspenso e selecione **Desbloquear**.

   A caixa de diálogo **Editar chave de criptografia** é exibida.
4. Na caixa de diálogo, no campo Frase de acesso, insira a frase de acesso para desbloquear esta chave.
5. Para especificar o período em que a chave permanecerá desbloqueada, na opção Duração, execute um destes procedimentos:
   - Para especificar que a chave continuará desbloqueada até você bloqueá-la explicitamente, no Rapid Recovery selecione **Até o bloqueio manual**.
   - Para especificar que a chave permaneça bloqueada por uma duração especificada que você pode configurar em horas, dias ou meses, faça o seguinte:
     - Selecione o campo de número e digite um valor entre 1 e 999.
     - Especifique horas, dias ou meses, respectivamente.
     - Depois, clique em **OK**.

     Essa opção está disponível para chaves de criptografia adicionadas por replicação.
     A caixa de diálogo é fechada e as alterações da chave de criptografia selecionada ficam visíveis na página de Chaves de criptografia.
   - Para especificar que a chave permaneça bloqueada até a data e hora escolhidas, faça o seguinte:
     - Selecione a opção **Até**.
     - No campo de texto ou usando os widgets calendário e relógio, especifique explicitamente os dados e a hora em que você deseja que a chave de criptografia seja travada.
     - Depois, clique em **OK**.

     Essa opção está disponível para chaves de criptografia adicionadas por replicação.
     A caixa de diálogo é fechada e as alterações da chave de criptografia selecionada ficam visíveis na página de Chaves de criptografia.

Bloquear uma chave de criptografia

Quando uma chave de criptografia estiver bloqueada, ela não pode ser aplicada a qualquer máquina protegida até que seja desbloqueada. Para bloquear uma chave de criptografia com o tipo Universal, é necessário primeiramente alterar o tipo para Replicado.

Conclua as etapas deste procedimento para bloquear uma chave de criptografia.

1. Navegar para o Rapid Recovery Core.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Chaves de criptografia**.

   A página **Chaves de criptografia** é exibida. A coluna Estado indica quais chaves de criptografia estão desbloqueadas e mostra o tipo de cada chave.
3. Localize a chave de criptografia que você deseja bloquear. Se o tipo dela for Universal, clique em seu menu suspenso e selecione **Alterar o tipo para Replicado**.

   A caixa de diálogo **Alterar o tipo da chave de criptografia** é exibida.
4. Na caixa de diálogo, confirme que você deseja alterar o tipo de chave para **Replicated**.
5. Se você alterou com sucesso o status da chave de criptografia para Replicado, clique em seu menu suspenso menu e selecione **Bloquear**.

   A caixa de diálogo **Bloquear chave de criptografia** é exibida.
6. Na caixa de diálogo, confirme que deseja bloquear a chave.

   A caixa de diálogo é fechada e o estado da chave de criptografia selecionada agora é bloqueado.

NOTE: Essa opção está disponível para chaves de criptografia adicionadas por replicação.

Editar uma chave de criptografia

Depois que uma chave de criptografia é definida, você pode editar o nome ou a descrição da chave. Essas propriedades aparecem quando você visualiza a lista de chaves de criptografia no painel Chaves de criptografia.

Execute as etapas deste procedimento para editar o nome ou a descrição de uma chave de criptografia desbloqueada existente.

CAUTION: Depois de editar o nome ou a descrição de uma chave de criptografia usada para proteger uma ou mais máquinas, o Rapid Recovery tira uma nova imagem de base. Esse snapshot da imagem de base ocorre para essa máquina no próximo snapshot programado ou forçado.

1. Navegar para o Rapid Recovery Core.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Chaves de criptografia**.

   A página **Chaves de criptografia** é exibida.
3. Localize a chave de criptografia que você quer editar e faça o seguinte:
   - Se a chave estiver bloqueada, é necessário desbloqueá-la. Consulte Desbloquear uma chave de criptografia.
   - Se a chave estiver desbloqueada, proceda conforme descrito abaixo.
4. Clique no menu suspenso para a chave de criptografia especificada e selecione **Editar**.

   A caixa de diálogo **Edit Encryption Key** (Editar chave de criptografia) é mostrada.
5. Na caixa de diálogo, edite o nome ou a descrição da chave de criptografia e clique em **OK**.

   A caixa de diálogo é fechada e as alterações da chave de criptografia selecionada ficam visíveis na página de **Chaves de criptografia**.

Alterar a frase de acesso de uma chave de criptografia

Para manter máxima segurança, você pode alterar a frase de acesso de qualquer chave de criptografia existente. Execute as etapas deste procedimento para alterar a frase de acesso de uma chave de criptografia.

CAUTION: Depois que você edita a frase de acesso de uma chave de criptografia usada para proteger uma ou mais máquinas, o Rapid Recovery Core captura um snapshot incremental dessa máquina no próximo snapshot programado ou forçado.

1. Navegar para o Rapid Recovery Core.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Chaves de criptografia**.

   A página **Chaves de criptografia** é exibida.
3. Localize a chave de criptografia que você deseja atualizar, clique no menu suspenso e selecione **Change passphrase** (Alterar senha).

   A caixa de diálogo **Change Passphrase** (Alterar senha) é mostrada.
4. Na caixa de diálogo, no campo **Frase de acesso**, digite a nova frase de acesso da criptografia.
5. No campo **Confirmar frase de acesso**, digite novamente a frase de acesso idêntica.
6. Clique em **OK**.

   A caixa de diálogo é fechada e a frase de acesso é atualizada.
7. Como opcional, caso você use uma dica no campo Descrição, edite a chave de criptografia para atualizar a dica. Para obter mais informações, consulte Editar uma chave de criptografia.

CAUTION: O Rapid Recovery usa a criptografia AES de 256 bits no modo encadeamento de blocos de codificação (CBC) com chaves de 256 bits. A Quest recomenda gravar a frase de acesso em um local seguro e manter essas informações atualizadas. O Quest Support não consegue recuperar uma frase de acesso. Sem a frase de acesso, você não pode recuperar informações dos pontos de recuperação criptografados.

Exportar uma chave de criptografia

Você pode exportar uma chave de criptografia de qualquer Rapid Recovery Core com a finalidade específica de usá-la em outro Core. Quando você executa esse procedimento, a chave é salva na pasta **Downloads** da conta de usuário do Windows ativa.

Execute as etapas deste procedimento para exportar uma chave de criptografia.

1. Navegar para o Rapid Recovery Core.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Chaves de criptografia**.

   A página **Chaves de criptografia** é exibida.
3. Localize a chave de criptografia que você deseja exportar, clique no menu suspenso e selecione **Export** (Exportar).

   A caixa de diálogo **Abrir chave de criptografia-[nome.chave]** é exibida.
4. Na caixa de diálogo, selecione **Salvar arquivo** para salvar e armazenar as chaves de criptografia em um local seguro e clique em **OK**.

O download da chave de criptografia é feito em forma de arquivo de texto no local padrão, como a pasta **Downloads** da conta de usuário do Windows ativa.

5. Como opção, se desejar importar essa chave para um Core diferente, copie o arquivo para um local acessível no Core escolhido.

Remover uma chave de criptografia

Quando você remove uma chave de criptografia na página Chave de criptografia, a chave é excluída do Rapid Recovery Core.

NOTE: A remoção de uma chave de criptografia não descriptografa os pontos de recuperação já salvos usando a chave. Você ainda precisa manter e fornecer a frase de acesso para a chave para recuperar dados para os pontos de recuperação criptografados existentes.

Você não pode remover uma chave de criptografia que já esteja associada a uma máquina protegida. Você deve primeiramente visualizar as definições de criptografia de cada máquina protegida que use a chave e desassociar a chave de criptografia que deseja remover. Para obter mais informações, consulte o tópico Desassociar uma chave de criptografia de uma máquina protegida.

Execute as etapas deste procedimento para remover uma chave de criptografia.

1. Navegar para o Rapid Recovery Core.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Chaves de criptografia**.

   A página **Chaves de criptografia** é exibida.
3. Localize a chave de criptografia que você quer remover. Clique em seu menu suspenso e selecione **Remover**.

   A caixa de diálogo **Remover a chave de criptografia** será exibida. Você verá uma mensagem confirmando a ação de remover a chave de criptografia.
4. Na caixa de diálogo, confirme que deseja remover a chave de criptografia.

   NOTE: A remoção de uma chave de criptografia não descriptografa os pontos de recuperação já salvos usando a chave. Você ainda precisa manter e fornecer a chave para recuperar dados para os pontos de recuperação criptografados existentes.

   A caixa de diálogo é fechada e a chave de criptografia removida não aparece mais na página **Chave de criptografia**.

Como alterar tipos de chave de criptografia

As chaves de criptografia listam um dos dois tipos possíveis no painel Chaves de criptografia: Universal ou Replicação. O tipo indica a provável origem da chave de criptografia e determina se você pode alterar os detalhes ou as frase de acesso. Você só pode modificar atributos caso o tipo seja Universal. Caso precise modificar esse atributos para uma chave com tipo Replicado, você deve alterar o tipo para Universal usando esse procedimento. Quando você alterar o tipo de uma chave de criptografia para Universal, ela é desbloqueada manualmente e pode ser usada para criptografar outras máquinas protegidas.

NOTE: Você deve saber a frase de acesso para alterar o tipo de Replicado para Universal.

As chaves de criptografia também têm dois estados possíveis: Bloqueado ou Desbloqueado. O estado determina se é possível aplicar uma chave de criptografia a uma máquina protegida ou restaurar dados de um ponto de recuperação criptografado. Você só pode alterar o tipo de uma chave de criptografia manualmente caso o estado seja Desbloqueado.

Quando você cria primeiro uma chave de criptografia, o tipo é Universal, e o estado é Desbloqueado. Você pode usar essa chave imediatamente (por exemplo, para criptografar cópias de segurança de uma máquina protegida). No entanto, um tipo de chave Universal não pode ser bloqueado manualmente. Caso queira bloquear manualmente uma chave de criptografia com um tipo de Universal, você deve alterar o tipo para Replicado usando esse procedimento.

Você não pode alterar um tipo da chave de criptografia caso esteja já em uso pontos de recuperação de criptografia para uma o mais máquinas protegidas.

Siga esse procedimento para alterar um tipo da chave de criptografia.

1. Navegar para o Rapid Recovery Core.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Chaves de criptografia**.

   A página **Chaves de criptografia** é exibida. Chaves de criptografia acessíveis ao Core são exibidas em uma tabela de resumo. Cada uma lista um tipo de Universal ou Replicado.
3. Localize a chave de criptografia que você deseja atualizar.
4. Caso você queira alterar uma chave de criptografia Universal para Replicação, faça o seguinte:
   a. Clique em seu menu suspenso e selecione **Change the type to Replicated** (Alterar o tipo para Replicado).

   A caixa de diálogo **Alterar o tipo da chave de criptografia** é exibida. Você vê uma mensagem confirmando que você deseja alterar o tipo para Replicado.

   - Na caixa de diálogo, confirme se você deseja alterar o tipo para Replicado.

   A caixa de diálogo é fechada, e o tipo de chave de criptografia é atualizado para Replicação.
5. Caso você queira alterar uma chave de criptografia Replicação para Universal, faça o seguinte:
   a. Clique em seu menu suspenso e selecione **Change the type to Universal** (Alterar o tipo para Universal).

   A caixa de diálogo **Alterar o tipo da chave de criptografia** é exibida. Você vê uma mensagem confirmando que você deseja alterar o tipo para Universal.

   - Na caixa de diálogo, no campo **Frase de acesso**, digite a frase de acesso e clique em **OK** para confirmar se você deseja alterar o tipo para Universal.

   A caixa de diálogo é fechada, e o tipo de chave de criptografia é atualizado para Universal.

Protegendo máquinas

Esta seção descreve como proteger, configurar e gerenciar as máquinas protegidas em seu ambiente do Rapid Recovery.

Sobre como proteger máquinas com Rapid Recovery

Para proteger seus dados usando o Rapid Recovery, você precisará adicionar as estações de trabalho, os servidores, os desktops e os notebooks que você deseja proteger ao Rapid Recovery Core.

No Rapid Recovery Core Console, usando um dos assistentes de proteção de máquina, você pode identificar as máquinas que deseja proteger. Você pode fazer o seguinte:

- Proteja uma máquina única usando o Assistente de proteção de máquina, que se conecta à máquina usando o nome de host ou o endereço IP da rede. Para obter mais informações sobre como proteger uma única máquina, consulte Proteção de uma máquina.
- Proteja um cluster de rede usando o assistente Proteger cluster, que se conecta ao cluster usando o nome de host ou o endereço IP da rede. Para obter mais informações sobre como proteger um cluster, consulte Proteger um cluster.
- Proteja várias máquinas simultaneamente usando o assistente de proteção de várias máquinas. Esse assistente permite conectar às máquinas associadas a um servidor do Microsoft Active Directory; a máquinas em um host do vCenter ou ESXi; ou a máquinas em um host ou cluster do Hyper-V. Também é possível inserir manualmente as informações de conexão (nome do host ou endereço IP da rede, nome de usuário e senha) de várias máquinas. Para obter mais informações sobre como proteger várias máquinas, consulte Sobre como proteger diversas máquinas.

NOTE: A Quest recomenda a limitação do número de máquinas protegidas simultaneamente a 50 ou menos para evitar restrições de recurso que possam causar uma falha na operação de proteção.

Ao identificar os requisitos de proteção para uma única máquina no assistente, você pode especificar quais volumes proteger. Quando você protege diversas máquinas, todos os volumes são protegidos por padrão. (Você pode alterar isso depois em uma máquina individual.)

Ao proteger uma máquina virtual em um host vCenter/ESXi ou Hyper-V, você deve definir se deseja proteger a máquina usando o recurso Rapid Snap para virtual ou instalando o Rapid Recovery Agent. Para obter mais informações, consulte Fatores ao escolher proteção com base em agente ou sem agente.

O assistente também permite definir um programa personalizado para proteção (ou reutilizar um programa existente).

Usando opções avançadas, você pode adicionar medidas de segurança adicionais especificando ou aplicando uma chave de criptografia a backups das máquinas que deseja proteger.

Por fim, caso algum não exista, você pode definir um repositório usando o assistente.

Após a instalação do software do agente, cada máquina deve ser reiniciado após a instalação.

Para obter mais informações sobre como proteger estações de trabalho e servidores, consulte Proteção de uma máquina.

Fatores ao escolher proteção com base em agente ou sem agente

O recurso Rapid Snap para virtual do Rapid Recovery é compatível com os hipervisores vCenter/ESXi ou Hyper-V. Esse recurso, também conhecido como proteção sem agente, permite proteger as VMs no Core sem instalar o software Rapid Recovery Agent em cada máquina convidada.

Recomendações gerais

Com a versão 6.2, o recurso Rapid Snap para virtual do Rapid Recovery quase atingiu a paridade com proteção fornecida com a instalação do software Rapid Recovery Agent. Como regra geral, a Quest recomenda usar proteção sem agente nas maquinas virtuais ESXi ou Hyper-V. Se o software agente for instalado em máquinas virtuais ESXi ou Hyper-V, a menos que haja um motivo atraente para proteger explicitamente a VM usando o Rapid Recovery Agent, a Quest recomenda remover o software do agente e proteger suas VMs sem agente.

Existem algumas vantagens na proteção sem agente e algumas limitações. Essas estão descritas no tópico Noções básicas sobre Rapid Snap for Virtual.

As exceções à recomendação de usar a proteção sem agentes são as seguintes:

- Coletar metadados para máquinas sem agente é mais lento do que para máquinas protegidas pelo software Rapid Recovery Agent. Se você enfrentar problemas de desempenho relacionados a metadados (especificamente para máquinas Exchange Server ou SQL Server protegidas), o Suporte de proteção de dados da Quest pode sugerir instalar o agente baseado em software em servidores de aplicativos específicos para fins de solução de problemas.
- Se proteger apenas uma ou duas VMs em um hipervisor com vários soquetes, você pode consumir menos licenças ao instalar o agente diretamente nas VMs em vez de no host.
- Se você precisar de recursos exclusivos para o Rapid Recovery Agent, instale o software do agente nas VMs relevantes.

Alguns recursos são exclusivos para proteção ao instalar o software Rapid Recovery Agent. Os seguintes exemplos se aplicam:

- A realização de uma verificação de capacidade de anexação do SQL é uma capacidade do software Rapid Recovery Agent. Se você estiver protegendo seu computador SQL Server sem agente, você deverá executar as verificações de capacidade de anexação do SQL usando uma instância do SQL Server instalado no servidor do Core. Para executar essa verificação, você deve ajustar a configuração de capacidade de anexação do Core no Core para **Usar o SQL Server no Core**.
- Os volumes dinâmicos protegidos sem agente são protegidos no nível do disco e não no nível do volume.
- Live Recovery é um recurso do software Rapid Recovery Agent. Você não pode usar esse recurso ao restaurar volumes protegidos usando o Rapid Snap for Virtual.

Se você precisar de um dos recursos descritos na lista anterior para uma VM específica, a Quest recomenda instalar o agente em vez de proteger a VM sem agente.

Para obter mais informações, consulte o tópico Noções básicas sobre Rapid Snap for Virtual.

Conceitos de consumo de licença da Versão 6.2

O Rapid Recoveryversão 6.2 descontinua o uso de pools de licenças específicas aplicáveis para Windows Server, hosts Hyper-V, soquetes VMware, servidores Exchange, servidores SQL, servidores Linux, e assim por diante. O novo modelo é muito simplificado.

Conforme descrito no tópico Gerenciar licenças, o Rapid Recovery versão 6.2 utiliza apenas dois pools de licença: Capacidade e Enterprise. Se o licenciamento do Core for configurado para usar um pool baseado em capacidade, você não pode usar outro tipo de pool.

NOTE: No futuro, a Quest planeja adicionar pools de licença baseados em outras unidades de medida. Os pools de Capacidade e Enterprise continuarão sendo suportados.

As soluções DL usam licenciamento baseado em capacidade e não são afetadas pelas restrições do pool de licenças. Ambientes do Rapid Recovery baseados em software que usam o licenciamento de capacidade de front-end também não recebem os benefícios de licença do uso de proteção sem agentes. Outros benefícios do uso de proteção sem agente são relevantes, mesmo quando pools de licença de capacidade estão em uso.

Se o ambiente do Rapid Recovery versão 6.2 usa um pool de licença Enterprise, as seguintes regras se aplicam:

- Os hosts de hipervisor Hyper-V ou vCenter/ESXi protegidos com Rapid Recovery Agent consomem uma licença do pool para cada soquete do processador. Se seu host de hipervisor tem seis soquetes de CPU, ele consome 6 licenças do pool Enterprise.
- Qualquer outra máquina (física ou virtual) protegida em seu Core com oRapid Recovery Agent consome uma licença desse pool. Isso é verdade mesmo para servidores de aplicativos (como o Exchange Server, SQL Server ou Oracle Database 12c) com vários soquetes de CPU.

Benefícios de licenciamento do uso de proteção sem agente

Você pode proteger máquinas virtuais convidadas em um host de hipervisor vCenter/ESXi executando o Assistente de proteção de diversas máquinas. Na página **Conexão** deste assistente, se você especificar **Proteger as VMs selecionadas sem usar agentes**, as VMs convidadas nesse host serão protegidas sem agente. Para essas VMs, nenhuma licença é consumida do pool de licenças. Enquanto o Rapid Recovery Agent não estiver instalado no host, adicionar esse host ao seu Core consome uma licença para cada soquete da CPU.

Quando você protege um servidor Hyper-V, o Rapid Recovery Agent é instalado no host. Para cada soquete de CPU no host de hipervisor, uma licença do seu pool Enterprise é consumida. Se você especificar a proteção do servidor Hyper-V sem agente, as VMs convidadas são protegidas sem agente, e para essas VMs, nenhuma licença é consumida do seu pool de licenças disponíveis.

Quando você protege um cluster Hyper-V, o Rapid Recovery Agent é instalado em cada nó do cluster. Apenas uma única licença é consumida do seu pool de licenças. O número total de soquetes da CPU no cluster é consumido. Se você especificar a proteção do cluster Hyper-V sem agente, as VMs convidadas são protegidas sem agente, e para essas VMs, nenhuma licença é consumida do seu pool de licenças disponíveis no cluster.

Os principais benefícios de licenciamento para usar o Rapid Snap para virtual é a redução do consumo de licenças do pool de licenças Enterprise para as máquinas virtuais que você protege. Se você especificar a proteção sem agentes para um host de hipervisor ESXi, ou um servidor Hyper-V ou cluster, todas as novas VMs criadas no host são automaticamente protegidas sem agente, e não consomem licenças do pool de licenças Enterprise.

Se algumas das VMs nesse host de hipervisor tinham anteriormente o Rapid Recovery Agent instalado e o seu Core estiver executando o Rapid Recovery versão 6.2, você deve escolher uma das seguintes opções:

- Remova o software do agente para proteger a VM sem agente. Nenhuma licença do seu pool é consumida.
- Adicione manualmente a máquina para proteção sem agente.
- Se você precisar que a máquina seja protegida pelo agente e o host estiver adicionado ao Core, associe a VM ao seu host pai. Você obtém o benefício da proteção baseada em agente e nenhuma licença é consumida.
- Não faça alterações. A VM é protegida usando as APIs no Rapid Recovery Agent e uma única licença é consumida.

Cada máquina virtual em um hipervisor adicionado ao seu Core é protegida sem agente sem consumir uma licença. Para obter esse benefício, você deve fazer o seguinte:

Os principais benefícios de licenciamento para usar o Rapid Snap para virtual é a redução do consumo de licenças do pool de licenças Enterprise para as máquinas virtuais que você protege. Cada máquina virtual em um

hipervisor adicionado ao seu Core é protegida sem agente sem consumir uma licença. Para obter esse benefício, você deve fazer o seguinte:

- **Proteger as VMs sem usar agentes.** Você pode proteger explicitamente várias VMs usando o Assistente para proteger várias máquinas. Ao proteger um host de hipervisor, você também pode selecionar a opção de **Proteção automática de novas máquinas virtuais** que protege implicitamente novas VMs quando elas são criadas.
- **Associe a VM convidada com seu host de hipervisor protegido.** Se o Rapid Recovery Agent estiver instalado, suas APIs (não as nativas para o hipervisor) são usadas para proteger a VM. No entanto, você pode reduzir as licenças consumidas associando as VMs ao host adicionado ao Core. Essa associação é realizada no nível da máquina para cada máquina virtual. O processo de vincular a VM convidada ao seu host de hipervisor pai é descrito na etapa 3 do procedimento Visualização e modificação das definições de máquina protegida.
- **Desinstale o agente.** A menos que recomendado de maneira diferente, remova da máquina virtual todas as cópias do Software do agente.

Para uma discussão dos benefícios e das limitações no que diz respeito a proteção sem agente, software adicional recomendado, requisitos mínimos para o host, e assim por diante, consulte o tópico Noções básicas sobre Rapid Snap for Virtual.

Sobre como proteger as máquinas Linux com o Rapid Recovery

O software Rapid Recovery Agent é compatível com vários sistemas operacionais baseados em Linux (para obter detalhes, consulte os requisitos do sistema atualmente definidos no *Guia de requisitos do sistema do Rapid Recovery*). O Rapid Recovery Core é compatível apenas com máquinas Windows. Embora seja possível gerenciar máquinas Linux protegidas no Rapid Recovery Core Console, vários procedimentos para máquinas Linux têm etapas que diferem dos procedimentos equivalentes no Windows. Além disso, você pode executar algumas ações diretamente em uma máquina Linux protegida usando o utilitário de linha de comando local_mount.

NOTE: O utilitário local_mount era conhecido anteriormente como aamount.

Se você quiser proteger uma única máquina Linux, agora pode usar o Assistente de proteção de máquinas. Consulte o tópico Proteção de uma máquina. Para proteger várias máquinas Linux ao mesmo tempo usando o assistente do Core Console, consulte o tópico Como proteger diversas máquinas manualmente.

Para implantar ou instalar o software Agent em uma máquina Linux no Core Console, é necessário ter o seguinte:

- A conta de usuário deve ter privilégios SUDO.
- A máquina Linux que você quer proteger deve ter acesso a um servidor SSH.

Se a máquina Linux que você deseja proteger não atender a estes pré-requisitos, consulte um administrador do Linux. Cumpra esses requisitos essenciais para poder concluir o assistente relevante para implantar e instalar o software Agent.

Sobre a proteção de servidores de banco de dados Oracle

O Rapid Recoveryversão 6.2 expande suporte a aplicativos para incluir proteção baseada em agente de servidores de bancos de dados relacionais Oracle 12c. Você pode proteger um servidor de banco de dados Oracle e todos os seus bancos de dados e realizar tarefas relacionadas.

Nesta versão, as seguintes restrições se aplicam:

- Oracle 12c é a única versão testada e suportada para proteção no Rapid Recovery Core. O uso de qualquer outra versão Oracle fica por sua conta e risco.
- Os servidores de bancos de dados Oracle protegidos devem executar as versões de 64 bits do Windows Server 2012 R2 x64 ou Windows Server 2016.
- Você deve instalar o software Rapid Recovery Agent (ouversão 6.2 posterior) no servidor Oracle. A proteção sem agente está planejada para uma versão futura.
- A proteção de bancos de dados Oracle 12c é limitada ao uso do Serviço de Instantâneos de Volume (VSS) no modo ARCHIVELOG.

  NOTE: O suporte para NOARCHIVELOG e (o modo de log padrão para bancos de dados Oracle) está planejado para uma versão futura. Os bancos de dados Oracle com modo ARCHIVELOG habilitado também devem ser configurados para arquivar todos os logs de de refazer on-line usando o processo ARCH (arquivo). Um administrador de banco de dados (DBA) pode alterar o modo e configurar o arquivamento de logs de refazer usando o Oracle SQL*Plus ou o Oracle Enterprise Manager. Para obter mais informações sobre como ativar o modo ARCHIVELOG e o arquivamento, consulte a documentação da Oracle ou um técnico qualificado do Oracle 12c DBA.

Para proteger totalmente os servidores Oracle, execute as seguintes tarefas:

- Instale o software Rapid Recovery Agent (versão 6.2 ou posterior) no servidor Oracle e inicie a proteção. Use o Assistente de proteção de máquina para localizar o servidor Oracle na rede, implante o software do agente e estabeleça uma programação de proteção. Para obter mais informações, consulte Sobre como proteger máquinas com Rapid Recovery.
- Digite as credenciais de cada banco de dados no Rapid Recovery Core Console. O Core armazena em cache suas credenciais com segurança e permite que você acesse os metadados na interface do usuário. Antes de inserir as credenciais, você não poderá ver os detalhes dos bancos de dados no servidor Oracle protegido. Para obter mais informações, consulte Inserir ou editar credenciais de bancos de dados Oracle.
- Ative o modo de log de arquivo para o servidor Oracle protegido e verifique o gravador VSS Oracle no Core Console. Para obter mais informações, consulte Ativar modo de log de arquivo e adicionar o gravador VSS para bancos de dados Oracle protegidos.
- Revise a política de truncamento de log e configure conforme necessário. Quando um banco de dados Oracle é definido para o modo de log de arquivo, os logs se acumulam rapidamente e consomem um espaço em disco substancial. Por esse motivo, um trabalho noturno é configurado por padrão para truncar automaticamente logs do Oracle. É possível configurar três opções de exclusão para esse trabalho noturno ou você pode desativar o trabalho noturno. Para obter mais informações, consulte Sobre o truncamento de logs do Oracle.

  Você também pode truncar logs de bancos de dados Oracle manualmente sob demanda. Para obter mais informações sobre esse procedimento, consulte Truncamento manual de logs de banco de dados Oracle.

Depois que você instalar o Agent, proteger a máquina em seu Core e definir as configurações corretamente, você pode fazer o seguinte:

- **Ver os metadados.** Na página **Resumo** da máquina protegida, você pode ver os metadados de cada banco de dados no servidor Oracle, incluindo a conexão e o status de cada arquivo de log, arquivo de controle e arquivo de dados.
- **Verificar integridade do banco de dados.** Você pode executar verificações de integridade no Core Console usando o utilitário DBVERIFY.
- **Truncar arquivos de log**, utilizando uma das três políticas de exclusão.
- **Restaurar bancos de dados.** Restaure volumes inteiros ou volumes que contenham bancos de dados selecionados. Quando você ativar o modo de arquivo de log, os instantâneos do banco de dados Oracle são consistentes de falhas, do ponto de vista do serviço Oracle.
- **Executar uma exportação virtual.** Você pode realizar uma exportação única ou configurar uma VM de standby virtual que atualiza constantemente uma VM com novas informações, conforme os backups no banco de dados protegido forem capturados.

  Se você inicializar uma VM de um banco de dados Oracle, talvez precise iniciar manualmente os serviços de banco de dados e desativar manualmente o modo de backup para arquivos de dados de bancos de dados.

Inserir ou editar credenciais de bancos de dados Oracle

Antes de executar este procedimento, você deve adicionar um servidor de banco de dados Oracle primeiro à proteção em seu Core.

Para inserir ou editar credenciais de banco de dados Oracle:

- A conta de usuário do Windows do usuário do Rapid Recovery que executará este procedimento deve ter privilégios SYSDBA no servidor de banco de dados protegido.
- O banco de dados deve ser acessível ao servidor do Rapid Recovery Core, e uma conexão deve ser estabelecida com êxito.

NOTE: SYSDBA é um privilégio administrativo de banco de dados dos sistemas Oracle que é necessário para executar operações administrativas de alto nível. Essas funções incluem criar, iniciar, encerrar, fazer backup ou recuperar um banco de dados Oracle.

Depois de proteger o servidor de banco de dados Oracle, você não poderá acessar os metadados do banco de dados nem ver detalhes do banco de dados até que você insira as credenciais de cada banco de dados. Esta etapa única armazena em cache as credenciais do banco de dados com segurança e fornece ao Core Console acesso às informações de status sobre todos os arquivos de log de transações protegidos, arquivos de controle e arquivos de dados que compõem os bancos de dados Oracle.

Por exemplo, na página **Resumo** da máquina Oracle protegida, antes inserir as credenciais, não é possível expandir detalhes sobre qualquer banco de dados protegido no painel de informações do servidor Oracle.

NOTE: Esta é uma etapa única necessária para cada novo banco de dados Oracle protegido.

Conclua as etapas deste procedimento para fornecer ao Rapid Recovery Core Console acesso aos metadados necessários para seus bancos de dados Oracle protegidos.

1. Navegue até a máquina Oracle protegida no Rapid Recovery Core Console.

   A página **Resumo** será exibida para a máquina selecionada.
2. Na página **Resumo**, role a tela até o painel de **Informações do servidor Oracle**.
3. Para o primeiro banco de dados na tabela, clique na lista suspensa (Mais opções) e selecione select **Edit Credentials** (Editar credenciais).

A caixa de diálogo **Edit Instance Credentials** (Editar credenciais da instância) será exibida.

4. Dois tipos de conexão são suportados: básica e TNS (Transparent Network Substrate), tecnologia de rede proprietária da Oracle). Execute um dos seguintes:

   - Para conectar usando uma conexão básica, insira as informações na tabela a seguir:

Opção	Descrição
Tipo de conexão	Básico
Nome do host	Digite o nome do host ou o endereço IP.
Porta	Digite a porta apropriada. A porta padrão aberta para essa finalidade é a 1521.
SID ou nome do serviço	Selecione o método de conexão apropriado. Você pode usar um dos seguintes: • **SID.** O Identificador do sistema (SID) Oracle é uma ID exclusiva que que identifica a instância do banco de dados. • **Nome do serviço.** O nome do serviço é um alias TNS usado para conectar remotamente ao seu banco de dados. **NOTE:** O nome do serviço pode ser encontrado no arquivo TNSNAMES.ORA.
Nome do serviço	O nome do serviço é o alias TNS que você fornece ao conectar remotamente ao seu banco de dados e este serviço.

   - Para conectar usando o TNS, insira as informações na tabela a seguir:

Opção	Descrição
Tipo de conexão	TNS
Alias da rede	Selecione esse menu suspenso para ver os aliases de banco de dados disponíveis para a rede e selecione o alias apropriado.

5. Dois tipos de credenciais são suportados: Oracle e Sistema operacional. Execute um dos seguintes:

   - Para conectar com as credenciais do Oracle, insira o nome de usuário e a senha do banco de dados Oracle nos campos de texto relevantes.

     NOTE: Sua conta de usuário do Windows deve ter privilégios SYSDBA.

   - Para conectar usando as credenciais em cache do sistema operacional, selecione **Operating System** (Sistema operacional).

     NOTE: Sua conta de usuário do Windows deve ser membro do grupo local ORA_DBA, o que garante que o usuário tenha privilégios SYSDBA.

6. Para verificar as credenciais, clique em **Verify** (Verificar).

Uma caixa de diálogo será exibida, indicando se a conexão de teste foi bem-sucedida.

7. Execute um dos seguintes:
   - Se a verificação foi bem-sucedida, clique em **OK** para fechar a caixa de diálogo da mensagem.
   - Se não foi bem-sucedida, feche a caixa de diálogo e revise as credenciais da instância até que a conexão seja verificada. Consulte o administrador do sistema se tiver dúvidas sobre as credenciais.
8. Na caixa de diálogo **Edit Instance Credentials** (Editar credenciais da instância), após a verificação bem-sucedida, clique em **OK**.

   A caixa de diálogo será fechada, e o Rapid Recovery Core Console aplicará imediatamente e armazenará em cache as credenciais. Logo depois, os metadados estarão disponíveis no Core Console, e o indicador de status do banco de dados selecionado exibirá o status verde (on-line).
9. Repita a etapa 3 até a etapa 8 para cada banco de dados listado no painel de informações do servidor Oracle.

Depois de inserir e armazenar em cache as credenciais para todos os bancos de dados nessa máquina Oracle protegida, execute os procedimentos descritos no tópico Ativar modo de log de arquivo e adicionar o gravador VSS para bancos de dados Oracle protegidos.

Ativar modo de log de arquivo e adicionar o gravador VSS para bancos de dados Oracle protegidos

Antes de executar este procedimento, você deve adicionar um servidor de banco de dados Oracle primeiro à proteção em seu Core e inserir as credenciais de cada banco de dados no Core Console.

Os aplicativos de banco de dados exigem a presença de uma combinação de arquivos específicos (como arquivos de configuração, log e controle), cada um definido para um estado específico, para poderem ser consistentes de aplicativo. No versão 6.2, os bancos de dados Oracle exigem que o modo de log de arquivo seja ativado. Até que você execute esse procedimento, os instantâneos do servidor de banco de dados será consistente de falhas, mas não consistente de aplicativo.

O gravador VSS Oracle é usado para capturar instantâneos usando o Serviço de Instantâneos de Volume. Esse gravador deve estar ativado.

NOTE: Estas são etapas únicas necessárias para cada novo banco de dados Oracle protegido.

Conclua as etapas deste procedimento para verificar se o modo de log de arquivo está ativado; para ativar esse modo, se necessário; e para adicionar o gravador VSS ao Core.

1. Navegue até a máquina Oracle protegida no Rapid Recovery Core Console.

   A página **Resumo** será exibida para a máquina selecionada.
2. Na página **Resumo**, role a tela até o painel de **Informações do servidor Oracle**.
3. No painel de **informações do servidor Oracle**, se você vir uma notificação dizendo que o modo de log de arquivo está desativado, clique em **Enable archive log mode for these databases** (Ativar modo de log de arquivo para estes bancos de dados) e depois clique para confirmar a reinicialização do instâncias de banco de dados.

   NOTE: Ativar o modo de arquivo causa a reinicialização das instâncias de banco de dados relevantes. Isso pode levar alguns minutos.
4. No painel de **informações do servidor Oracle**, se você vir uma notificação dizendo que o gravador VSS Oracle foi excluído dos instantâneos, clique em **Include Oracle VSS Writer** (Incluir gravador VSS Oracle) e clique para confirmar.

   A mensagem de aviso será fechada, e o gravador VSS é adicionado ao Core.
5. Opcionalmente, você pode acompanhar o progresso da ativação do modo de log de arquivo ou da adição de um gravador VSS. Para obter mais informações, consulte Visualizar tarefas.

Sobre o truncamento de logs do Oracle

O modo de log de arquivo, que é necessário para suporte do Oracle no versão 6.2, faz com que um número substancial de arquivos de log se acumulem no servidor de banco de dados, usando um espaço de armazenamento valioso. Os arquivos de log relevantes são incluídos nos backups do servidor Oracle cada vez que um instantâneo de ponto de recuperação é capturado, tornando os logs locais supérfluos. Por esse motivo, o Rapid Recovery Core inclui vários métodos de truncamento de logs do Oracle.

1. O Rapid Recovery Core inclui todas as configurações de trabalho noturno para truncar logs do Oracle. O truncamento de logs do Oracle é ativado por padrão como trabalho noturno utilizando a política de exclusão **Automática**. Nesse modelo, os logs são truncados uma vez por dia quando os trabalhos noturnos são executados.

   Essa configuração foi projetada para atender às necessidades da maioria dos usuários. Se você estiver satisfeito com essa abordagem, não é necessário alterar a configuração. Ela é ativada por padrão.
2. Você pode personalizar a configuração de trabalho noturno de truncamento de log do Oracle para um servidor Oracle específico. Você pode escolher entre outras duas políticas de exclusão:

   - A política de exclusão **Manter mais recentes** permite especificar o tempo (n dias, semanas, meses ou anos) em que os logs do Oracle serão mantidos antes do truncamento. Quando o período expirar, os arquivos de log além do limite serão truncados uma vez por dia quando os trabalhos noturnos forem executados.
   - A política de exclusão **Manter número especificado** permite que você especifique um número de arquivos de log para manter. Depois que esse limite for atingido, os logs mais recentes serão mantidos, e os logs mais antigos são truncados uma vez por dia quando os trabalhos noturnos forem executados.

   Para obter mais informações sobre o truncamento de trabalhos como um trabalho noturno, consulte o tópico Noções básicas sobre trabalhos noturnos.
3. Você também pode truncar logs manualmente sob demanda a qualquer momento. Para obter mais informações sobre como fazer isso, consulte Truncamento manual de logs de banco de dados Oracle.

O truncamento de logs do Oracle, por trabalho noturno ou sob demanda manualmente, ocorre sem a necessidade de um trabalho de transferência.

Truncamento manual de logs de banco de dados Oracle

Este procedimento é apropriado somente para servidores de banco de dados Oracle protegidos no Core.

Para dar suporte à proteção de bancos de dados Oracle no versão 6.2Rapid Recovery, um trabalho noturno para truncar logs de arquivo do Oracle é ativado por padrão. Você pode desativar esse trabalho noturno, o que resultará em uma quantidade substancial de arquivos de log acumulado no servidor de banco de dados local.

Para qualquer servidor Oracle protegido, você pode truncar manualmente logs de banco de dados Oracle sob demanda a qualquer momento. O truncamento excluirá os logs de arquivo do servidor local. Em cada ponto de recuperação salvo em seu repositório, os logs de banco continuam a refletir o estado do banco de dados no momento em que o instantâneo de backup foi capturado.

Conclua as etapas deste procedimento para truncar manualmente arquivos de log do Oracle.

1. Navegue até a máquina Oracle protegida no Rapid Recovery Core Console.

   A página **Resumo** será exibida para a máquina selecionada.
2. Na página **Resumo**, role a tela até o painel de **Informações do servidor Oracle**.
3. Na linha da tabela que representa a instância do banco de dados Oracle para a qual você deseja truncar logs, clique na lista suspensa (Mais opções) e selecione **Forçar truncamento de log**.

   A caixa de diálogo **Forçar truncamento de log** será exibida.
4. Se você quiser excluir todos os logs do Oracle do servidor de banco de dados local, no menu suspenso **Política de exclusão**, selecione **Automática** e clique em **Forçar**.

Um trabalho de truncamento de log entrará na fila. Se o sistema não estiver ocupado, o trabalho será executado imediatamente e os logs serão truncados.

5. Se quiser excluir todos os logs armazenados localmente do servidor Oracle (cópias deles são armazenadas no ponto de recuperação mais recente), faça o seguinte:
    a. No menu suspenso **Política de exclusão**, selecione **Manter mais recentes**.
    b. No campo de texto **Manter logs por**, digite um número e, no menu suspenso de período, selecione o período relevante (**dias, semanas, meses** ou **anos**).
    c. Clique em **Forçar**.

    Um trabalho de truncamento de log entrará na fila. Se o sistema não estiver ocupado, o trabalho será executado imediatamente e os logs serão truncados.
6. Se você quiser manter um número específico de arquivos de log do Oracle e truncar os logs restantes, faça o seguinte:
    a. No menu suspenso **Política de exclusão**, selecione **Manter número especificado**.
    b. No campo de texto **Número de arquivos**, digite um número que representa a quantidade de logs de banco de dados mais recentes que devem ser mantidos.
    c. Clique em **Forçar**.

    Um trabalho de truncamento de log entrará na fila. Se o sistema não estiver ocupado, o trabalho será executado imediatamente e os logs serão truncados.
7. Se você quiser truncar logs de outras instâncias de banco de dados nesse servidor, repita a etapa 3 até a etapa 6 para cada banco de dados relevante listado no painel de Informações do servidor Oracle.

Gerenciamento de servidores de aplicativos protegidos no Rapid Recovery Core

O Rapid Recovery inclui suporte para servidores de aplicativos, como SQL Server, Exchange Server e Oracle. Para obter mais informações sobre suportes do Rapid Recovery de versões específicas, consulte o *Guia de requisitos do sistema do Rapid Recovery*.

As opções específicas para esses aplicativos suportados são exibidas no Rapid Recovery Core Console somente quando uma instância do software e arquivos relacionados são detectados em servidores protegidos. Nesses casos, opções adicionais estão disponíveis quando você selecionar a máquina protegida do Console do Core.

Se você selecionar um SQL Server protegido no menu de navegação à esquerda, as opções do menu que são exibidas para a máquina protegida incluem o menu suspenso **SQL Server**.

Por exemplo, se você selecionar um Exchange server protegido no menu de navegação à esquerda, as opções de menu que são exibidas para a máquina protegida incluem uma opção de menu suspenso **Exchange**.

Se você selecionar um servidor Oracle protegido, na página **Resumo** dessa máquina protegida, role para baixo até o painel de informações do servidor Oracle que é exclusivo para servidores de banco de dados da Oracle protegidos.

Enquanto essas opções funcionarem de forma diferente, haverá uniformização. As funções que você pode realizar apenas para servidores SQL Server, Exchange Server e Oracle protegidos são:

- **Forçamento do truncamento de log do server.** O SQL Server, os servidores de e-mail Exchange e os servidores de banco de dados da Oracle contêm registros de servidor. O processo para truncar os logs do SQL Server identifica o espaço disponível no servidor. Quando você truncar logs de um Exchange server, além de identificar o espaço disponível, o processo libera mais espaço no server. O mesmo é verdadeiro para Oracle, o truncamento de log remove os arquivos de log de arquivamento do servidor Oracle, liberando espaço no servidor protegido.
- **Definição de credenciais para o respectivo server.** Os SQL servers permitem que você defina credenciais para uma máquina com SQL Server protegido, ou defina credenciais padrão para todos os

SQL servers protegidos. Os servidores Exchange e Oracle permitem que você defina credenciais para a máquina protegida na página **Resumo** para o servidor protegido.

- **Exibir o estado para verificações em pontos de recuperação do SQL Server, Exchange Server ou servidor Oracle**. Os pontos de recuperação capturados de um SQL Server, Exchange Server ou servidor Oracle protegido têm indicadores de status de cor correspondente. Essas cores indicam o sucesso ou a falha de diversas verificações relevantes para esses servidores de aplicativos.

Os tópicos a seguir discutem o gerenciamento de computadores protegidos SQL Server, Exchange Server ou Oracle:

- Noções básicas sobre os indicadores de status do ponto de recuperação
- Definições e funções para servidores SQL protegidos
- Definições e funções para servidores protegidos do Exchange
- Sobre a proteção de servidores de banco de dados Oracle

Sobre a proteção de clusters do servidor

No Rapid Recovery, a proteção de cluster do servidor está associada às máquinas protegidas do Rapid Recovery instaladas em nós de cluster individuais (ou seja, máquinas individuais no cluster) e ao Rapid Recovery Core, que protege essas máquinas como se fossem uma única máquina composta.

É fácil configurar um Rapid Recovery Core para proteger e gerenciar um cluster. No Core Console, um cluster é organizado como uma entidade separada, que atua como um contêiner que inclui os nós relacionados. Por exemplo, na área de navegação à esquerda, no menu **Máquinas protegidas**, os clusters protegidos são relacionados. Logo abaixo de cada cluster, os nós individuais ou máquinas de agente associados aparecerão. Cada um desses é uma máquina protegida na qual o software do agente do Rapid Recovery é instalado. Se você clicar no cluster, a página **Resumo** do cluster aparece no Core Console.

Nos níveis do Core e cluster, você pode ver informações sobre o cluster, como a lista de nós relacionados e volumes compartilhados. Ao exibir as informações de um cluster no Core Console, você pode clicar em **Nós protegidos** no menu de navegação superior para ver uma tabela de resumo dos nós individuais do cluster. Dessa tabela de resumo, você pode realizar funções para cada nó, como forçar um snapshot; realizar uma exportação única ou configurar um standby virtual; montar ou visualizar pontos de recuperação; restaurar a partir de um ponto de recuperação; converter o nó do cluster para sua própria máquina protegida; ou remover a proteção do nó. Se o nó for um Exchange ou SQL Server, você também verá a opção de truncar logs.

No nível do cluster, você também poderá ver os metadados correspondentes do cluster do Exchange e SQL para os nós do cluster. Você pode especificar as definições de todo o cluster e dos volumes compartilhados desse cluster.

Se você clicar em qualquer nó do cluster no menu de navegação à esquerda, as informações mostradas no Core Console são específicas desse nó do cluster. Aqui você pode visualizar informações específicas para esse nó ou configurar as definições apenas desse nó.

Para obter informações sobre as versões de aplicativos com suporte, as configurações em cluster e sobre o suporte para volumes compartilhados clusterizados, consulte o *Guia de requisitos do sistema do Rapid Recovery*.

Noções básicas sobre Rapid Snap for Virtual

O recurso Rapid Snap for Virtual do Rapid Recovery também é conhecido como proteção sem agente, pois é possível proteger máquinas virtuais (VMs) no Core sem instalar o agente do Rapid Recovery em cada máquina virtual.

CAUTION: A Quest **recomenda limitar a proteção sem agente a não mais do que 200 VMs por vez. Não selecione mais de 200 VMs ao usar o Assistente de proteção de diversas máquinas. A tentativa de iniciar a proteção de mais de 200 VMs resulta em um baixo desempenho da interface do usuário. Não há limite de quantas VMs um Core pode proteger sem agente com o passar do tempo. Por exemplo, você pode proteger 200 VMs hoje em dia e outras 200 VMs amanhã.**

Para obter mais informações, consulte Como proteger VMs VMware vCenter/ESXi e Como proteger VMs em servidores e clusters Hyper-V.

Como proteger VMs VMware vCenter/ESXi

O Rapid Recovery permite que você proteja VMs vCenter/ESXi sem instalar o Rapid Recovery Agent na VM ou no host ESXi, obtendo proteção plena sem agente. O Rapid Recovery usa o cliente ESXi e a interface de programação de aplicativo (API) nativa do VMware para detectar e proteger VMs selecionadas em um único host. Em seguida, o Rapid Recovery Core se comunica com o disco de máquina virtual (VMDK) para determinar os detalhes necessários dos volumes protegidos. Como o Rapid Recovery cria pontos de recuperação com base em volumes, e não em VMDKs, cada volume pode ser montado, restaurado e exportado separadamente.

O Rapid Recovery não protege tecnicamente um host de hipervisor VMware vCenter/ESXi. Ao selecionar um host vCenter/ESXi usando o Assistente de proteção de diversas máquinas, você adiciona o host como uma entidade pai no seu Rapid Recovery Core. Nenhum arquivo de dados ou dados do host real são incluídos em instantâneos no Core. No entanto, os convidados da VM no host podem ser protegidos. As VMs protegidas são representadas na GUI do Core como filhos sob o host pai. Se você selecionar proteção sem agente para as VMs ESXi, o ícone para a VM protegida () aparece de forma diferente do ícone em uma VM ESXi protegida usando o Rapid Recovery Agent (por exemplo, ).

NOTE: A Quest recomenda instalar as Ferramentas VMware nas máquinas virtuais (VMs) que você deseja proteger em hosts ESXi ou vSphere. Quando Ferramentas VMware são instaladas em uma VM usando-se um sistema operacional (OS) Windows, os backups que o Rapid Recovery Core captura usam o Serviço de Cópias de Sombra de Volume (VSS) da Microsoft. Isso fornece a capacidade de backups consistentes de aplicativo. Para obter informações sobre o comportamento de VMs sem agente com ou sem Ferramentas VMware, consulte Benefícios de instalar as ferramentas do hipervisor para proteção sem agente e também Entendendo backups consistentes de falhas e consistentes de aplicativo.

Quando ferramentas VMware estão instaladas, a proteção sem agente usa o VMware Changed Block Tracking (CBT) para reduzir o tempo necessário para instantâneos incrementais. CBT determina quais blocos mudaram no arquivo VMDK, permitindo que o Rapid Recovery fizesse uma cópia de segurança apenas das partes do disco que mudaram desde o snapshot mais recente. Esse método de cópia de segurança normalmente resulta em operações mais curtas e consumo de recursos reduzido em elementos de rede e armazenamento.

Existem várias vantagens em usar a proteção sem agente. Entre alguns dos atributos mais úteis estão as seguintes características:

- Não há software adicional obrigatório na máquina de host.
- A proteção sem agente permite optar por proteger automaticamente novas VMs adicionadas ao host ESXi ou ao host Hyper-V.
- Uma reinicialização não é necessária durante o processo de proteção.
- As credenciais não são obrigatórias para cada VM individual.
- A proteção sem agente permite proteger uma VM mesmo que ela esteja desligada.
- A proteção sem agente permite recuperar para discos.
- A proteção sem agente dá suporte a todos os sistemas operacionais convidados.
- Se você associar uma VM convidada ao seu host de hipervisor pai protegido, uma licença Enterprise não é consumida ao proteger a VM no Core.
- Se preferir, você pode proteger e coletar metadados paraSQL Server e o Exchange.
- O Core (e não o Agent) pode executar verificações de capacidade de anexação, truncamento de log e verificações de capacidade de montagem em pontos de recuperação capturados deservidores SQL e Exchange protegidos.
- A proteção sem agente permite exportar discos ou volumes dinâmicos.

> **NOTE:** Caso sejam complexos (distribuídos, espelhados, estendidos ou RAID), os volumes são exportados como as imagens de disco e analisados em volumes após a conclusão da operação de exportação na VM exportada.

Embora haja muitos motivos para usar a proteção sem agente para VMs ESXi, opte pelo método de proteção que melhor atenda às necessidades de ambientes e empresa. Além das vantagens mencionadas anteriormente, também existem as seguintes considerações a serem mantidas em mente durante a escolha da proteção sem agente:

- A proteção sem agente de servidores de banco de dados Oracle não coleta metadados relacionados à Oracle. Enquanto os arquivos e o sistema operacional são copiados em instantâneos, nenhum recurso relacionado à Oracle é compatível. Para o suporte de aplicativos de banco de dados da Oracle, proteja o seu servidor usando o Rapid Recovery Agent.
- A proteção sem agente não dá suporte à proteção de volumes dinâmicos (por exemplo, estendidos, particionados, espelhados ou volumes RAID) no nível de volume. Ela os protege no nível do disco.
- A proteção sem agente não dá suporte ao Live Recovery. Para obter mais informações sobre esse recurso, consulte Noções básicas sobre Live Recovery.
- Durante o processo de restauração de um volume único para a VM protegida, a VM é reiniciada automaticamente.
- A proteção sem agente não exibe o espaço real usado em uma VM caso o tipo de disco virtual seja zerado.

Caso você opte por usar a proteção sem agente para as VMs ESXi, o host deve atender às exigências mínimas a seguir para a proteção sem agente para ser bem-sucedido.

- A máquina de host deve executar o ESXi versão 5.0.0 compilação 623860 ou posterior.
- O computador host deve atender aos requisitos mínimos do sistema declarado no *Guia de requisitos do sistema do Rapid Recovery*.
- Para a proteção no nível de volume, VMDKs devem incluir tabelas de partição MBR (Master Boot Record [registro da inicialização mestre]) ou tabelas de partição GUID (GPTs). VMDKs sem essas tabelas de partição são protegidas como discos inteiros, e não volumes individuais.
- Cada máquina virtual VMware deve ter Ferramentas VMware instaladas para assegurar a consistência do snapshot.

Como proteger VMs em servidores e clusters Hyper-V

Para proteger um VMs do Hyper-V sem agente, não é necessário instalar o Rapid Recovery Agent em cada VM. Você só precisa instalá-lo no computador host ou nos nós de cluster. O agente protege o disco rígido virtual no host e converte quaisquer alterações nos arquivos de disco rígido em uma imagem de volume ou de disco, dependendo do sistema de arquivos. Um novo driver fornece o suporte no nível de arquivo para máquinas virtuais em hosts e em volumes compartilhados clusterizados (CSVs).

O suporte sem agente para o Hyper-V é determinado pelo sistema operacional no host. Uma lista completa de sistemas operacionais e componentes do Rapid Recovery suportados para cada um, é mantido no *Guia de requisitos do sistema do Rapid Recovery*. Para obter mais informações, consulte o tópico "Instalação do sistema operacional e matriz de compatibilidade do Rapid Recovery release 6.2" neste documento.

A Quest recomenda que os serviços de integração do Hyper-V sejam instalados nas máquinas virtuais (VMs) que você deseja proteger em hosts Hyper-V. Quando os serviços de integração do Hyper-V são instalados em uma VM usando um sistema operacional Windows, os backups que o Rapid Recovery Core captura usam o Microsoft VSS. Isso fornece a capacidade de backups consistentes de aplicativo. Para obter informações sobre o comportamento de VMs sem agente com ou sem os Serviços de integração do Hyper-V, consulte Benefícios de instalar as ferramentas do hipervisor para proteção sem agente e também Entendendo backups consistentes de falhas e consistentes de aplicativo.

NOTE: O Rapid Recovery suporta o formato de arquivo de disco VHDx. Ele não suporta o formato VHD.

Para proteger máquinas virtuais em um CSV, o Rapid Recovery Agent e o driver precisam ser instalados em cada nó de cluster usando o recurso de implantação automática no assistente de proteção de diversas máquinas. Dos nós, o agente pode proteger todas as VMs em funcionamento nos CSVs, criando dois tipos de alterações para cada arquivo. O primeiro tipo de alteração é salvo apenas antes ou depois de um instantâneo ou de uma reinicialização de sistema limpo. O segundo tipo de alteração reside no disco, o que possibilita um instantâneo incremental disponível mesmo em caso de falta de energia ou desligamento sujo. O agente instalado no nó mescla todas as alterações em apenas uma antes de transferir os dados.

Quando um host ou um nó está sendo executado, o Rapid Recovery cria um backup. Se o host não estiver em execução, nenhum backup pode ser criado; no entanto, se um dos nós não estiver em execução, o Rapid Recovery pode continuar a tirar instantâneos das VMs no cluster.

NOTE: Para obter um melhor desempenho, é recomendado que a quantidade máxima de transferências simultâneas para o host ou nó Hyper-V seja definida como 1, que é a configuração padrão.

A proteção Hyper-V sem agente tem muitos dos mesmos recursos da proteção tradicional, em que o agente está instalado em cada máquina virtual, incluindo:

- Arquivamento
- Verificações de integridade do ponto de recuperação
- Como montar pontos de recuperação
- Descoberta automática de novas máquinas virtuais (exclusiva para a proteção sem agente)
- Como protegerservidores SQL e Exchange e coletar seus metadados
- Como realizar verificações de capacidade de montagem do Exchange
- Como realizarverificações de capacidade de anexação do SQL
- Replicação
- Restauração de máquinas virtuais, inclusive a restauração para CSVs ou para pastas compartilhadas CIF
- Restaurar arquivos em um formato VHDX convidado
- Rollup
- Exportação virtual para VMs Hyper-V e outros hipervisores, incluindo ESXi, VMware Workstation e VirtualBox

Entretanto, há limitações a serem consideradas ao escolher a proteção Hyper-V sem agente. Recursos que não são executados incluem:

- Live Recovery
- Restaurar VMs no CIFS usando o formato VHD
- Restaurar arquivos em um formato VHD (.vhd) convidado
- Restaurar arquivos em um formato VHD Set (.vhds) convidado

NOTE: Para um instantâneo consistente com aplicativo, você precisa ter o Controlador SCSI instalado em cada máquina virtual. Sem esse controlador, o resultado é sempre um instantâneo consistente com falha.

Suporte a aplicativos

O Rapid Snap for Virtual permite que você ative a proteção sem agentes deaplicativos do SQL Server e do Exchange executados em VMs Hyper-V e ESXi. Este recurso opcional está disponível para VMs que executam sistemas operacionais Windows.

NOTE: O suporte a aplicativos não se aplica a aplicativos instalados em VMs Linux.

Depois de ativar o suporte a aplicativos, os metadados dos aplicativos são exibidos na página **Resumo** da VM, assim como um ícone ao lado do nome da VM na página **Máquinas**. Se houver um erro que impeça o suporte íntegro a aplicativos, o ícone mudará de verde para vermelho.

Antes de optar por uma proteção sem agente de umSQL Server ou Exchange Server, observe as seguintes considerações:

- Para proteger o aplicativo, a VM deve estar ligada. O Core não recupera metadados de máquinas que estão desligadas.
- As ferramentas VMware ou os utilitários de serviços de integração do Hyper-V devem ser instalados nas VMs que você deseja proteger.
- Em uma VM que tenha o Exchange Server e o SQL Server instalados, não haverá capacidade de truncar os logs separadamente. Se os dois aplicativos estiverem instalados, os logs serão truncados em conjunto.
- As verificações de capacidade de anexação do SQL Server estão disponíveis apenas no Core e não podem ser conduzidas na máquina protegida.
- Para executar o truncamento de logs em uma VM ESXi, o host precisa usar o ESXi versão 6.5 ou posterior.

Benefícios de instalar as ferramentas do hipervisor para proteção sem agente

Ao proteger máquinas virtuais (VMs) sem usar o Rapid Recovery Agent, a Quest recomenda instalar Ferramentas VMware em máquinas virtuais protegidas em hosts vSphere ou ESXi. Da mesma forma, a Quest recomenda instalar os serviços de integração de Hyper-V nos VMs que você deseja proteger nos hosts Hyper-V.

Instalar esses utilitários de hipervisor nativo permite ao Rapid Recovery aproveitar todas as vantagens da funcionalidade Microsoft Volume Shadow Copy Services (VSS).

Quando esses utilitários estão instalados em máquinas virtuais com sistemas operacionais Windows, os backups que o Rapid Recovery Core captura também podem usar o VSS. Quando essas ferramentas não estão instaladas, o Rapid Recovery ainda coleta instantâneos, mas apenas em um estado consistente com falhas. Para obter mais informações, consulte Entendendo backups consistentes de falhas e consistentes de aplicativo.

As condições a seguir se aplicam se Ferramentas VMware ou Serviços de integração do Hyper-V estiverem instalados e a VM estiver ligada:

Tabela 40. Condições de tipo de backup para máquinas virtuais

Ferramenta do hipervisor	VM ligada	Tipo de backup
Não instalado	Sim	Consistentes de falhas
Não instalado	Não (desligamento anormal)	Consistentes de falhas
Não instalado	Não (desligamento normal)	Consistentes de aplicativo
Instalado	Sim	Consistentes de aplicativo
Instalado	Não (desligamento anormal)	Consistentes de falhas
Instalado	Não (desligamento normal)	Consistentes de aplicativo

Entendendo backups consistentes de falhas e consistentes de aplicativo

Ao proteger máquinas virtuais sem agente usando o recurso do Rapid Snap for Virtual, os dados nos instantâneos de backup que você captura podem estar em um dos dois estados:

- Consistentes de falhas. No mínimo, todos os backups sem agentes capturados pelo Rapid Recovery Core são consistentes de falhas. O backup é um instantâneo de todos os dados e dos arquivos do sistema operacional em cada volume protegido no momento em que os arquivos foram capturados. Se a restauração for feita a partir de um ponto de recuperação consistente de falhas, o sistema operacional da máquina virtual é iniciado e pode ler e entender o sistema de arquivos e todos os arquivos nela contidos.

  Se você se recuperar um aplicativo transacional de um estado consistente de falha, o banco de dados retorna ao último estado válido. Esse estado válido mais recente pode ser da hora da falha ou anterior à ela. Se for anterior, o banco de dados deve encaminhar algum trabalho para fazer os arquivos de dados corresponderem às informações nos registros. Esse processo leva algum tempo na primeira vez em que o banco de dados é aberto, o que causa um atraso na inicialização da máquina.
- **Consistentes de aplicativo**. Os backups consistentes de aplicativo usam o Serviço de Cópias de Sombra de Volume (VSS) da Microsoft para garantir a consistência dos dados de aplicativos quando uma cópia de sombra é criada. Usando gravadores VSS, as operações pendentes de entrada/saída são concluídas e os arquivos de registro confirmados antes dos instantâneos sendo capturados. Como resultado, se você restaurar a partir de um ponto de recuperação consistente de aplicativo, o sistema operacional da máquina virtual é iniciado e pode ler e entender o sistema de arquivos. Além disso, arquivos para aplicativos transacionais, como SQL Server ou Exchange, estão em um estado consistente. Por exemplo, os logs do SQL Server combinam os arquivos de dados e o banco de dados é aberto rapidamente sem precisar de reparos.

Noções básicas do instalador de software do agente Rapid Recovery

O Rapid Recovery permite baixar instaladores do Rapid Recovery Core. Na página **Downloads**, você pode optar por baixar o Agent Installer, o Local Mount Utility (LMU) ou um arquivo MIB SNMP. Para obter mais informações sobre o LMU, consulte O Local Mount Utility. Para obter mais informações sobre o SNMP, consulte Definir as definições do SNMP.

NOTE: Para acessar o Agent Installer, consulte Como baixar o Rapid Recovery Agent Installer. Para obter mais informações sobre a implantação do Agent Installer, consulte o Guia de instalação e atualização do Rapid Recovery.

O Agent Installer é usado para instalar o aplicativo do agente Rapid Recovery em máquinas que devem ser protegidas pelo Rapid Recovery Core. Se você determinar que possui uma máquina que exige o Agent Installer, poderá baixar o instalador da Web a partir da página Downloads do Rapid Recovery Core.

NOTE: O download do Core é feito a partir do Portal de licenças do Rapid Recovery. Para baixar o instalador do Rapid Recovery Core, acesse https://licenseportal.com. Para obter mais informações, consulte o Guia do usuário do Portal de licenças do Rapid Recovery.

Como baixar o Rapid Recovery Agent Installer

Baixe o Rapid Recovery Agent Installer e o implante em qualquer máquina que você deseja proteger no Rapid Recovery Core. Execute as etapas deste procedimento para baixar o instalador da Web.

1. Para baixar o instalador da Web do agente diretamente na máquina que você deseja proteger, faça o seguinte:
    a. Em um navegador da Web, abra o Portal de licenças do Rapid Recovery em https://licenseportal.com.
    b. No menu de navegação esquerdo, clique em **Downloads**.
    c. No painel **Aplicativos com base em Windows**, role até a linha **Windows Agent** e clique em **Baixar** para o instalador apropriado (sistemas 32 ou 64 bits).

    O arquivo do instalador, por exemplo, `Agent-X64-6.0.1.xxxx.exe`, é salvo na pasta de destino de downloads.
2. Para baixar o instalador da web no Core, na barra de ícones Core Console, clique no ícone **Mais** e selecione **Downloads**.
3. Na página **Downloads**, no painel **Agente**, clique em **Baixar instalador da web**.
4. Na caixa de diálogo **Abrindo Agent-Web.exe**, clique em **Salvar arquivo**.

    O arquivo do instalador, por exemplo, `Agent-X64-6.0.1.xxxx.exe`, é salvo na pasta de destino de downloads.
5. Mova o instalador para a máquina apropriada e instale o software do agente Rapid Recovery.

    Para obter mais informações sobre a instalação do software do agente Rapid Recovery, consulte oGuia de instalação e upgrade doRapid Recovery.

Implantação do agente em várias máquinas simultaneamente a partir do Core Console

É possível implantar o software Rapid Recovery Agent simultaneamente em várias máquinas Windows. As máquinas podem fazer parte de um domínio do Active Directory, um host virtual vCenter ou ESX(i) ou um host virtual Hyper-V; ou podem ser máquinas já protegidas pelo Rapid Recovery Core local, como no caso de uma atualização do software Rapid Recovery Agent. Você também tem a opção de implantar o software manualmente em máquinas que não são necessariamente associadas a um domínio ou host específico.

Você pode também implantar manualmente o software Rapid Recovery Agent em uma ou mais máquinas Linux do Core Console.

> **CAUTION: Se o AppAssure Agent já foi instalado anteriormente em uma máquina Linux, antes de instalar o Rapid Recovery Agent, remova o AppAssure Agent da máquina usando um script shell. Para obter mais informações sobre como remover o agente de uma máquina Linux, consulte o tópico "Desinstalar o software AppAssure Agent de uma máquina Linux" no *Guia de instalação e atualização do Rapid Recovery.* Para implantar o software do agente com sucesso em máquinas Linux, consulte os pré-requisitos no tópico "Sobre como instalar o software do agente em máquinas Linux" no mesmo documento.**

Implantar o software Rapid Recovery Agent não protege as máquinas automaticamente. Após a implantação, você precisa selecionar a opção **Proteger diversas máquinas** na barra de botões do Core Console.

NOTE: O recurso com o qual você faz a implantação em várias máquinas simultaneamente foi anteriormente chamado de implantação em massa. O recurso com o qual você protege várias máquinas simultaneamente foi anteriormente chamado de proteção em massa.

Para implantar e proteger várias máquinas simultaneamente, realize as seguintes tarefas:

- Implantar o Rapid Recovery Agent em várias máquinas. Consulte Implantação do agente em várias máquinas simultaneamente a partir do Core Console.
- Monitorar a implantação. Consulte Verificar a implantação em várias máquinas.
- Proteger várias máquinas. Consulte Sobre como proteger diversas máquinas.

  NOTE: Se você tiver selecionado a opção Proteger máquina após instalação durante a implantação, ignore esta tarefa.
- Monitorar a atividade da proteção em massa. Consulte Monitorar a proteção de várias máquinas.

Como usar o assistente de implantação do software do agente para implantar em uma ou mais máquinas

Você pode simplificar a tarefa de implantação do software Rapid Recovery Agent em uma ou mais máquinas usando o Assistente de implantação do software do agente.

Se estiver implantando em máquinas Linux, esse método é adequado.

NOTE: No passado, esse recurso foi chamado de "implantação em massa".

Ao usar o Assistente de implantação do software do agente, o Rapid Recovery Core pode:

1. Detectar máquinas Windows em um domínio do Active Directory e enviar por push o software do agente para as máquinas que você selecionar.
2. Conectar a um host VMware vCenter ou ESXi, detectar os convidados e enviar por push o software do agente para as máquinas que você selecionar.
3. Conectar a um Rapid Recovery Core local e implantar o software do agente atual (mais recentes) nas máquinas Windows que o Core já protege. (Para máquinas Linux, use a opção para implantar manualmente.)
4. Conectar a um servidor ou cluster Hyper-V, detectar os convidados e enviar por push o software do agente para as máquinas que você selecionar.
5. Especificar manualmente máquinas Linux ou Windows, utilizando os endereços IP e as credenciais, e enviar por push o software do agente para as máquinas que você selecionar.

Do Core Console, você pode realizar qualquer uma das seguintes tarefas:

- Implantar em máquinas de um domínio Active Directory
- Implantar em máquinas em um host virtual VMware vCenter/ESXi
- Aplicar um upgrade do Software do agente Rapid Recovery em máquinas protegidas
- Implantar nas máquinas manualmente

NOTE: A Quest recomenda limitar o número de máquinas para as quais você implanta simultaneamente para 50 ou menos, de forma a evitar limitações de recursos que podem causar falha da operação de implantação.

NOTE: As máquinas de destino devem ter acesso à Internet para baixar e instalar bits, porque o Rapid Recovery usa a versão da Web do instalador do Rapid Recovery Agent para implantar os componentes de instalação. Se o acesso à Internet não estiver disponível, use o Core Console para baixar o instalador para uma mídia de armazenamento, como uma unidade USB. Em seguida, instale fisicamente o software nas máquinas que você quer proteger. Para obter mais informações, consulte Como baixar o Rapid Recovery Agent Installer.

Implantar em máquinas de um domínio Active Directory

Antes de iniciar este procedimento, tenha em mãos as informações de domínio e credenciais de login para o servidor Active Directory.

Use este procedimento para implantar simultaneamente o Software do agente Rapid Recovery em uma ou mais máquinas em um domínio Active Directory.

1. No Rapid Recovery Core Console, clique menu suspenso no **Proteger** e clique em **Implantar Software do agente**.

   O Assistente para implantar o software do agente é aberto.
2. Na página **Conexão** do assistente, na lista suspensa **Origem**, selecione **Active Directory**.
3. Insira as informações de domínio e as credenciais de logon conforme descrito na tabela a seguir.

Tabela 41. Informações e credenciais do domínio

Caixa de texto	Descrição
Host	O nome de host ou endereço IP do domínio Active Directory.
Nome de usuário	O nome de usuário utilizado para se conectar ao domínio, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
Senha	A senha usada para se conectar ao domínio.

4. Clique em **Avançar**.
5. Na página **Máquinas**, selecione as máquinas em que você deseja implantar o Software do Agente Rapid Recovery.
6. Como opção, para reinicializar automaticamente as máquinas protegidas após a instalação do agente, selecione **Após a instalação, reiniciar a máquina automaticamente (recomendado)**.
7. Clique em **Concluir**.

   O sistema verifica automaticamente cada máquina que você selecionou.

   Se o Rapid Recovery detectar alguma preocupação durante a verificação automática, o assistente avança para uma página Avisos em que você pode retirar as máquinas da seleção e verificar manualmente as máquinas selecionadas. Se as máquinas que você adicionou passarem na verificação automática, elas serão exibidas no painel Implantar Agente nas máquinas.
8. Se a página de aviso apareceu e você ainda está satisfeito com suas seleções, clique em **Concluir** novamente.

O Software do agente Rapid Recovery é implantado nas máquinas especificadas. As máquinas ainda não estão protegidas. A proteção começa após concluir o Como proteger diversas máquinas em um domínio Active Directory.

Implantar em máquinas em um host virtual VMware vCenter/ESXi

Use este procedimento para implantar simultaneamente o software Rapid Recovery Agent em uma ou mais máquinas em um host virtual VMware vCenter/ESXi.

Antes de começar este procedimento, você precisa ter as seguintes informações:

- Credenciais de login para o host virtual VMware vCenter/ESXi.
- Local do host.
- Credenciais de login para cada máquina que você quer proteger.

NOTE: Todas as máquinas virtuais devem ter Ferramentas de VMware instaladas; caso contrário, o Rapid Recovery não consegue detectar o nome do host da máquina virtual na qual implantar. Em vez do nome do host, o Rapid Recovery usa o nome da máquina virtual, o que pode causar problemas se o nome do host for diferente do nome da máquina virtual.

1. No Rapid Recovery Core Console, clique menu suspenso no **Proteger** e clique em **Implantar Software do agente**.

   O **Assistente para implantar o software do agente é** aberto.
2. Na página **Conexão** do assistente, na lista suspensa **Origem**, selecione **vCenter / ESXi**.
3. Insira as informações do host e insira as credenciais conforme descrito na tabela a seguir.

Tabela 42. Definições de conexão do vCenter/ESXi

Caixa de texto	Descrição
Host	O nome ou endereço IP do host virtual VMware vCenter Server/ESXi.
Porta	A porta usada para se conectar ao host virtual. A definição padrão é 443.
Nome de usuário	O nome de usuário utilizado para se conectar ao host virtual; por exemplo, Administrador ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador.
Senha	A senha usada para se conectar ao host virtual.

4. Clique em **Avançar**.
5. Na página **Criar** do assistente, selecione uma das opções a seguir no menu suspenso:
   - Hosts e clusters
   - VMs e modelos
6. Expanda a lista de máquinas e selecione as máquinas virtuais nas quais você deseja implantar o software.

   Uma notificação será exibida se o Rapid Recovery detectar que uma máquina está offline ou que as Ferramentas VMware não estão instaladas.
7. Se desejar reiniciar as máquinas automaticamente após a implantação, selecione **Após a instalação do Agente, reiniciar a máquina automaticamente (Recomendado)**.
8. Clique em **Avançar**.

   O Rapid Recovery verifica automaticamente cada máquina que você selecionou.
9. Na página **Ajustes** do assistente, insira as credenciais para cada máquina no seguinte formato: `hostname::username::password`.

NOTE: Insira uma máquina em cada linha.

10. Clique em **Concluir**.

    O sistema verifica automaticamente cada máquina que você selecionou.

    Se o Rapid Recovery detectar alguma preocupação durante a verificação automática, o assistente avança para uma página de Avisos em que você pode retirar as máquinas da seleção e verificar manualmente as máquinas selecionadas. Se as máquinas que você adicionou passarem na verificação automática, elas serão exibidas no painel Implantar Agente nas máquinas.

11. Se a página de aviso apareceu e você ainda está satisfeito com suas seleções, clique em **Concluir** novamente.

O Software do agente Rapid Recovery é implantado nas máquinas especificadas. As máquinas ainda não estão protegidas. A proteção começa após concluir o Proteger diversas máquinas em um host virtual VMware vCenter/ESXi.

Aplicar um upgrade do Software do agente Rapid Recovery em máquinas protegidas

Você pode usar o Assistente para implementar software do agente para enviar um upgrade do Software do agente Rapid Recovery para máquinas Windows que já estão protegidas pelo Rapid Recovery Core local.

NOTE: Para usuários Linux, se a versão anterior do agente tiver a marca AppAssure (versão 5.4.3 ou anterior), você precisará primeiro remover o software do agente usando o script shell adequado para a versão específica do AppAssure Agent. Remover o AppAssure Agent depois de instalar o Rapid Recovery Agent pode desfazer a conexão entre a máquina Linux e o Core. Para obter mais informações sobre como desinstalar o AppAssure Agent de uma máquina Linux, consulte Desinstalar o software AppAssure Agent de uma máquina Linux no *Guia de instalação e atualização do Rapid Recovery*.

1. No Rapid Recovery Core Console, clique menu suspenso no **Proteger** e clique em **Implantar Software do agente**.

   O **Assistente para implantar o software do agente** é aberto.

2. Na página **Conexão** do assistente, na lista suspensa **Origem**, selecione **Core local**.
3. Clique em **Avançar**.
4. Na página **Máquinas** do assistente, selecione as máquinas nas quais você deseja implantar um upgrade do Software do Agente Rapid Recovery.

   NOTE: Neste momento, você não poderá usar esse processo para atualizar máquinas Linux protegidas.

5. A prática recomendada é reiniciar cada máquina depois de instalar ou atualizar o software do Agente. Se desejar reiniciar as máquinas após a implantação, deixe a opção padrão **Após a instalação do Agente, reiniciar a máquina automaticamente (Recomendado)**. Caso não queira reiniciar as máquinas imediatamente, desmarque essa opção.
6. Clique em **Concluir**.

   O sistema verifica automaticamente cada máquina que você selecionou.

   Se o Rapid Recovery detectar alguma preocupação durante a verificação automática, o assistente avança para uma página **Avisos** em que você pode retirar as máquinas da seleção e verificar manualmente as máquinas selecionadas. Se as máquinas que você adicionou passarem na verificação automática, elas serão exibidas no painel **Implantar Agente** nas máquinas.

7. Se a página de **Avisos** for exibida e você ainda estiver satisfeito com suas seleções, clique novamente em **Concluir**.

Implantar nas máquinas manualmente

Use o procedimento a seguir para implantar o Rapid Recovery Agent em várias máquinas de qualquer tipo de host que não seja o Core local, Active Directory, vCenter/ESXi ou Hyper-V.

> **CAUTION: Se o AppAssure Agent já foi instalado anteriormente em uma máquina Linux, antes de instalar o Rapid Recovery Agent, remova o AppAssure Agent da máquina usando um script shell. Para obter mais informações sobre como remover o agente de uma máquina Linux, consulte o tópico "Desinstalar o software AppAssure Agent de uma máquina Linux" no *Guia de instalação e atualização do Rapid Recovery.* Para implantar o software do agente com sucesso em máquinas Linux, consulte os pré-requisitos no tópico "Sobre como instalar o software do agente em máquinas Linux" no mesmo documento.**

1. No Rapid Recovery Core Console, clique no menu suspenso **Proteger** e selecione **Implantar software do agente**.

   O **Assistente para implantar o software do agente** é aberto.
2. Na página **Conexão** do assistente, na lista suspensa **Origem**, selecione **Manualmente**.
3. Clique em **Avançar**.
4. Na página **Máquinas** do assistente, para cada máquina em que deseja implantar o Agent, insira os detalhes da máquina na caixa de diálogo. Pressione **Enter** para separar informações para cada máquina. Use o formato `nome do host::nome de usuário::senha`. Para máquinas Windows, a configuração da porta é opcional. Para máquinas Linux, sempre inclua a porta SSH, que, por padrão, é 22. Os exemplos incluem:

   ```
   10.255.255.255::administrator::&11@yYz90z
   abc-host-00-1::administrator::99!zU$o83r::8006
   Linux-host-00-2::administrator::p@$$w0rD::22
   ```
5. Se desejar reiniciar as máquinas automaticamente após a implantação, selecione **Após a instalação do Agente, reiniciar a máquina automaticamente (Recomendado)**.
6. Clique em **Concluir**.

   O sistema verifica automaticamente cada máquina que você selecionou.

   Se o Rapid Recovery detectar alguma preocupação durante a verificação automática, o assistente avança para uma página **Avisos** em que você pode retirar as máquinas da seleção e verificar manualmente as máquinas selecionadas. Se as máquinas que você adicionou passarem na verificação automática, elas serão exibidas no painel **Implantar Agente nas máquinas**.
7. Se a página de **Avisos** for exibida e você ainda estiver satisfeito com suas seleções, clique novamente em **Concluir**.

O Software do agente Rapid Recovery é implantado nas máquinas especificadas. As máquinas ainda não estão protegidas. A proteção começa após concluir o Como proteger diversas máquinas manualmente.

Verificar a implantação em várias máquinas

Depois de implantar o software do agente Rapid Recovery em duas ou mais máquinas simultaneamente, você poderá verificar o sucesso visualizando cada máquina listada no menu Máquinas protegidas.

Você também pode visualizar informações em relação ao processo de implantação em massa na página Eventos. Execute as etapas deste procedimento para verificar uma implantação.

1. Navegue para o Rapid Recovery Core Console, clique em (Eventos) e clique em **Alertas**.

   Os eventos de alerta aparecem na lista, mostrando a hora em que o evento foi iniciado e uma mensagem. Para cada implantação bem-sucedida do software do agente, você verá um alerta indicando que a máquina protegida foi adicionada.
2. Opcionalmente, clique em qualquer link de uma máquina protegida.

A página **Resumo** da máquina selecionada é exibida, mostrando informações pertinentes, inclusive:

- O nome do host da máquina protegida.
- O último instantâneo, se aplicável.
- A hora do próximo snapshot programado, com base no programa de proteção da máquina selecionada.
- A chave de criptografia, caso haja alguma, usada nessa máquina protegida.
- A versão do software do agente.

Modificar definições de implantação

Execute as etapas deste procedimento para modificar as definições de implementação.

1. No Rapid Recovery Core Console, clique em (Configurações).
2. Na página **Definições**, na coluna à esquerda, clique em **Implantar** para navegar para a seção Implantar.
3. Modifique qualquer uma das opções a seguir clicando na definição que você deseja alterar para torná-la editável como uma caixa de texto ou uma lista suspensa e clique em para salvar a configuração.

Tabela 43. Opções de implantação

Opção	Descrição
Agent Installer Name (Nome do instalador do agente)	Digite o nome do arquivo executável do agente. O padrão é Agent-web.exe.
Core Address (Endereço do núcleo)	Digite o endereço do Core.
Falha ao receber o tempo limite	Digite o número de minutos para aguardar sem atividade antes do tempo limite.
Máximo de instalações paralelas	Digite um número para o máximo de instalações que você deseja instalar simultaneamente. O padrão e o limite são 100.
Reinício automático após a instalação	Marque a caixa de seleção para Sim ou a desmarque para Não.
Proteger após implantação	Marque a caixa de seleção para Sim ou a desmarque para Não.

Noções básicas sobre programações de proteção

Um programa de proteção define quando os backups são transferidos de máquinas de agente protegidas para o Rapid Recovery Core.

A primeira transferência de backup para qualquer máquina adicionada à proteção no Core é chamada de instantâneo de imagem de base. Todos os dados em todos os volumes especificados (inclusive o sistema operacional, os aplicativos e as definições) são salvos no repositório, o que pode ser muito demorado dependendo do volume de dados transferidos. Depois disso, os instantâneos incrementais (backups menores, contendo apenas dados alterados na máquina protegida desde o último backup) serão salvos no repositório regularmente com base no intervalo definido (por exemplo, a cada 60 minutos). Esse tipo de backup contém menos dados que uma imagem de base, e por isso a transferência demora menos.

As programações de proteção são inicialmente definidas usando o Assistente de proteção de máquina ou o Assistente de proteção de diversas máquinas. Usando um assistente, você pode personalizar os programas de proteção (escolhendo períodos ou um tempo de proteção diária) para atender às necessidades da empresa. Você pode modificar o programa existente ou criar um novo programa a qualquer momento na caixa de diálogo Programa de proteção na página de resumo de uma máquina protegida.

O Rapid Recovery fornece um programa de proteção padrão, que inclui um único período abrangendo todos os dias da semana, com um único período definido (das 0h00 às 23h59). O intervalo padrão (o período entre os instantâneos) é de 60 minutos. Ao habilitar a proteção primeiro, você também ativa o programa. Assim, usando as configurações padrão, independentemente da hora atual do dia, o primeiro backup ocorrerá a cada hora (00:00, 01:00, 02:00 e assim por diante).

Selecionar períodos permite visualizar o programa de proteção padrão e fazer os ajustes de acordo. Selecionar um tempo de proteção diária faz o Rapid Recovery Core criar uma cópia de segurança das máquinas protegidas designadas uma vez por dia na hora especificada por você.

Você pode personalizar o programa para definir horas de pico e fora do pico usando os períodos de dias da semana e fins de semana disponíveis. Por exemplo, caso as máquinas protegidas estejam em uso principalmente em dias da semana, você pode diminuir o intervalo do período de dias da semana para 20 minutos, o que resulta em três snapshots a cada hora. Ou você pode aumentar o intervalo do período de fins de semana de 60 minutos para 180 minutos, o que resulta em snapshots a cada três horas quando o tráfego está baixo.

Como alternativa, você pode modificar a programação padrão para definir horários de pico e fora de pico diariamente. Para isso, altere a hora final e a inicial padrão para um intervalo de tempo menor (por exemplo, das 0h00 às 16h59) e defina um intervalo apropriado (por exemplo, 20 minutos). Isso representa backups frequentes durante períodos de pico. Você pode adicionar depois um intervalo de hora de dias da semana para o tempo restante (das 17h00 às 23h59) e definir um intervalo apropriado (presumivelmente maior) (por exemplo, 180 minutos). Essas configurações definem um período fora de pico que inclui das 17h00 à meia-noite todos os dias. Essa personalização resulta em snapshots a cada três horas das 17h00 às 23h59 e em snapshots a cada 20 minutos das 0h00 às 16h59.

Quando você modifica ou cria um programa de proteção usando a caixa de diálogo Programa de proteção, o Rapid Recovery dá a opção de salvar esse programa como um modelo reutilizável que você pode aplicar a outras máquinas protegidas depois.

Entre outras opções nos assistentes de proteção estão a definição de um tempo de proteção diária. Isso resulta em um único backup diário no período definido (a configuração padrão é meia-noite).

Ao proteger uma ou várias máquinas usando um assistente, você pode pausar a proteção inicialmente, o que define o programa de proteção sem proteger as máquinas. Quando estiver pronto para começar a proteger suas máquinas com base na programação de proteção estabelecida, você deverá retomar a proteção explicitamente. Para obter mais informações sobre a retomada da proteção, consulte Pausar e retomar a

replicação. Opcionalmente, se quiser proteger imediatamente uma máquina, você pode forçar um instantâneo. Para obter mais informações, consulte Forçar um snapshot.

See also: Criar programações de proteção personalizada no Modo Simples
See also: Criar vários períodos de programação de proteção no Modo Avançado

Proteção de uma máquina

Se o software Rapid Recovery Agent já estiver instalado na máquina que você deseja proteger, mas ela ainda não foi reiniciada, faça isso agora.

Este tópico descreve como começar a proteger os dados em uma única máquina especificada usando o Assistente de proteção de máquina. Para proteger várias máquinas simultaneamente usando um único processo, consulte Sobre como proteger diversas máquinas.

NOTE: A menos que você esteja usando uma proteção sem agente em um host VMware ou ESXi ou em um host Hyper-V, o computador que você quer proteger precisa ter o software Rapid Recovery Agent instalado para ficar protegido. Você pode optar por instalar o software Agent antes deste procedimento ou implantá-lo na máquina de destino como parte da conclusão do Assistente de proteção de máquina. Para obter mais informações sobre a proteção sem agentes e suas restrições, consulte Noções básicas sobre Rapid Snap for Virtual.

NOTE: Para obter mais informações sobre como instalar o software Agent, consulte a seção "Como instalar o software Rapid Recovery Agent" no *Guia de instalação e atualização do Rapid Recovery*. Se o software Agent não estiver instalado antes de proteger uma máquina, não será possível selecionar volumes específicos para proteção como parte desse assistente. Nesse caso, por padrão, todos os volumes na máquina protegida sem agente serão protegidos. O Rapid Recovery suporta a proteção e recuperação de máquinas configuradas com partições EISA. O suporte também foi estendido para máquinas com Windows 8 e 8.1, e Windows 2012 e 2012 R2, que usam o Windows Recovery Environment (Windows RE).

Ao adicionar proteção, é preciso definir as informações de conexão, como o endereço IP e a porta, e fornecer credenciais para a máquina que deseja proteger. Como opção, você pode fornecer um nome de exibição para aparecer no Core Console em vez do endereço IP. Se isso for alterado, o endereço IP da máquina protegida não aparecerá quando você visualizar detalhes no Core Console. Defina também a programação de proteção da máquina.

O processo de proteção inclui etapas opcionais que podem ser acessadas se você selecionar uma configuração avançada. As opções avançadas incluem funções de repositório e criptografia. Por exemplo, você pode especificar um repositório existente do Rapid Recovery para salvar instantâneos ou criar um novo repositório. Também é possível especificar uma chave de criptografia existente (ou adicionar uma nova chave de criptografia) para ser aplicada aos dados dessa máquina salvos no Core. Para obter mais informações sobre as chaves de criptografia, consulte Criptografia.

O fluxo de trabalho do assistente de proteção pode ser ligeiramente diferente com base no seu ambiente. Por exemplo, se o software Rapid Recovery Agent estiver instalado na máquina que você deseja proteger, não será solicitada a instalação dele com o assistente. De forma semelhante, se um repositório já existir no Core, você não será solicitado a criar outro.

CAUTION: O Rapid Recovery não oferece suporte a bare metal restores (BMRs) de máquinas Linux com partições de inicialização ext2. Uma BMR realizada em uma máquina com esse tipo de partição resulta em uma máquina não inicializável. Se quiser realizar uma BMR dessa máquina no futuro, você terá que converter as partições ext2 para ext3 ou ext4 antes de começar a proteger e criar cópias de segurança da máquina.

1. Execute um dos seguintes:
   - Se você estiver iniciando a partir do Assistente de proteção de máquina, vá para a etapa 2.
   - Se você estiver iniciando a partir do Rapid Recovery Core Console, clique em **Proteger** na barra de botões.

Aparece o **Assistente de proteção de máquina**.

2. Na página **Welcome** (Bem-vindo), selecione as opções de instalação adequadas:
   - Se não for preciso definir um repositório ou estabelecer a criptografia, selecione **Típico**.
   - Se você precisar criar um repositório ou definir um repositório diferente para cópias de segurança da máquina selecionada, ou ainda se desejar estabelecer a criptografia usando o assistente, selecione **Avançado (exibir etapas opcionais)**.
   - Como opção, se você não quiser ver a página **Bem-Vindo** do Assistente de proteção de máquina no futuro, selecione a opção **Ignorar essa página de Boas vindas na próxima vez que o assistente for aberto**.
3. Quando estiver satisfeito com suas seleções na página Bem-Vindo, clique em **Avançar**.

   A página **Connection** (Conexão) é mostrada.
4. Na página **Conexão**, digite as informações da máquina que você quer conectar, conforme descrito na tabela a seguir, e clique em **Avançar**.

Tabela 44. Definições de conexão da máquina

Caixa de texto	Descrição
Sistema operacional	Selecione Windows ou Linux, de acordo com o sistema operacional da máquina que você deseja proteger.
Host	O nome de host ou endereço IP da máquina que deseja proteger.
Porta	O número da porta pela qual o Rapid Recovery Core se comunica com o Agent na máquina. O número de porta padrão é 8006.
Nome de usuário	O nome de usuário utilizado para se conectar a essa máquina; por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
Senha	A senha usada para se conectar à máquina.

Se a página **Instalar Agente** aparecer ao lado do Assistente de proteção de máquina, isso significa que o Rapid Recovery não detectou o Rapid Recovery Agent na máquina e instalará a versão atual do software. Vá para a etapa 6.

Se a página **Atualizar Agente** aparecer em seguida no assistente, isso significa que uma versão mais antiga do software do agente está instalada na máquina a ser protegida.

NOTE: O software Agent deve ser instalado na máquina que você deseja proteger, e a máquina deve ser reiniciada antes que possa fazer a cópia de segurança no Core. Para fazer o instalador reiniciar a máquina protegida, selecione a opção **Após a instalação, reiniciar a máquina automaticamente (recomendado)** antes de clicar em Avançar.

5. Na página **Atualizar Agente**, realize um dos procedimentos a seguir:
   - Para implantar a nova versão do o software Agent (correspondente à versão do Rapid Recovery Core), selecione **Atualizar o software Rapid Recovery Agent para a versão mais recente**.
   - Para continuar protegendo a máquina sem atualizar a versão do software Agent, desmarque a opção **Atualizar o software Rapid Recovery Agent para a versão mais recente**.
6. Clique em **Avançar**.

A página **Proteção** é exibida.

7. Opcionalmente, na página **Proteção**, se você quiser um nome que não seja o endereço IP para ser exibido no Rapid Recovery Core Consolepara essa máquina protegida, digite um nome na caixa de diálogo no campo **Nome de exibição**.

   Você pode inserir até 64 caracteres. Não use os caracteres especiais descritos no tópico . Além disso, não inicie o nome de exibição com nenhuma das combinações de caracteres descritas no tópico .

8. Selecione as configurações de programação de proteção adequadas, como descrito a seguir:

   - Para usar a programação de proteção padrão, na opção **Definições de programação**, selecione **Proteção padrão (instantâneos de todos os volumes a cada hora)**.

     Na programação de proteção padrão, o Core gera snapshots de todos os volumes na máquina protegida a cada hora. Para alterar as definições de proteção a qualquer momento depois de fechar o assistente, o que inclui a seleção dos volumes a serem protegidos, vá para a página **Resumo** da máquina protegida específica.

   - Para definir uma programação de proteção diferente, na opção **Definições de programação**, selecione **Proteção personalizada**.

     As opções de agendamento são adicionadas ao fluxo de trabalho do assistente.

9. Na parte inferior da página de **Proteção**, se você estiver renovando a proteção de uma máquina anteriormente protegida neste Core e deseja especificar um repositório diferente do repositório original, selecione a opção **Selecionar um novo repositório para esta máquina**.

   Opções avançadas (incluindo Repositório e Criptografia) são adicionadas ao fluxo de trabalho do assistente.

10. Prossiga com a configuração da seguinte maneira:

    - Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina na etapa 2 e a proteção padrão tiver sido especificada, e se houver um repositório, clique em **Concluir** para confirmar suas escolhas, fechar o assistente e proteger a máquina especificada.
    - Se você tiver selecionado uma configuração típica para o assistente de proteção de máquina e especificado proteção padrão e se nenhum repositório existe, em seguida, clique em **Avançar** e vá para a etapa 13 para criar um repositório.
    - Se uma configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** e continue na etapa 11 para escolher os volumes a proteger.
    - Se você tiver selecionado uma configuração avançada no Assistente de proteção de máquina na etapa 2 e especificado a proteção padrão, clique em **Avançar** e continue na etapa 13 para ver as opções de repositório e criptografia.
    - Se a configuração Avançado tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** e vá para a etapa 11 para escolher os volumes a proteger.

    Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.

11. Na página **Volumes de proteção**, selecione os volumes que deseja proteger. Se você não deseja incluir na proteção algum volume relacionado, clique na coluna Verificar para limpar a seleção. Depois, clique em **Avançar**.

    NOTE: Normalmente, é uma boa prática proteger, no mínimo, o volume Reservado pelo sistema e o volume em que se encontra o sistema operacional (normalmente a unidade C).

12. Na página **Programa de proteção**, defina um programa de proteção personalizado e clique em **Avançar**. Para obter detalhes sobre a definição de uma programação de proteção personalizada, consulte Criar programações de proteção personalizada no Modo Simples.

Se você já possui informações de repositório configuradas, não indicou que deseja alterar o repositório e selecionou a opção Avançado na etapa 2, a página **Criptografia** será exibida. Vá para a etapa 16.

Se você já possui informações de repositório configuradas e selecionou a opção Avançado na etapa 2, ou se indicou que deseja alterar o repositório, a página **Repositório** será exibida. Vá para a etapa 13.

13. Na página **Repositório**, faça o seguinte:
    - Se você já tiver um repositório e quiser armazenar os dados dessa máquina para proteção no repositório existente, faça o seguinte:
        1. Selecione **Utilize um repositório existente**.
        2. Selecione um repositório existente na lista.
        3. Clique em **Avançar**.

        A página **Criptografia** é exibida. Passe à Etapa 15 para definir criptografia como opção.
    - Se deseja criar um repositório, clique na página **Repositório**, insira as informações descritas na tabela a seguir e, em seguida, clique em **Avançar** ou em **Concluir**, conforme apropriado.

Tabela 45. Configurações do repositório

Caixa de texto	Descrição
Nome	Insira o nome de exibição do repositório. Por padrão, essa caixa de texto consiste na palavra Repositório e um número, que corresponde ao número de repositórios neste Core. Por exemplo, se este for o primeiro repositório, o nome padrão é Repositório 1. Altere o nome conforme a necessidade. Nomes de repositório devem conter entre 1 e 40 caracteres alfanuméricos, incluindo espaços. Não use ou .
Local	Insira o local para armazenar os dados protegidos. Esse volume deve ser um local de armazenamento principal. A localização pode ser local (uma unidade no Core) ou pode ser uma unidade de rede de compartilhamento CIFS. Para um compartilhamento CIFS, o caminho deve começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido. **CAUTION: Defina uma pasta dedicada na raiz do local de armazenamento do seu repositório. Não especifique o local da raiz. Por exemplo, use `E:\Repository\`, e não `E:\`. Se o repositório que você está criando nessa etapa for removido mais tarde, todos os arquivos no local de armazenamento do seu repositório serão excluídos. Se você definir o local de armazenamento na raiz, todos os outros arquivos no volume (por exemplo: `E:\`) são excluídos, o que poderia resultar em uma perda de dados catastrófica.** Por exemplo, digite `X:\Repository\Data`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Digite um nome de usuário para um usuário com acesso administrativo. Essa informação é necessária somente quando o local do repositório especificado é um caminho da rede.
Senha	Digite a senha para o usuário com acesso administrativo. Essa informação é necessária somente quando o local do repositório especificado é um caminho da rede.

Caixa de texto	Descrição
Caminho de metadados	Insira o local para armazenar os metadados protegidos. Por exemplo, digite `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

14. Na página **Configuração de repositório**, configure a quantidade de espaço em disco a ser alocada para o repositório. A Quest recomenda reservar 20% do volume para metadados, que é o padrão. Opcionalmente, usando o controle deslizante ou o campo **Tamanho**, você pode alocar mais ou menos espaço no volume para o repositório.
15. Opcionalmente, se você deseja exibir e inserir informações detalhadas sobre as configurações do local de armazenamento, selecione **Mostrar opções avançadas** e ajuste as configurações conforme descrito na tabela a seguir. Para ocultar essas opções, desmarque a opção **Exibir opções avançadas**. Ao concluir a configuração do repositório, clique em **Avançar** ou em **Concluir**, conforme apropriado.

Tabela 46. Detalhes da Configuração de armazenamento

Caixa de texto	Descrição
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é 512.
Bytes por registro	Especifique a média de bytes por registro. O valor padrão é 8192.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Em • Desligar • Sincronizar Se definido como Ligado, que é o padrão, o Windows controla o armazenamento em cache. Isso é apropriado para o Windows 10 e para versões do Windows Server 2012 e posterior. **NOTE:** Definir a política de cache de gravação como Ligado pode resultar em desempenho mais rápido. Se você estiver utilizando o Windows Server 2008 R2 SP2, a recomendação de configuração será Desativado. Se configurado como Desativado, o Rapid Recovery controla o armazenamento em cache. Se definido como Sincronizar, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.

Se você selecionar a opção **Avançado** Etapa 1, a página **Criptografia** é exibida.

16. Opcionalmente, na página **Criptografia**, se você deseja usar chaves de criptografia para os dados armazenados no repositório, selecione **Criptografar dados em repouso em um repositório** e, em seguida, execute uma das seguintes ações:
    - Para selecionar uma chave de criptografia existente a ser aplicada a todos os novos dados armazenados no repositório, selecione **Criptografar dados usando criptografia baseada no Core**

com uma chave existente, e, no menu suspenso **Selecionar chave de criptografia**, selecione a chave de criptografia.

- Para definir uma nova chave de criptografia neste momento a ser aplicada a todos os futuros dados armazenados no repositório, selecione **Criptografar dados usando criptografia baseada no Core com uma nova chave**, e, em seguida, digite as informações referentes à chave, conforme descrito na tabela abaixo:

Tabela 47. Definir nova chave de criptografia

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia. Os nomes de chaves de criptografia devem ter entre 1 e 64 caracteres alfanuméricos. Não use caracteres proibidos ou frases proibidas.
Descrição	Insira um comentário descritivo para a chave de criptografia. Essas informações aparecem no campo Descrição ao visualizar uma lista de chaves de criptografia no Rapid Recovery Core Console. As descrições podem conter até 254 caracteres. A melhor prática é evitar o uso de caracteres proibidos e frases proibidas.
Senha	Insira a frase de acesso usada para controlar o acesso. A melhor prática é evitar o uso de caracteres proibidos. Armazene a frase de acesso em um local seguro. O Suporte de proteção de dados da Quest não pode recuperar uma senha. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais máquinas protegidas, você não poderá recuperar os dados caso perca a frase de acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso. Usado para confirmar a entrada da frase de acesso.

17. Opcionalmente, na página **Criptografia**, para criptografar todos os dados transportados em uma rede, selecione **Criptografar os dados transportados em uma rede**. Essa opção é ativada por padrão; portanto, se não quiser criptografar dados dessa forma, desmarque essa opção.
18. Clique em **Concluir** para salvar e aplicar suas definições.

    Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.

Proteger um cluster

Este tópico descreve como adicionar um cluster para proteção no Rapid Recovery. Ao adicionar um cluster para proteção, você precisa especificar o nome do host ou endereço IP do cluster, o aplicativo de cluster, ou um dos nós ou máquinas do cluster que inclua o software do agente do Rapid Recovery.

NOTE: Um repositório é usado para armazenar os snapshots de dados capturados a partir de seus nós protegidos. Antes de começar a proteger os dados em seu cluster, você deve ter definido pelo menos um repositório associado ao seu Rapid Recovery Core.

Para obter informações sobre definição de repositórios, consulte Noções básicas sobre repositórios.

1. No Console do Rapid Recovery Core, clique no menu suspenso do botão **Proteger** e, em seguida, clique em **Proteger Cluster**.
2. Na página **Bem-Vindo** do assistente, selecione uma das seguintes opções:
   - Típico
   - Avançado (exibir etapas opcionais)
3. Clique em **Avançar**.
4. Na página **Conexão** do assistente, insira as seguintes informações.

Tabela 48. Definições de Conectar-se ao cluster

Caixa de texto	Descrição
Host	O nome do host ou endereço IP do cluster, o aplicativo de cluster ou um dos nós do cluster.
Porta	O número da porta na máquina através da qual o Rapid RecoveryCore se comunica com o agente. A porta padrão é 8006.
Nome de usuário	O nome de usuário do administrador de domínio usado para se conectar a essa máquina; por exemplo, domain_name\administrator. **NOTE:** O nome de domínio é obrigatório. Não é possível conectar-se ao cluster usando o nome de usuário do administrador local.
Senha	A senha usada para se conectar à máquina.

5. Clique em **Avançar**.

   NOTE: Se os nós de cluster já tiverem uma versão mais antiga do Rapid Recovery Agent instalada, uma página de atualização aparecerá no assistente e oferecerá a oportunidade de atualizar o agente.
6. Na página **Nós** do assistente, selecione os nós que você deseja proteger.

   O sistema verifica automaticamente todas as máquinas que você selecionou.
7. Clique em **Avançar**.

   Caso a página **Proteção** seja exibida depois do Assistente de proteção de clusters, vá para a etapa 11.

   Se o software do agente ainda não tiver sido implementado nas máquinas que você deseja proteger ou se alguma das máquinas especificadas não puder ser protegida por outro motivo, as máquinas selecionadas aparecerão na página Avisos.
8. Como opção, na página **Avisos** do assistente, você pode verificar qualquer máquina selecionando a máquina e clicando em **Verificar** na barra de ferramentas.
9. Como opção, na página **Avisos**, selecione **Após a instalação do Agente, reiniciar as máquinas automaticamente**.

   NOTE: A Quest recomenda esta opção. Reinicie as máquinas agente antes de protegê-las.
10. Se o status indicar que a máquina está acessível, clique em **Avançar** para instalar o software Rapid Recovery Agent.

    A página **Proteção** é exibida.
11. Opcionalmente, na página **Proteção**, se você quiser um nome que não seja o endereço IP para ser exibido no Rapid Recovery Core Consolepara essa máquina protegida, digite um nome na caixa de diálogo no campo **Nome de exibição**.

Você pode inserir até 64 caracteres. Não use os caracteres especiais descritos no tópico . Além disso, não inicie o nome de exibição com nenhuma das combinações de caracteres descritas no tópico .

12. Selecione as configurações de programação de proteção adequadas, como descrito a seguir:

    - Para usar a programação de proteção padrão, na opção Definições de programação, selecione **Proteção padrão (instantâneos de todos os volumes a cada hora)**.

    Na programação de proteção padrão, o Core gera snapshots de todos os volumes na máquina protegida a cada hora. Para alterar as definições de proteção a qualquer momento depois de fechar o assistente, o que inclui a seleção dos volumes a serem protegidos, vá para a página **Resumo** da máquina protegida específica.

    - Para definir uma programação de proteção diferente, na opção Definições de programação, selecione **Proteção personalizada**.

13. Prossiga com a configuração da seguinte maneira:

    - Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção padrão tiver sido especificada, e se houver um repositório, clique em **Concluir** para confirmar suas escolhas, fechar o assistente e proteger a máquina especificada.
    - Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção padrão tiver sido especificada, e se houver um repositório, clique em **Avançar** e vá para a Etapa 16 para criar um repositório.
    - Se uma configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** e continue na etapa seguinte para escolher os volumes a proteger.
    - Se você tiver selecionado uma configuração avançada no Assistente de proteção de máquina e especificado a proteção padrão, clique em **Avançar** e continue para a Etapa 16 para ver as opções de repositório e criptografia.
    - Se a configuração Avançado tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** e continue na etapa seguinte para escolher os volumes a proteger.

    Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.

14. Na página **Volumes de proteção**, selecione os volumes que deseja proteger. Se você não deseja incluir na proteção algum volume relacionado, clique na coluna Verificar para limpar a seleção. Depois, clique em **Avançar**.

    NOTE: Normalmente, é uma boa prática proteger, no mínimo, o volume Reservado pelo sistema e o volume em que se encontra o sistema operacional (normalmente a unidade C).

15. Na página **Programa de proteção**, defina um programa de proteção personalizado e clique em **Avançar**. Para obter detalhes sobre a definição de uma programação de proteção personalizada, consulte Criar programações de proteção personalizada no Modo Simples.

    Se as informações de repositório já estiverem configuradas e você tiver selecionado a opção Avançado na Etapa 1, a página Criptografia é exibida. Vá para a Etapa 19.

16. Na página **Repositório**, faça o seguinte:

    - Se você já tiver um repositório e quiser armazenar os dados dessa máquina para proteção no repositório existente, faça o seguinte:

      1. Selecione **Utilize um repositório existente**.
      2. Selecione um repositório existente na lista.
      3. Clique em **Avançar**.

A página **Criptografia** é exibida. Passe à Etapa 19 para definir criptografia como opção.

- Se deseja criar um repositório, clique na página **Repositório**, insira as informações descritas na tabela a seguir e, em seguida, clique em **Avançar** ou em **Concluir**, conforme apropriado.

Tabela 49. Configurações do repositório

Caixa de texto	Descrição
Nome	Insira o nome de exibição do repositório. Por padrão, essa caixa de texto consiste na palavra Repositório e um número, que corresponde ao número de repositórios neste Core. Por exemplo, se este for o primeiro repositório, o nome padrão é Repositório 1. Altere o nome conforme a necessidade. Nomes de repositório devem conter entre 1 e 40 caracteres alfanuméricos, incluindo espaços. Não use ou .
Local	Insira o local para armazenar os dados protegidos. Esse volume deve ser um local de armazenamento principal. A localização pode ser local (uma unidade no Core) ou pode ser uma unidade de rede de compartilhamento CIFS. Para um compartilhamento CIFS, o caminho deve começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido. **CAUTION: Defina uma pasta dedicada na raiz do local de armazenamento do seu repositório. Não especifique o local da raiz. Por exemplo, use `E:\Repository\`, e não `E:\`. Se o repositório que você está criando nessa etapa for removido mais tarde, todos os arquivos no local de armazenamento do seu repositório serão excluídos. Se você definir o local de armazenamento na raiz, todos os outros arquivos no volume (por exemplo: `E:\`) são excluídos, o que poderia resultar em uma perda de dados catastrófica.** Por exemplo, digite `X:\Repository\Data`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Digite um nome de usuário para um usuário com acesso administrativo. Essa informação é necessária somente quando o local do repositório especificado é um caminho da rede.
Senha	Digite a senha para o usuário com acesso administrativo. Essa informação é necessária somente quando o local do repositório especificado é um caminho da rede.
Caminho de metadados	Insira o local para armazenar os metadados protegidos. Por exemplo, digite `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

17. Na página **Configuração de repositório**, configure a quantidade de espaço em disco a ser alocada para o repositório. A Quest recomenda reservar 20% do volume para metadados, que é o padrão. Opcionalmente,

usando o controle deslizante ou o campo **Tamanho**, você pode alocar mais ou menos espaço no volume para o repositório.

18. Opcionalmente, se você deseja exibir e inserir informações detalhadas sobre as configurações do local de armazenamento, selecione **Mostrar opções avançadas** e ajuste as configurações conforme descrito na tabela a seguir. Para ocultar essas opções, desmarque a opção **Exibir opções avançadas**. Ao concluir a configuração do repositório, clique em **Avançar** ou em **Concluir**, conforme apropriado.

Tabela 50. Detalhes da Configuração de armazenamento

Caixa de texto	Descrição
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é 512.
Bytes por registro	Especifique a média de bytes por registro. O valor padrão é 8192.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Em • Desligar • Sincronizar Se definido como Ligado, que é o padrão, o Windows controla o armazenamento em cache. Isso é apropriado para o Windows 10 e para versões do Windows Server 2012 e posterior. **NOTE:** Definir a política de cache de gravação como Ligado pode resultar em desempenho mais rápido. Se você estiver utilizando o Windows Server 2008 R2 SP2, a recomendação de configuração será Desativado. Se configurado como Desativado, o Rapid Recovery controla o armazenamento em cache. Se definido como Sincronizar, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.

Se você selecionar a opção **Avançado** Etapa 1, a página **Criptografia** é exibida.

19. Opcionalmente, na página **Criptografia**, se você deseja usar chaves de criptografia para os dados armazenados no repositório, selecione **Criptografar dados em repouso em um repositório** e, em seguida, execute uma das seguintes ações:
    - Para selecionar uma chave de criptografia existente a ser aplicada a todos os novos dados armazenados no repositório, selecione **Criptografar dados usando criptografia baseada no Core com uma chave existente**, e, no menu suspenso **Selecionar chave de criptografia**, selecione a chave de criptografia.
    - Para definir uma nova chave de criptografia neste momento a ser aplicada a todos os futuros dados armazenados no repositório, selecione **Criptografar dados usando criptografia baseada no Core com uma nova chave**, e, em seguida, digite as informações referentes à chave, conforme descrito na tabela abaixo:

Tabela 51. Definir nova chave de criptografia

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia.

Caixa de texto	Descrição
	Os nomes de chaves de criptografia devem ter entre 1 e 64 caracteres alfanuméricos. Não use caracteres proibidos ou frases proibidas.
Descrição	Insira um comentário descritivo para a chave de criptografia. Essas informações aparecem no campo Descrição ao visualizar uma lista de chaves de criptografia no Rapid Recovery Core Console. As descrições podem conter até 254 caracteres. A melhor prática é evitar o uso de caracteres proibidos e frases proibidas.
Senha	Insira a frase de acesso usada para controlar o acesso. A melhor prática é evitar o uso de caracteres proibidos. Armazene a frase de acesso em um local seguro. O Suporte de proteção de dados da Quest não pode recuperar uma senha. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais máquinas protegidas, você não poderá recuperar os dados caso perca a frase de acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso. Usado para confirmar a entrada da frase de acesso.

20. Opcionalmente, na página **Criptografia**, para criptografar todos os dados transportados em uma rede, selecione **Criptografar os dados transportados em uma rede**. Essa opção é ativada por padrão; portanto, se não quiser criptografar dados dessa forma, desmarque essa opção.
21. Clique em **Concluir** para salvar e aplicar suas definições.

    Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.

Proteger nós em um cluster

Essa tarefa requer que você proteja um cluster, em primeiro lugar. Para obter mais informações, consulte Proteger um cluster.

Este tópico descreve como proteger os dados em um nó de cluster ou máquina que possua um agente do Rapid Recovery instalado. Este procedimento permite que você adicione nós individuais para proteção que podem ter sido omitidos quando você protegeu um cluster.

1. No Rapid Recovery Core Console, em Máquina protegida, clique no cluster com os nós que você deseja proteger.
2. Na página Resumo do cluster, clique em **Nós protegidos**.
3. Na página Nós protegidos, clique em **Proteger nó do cluster**.
4. Na caixa de diálogo Proteger nó do cluster, selecione ou insira, conforme apropriado, as seguintes informações.

Tabela 52. Definições de Proteger nó de cluster

Caixa de texto	Descrição
Host	Uma lista suspensa de nós disponíveis para proteção no cluster.
Porta	Número da porta sobre a qual o Rapid Recovery Core se comunica com o agente do nó.

Caixa de texto	Descrição
Nome de usuário	O nome de usuário do administrador de domínio usado para se conectar a esse nó; por exemplo, example_domain\administrator ou administrator@example_domain.com.
Senha	A senha usada para se conectar à máquina.

5. Para adicionar o nó, clique em **Conectar**.
6. Para começar a proteger esse nó com as configurações de proteção padrão, vá para a Etapa 13.

   NOTE: As definições padrão garantem que todos os volumes da máquina sejam protegidos com uma programação a cada 60 minutos.
7. Na caixa de diálogo Proteger [nome do nó], se desejar utilizar um repositório diferente do repositório da configuração padrão, utilize a lista suspensa para selecionar um repositório.
8. Se desejar proteger pontos de recuperação para esse cluster utilizando a criptografia com base no Core, utilize a lista suspensa para selecionar uma chave de criptografia.
9. Se não quiser que a proteção comece imediatamente após a conclusão desse procedimento, selecione **Pausar proteção inicialmente**.
10. Para inserir as definições personalizadas (por exemplo, para personalizar o programa de proteção dos volumes compartilhados), faça o seguinte:
    a. Para personalizar as configurações de um volume individual, ao lado do volume que você deseja personalizar, clique em **Função**, ao lado do volume relevante.
    b. Consulte Criar programações de proteção personalizada no Modo Simples.
11. Clique em **Protect** (Proteger).

Criar programações de proteção personalizada no Modo Simples

O procedimento para a criação de uma programação de proteção personalizada de dentro de um assistente de proteção é idêntico ao procedimento para a criação de uma programação de proteção de uma máquina existente no Modo Simples. As programações de proteção criadas em um assistente ou no Modo Simples não são salvas como modelos. Para criar modelos ou várias programações de proteção, consulte Criar vários períodos de programação de proteção no Modo Avançado. Execute as etapas descritas neste procedimento para criar programações personalizadas usando o Rapid Recovery para fazer backup de dados das máquinas protegidas.

1. Selecione uma das seguintes opções:
   - Se estiver usando um assistente de proteção (Proteger máquina, Proteger várias máquinas, Proteção de um cluster), na página **Proteção** do assistente, selecione **Proteção personalizada** e, em seguida, clique em **Avançar**.
   - Se estiver criando uma programação de proteção para uma máquina que já está protegida, na página Resumo da máquina protegida, expanda os volumes da máquina protegida, selecione os volumes aplicáveis e clique em **Definir uma programação**.

   A página ou a caixa de diálogo **Programação de proteção** é exibida.
2. Na página ou na caixa de diálogo **Programação de proteção**, siga uma das seguintes opções:
   - Para definir um período de proteção que execute em determinados dias e em horários especificados, selecione **Períodos** e depois vá para a Etapa 3.
   - Para definir um horário específico para fazer o backup da máquina todos os dias, selecione **Horário de proteção diária** e, em seguida, continue na Etapa 7.
3. Para alterar a programação de intervalos para qualquer período, siga as seguintes etapas:
   a. Crie um período de tempo, selecionando uma hora **De** e uma hora **Até**.

b. Para cada período, clique na caixa de texto de intervalo e digite um intervalo apropriado em minutos.

Por exemplo, destaque o intervalo padrão de 60 e o substitua pelo valor 20 para realizar snapshots a cada 20 minutos durante esse período.

4. Para personalizar os instantâneos para horários comerciais de pico e fora de pico, siga as seguintes etapas: defina um intervalo ideal para o intervalo de pico, selecione **Obter instantâneos no restante do tempo** e, em seguida, defina um intervalo fora do horário de pico da seguinte forma:
   a. Selecione **Dias úteis**.
   b. Defina as horas **De** e **Até** para criar um intervalo durante o seu horário comercial de pico.
   c. Na caixa **A cada X minutos**, digite um intervalo em minutos para com que frequência o Rapid Recovery deve criar pontos de recuperação durante este intervalo de horário comercial de pico.

   Por exemplo, destaque o intervalo padrão de 60 e o substitua pelo valor 20 para realizar snapshots a cada 20 minutos durante esse o intervalo de hora selecionado para esse período.
   d. Para programar instantâneos durante horários comerciais fora do horário de pico, selecione **Obter instantâneos no restante do tempo**.
   e. Na caixa **A cada X minutos**, digite um intervalo em minutos para com que frequência o Rapid Recovery deve criar pontos de recuperação durante este intervalo de horário comercial fora de pico.

   Por exemplo, como há menos atividade de negócios durante essas horas e menos alterações para fazer backup, você pode decidir tomar um número menor de instantâneos e manter o intervalo padrão de 60 minutos.
5. Vá para a Etapa 7.
6. Para definir uma única hora do dia para uma única cópia de segurança diária, selecione **Tempo de proteção diária** e insira a hora no formato HH:MM. Por exemplo, para fazer uma cópia de segurança diária às 21h, insira 21:00.
7. Para definir a programação sem iniciar as cópias de segurança, selecione **Pausar proteção inicialmente**.

   Depois que a proteção é pausada no assistente, ela permanece em pausa até que você a retome explicitamente. Depois de retomar a proteção, as cópias de segurança ocorrerão com base na programação estabelecida. Para obter mais informações sobre como retomar proteção, consulte Como pausar e retomar proteção.
8. Quando estiver satisfeito com as alterações feitas na sua programação de proteção, clique em **Concluir** ou **Avançar**, conforme o caso.

   Se você estiver usando um assistente, vá para a próxima etapa do assistente. Consulte o procedimento do assistente apropriado para concluir os requisitos restantes.

See also: Noções básicas sobre programações de proteção
See also: Criar programações de proteção personalizada no Modo Simples
See also: Criar vários períodos de programação de proteção no Modo Avançado

Criar vários períodos de programação de proteção no Modo Avançado

Um programa de proteção define quando os backups são transferidos de máquinas protegidas para o Rapid Recovery Core. As programações de proteção são inicialmente definidas usando o Assistente de proteção de máquina ou o Assistente de proteção de diversas máquinas.

É possível modificar a programação de proteção existente a qualquer momento na página Resumo de uma máquina protegida específica.

NOTE: Para obter informações conceituais sobre o programa de proteção, consulte Noções básicas sobre programações de proteção. Para obter informações sobre a proteção de uma única máquina, consulte Proteção de uma máquina. Para obter informações sobre proteção em massa (de várias máquinas), consulte Sobre como proteger diversas máquinas. Para obter informações sobre personalização de períodos de proteção ao proteger um agente usando um desses assistentes, consulte Criar programações de proteção personalizada no Modo Simples. Para obter informações sobre a modificação de um programa de proteção existente, consulte Criar vários períodos de programação de proteção no Modo Avançado.

Execute as etapas deste procedimento para modificar uma programação de proteção existente para volumes de uma máquina protegida.

1. No Core Console, na lista de máquinas protegidas, clique no nome da máquina que tem o programa de proteção que você deseja alterar.
2. Na página Resumo da máquina que você selecionou, no painel Volumes, expanda os volumes da máquina protegida, selecione os volumes aplicáveis e, em seguida, clique em **Definir uma programação**.

   Inicialmente, todos os volumes compartilham uma programação de proteção.

   Para selecionar todos os volumes de uma só vez, clique na caixa de seleção na linha de cabeçalho. Clique em (Grupo de proteção) para expandir os volumes que estão sendo protegidos, de modo que você possa ver todos os volumes, e selecione um ou mais.

   NOTE: Normalmente, é uma boa prática proteger, no mínimo, o volume Reservado pelo sistema e o volume em que se encontra o sistema operacional (normalmente a unidade C).

   A caixa de diálogo **Programação de proteção** é exibida.
3. Na caixa de diálogo **Programação de proteção**, realize um dos procedimentos a seguir:
   - Para modificar o período de programação existente na página inicial da caixa de diálogo, que é chamado de Modo Simples, consulte o procedimento para Criar vários períodos de programação de proteção no Modo Avançado.
   - Se você tiver criado um modelo de programa de proteção anteriormente e quiser aplicá-lo a essa máquina protegida, clique em **Modo Avançado**, selecione o modelo na lista suspensa **Modelos**, clique em **OK** para confirmar e vá para a etapa 7.
   - Se você quiser remover um período existente do programa, desmarque as caixas de seleção ao lado de cada opção de período e vá para a etapa 7. Entre as opções estão:
     - Dias da semana (seg-sex): esse intervalo de tempo indica uma semana útil típica com cinco dias.
     - Fins de semana (sáb, dom): esse intervalo de tempo indica um fim de semana típico.
   - Se você quiser salvar um novo programa de proteção como um modelo, clique em **Modo Avançado** e continue na etapa 4.
4. Um período é um intervalo especificado durante o qual você determina quantos minutos devem passar entre cada instantâneo obtido. Se a hora inicial e final do dia da semana forem 00:00 a 23:59, existe um único período. Para alterar a hora inicial e final de um período definido, faça o seguinte:
   a. Selecione o período adequado.
   b. Para alterar a hora inicial desse período, use o ícone de relógio em **Hora inicial**.

   Por exemplo, use as setas para exibir o horário 08:00.

   c. Para alterar a hora final desse período, use o ícone de relógio em **Hora final**.

   Por exemplo, use as setas para exibir o horário 18:00.

   d. Altere o intervalo de acordo com suas necessidades. Por exemplo, ao definir um período de pico, altere o intervalo de 60 para 20 minutos para tirar snapshots três vezes por hora.

   Uma barra azul fornece uma representação visual deste intervalo.
5. Se você tiver definido um período diferente de 00:00 a 23:59 na etapa 7 e quiser que os backups sejam realizados nos intervalos de tempo restantes, você precisa adicionar mais períodos para definir a proteção fazendo o seguinte:

a. Na categoria adequada, clique em **Adicionar período**.

b. Clique no ícone de relógio e selecione as horas inicial e final desejadas, conforme apropriado.

Por exemplo, defina a hora inicial em 0h e a hora final em 7h59.

c. Altere o intervalo de acordo com suas necessidades. Por exemplo, ao definir um período fora do pico, altere o intervalo de 60 para 120 minutos para tirar snapshots a cada duas horas.

6. Se necessário, continue a criar mais períodos, definindo horas iniciais e finais e intervalos conforme apropriado.

> **NOTE:** Se quiser remover um período adicionado por você, clique no ícone de lixo no canto direito do período e clique em **Sim** para confirmar.

7. Para criar um modelo a partir do programa definido, clique em **Salvar como modelo**.
8. Na caixa de diálogo Salvar modelo, digite um nome para o modelo e clique em **Salvar**.
9. Quando seu programa de proteção atender às suas necessidades, clique em **Aplicar**.

A caixa de diálogo Programação de proteção é fechada.

See also: Noções básicas sobre programações de proteção
See also: Criar programações de proteção personalizada no Modo Simples
See also: Criar vários períodos de programação de proteção no Modo Avançado

Pausar e retomar a proteção

Ao pausar a proteção, você para temporariamente todas as transferências de dados da máquina selecionada para o Rapid Recovery Core. Quando você retoma a proteção, o Rapid Recovery Core segue os requisitos no programa de proteção, fazendo regularmente o backup dos dados com base nesse programa.

Você pode pausar a proteção para qualquer máquina protegida por Rapid Recovery:

- Ao estabelecer a proteção usando o Assistente de proteção de máquina ou o Assistente de proteção de diversas máquinas.
- No menu suspenso Máquinas protegidas na área de navegação à esquerda do Rapid Recovery Core (pausando a proteção para todas as máquinas protegidas).
- Na página Máquinas protegidas (acessível ao clicar no menu Máquinas protegidas).
- Em uma máquina protegida específica no menu suspenso Máquinas protegidas.
- Na parte superior de qualquer página de uma máquina protegida específica.

Se você pausar a proteção usando o Assistente de proteção de máquina ou o Assistente de proteção de diversas máquinas, ela será pausada até ser retomada explicitamente.

Se você pausar a proteção fora de um assistente, poderá escolher se quer fazer isso até ela ser retomada ou por um período designado (especificado em qualquer combinação de dias, horas e minutos). Se você pausar por um período, quando esse tempo acabar, o sistema retomará automaticamente a proteção com base na programação de proteção.

Você pode retomar a proteção para qualquer máquina protegida por Rapid Recovery pausada:

- No menu suspenso Máquinas protegidas na área de navegação à esquerda do Rapid Recovery Core (retomando a proteção para todas as máquinas protegidas).
- Em uma máquina protegida específica no menu suspenso Máquinas protegidas.
- Na página Máquinas protegidas (acessível ao clicar no menu Máquinas protegidas).
- Na parte superior de qualquer página de uma máquina protegida específica.

Use o procedimento a seguir para pausar ou retomar a proteção, conforme o caso.

1. No Rapid Recovery Core Console, para pausar a proteção de todas as máquinas, clique no menu suspenso Máquinas protegidas na área de navegação à esquerda e faça o seguinte:

a. Selecione **Pausar proteção**.

A caixa de diálogo Pausar proteção é exibida.

b. Selecione a definição apropriada, usando uma das opções descritas abaixo, e clique em **OK**.

- Se quiser pausar a proteção até retomá-la explicitamente, selecione **Pausar até ser retomada**.
- Se você quiser pausar a proteção por um período específico, selecione **Pausar por** e depois, nos controles de Dias, Horas e Minutos, digite ou selecione o período de pausa apropriado, conforme o caso.

2. Para retomar a proteção de todas as máquinas, faça o seguinte:
   a. Selecione **Retomar proteção**.

   A caixa de diálogo Retomar proteção é exibida.

   b. Na caixa de diálogo Retomar proteção, selecione **Sim**.

   A caixa de diálogo Retomar proteção é fechada e a proteção é retomada para todas as máquinas.
3. Para pausar a proteção de uma única máquina, na área de navegação à esquerda, clique no menu suspenso à direita da máquina que você deseja afetar e faça o seguinte:
   a. Selecione **Pausar proteção**.

   A caixa de diálogo Pausar proteção é exibida.

   b. Selecione a definição apropriada, usando uma das opções descritas abaixo, e clique em **OK**.

   - Se quiser pausar a proteção até retomá-la explicitamente, selecione **Pausar até ser retomada**.
   - Se você quiser pausar a proteção por um período específico, selecione **Pausar por** e depois, nos controles de Dias, Horas e Minutos, digite ou selecione o período de pausa apropriado, conforme o caso.
4. Para retomar a proteção de uma única máquina, faça o seguinte:
   a. Selecione **Retomar proteção**.

   A caixa de diálogo Retomar proteção é exibida.

   b. Na caixa de diálogo Retomar proteção, selecione **Sim**.

   A caixa de diálogo Retomar proteção é fechada e a proteção é retomada para a máquina selecionada.
5. Para pausar a proteção de uma única máquina nas páginas de máquina, navegue até a máquina que você deseja afetar.

   A página Resumo é exibida para a máquina selecionada.

   a. Na parte superior da página, clique em **Pausar**.

   A caixa de diálogo Pausar proteção é exibida.

   b. Selecione a definição apropriada, usando uma das opções descritas abaixo, e clique em **OK**.

   - Se quiser pausar a proteção até retomá-la explicitamente, selecione **Pausar até ser retomada**.
   - Se você quiser pausar a proteção por um período específico, selecione **Pausar por** e depois, nos controles de Dias, Horas e Minutos, digite ou selecione o período de pausa apropriado, conforme o caso.
6. Caso queira retomar a proteção, faça o seguinte:
   a. Na parte superior da página, clique em **Retomar**.
   b. Na caixa de diálogo Retomar proteção, clique em **Sim**.

   A caixa de diálogo Retomar proteção é fechada, e a proteção é retomada para a máquina selecionada.

Sobre como proteger diversas máquinas

Você pode adicionar duas ou mais máquinas Windows para proteção no Rapid Recovery Core simultaneamente usando o Assistente de proteção de diversas máquinas. Para proteger os dados usando o Rapid Recovery, você precisa adicionar as estações de trabalho e os servidores no Rapid Recovery Core Console; por exemplo, o Exchange Server, o SQL Server, o servidor Linux etc.

Assim como acontece na proteção de máquinas individuais, a proteção de diversas máquinas simultaneamente requer a instalação do software do agente Rapid Recovery em cada máquina que você deseja proteger.

NOTE: Como uma exceção a essa regra, caso esteja protegendo máquinas virtuais em um host do VMware/ESXi ou Hyper-V, você pode usar a proteção sem agente. Para obter mais informações, inclusive restrições da proteção sem agente, consulte Noções básicas sobre Rapid Snap for Virtual.

As máquinas protegidas devem ser configuradas com uma política de segurança que possibilite a instalação remota.

Para se conectar às máquinas, elas devem ser ligadas e estar acessíveis.

Há mais de um método de implementar o software Agent em várias máquinas simultaneamente. Por exemplo:

- Você pode instalar o software do agente Rapid Recovery em diversas máquinas usando o Assistente implantar software do agente. Para obter mais informações, consulte Como usar o assistente de implantação do software do agente para implantar em uma ou mais máquinas.
- Você pode implantar o software do agente Rapid Recovery como parte do Assistente de proteção de diversas máquinas.

O processo de proteger diversas máquinas inclui etapas opcionais que você pode acessar caso selecione uma configuração avançada. As opções avançadas incluem funções de repositório e criptografia. Por exemplo, você pode especificar um repositório do Rapid Recovery existente para salvar snapshots ou criar um novo repositório. Você também pode especificar uma chave de criptografia existente (ou adicionar uma nova chave de criptografia) para aplicar os dados salvos no Core para as máquinas protegidas.

O fluxo de trabalho do Assistente de proteção de diversas máquinas pode ser ligeiramente diferente com base no seu ambiente. Por exemplo, caso o software do agente Rapid Recovery esteja instalado nas máquinas que você deseja proteger, você não deve instalá-lo pelo assistente. Da mesma forma, caso um repositório já exista no Core, você não precisa criar um.

Ao proteger diversas máquinas, siga o procedimento apropriado, com base na configuração. Consulte as seguintes opções para proteger diversas máquinas:

- Como proteger diversas máquinas em um domínio Active Directory
- Proteger diversas máquinas em um host virtual VMware vCenter/ESXi
- Proteger diversas máquinas em um host virtual Hyper-V
- Como proteger diversas máquinas manualmente

Como proteger diversas máquinas em um domínio Active Directory

Use esse procedimento para proteger simultaneamente uma ou mais máquinas em um domínio Active Directory.

1. No Rapid Recovery Core Console, clique no menu suspenso **Proteger** e, em seguida, clique em **Proteger diversas máquinas**.

   O Assistente de proteção de diversas máquinas será exibido.
2. Na página **Bem-Vindo** do assistente, selecione uma das seguintes opções:
   - Típico
   - Avançado (exibir etapas opcionais)
3. Clique em **Avançar**.
4. Na página **Conexão** do assistente, na lista suspensa **Origem**, selecione **Active Directory**.
5. Insira as informações de domínio e as credenciais de logon conforme descrito na tabela a seguir.

Tabela 53. Informações e credenciais do domínio

Caixa de texto	Descrição
Host	O nome de host ou endereço IP do domínio Active Directory.
Nome de usuário	O nome de usuário utilizado para se conectar ao domínio, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
Senha	A senha usada para se conectar ao domínio.

6. Clique em **Avançar**.
7. Na página **Selecionar máquinas** do assistente, selecione as máquinas que você deseja proteger.

   O sistema verifica automaticamente todas as máquinas que você selecionou.
8. Clique em **Avançar**.

   Se a página **Proteção** for exibida em seguida no Assistente de proteção de diversas máquinas, vá para a Etapa 12.

   Se o software do agente ainda não tiver sido implementado nas máquinas que você deseja proteger ou se alguma das máquinas especificadas não puder ser protegida por outro motivo, as máquinas selecionadas aparecerão na página Avisos.
9. Como opção, na página **Avisos** do assistente, você pode verificar qualquer máquina selecionando a máquina e clicando em **Verificar** na barra de ferramentas.
10. Como opção, na página **Avisos**, selecione **Após a instalação do Agente, reiniciar as máquinas automaticamente**.

    NOTE: A Quest recomenda esta opção. Reinicie as máquinas agente antes de protegê-las.
11. Se o status indicar que a máquina está acessível, clique em **Avançar** para instalar o software Rapid Recovery Agent.

    A página **Proteção** é exibida.
12. Opcionalmente, na página **Proteção**, se você quiser um nome que não seja o endereço IP para ser exibido no Rapid Recovery Core Consolepara essa máquina protegida, digite um nome na caixa de diálogo no campo **Nome de exibição**.

Você pode inserir até 64 caracteres. Não use os caracteres especiais descritos no tópico . Além disso, não inicie o nome de exibição com nenhuma das combinações de caracteres descritas no tópico .

13. Selecione as configurações de programação de proteção adequadas, como descrito a seguir:

    - Para usar a programação de proteção padrão, na opção Definições de programação, selecione **Proteção padrão (instantâneos de todos os volumes a cada hora)**.

    Na programação de proteção padrão, o Core gera snapshots de todos os volumes na máquina protegida a cada hora. Para alterar as definições de proteção a qualquer momento depois de fechar o assistente, o que inclui a seleção dos volumes a serem protegidos, vá para a página **Resumo** da máquina protegida específica.

    - Para definir uma programação de proteção diferente, na opção Definições de programação, selecione **Proteção personalizada**.

14. Prossiga com a configuração da seguinte maneira:

    - Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção padrão tiver sido especificada, e se houver um repositório, clique em **Concluir** para confirmar suas escolhas, fechar o assistente e proteger a máquina especificada.
    - Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção padrão tiver sido especificada, e se houver um repositório, clique em **Avançar** e vá para a Etapa 17 para criar um repositório.
    - Se uma configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** e continue na etapa seguinte para escolher os volumes a proteger.
    - Se você tiver selecionado uma configuração avançada no Assistente de proteção de máquina e especificado a proteção padrão, clique em **Avançar** e continue para a Etapa 17 para ver as opções de repositório e criptografia.
    - Se a configuração Avançado tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** e continue na etapa seguinte para escolher os volumes a proteger.

    Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.

15. Na página **Volumes de proteção**, selecione os volumes que deseja proteger. Se você não deseja incluir na proteção algum volume relacionado, clique na coluna Verificar para limpar a seleção. Depois, clique em **Avançar**.

    NOTE: Normalmente, é uma boa prática proteger, no mínimo, o volume Reservado pelo sistema e o volume em que se encontra o sistema operacional (normalmente a unidade C).

16. Na página **Programa de proteção**, defina um programa de proteção personalizado e clique em **Avançar**. Para obter detalhes sobre a definição de uma programação de proteção personalizada, consulte Criar programações de proteção personalizada no Modo Simples.

    Se as informações de repositório já estiverem configuradas e você tiver selecionado a opção Avançado na Etapa 1, a página Criptografia é exibida. Vá para a Etapa 20.

17. Na página **Repositório**, faça o seguinte:

    - Se você já tiver um repositório e quiser armazenar os dados dessa máquina para proteção no repositório existente, faça o seguinte:

      1. Selecione **Utilize um repositório existente**.
      2. Selecione um repositório existente na lista.
      3. Clique em **Avançar**.

A página **Criptografia** é exibida. Passe à Etapa 20 para definir criptografia como opção.

- Se deseja criar um repositório, clique na página **Repositório**, insira as informações descritas na tabela a seguir e, em seguida, clique em **Avançar** ou em **Concluir**, conforme apropriado.

Tabela 54. Configurações do repositório

Caixa de texto	Descrição
Nome	Insira o nome de exibição do repositório. Por padrão, essa caixa de texto consiste na palavra Repositório e um número, que corresponde ao número de repositórios neste Core. Por exemplo, se este for o primeiro repositório, o nome padrão é Repositório 1. Altere o nome conforme a necessidade. Nomes de repositório devem conter entre 1 e 40 caracteres alfanuméricos, incluindo espaços. Não use ou .
Local	Insira o local para armazenar os dados protegidos. Esse volume deve ser um local de armazenamento principal. A localização pode ser local (uma unidade no Core) ou pode ser uma unidade de rede de compartilhamento CIFS. Para um compartilhamento CIFS, o caminho deve começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido. **CAUTION: Defina uma pasta dedicada na raiz do local de armazenamento do seu repositório. Não especifique o local da raiz. Por exemplo, use `E:\Repository\`, e não `E:\`. Se o repositório que você está criando nessa etapa for removido mais tarde, todos os arquivos no local de armazenamento do seu repositório serão excluídos. Se você definir o local de armazenamento na raiz, todos os outros arquivos no volume (por exemplo: `E:\`) são excluídos, o que poderia resultar em uma perda de dados catastrófica.** Por exemplo, digite `X:\Repository\Data`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Digite um nome de usuário para um usuário com acesso administrativo. Essa informação é necessária somente quando o local do repositório especificado é um caminho da rede.
Senha	Digite a senha para o usuário com acesso administrativo. Essa informação é necessária somente quando o local do repositório especificado é um caminho da rede.
Caminho de metadados	Insira o local para armazenar os metadados protegidos. Por exemplo, digite `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

18. Na página **Configuração de repositório**, configure a quantidade de espaço em disco a ser alocada para o repositório. A Quest recomenda reservar 20% do volume para metadados, que é o padrão. Opcionalmente,

usando o controle deslizante ou o campo **Tamanho**, você pode alocar mais ou menos espaço no volume para o repositório.

19. Opcionalmente, se você deseja exibir e inserir informações detalhadas sobre as configurações do local de armazenamento, selecione **Mostrar opções avançadas** e ajuste as configurações conforme descrito na tabela a seguir. Para ocultar essas opções, desmarque a opção **Exibir opções avançadas**. Ao concluir a configuração do repositório, clique em **Avançar** ou em **Concluir**, conforme apropriado.

Tabela 55. Detalhes da Configuração de armazenamento

Caixa de texto	Descrição
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é 512.
Bytes por registro	Especifique a média de bytes por registro. O valor padrão é 8192.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Em • Desligar • Sincronizar Se definido como Ligado, que é o padrão, o Windows controla o armazenamento em cache. Isso é apropriado para o Windows 10 e para versões do Windows Server 2012 e posterior. **NOTE:** Definir a política de cache de gravação como Ligado pode resultar em desempenho mais rápido. Se você estiver utilizando o Windows Server 2008 R2 SP2, a recomendação de configuração será Desativado. Se configurado como Desativado, o Rapid Recovery controla o armazenamento em cache. Se definido como Sincronizar, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.

Se você selecionar a opção **Avançado** Etapa 1, a página **Criptografia** é exibida.

20. Opcionalmente, na página **Criptografia**, se você deseja usar chaves de criptografia para os dados armazenados no repositório, selecione **Criptografar dados em repouso em um repositório** e, em seguida, execute uma das seguintes ações:
    - Para selecionar uma chave de criptografia existente a ser aplicada a todos os novos dados armazenados no repositório, selecione **Criptografar dados usando criptografia baseada no Core com uma chave existente**, e, no menu suspenso **Selecionar chave de criptografia**, selecione a chave de criptografia.
    - Para definir uma nova chave de criptografia neste momento a ser aplicada a todos os futuros dados armazenados no repositório, selecione **Criptografar dados usando criptografia baseada no Core com uma nova chave**, e, em seguida, digite as informações referentes à chave, conforme descrito na tabela abaixo:

Tabela 56. Definir nova chave de criptografia

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia.

Caixa de texto	Descrição
	Os nomes de chaves de criptografia devem ter entre 1 e 64 caracteres alfanuméricos. Não use caracteres proibidos ou frases proibidas.
Descrição	Insira um comentário descritivo para a chave de criptografia. Essas informações aparecem no campo Descrição ao visualizar uma lista de chaves de criptografia no Rapid Recovery Core Console. As descrições podem conter até 254 caracteres. A melhor prática é evitar o uso de caracteres proibidos e frases proibidas.
Senha	Insira a frase de acesso usada para controlar o acesso. A melhor prática é evitar o uso de caracteres proibidos. Armazene a frase de acesso em um local seguro. O Suporte de proteção de dados da Quest não pode recuperar uma senha. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais máquinas protegidas, você não poderá recuperar os dados caso perca a frase de acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso. Usado para confirmar a entrada da frase de acesso.

21. Opcionalmente, na página **Criptografia**, para criptografar todos os dados transportados em uma rede, selecione **Criptografar os dados transportados em uma rede**. Essa opção é ativada por padrão; portanto, se não quiser criptografar dados dessa forma, desmarque essa opção.
22. Clique em **Concluir** para salvar e aplicar suas definições.

    Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.

O software Rapid Recovery Agent é implantado nas máquinas especificadas, se necessário, e as máquinas são adicionadas à proteção no Core.

Proteger diversas máquinas em um host virtual VMware vCenter/ESXi

Use este procedimento para proteger simultaneamente uma ou mais máquinas em um host virtual VMware vCenter/ESXi.

CAUTION: Se você usar proteção sem agente, a Quest **recomenda que você limite a proteção para não mais de 200.VMs ao mesmo tempo. Por exemplo, não selecione mais de 200 VMs ao usar o Assistente de proteção de diversas máquinas. Proteger mais de 200 VMs resultará em lentidão no desempenho. Não há limite de quantas VMs um Core pode proteger sem agente com o passar do tempo. Por exemplo, você pode proteger 200 VMs hoje em dia e outras 200 VMs amanhã.**

1. No Rapid Recovery Core Console, clique no menu suspenso **Proteger** e, em seguida, clique em **Proteger diversas máquinas**.

O Assistente de proteção de diversas máquinas será exibido.

2. Na página **Bem-Vindo**, selecione uma das seguintes opções:
   - Típico
   - Avançado (exibir etapas opcionais)
3. Clique em **Avançar**.
4. Na página **Conexão** do assistente, na lista suspensa **Origem**, selecione **vCenter / ESXi**.
5. Insira as informações do host e insira as credenciais conforme descrito na tabela a seguir.

Tabela 57. Definições de conexão do vCenter/ESXi

Caixa de texto	Descrição
Host	O nome ou endereço IP do host virtual VMware vCenter Server/ESXi.
Porta	A porta usada para se conectar ao host virtual. A definição padrão é 443.
Nome de usuário	O nome de usuário utilizado para se conectar ao host virtual; por exemplo, Administrador ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador.
Senha	A senha usada para se conectar ao host virtual.

   - Para usar proteção sem agente, selecione **Proteger VMs selecionadas sem agente**e, em seguida, consulte Proteger máquinas virtuais vCenter/ESXi usando a proteção sem agente.
6. Clique em **Avançar**.
7. Na página **Selecionar computadores**, realize um dos procedimentos a seguir:
   - Na lista visível de VMs, selecione as VMs que você deseja proteger.
   - Para navegar através da estrutura de árvore do VMware para localizar mais VMs, clique em **Exibir árvore** e selecione **Hosts e clusters** ou **VMs e modelos**. Selecione as VMs que deseja proteger.

   Uma notificação será exibida se o Rapid Recovery detectar que uma máquina está offline ou não tem as ferramentas VMware instaladas.
8. Clique em **Avançar**.
9. Na página **Ajustes**, digite as credenciais para cada máquina no seguinte formato: `hostname::username::password`.

   NOTE: Insira uma máquina em cada linha.
10. Clique em **Avançar**.

    Se a página **Proteção** for exibida em seguida no Assistente de proteção de diversas máquinas, vá para a Etapa 14.

    Se o software do agente ainda não tiver sido implementado nas máquinas que você deseja proteger ou se alguma das máquinas especificadas não puder ser protegida por outro motivo, as máquinas selecionadas aparecerão na página **Avisos**.
11. Como opção, na página **Avisos**, você pode confirmar qualquer máquina selecionando-a e depois clicando em **Verificar** na barra de ferramentas.
12. Como opção, na página **Avisos**, selecione **Após a instalação do Agente, reiniciar as máquinas automaticamente**.

    NOTE: A Quest recomenda esta opção. Reinicie as máquinas agente antes de protegê-las.
13. Se o status indicar que a máquina está acessível, clique em **Avançar** para instalar o software Agent.

A página **Proteção** é exibida.

14. Opcionalmente, na página **Proteção**, se você quiser um nome que não seja o endereço IP para ser exibido no Rapid Recovery Core Consolepara essa máquina protegida, digite um nome na caixa de diálogo no campo **Nome de exibição**.

    Você pode inserir até 64 caracteres. Não use os caracteres especiais descritos no tópico . Além disso, não inicie o nome de exibição com nenhuma das combinações de caracteres descritas no tópico .

15. Selecione as configurações de programação de proteção adequadas, como descrito a seguir:

    - Para usar a programação de proteção padrão, na opção Definições de programação, selecione **Proteção padrão (instantâneos de todos os volumes a cada hora)**.

    Na programação de proteção padrão, o Core gera snapshots de todos os volumes na máquina protegida a cada hora. Para alterar as definições de proteção a qualquer momento depois de fechar o assistente, o que inclui a seleção dos volumes a serem protegidos, vá para a página **Resumo** da máquina protegida específica.

    - Para definir uma programação de proteção diferente, na opção Definições de programação, selecione **Proteção personalizada**.

16. Prossiga com a configuração da seguinte maneira:

    - Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção padrão tiver sido especificada, e se houver um repositório, clique em **Concluir** para confirmar suas escolhas, fechar o assistente e proteger a máquina especificada.
    - Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção padrão tiver sido especificada, e se houver um repositório, clique em **Avançar** e vá para a Etapa 19 para criar um repositório.
    - Se uma configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** e continue na etapa seguinte para escolher os volumes a proteger.
    - Se você tiver selecionado uma configuração avançada no Assistente de proteção de máquina e especificado a proteção padrão, clique em **Avançar** e continue para a Etapa 19 para ver as opções de repositório e criptografia.
    - Se a configuração Avançado tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** e continue na etapa seguinte para escolher os volumes a proteger.

    Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.

17. Na página **Volumes de proteção**, selecione os volumes que deseja proteger. Se você não deseja incluir na proteção algum volume relacionado, clique na coluna Verificar para limpar a seleção. Depois, clique em **Avançar**.

    NOTE: Normalmente, é uma boa prática proteger, no mínimo, o volume Reservado pelo sistema e o volume em que se encontra o sistema operacional (normalmente a unidade C).

18. Na página **Programa de proteção**, defina um programa de proteção personalizado e clique em **Avançar**. Para obter detalhes sobre a definição de uma programação de proteção personalizada, consulte Criar programações de proteção personalizada no Modo Simples.

    Se as informações de repositório já estiverem configuradas e você tiver selecionado a opção Avançado na Etapa 1, a página Criptografia é exibida. Vá para a Etapa 22.

19. Na página **Repositório**, faça o seguinte:

    - Se você já tiver um repositório e quiser armazenar os dados dessa máquina para proteção no repositório existente, faça o seguinte:

      1. Selecione **Utilize um repositório existente**.

2. Selecione um repositório existente na lista.
3. Clique em **Avançar**.

   A página **Criptografia** é exibida. Passe à Etapa 22 para definir criptografia como opção.

- Se deseja criar um repositório, clique na página **Repositório**, insira as informações descritas na tabela a seguir e, em seguida, clique em **Avançar** ou em **Concluir**, conforme apropriado.

Tabela 58. Configurações do repositório

Caixa de texto	Descrição
Nome	Insira o nome de exibição do repositório. Por padrão, essa caixa de texto consiste na palavra Repositório e um número, que corresponde ao número de repositórios neste Core. Por exemplo, se este for o primeiro repositório, o nome padrão é Repositório 1. Altere o nome conforme a necessidade. Nomes de repositório devem conter entre 1 e 40 caracteres alfanuméricos, incluindo espaços. Não use ou .
Local	Insira o local para armazenar os dados protegidos. Esse volume deve ser um local de armazenamento principal. A localização pode ser local (uma unidade no Core) ou pode ser uma unidade de rede de compartilhamento CIFS. Para um compartilhamento CIFS, o caminho deve começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido. **CAUTION: Defina uma pasta dedicada na raiz do local de armazenamento do seu repositório. Não especifique o local da raiz. Por exemplo, use `E:\Repository\`, e não `E:\`. Se o repositório que você está criando nessa etapa for removido mais tarde, todos os arquivos no local de armazenamento do seu repositório serão excluídos. Se você definir o local de armazenamento na raiz, todos os outros arquivos no volume (por exemplo: `E:\`) são excluídos, o que poderia resultar em uma perda de dados catastrófica.** Por exemplo, digite `X:\Repository\Data`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Digite um nome de usuário para um usuário com acesso administrativo. Essa informação é necessária somente quando o local do repositório especificado é um caminho da rede.
Senha	Digite a senha para o usuário com acesso administrativo. Essa informação é necessária somente quando o local do repositório especificado é um caminho da rede.
Caminho de metadados	Insira o local para armazenar os metadados protegidos. Por exemplo, digite `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

20. Na página **Configuração de repositório**, configure a quantidade de espaço em disco a ser alocada para o repositório. A Quest recomenda reservar 20% do volume para metadados, que é o padrão. Opcionalmente,

usando o controle deslizante ou o campo **Tamanho**, você pode alocar mais ou menos espaço no volume para o repositório.

21. Opcionalmente, se você deseja exibir e inserir informações detalhadas sobre as configurações do local de armazenamento, selecione **Mostrar opções avançadas** e ajuste as configurações conforme descrito na tabela a seguir. Para ocultar essas opções, desmarque a opção **Exibir opções avançadas**. Ao concluir a configuração do repositório, clique em **Avançar** ou em **Concluir**, conforme apropriado.

Tabela 59. Detalhes da Configuração de armazenamento

Caixa de texto	Descrição
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é 512.
Bytes por registro	Especifique a média de bytes por registro. O valor padrão é 8192.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Em • Desligar • Sincronizar Se definido como Ligado, que é o padrão, o Windows controla o armazenamento em cache. Isso é apropriado para o Windows 10 e para versões do Windows Server 2012 e posterior. **NOTE:** Definir a política de cache de gravação como Ligado pode resultar em desempenho mais rápido. Se você estiver utilizando o Windows Server 2008 R2 SP2, a recomendação de configuração será Desativado. Se configurado como Desativado, o Rapid Recovery controla o armazenamento em cache. Se definido como Sincronizar, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.

Se você selecionar a opção **Avançado** Etapa 1, a página **Criptografia** é exibida.

22. Opcionalmente, na página **Criptografia**, se você deseja usar chaves de criptografia para os dados armazenados no repositório, selecione **Criptografar dados em repouso em um repositório** e, em seguida, execute uma das seguintes ações:
    - Para selecionar uma chave de criptografia existente a ser aplicada a todos os novos dados armazenados no repositório, selecione **Criptografar dados usando criptografia baseada no Core com uma chave existente**, e, no menu suspenso **Selecionar chave de criptografia**, selecione a chave de criptografia.
    - Para definir uma nova chave de criptografia neste momento a ser aplicada a todos os futuros dados armazenados no repositório, selecione **Criptografar dados usando criptografia baseada no Core com uma nova chave**, e, em seguida, digite as informações referentes à chave, conforme descrito na tabela abaixo:

Tabela 60. Definir nova chave de criptografia

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia.

Caixa de texto	Descrição
	Os nomes de chaves de criptografia devem ter entre 1 e 64 caracteres alfanuméricos. Não use caracteres proibidos ou frases proibidas.
Descrição	Insira um comentário descritivo para a chave de criptografia. Essas informações aparecem no campo Descrição ao visualizar uma lista de chaves de criptografia no Rapid Recovery Core Console. As descrições podem conter até 254 caracteres. A melhor prática é evitar o uso de caracteres proibidos e frases proibidas.
Senha	Insira a frase de acesso usada para controlar o acesso. A melhor prática é evitar o uso de caracteres proibidos. Armazene a frase de acesso em um local seguro. O Suporte de proteção de dados da Quest não pode recuperar uma senha. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais máquinas protegidas, você não poderá recuperar os dados caso perca a frase de acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso. Usado para confirmar a entrada da frase de acesso.

23. Opcionalmente, na página **Criptografia**, para criptografar todos os dados transportados em uma rede, selecione **Criptografar os dados transportados em uma rede**. Essa opção é ativada por padrão; portanto, se não quiser criptografar dados dessa forma, desmarque essa opção.
24. Clique em **Concluir** para salvar e aplicar suas definições.

    Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.

O software Rapid Recovery Agent é implantado nas máquinas especificadas, se necessário, e as máquinas são adicionadas à proteção no Core.

Proteger máquinas virtuais vCenter/ESXi usando a proteção sem agente

Conclua o procedimento a seguir para proteger máquinas virtuais ESX sem agente.

NOTE: Rapid Recovery recomenda que Ferramentas VMware sejam instaladas em máquinas virtuais (VMs) que você deseja proteger em hosts ESXi ou vSphere. Quando Ferramentas VMware são instaladas em uma VM usando-se um sistema operacional (OS) Windows, os backups que o Core do Rapid Recovery captura usam Microsoft Volume Shadow Services (VSS). Para obter informações sobre o comportamento de VMs sem agente com ou sem Ferramentas VMware, consulte Benefícios de instalar as ferramentas do hipervisor para proteção sem agente.

CAUTION: A Quest **recomenda limitar a proteção sem agente a não mais do que 200 VMs por vez. Por exemplo, não selecione mais de 200 VMs ao usar o Assistente de proteção de diversas máquinas. Proteger mais de 200 VMs resultará em lentidão no desempenho. Não há limite de quantas VMs um Core pode proteger sem agente com o passar do tempo. Por exemplo, você pode proteger 200 VMs hoje em dia e outras 200 VMs amanhã.**

1. No Console do Rapid Recovery Core, clique no menu suspenso **Proteger** e, em seguida, clique em **Proteger diversas máquinas**.

O Assistente de proteção de diversas máquinas será exibido.

2. Na página **Bem-Vindo**, selecione uma das seguintes opções:
   - Típico
   - Avançado (exibir etapas opcionais)
3. Clique em **Avançar**.
4. Na página **Conexão** do assistente, na lista suspensa **Origem**, selecione **vCenter/ESX(i)**.
5. Insira as informações do host e insira as credenciais conforme descrito na tabela a seguir.

Tabela 61. Definições de conexão do vCenter/ESX(i)

Caixa de texto	Descrição
Host	Nome ou endereço IP do host virtual.
Porta	A porta usada para se conectar ao host virtual. A definição padrão é 443.
Nome de usuário	O nome de usuário utilizado para se conectar ao host virtual; por exemplo, Administrador ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador.
Senha	A senha usada para se conectar ao host virtual.

6. Certifique-se de que **Proteger VMs selecionadas sem agente** esteja marcado. (Essa opção é selecionada por padrão.)
7. Na página **Selecionar computadores**, realize um dos procedimentos a seguir:
   - Na lista visível de VMs, selecione as VMs que você deseja proteger.
   - Para navegar através da estrutura de árvore do VMware para localizar mais VMs, clique em **Exibir árvore** e selecione **Hosts e clusters** ou **VMs e modelos**. Selecione as VMs que deseja proteger.
8. Caso você queira proteger automaticamente novas VMs quando elas forem adicionadas ao host, selecione **Proteger máquinas novas automaticamente** e, em seguida, clique em **Avançar**.

   NOTE: VMware Changed Block Tracking (CBT) deve estar ativado em todas as VMs que você deseja proteger. Caso ele não esteja habilitado, o Rapid Recovery habilita automaticamente o CBT para assegurar a proteção.

   a. Na página **Proteção automática**, selecione todos os contêineres nos quais você deseja adicionar novas máquinas.
9. Clique em **Avançar**.

   Se a página **Proteção** for exibida em seguida no Assistente de proteção de diversas máquinas, vá para a Etapa 12.

   Se o software do agente ainda não tiver sido implementado nas máquinas que você deseja proteger ou se alguma das máquinas especificadas não puder ser protegida por outro motivo, as máquinas selecionadas aparecerão na página **Avisos**.
10. Como opção, na página **Avisos**, você pode confirmar qualquer máquina selecionando-a e depois clicando em **Verificar** na barra de ferramentas.
11. Clique em **Avançar**.

    A **Proteção** é exibida.
12. Selecione as configurações de programação de proteção adequadas, como descrito a seguir:
    - Para usar a programação de proteção padrão, na opção Definições de programação, selecione **Proteção padrão (instantâneos de todos os volumes a cada hora)**.

Na programação de proteção padrão, o Core gera snapshots de todos os volumes na máquina protegida a cada hora. Para alterar as definições de proteção a qualquer momento depois de fechar o assistente, o que inclui a seleção dos volumes a serem protegidos, vá para a página **Resumo** da máquina protegida específica.

- Para definir uma programação de proteção diferente, na opção Definições de programação, selecione **Proteção personalizada**.

13. Prossiga com a configuração da seguinte maneira:
    - Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção padrão tiver sido especificada, e se houver um repositório, clique em **Concluir** para confirmar suas escolhas, fechar o assistente e proteger a máquina especificada.
    - Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção padrão tiver sido especificada, e se houver um repositório, clique em **Avançar** e vá para a Etapa 15 para criar um repositório.
    - Se uma configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** e continue na etapa seguinte para escolher os volumes a proteger.
    - Se você tiver selecionado uma configuração avançada no Assistente de proteção de máquina e especificado a proteção padrão, clique em **Avançar** e continue para a Etapa 15 para ver as opções de repositório e criptografia.
    - Se a configuração Avançado tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** e continue na etapa seguinte para escolher os volumes a proteger.

    Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.
14. Na página **Programa de proteção**, defina um programa de proteção personalizado e clique em **Avançar**. Para obter detalhes sobre a definição de uma programação de proteção personalizada, consulte Criar programações de proteção personalizada no Modo Simples.

    Se as informações de repositório já estiverem configuradas e você tiver selecionado a opção Avançado na Etapa 1, a página Criptografia é exibida. Vá para a Etapa 18.
15. Na página **Repositório**, faça o seguinte:
    - Se você já tiver um repositório e quiser armazenar os dados dessa máquina para proteção no repositório existente, faça o seguinte:
        1. Selecione **Utilize um repositório existente**.
        2. Selecione um repositório existente na lista.
        3. Clique em **Avançar**.

        A página **Criptografia** é exibida. Passe à Etapa 18 para definir criptografia como opção.
    - Se deseja criar um repositório, clique na página **Repositório**, insira as informações descritas na tabela a seguir e, em seguida, clique em **Avançar** ou em **Concluir**, conforme apropriado.

Tabela 62. Configurações do repositório

Caixa de texto	Descrição
Nome	Insira o nome de exibição do repositório. Por padrão, essa caixa de texto consiste na palavra Repositório e um número, que corresponde ao número de repositórios neste Core. Por exemplo, se este for o primeiro repositório, o nome padrão é Repositório 1. Altere o nome conforme a necessidade.

Caixa de texto	Descrição
	Nomes de repositório devem conter entre 1 e 40 caracteres alfanuméricos, incluindo espaços. Não use ou .
Local	Insira o local para armazenar os dados protegidos. Esse volume deve ser um local de armazenamento principal. A localização pode ser local (uma unidade no Core) ou pode ser uma unidade de rede de compartilhamento CIFS. Para um compartilhamento CIFS, o caminho deve começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido. **CAUTION: Defina uma pasta dedicada na raiz do local de armazenamento do seu repositório. Não especifique o local da raiz. Por exemplo, use `E:\Repository\`, e não `E:\`. Se o repositório que você está criando nessa etapa for removido mais tarde, todos os arquivos no local de armazenamento do seu repositório serão excluídos. Se você definir o local de armazenamento na raiz, todos os outros arquivos no volume (por exemplo: `E:\`) são excluídos, o que poderia resultar em uma perda de dados catastrófica.** Por exemplo, digite `X:\Repository\Data`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Digite um nome de usuário para um usuário com acesso administrativo. Essa informação é necessária somente quando o local do repositório especificado é um caminho da rede.
Senha	Digite a senha para o usuário com acesso administrativo. Essa informação é necessária somente quando o local do repositório especificado é um caminho da rede.
Caminho de metadados	Insira o local para armazenar os metadados protegidos. Por exemplo, digite `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

16. Na página **Configuração de repositório**, configure a quantidade de espaço em disco a ser alocada para o repositório. A Quest recomenda reservar 20% do volume para metadados, que é o padrão. Opcionalmente, usando o controle deslizante ou o campo **Tamanho**, você pode alocar mais ou menos espaço no volume para o repositório.
17. Opcionalmente, se você deseja exibir e inserir informações detalhadas sobre as configurações do local de armazenamento, selecione **Mostrar opções avançadas** e ajuste as configurações conforme descrito na tabela a seguir. Para ocultar essas opções, desmarque a opção **Exibir opções avançadas**. Ao concluir a configuração do repositório, clique em **Avançar** ou em **Concluir**, conforme apropriado.

Tabela 63. Detalhes da Configuração de armazenamento

Caixa de texto	Descrição
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é 512.

Caixa de texto	Descrição
Bytes por registro	Especifique a média de bytes por registro. O valor padrão é 8192.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Em • Desligar • Sincronizar Se definido como Ligado, que é o padrão, o Windows controla o armazenamento em cache. Isso é apropriado para o Windows 10 e para versões do Windows Server 2012 e posterior. **NOTE:** Definir a política de cache de gravação como Ligado pode resultar em desempenho mais rápido. Se você estiver utilizando o Windows Server 2008 R2 SP2, a recomendação de configuração será Desativado. Se configurado como Desativado, o Rapid Recovery controla o armazenamento em cache. Se definido como Sincronizar, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.

Se você selecionar a opção **Avançado** Etapa 1, a página **Criptografia** é exibida.

18. Opcionalmente, na página **Criptografia**, se você deseja usar chaves de criptografia para os dados armazenados no repositório, selecione **Criptografar dados em repouso em um repositório** e, em seguida, execute uma das seguintes ações:
    - Para selecionar uma chave de criptografia existente a ser aplicada a todos os novos dados armazenados no repositório, selecione **Criptografar dados usando criptografia baseada no Core com uma chave existente**, e, no menu suspenso **Selecionar chave de criptografia**, selecione a chave de criptografia.
    - Para definir uma nova chave de criptografia neste momento a ser aplicada a todos os futuros dados armazenados no repositório, selecione **Criptografar dados usando criptografia baseada no Core com uma nova chave**, e, em seguida, digite as informações referentes à chave, conforme descrito na tabela abaixo:

Tabela 64. Definir nova chave de criptografia

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia. Os nomes de chaves de criptografia devem ter entre 1 e 64 caracteres alfanuméricos. Não use caracteres proibidos ou frases proibidas.
Descrição	Insira um comentário descritivo para a chave de criptografia. Essas informações aparecem no campo Descrição ao visualizar uma lista de chaves de criptografia no Rapid Recovery Core Console. As descrições podem conter até 254 caracteres. A melhor prática é evitar o uso de caracteres proibidos e frases proibidas.
Senha	Insira a frase de acesso usada para controlar o acesso. A melhor prática é evitar o uso de caracteres proibidos. Armazene a frase de acesso em um local seguro. O Suporte de proteção de dados da Quest não pode recuperar uma senha. Depois de criar uma chave de criptografia e

Caixa de texto	Descrição
	aplicá-la a uma ou mais máquinas protegidas, você não poderá recuperar os dados caso perca a frase de acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso. Usado para confirmar a entrada da frase de acesso.

19. Opcionalmente, na página **Criptografia**, para criptografar todos os dados transportados em uma rede, selecione **Criptografar os dados transportados em uma rede**. Essa opção é ativada por padrão; portanto, se não quiser criptografar dados dessa forma, desmarque essa opção.
20. Clique em **Concluir** para salvar e aplicar suas definições.

    Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.

Proteger diversas máquinas em um host virtual Hyper-V

Use este procedimento para proteger simultaneamente uma ou mais máquinas em um host virtual Hyper-V.

CAUTION: Se você usar proteção sem agente, a Quest recomenda que você limite a proteção para não mais de 200.VMs ao mesmo tempo. Por exemplo, não selecione mais de 200 VMs ao usar o Assistente de proteção de diversas máquinas. Proteger mais de 200 VMs resultará em lentidão no desempenho. Não há limite de quantas VMs um Core pode proteger sem agente com o passar do tempo. Por exemplo, você pode proteger 200 VMs hoje em dia e outras 200 VMs amanhã.

1. No Console do Rapid Recovery Core, clique no menu suspenso **Proteger** e, em seguida, clique em **Proteger diversas máquinas**.

   O Assistente de proteção de diversas máquinas será exibido.
2. Na página Bem-Vindo, selecione uma das seguintes opções:
   - Típico
   - Avançado (exibir etapas opcionais)
3. Clique em **Avançar**.
4. Na página **Conexão** do assistente, na lista suspensa **Origem**, selecione uma das seguintes opções:
   - Servidor Hyper-V
   - Cluster Hyper-V
5. Insira as informações do host e insira as credenciais conforme descrito na tabela a seguir.

Tabela 65. Definições de conexão do Hyper-V

Caixa de texto	Descrição
Host	Nome ou endereço IP do host virtual.
Porta	A porta usada para se conectar ao host virtual. A definição padrão é 8006.
Nome de usuário	O nome de usuário utilizado para se conectar ao host virtual; por exemplo, Administrador ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador.

Caixa de texto	Descrição
Senha	A senha usada para se conectar ao host virtual.

6. Ou se você quiser usar a proteção sem agente, selecione **Proteger o servidor Hyper-V sem a exigência de um agente em máquinas virtuais convidadas** e, em seguida, consulte Proteger máquinas virtuais Hyper-V usando a proteção sem agente.
7. Clique em **Avançar**.
8. Na página **Máquinas**, selecione as VMs que você deseja proteger.
9. Opcionalmente, se você quiser proteger automaticamente novas máquinas virtuais quando adicionadas ao host, selecione **Proteger automaticamente novas máquinas virtuais**.
10. Clique em **Avançar**.
11. Na página **Ajustes**, digite as credenciais para cada máquina no seguinte formato: `hostname::username::password`.

    NOTE: Insira uma máquina em cada linha.

12. Clique em **Avançar**.

    Se a página **Proteção** for exibida em seguida no Assistente de proteção de diversas máquinas, vá para a Etapa 15.

    Se o software do agente estiver presente nas máquinas que você deseja proteger ou se alguma das máquinas especificadas não puder ser protegida por outro motivo, as máquinas selecionadas aparecerão na página **Avisos**.

13. Como opção, na página **Avisos**, você pode confirmar qualquer máquina selecionando-a e depois clicando em **Verificar** na barra de ferramentas.
14. Como opção, na página **Avisos**, selecione **Após a instalação do Agente, reiniciar as máquinas automaticamente**.

    NOTE: A Quest recomenda esta opção. Reinicie as máquinas agente antes de protegê-las.

15. Se o status indicar que a máquina está acessível, clique em **Avançar** para instalar o software Agent.

    A página **Proteção** é exibida.
16. Opcionalmente, na página **Proteção**, se você quiser um nome que não seja o endereço IP para ser exibido no Rapid Recovery Core Consolepara essa máquina protegida, digite um nome na caixa de diálogo no campo **Nome de exibição**.

    Você pode inserir até 64 caracteres. Não use os caracteres especiais descritos no tópico . Além disso, não inicie o nome de exibição com nenhuma das combinações de caracteres descritas no tópico .
17. Selecione as configurações de programação de proteção adequadas, como descrito a seguir:

    - Para usar a programação de proteção padrão, na opção Definições de programação, selecione **Proteção padrão (instantâneos de todos os volumes a cada hora)**.

    Na programação de proteção padrão, o Core gera snapshots de todos os volumes na máquina protegida a cada hora. Para alterar as definições de proteção a qualquer momento depois de fechar o assistente,

o que inclui a seleção dos volumes a serem protegidos, vá para a página **Resumo** da máquina protegida específica.

- Para definir uma programação de proteção diferente, na opção Definições de programação, selecione **Proteção personalizada**.

18. Prossiga com a configuração da seguinte maneira:
    - Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção padrão tiver sido especificada, e se houver um repositório, clique em **Concluir** para confirmar suas escolhas, fechar o assistente e proteger a máquina especificada.
    - Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção padrão tiver sido especificada, e se houver um repositório, clique em **Avançar** e vá para a Etapa 20 para criar um repositório.
    - Se uma configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** e continue na etapa seguinte para escolher os volumes a proteger.
    - Se você tiver selecionado uma configuração avançada no Assistente de proteção de máquina e especificado a proteção padrão, clique em **Avançar** e continue para a Etapa 20 para ver as opções de repositório e criptografia.
    - Se a configuração Avançado tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** e continue na etapa seguinte para escolher os volumes a proteger.

    Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.
19. Na página **Volumes de proteção**, selecione os volumes que deseja proteger. Se você não deseja incluir na proteção algum volume relacionado, clique na coluna Verificar para limpar a seleção. Depois, clique em **Avançar**.

    NOTE: Normalmente, é uma boa prática proteger, no mínimo, o volume Reservado pelo sistema e o volume em que se encontra o sistema operacional (normalmente a unidade C).
20. Na página **Programa de proteção**, defina um programa de proteção personalizado e clique em **Avançar**. Para obter detalhes sobre a definição de uma programação de proteção personalizada, consulte Criar programações de proteção personalizada no Modo Simples.

    Se as informações de repositório já estiverem configuradas e você tiver selecionado a opção Avançado na Etapa 1, a página Criptografia é exibida. Vá para a Etapa 23.
21. Na página **Repositório**, faça o seguinte:
    - Se você já tiver um repositório e quiser armazenar os dados dessa máquina para proteção no repositório existente, faça o seguinte:
        1. Selecione **Utilize um repositório existente**.
        2. Selecione um repositório existente na lista.
        3. Clique em **Avançar**.

        A página **Criptografia** é exibida. Passe à Etapa 23 para definir criptografia como opção.
    - Se deseja criar um repositório, clique na página **Repositório**, insira as informações descritas na tabela a seguir e, em seguida, clique em **Avançar** ou em **Concluir**, conforme apropriado.

Tabela 66. Configurações do repositório

Caixa de texto	Descrição
Nome	Insira o nome de exibição do repositório.

Caixa de texto	Descrição
	Por padrão, essa caixa de texto consiste na palavra Repositório e um número, que corresponde ao número de repositórios neste Core. Por exemplo, se este for o primeiro repositório, o nome padrão é Repositório 1. Altere o nome conforme a necessidade. Nomes de repositório devem conter entre 1 e 40 caracteres alfanuméricos, incluindo espaços. Não use ou .
Local	Insira o local para armazenar os dados protegidos. Esse volume deve ser um local de armazenamento principal. A localização pode ser local (uma unidade no Core) ou pode ser uma unidade de rede de compartilhamento CIFS. Para um compartilhamento CIFS, o caminho deve começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido. **CAUTION: Defina uma pasta dedicada na raiz do local de armazenamento do seu repositório. Não especifique o local da raiz. Por exemplo, use `E:\Repository\`, e não `E:\`. Se o repositório que você está criando nessa etapa for removido mais tarde, todos os arquivos no local de armazenamento do seu repositório serão excluídos. Se você definir o local de armazenamento na raiz, todos os outros arquivos no volume (por exemplo: `E:\`) são excluídos, o que poderia resultar em uma perda de dados catastrófica.** Por exemplo, digite `X:\Repository\Data`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Digite um nome de usuário para um usuário com acesso administrativo. Essa informação é necessária somente quando o local do repositório especificado é um caminho da rede.
Senha	Digite a senha para o usuário com acesso administrativo. Essa informação é necessária somente quando o local do repositório especificado é um caminho da rede.
Caminho de metadados	Insira o local para armazenar os metadados protegidos. Por exemplo, digite `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

22. Na página **Configuração de repositório**, configure a quantidade de espaço em disco a ser alocada para o repositório. A Quest recomenda reservar 20% do volume para metadados, que é o padrão. Opcionalmente, usando o controle deslizante ou o campo **Tamanho**, você pode alocar mais ou menos espaço no volume para o repositório.
23. Opcionalmente, se você deseja exibir e inserir informações detalhadas sobre as configurações do local de armazenamento, selecione **Mostrar opções avançadas** e ajuste as configurações conforme descrito na tabela a seguir. Para ocultar essas opções, desmarque a opção **Exibir opções avançadas**. Ao concluir a configuração do repositório, clique em **Avançar** ou em **Concluir**, conforme apropriado.

Tabela 67. Detalhes da Configuração de armazenamento

Caixa de texto	Descrição
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é 512.
Bytes por registro	Especifique a média de bytes por registro. O valor padrão é 8192.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Em • Desligar • Sincronizar Se definido como Ligado, que é o padrão, o Windows controla o armazenamento em cache. Isso é apropriado para o Windows 10 e para versões do Windows Server 2012 e posterior. **NOTE:** Definir a política de cache de gravação como Ligado pode resultar em desempenho mais rápido. Se você estiver utilizando o Windows Server 2008 R2 SP2, a recomendação de configuração será Desativado. Se configurado como Desativado, o Rapid Recovery controla o armazenamento em cache. Se definido como Sincronizar, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.

Se você selecionar a opção **Avançado** Etapa 1, a página **Criptografia** é exibida.

24. Opcionalmente, na página **Criptografia**, se você deseja usar chaves de criptografia para os dados armazenados no repositório, selecione **Criptografar dados em repouso em um repositório** e, em seguida, execute uma das seguintes ações:
    - Para selecionar uma chave de criptografia existente a ser aplicada a todos os novos dados armazenados no repositório, selecione **Criptografar dados usando criptografia baseada no Core com uma chave existente**, e, no menu suspenso **Selecionar chave de criptografia**, selecione a chave de criptografia.
    - Para definir uma nova chave de criptografia neste momento a ser aplicada a todos os futuros dados armazenados no repositório, selecione **Criptografar dados usando criptografia baseada no Core com uma nova chave**, e, em seguida, digite as informações referentes à chave, conforme descrito na tabela abaixo:

Tabela 68. Definir nova chave de criptografia

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia. Os nomes de chaves de criptografia devem ter entre 1 e 64 caracteres alfanuméricos. Não use caracteres proibidos ou frases proibidas.
Descrição	Insira um comentário descritivo para a chave de criptografia. Essas informações aparecem no campo Descrição ao visualizar uma lista de chaves de criptografia no Rapid Recovery Core Console. As descrições podem conter até 254 caracteres. A melhor prática é evitar o uso de caracteres proibidos e frases proibidas.

Caixa de texto	Descrição
Senha	Insira a frase de acesso usada para controlar o acesso. A melhor prática é evitar o uso de caracteres proibidos. Armazene a frase de acesso em um local seguro. O Suporte de proteção de dados da Quest não pode recuperar uma senha. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais máquinas protegidas, você não poderá recuperar os dados caso perca a frase de acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso. Usado para confirmar a entrada da frase de acesso.

25. Opcionalmente, na página **Criptografia**, para criptografar todos os dados transportados em uma rede, selecione **Criptografar os dados transportados em uma rede**. Essa opção é ativada por padrão; portanto, se não quiser criptografar dados dessa forma, desmarque essa opção.
26. Clique em **Concluir** para salvar e aplicar suas definições.

    Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.

O software do agente do Rapid Recovery é implantado nas máquinas especificadas, se necessário, e as máquinas são adicionadas à proteção no Core.

Proteger máquinas virtuais Hyper-V usando a proteção sem agente

O recurso Rapid Snap for Virtual permite que você proteja clusters ou máquinas virtuais Hyper-V sem agente, instalando o Rapid Recovery Agent apenas no host Hyper-V em vez de em cada máquina virtual (VM).

CAUTION: A Quest recomenda limitar a proteção sem agente a não mais do que 200 VMs por vez. Por exemplo, não selecione mais de 200 VMs ao usar o Assistente de proteção de diversas máquinas. Proteger mais de 200 VMs resultará em lentidão no desempenho. Não há limite de quantas VMs um Core pode proteger sem agente com o passar do tempo. Por exemplo, você pode proteger 200 VMs hoje em dia e outras 200 VMs amanhã.

1. No Console do Rapid Recovery Core, clique no menu suspenso **Proteger** e, em seguida, clique em **Proteger diversas máquinas**.

   O Assistente de proteção de diversas máquinas será exibido.
2. Na página **Bem-Vindo**, selecione uma das seguintes opções:
   - Típico
   - Avançado (exibir etapas opcionais)
3. Clique em **Avançar**.
4. Na página **Conexão** do assistente, na lista suspensa **Origem**, selecione uma das seguintes opções:
   - Servidor Hyper-V
   - Cluster Hyper-V
5. Insira as informações do host e insira as credenciais conforme descrito na tabela a seguir.

Tabela 69. Definições de conexão do Hyper-V

Caixa de texto	Descrição
Host	Nome ou endereço IP do host virtual.
Porta	A porta usada para se conectar ao host virtual. A definição padrão é 8006.
Nome de usuário	O nome de usuário utilizado para se conectar ao host virtual; por exemplo, Administrador ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador.
Senha	A senha usada para se conectar ao host virtual.

6. Certifique-se de que **Proteger o servidor Hyper-V sem a exigência de um agente em máquinas virtuais convidadas** ou **Proteger o cluster Hyper-V sem a exigência de um agente em máquinas virtuais convidadas**, dependendo da sua escolha na etapa 4, esteja selecionado. (Essa opção é selecionada por padrão.)
7. Clique em **Avançar**.
8. Na página **Selecionar máquinas**, selecione as VMs que você deseja proteger.
9. Opcionalmente, se você quiser proteger automaticamente novas máquinas virtuais quando adicionadas ao host, selecione **Proteger automaticamente novas máquinas virtuais**.
10. Clique em **Avançar**.
11. Opcionalmente, na página **Proteção**, se você quiser um nome que não seja o endereço IP para ser exibido no Rapid Recovery Core Consolepara essa máquina protegida, digite um nome na caixa de diálogo no campo **Nome de exibição**.

    Você pode inserir até 64 caracteres. Não use os caracteres especiais descritos no tópico . Além disso, não inicie o nome de exibição com nenhuma das combinações de caracteres descritas no tópico .
12. Selecione as configurações de programação de proteção adequadas, como descrito a seguir:

    - Para usar a programação de proteção padrão, na opção Definições de programação, selecione **Proteção padrão (instantâneos de todos os volumes a cada hora)**.

    Na programação de proteção padrão, o Core gera snapshots de todos os volumes na máquina protegida a cada hora. Para alterar as definições de proteção a qualquer momento depois de fechar o assistente,

o que inclui a seleção dos volumes a serem protegidos, vá para a página **Resumo** da máquina protegida específica.

- Para definir uma programação de proteção diferente, na opção Definições de programação, selecione **Proteção personalizada**.

13. Prossiga com a configuração da seguinte maneira:
    - Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção padrão tiver sido especificada, e se houver um repositório, clique em **Concluir** para confirmar suas escolhas, fechar o assistente e proteger a máquina especificada.
    - Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção padrão tiver sido especificada, e se houver um repositório, clique em **Avançar** e vá para a Etapa 16 para criar um repositório.
    - Se uma configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** e continue na etapa seguinte para escolher os volumes a proteger.
    - Se você tiver selecionado uma configuração avançada no Assistente de proteção de máquina e especificado a proteção padrão, clique em **Avançar** e continue para a Etapa 16 para ver as opções de repositório e criptografia.
    - Se a configuração Avançado tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** e continue na etapa seguinte para escolher os volumes a proteger.

    Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.
14. Na página **Volumes de proteção**, selecione os volumes que deseja proteger. Se você não deseja incluir na proteção algum volume relacionado, clique na coluna Verificar para limpar a seleção. Depois, clique em **Avançar**.

    NOTE: Normalmente, é uma boa prática proteger, no mínimo, o volume Reservado pelo sistema e o volume em que se encontra o sistema operacional (normalmente a unidade C).
15. Na página **Programa de proteção**, defina um programa de proteção personalizado e clique em **Avançar**. Para obter detalhes sobre a definição de uma programação de proteção personalizada, consulte Criar programações de proteção personalizada no Modo Simples.

    Se as informações de repositório já estiverem configuradas e você tiver selecionado a opção Avançado na Etapa 1, a página Criptografia é exibida. Vá para a Etapa 19.
16. Na página **Repositório**, faça o seguinte:
    - Se você já tiver um repositório e quiser armazenar os dados dessa máquina para proteção no repositório existente, faça o seguinte:
      1. Selecione **Utilize um repositório existente**.
      2. Selecione um repositório existente na lista.
      3. Clique em **Avançar**.

      A página **Criptografia** é exibida. Passe à Etapa 19 para definir criptografia como opção.
    - Se deseja criar um repositório, clique na página **Repositório**, insira as informações descritas na tabela a seguir e, em seguida, clique em **Avançar** ou em **Concluir**, conforme apropriado.

Tabela 70. Configurações do repositório

Caixa de texto	Descrição
Nome	Insira o nome de exibição do repositório.

Caixa de texto	Descrição
	Por padrão, essa caixa de texto consiste na palavra Repositório e um número, que corresponde ao número de repositórios neste Core. Por exemplo, se este for o primeiro repositório, o nome padrão é Repositório 1. Altere o nome conforme a necessidade. Nomes de repositório devem conter entre 1 e 40 caracteres alfanuméricos, incluindo espaços. Não use ou .
Local	Insira o local para armazenar os dados protegidos. Esse volume deve ser um local de armazenamento principal. A localização pode ser local (uma unidade no Core) ou pode ser uma unidade de rede de compartilhamento CIFS. Para um compartilhamento CIFS, o caminho deve começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido. **CAUTION: Defina uma pasta dedicada na raiz do local de armazenamento do seu repositório. Não especifique o local da raiz. Por exemplo, use `E:\Repository\`, e não `E:\`. Se o repositório que você está criando nessa etapa for removido mais tarde, todos os arquivos no local de armazenamento do seu repositório serão excluídos. Se você definir o local de armazenamento na raiz, todos os outros arquivos no volume (por exemplo: `E:\`) são excluídos, o que poderia resultar em uma perda de dados catastrófica.** Por exemplo, digite `X:\Repository\Data`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Digite um nome de usuário para um usuário com acesso administrativo. Essa informação é necessária somente quando o local do repositório especificado é um caminho da rede.
Senha	Digite a senha para o usuário com acesso administrativo. Essa informação é necessária somente quando o local do repositório especificado é um caminho da rede.
Caminho de metadados	Insira o local para armazenar os metadados protegidos. Por exemplo, digite `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

17. Na página **Configuração de repositório**, configure a quantidade de espaço em disco a ser alocada para o repositório. A Quest recomenda reservar 20% do volume para metadados, que é o padrão. Opcionalmente, usando o controle deslizante ou o campo **Tamanho**, você pode alocar mais ou menos espaço no volume para o repositório.
18. Opcionalmente, se você deseja exibir e inserir informações detalhadas sobre as configurações do local de armazenamento, selecione **Mostrar opções avançadas** e ajuste as configurações conforme descrito na tabela a seguir. Para ocultar essas opções, desmarque a opção **Exibir opções avançadas**. Ao concluir a configuração do repositório, clique em **Avançar** ou em **Concluir**, conforme apropriado.

Tabela 71. Detalhes da Configuração de armazenamento

Caixa de texto	Descrição
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é 512.
Bytes por registro	Especifique a média de bytes por registro. O valor padrão é 8192.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Em • Desligar • Sincronizar Se definido como Ligado, que é o padrão, o Windows controla o armazenamento em cache. Isso é apropriado para o Windows 10 e para versões do Windows Server 2012 e posterior. **NOTE:** Definir a política de cache de gravação como Ligado pode resultar em desempenho mais rápido. Se você estiver utilizando o Windows Server 2008 R2 SP2, a recomendação de configuração será Desativado. Se configurado como Desativado, o Rapid Recovery controla o armazenamento em cache. Se definido como Sincronizar, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.

Se você selecionar a opção **Avançado** Etapa 1, a página **Criptografia** é exibida.

19. Opcionalmente, na página **Criptografia**, se você deseja usar chaves de criptografia para os dados armazenados no repositório, selecione **Criptografar dados em repouso em um repositório** e, em seguida, execute uma das seguintes ações:
    - Para selecionar uma chave de criptografia existente a ser aplicada a todos os novos dados armazenados no repositório, selecione **Criptografar dados usando criptografia baseada no Core com uma chave existente**, e, no menu suspenso **Selecionar chave de criptografia**, selecione a chave de criptografia.
    - Para definir uma nova chave de criptografia neste momento a ser aplicada a todos os futuros dados armazenados no repositório, selecione **Criptografar dados usando criptografia baseada no Core com uma nova chave**, e, em seguida, digite as informações referentes à chave, conforme descrito na tabela abaixo:

Tabela 72. Definir nova chave de criptografia

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia. Os nomes de chaves de criptografia devem ter entre 1 e 64 caracteres alfanuméricos. Não use caracteres proibidos ou frases proibidas.
Descrição	Insira um comentário descritivo para a chave de criptografia. Essas informações aparecem no campo Descrição ao visualizar uma lista de chaves de criptografia no Rapid Recovery Core Console. As descrições podem conter até 254 caracteres. A melhor prática é evitar o uso de caracteres proibidos e frases proibidas.

Caixa de texto	Descrição
Senha	Insira a frase de acesso usada para controlar o acesso. A melhor prática é evitar o uso de caracteres proibidos. Armazene a frase de acesso em um local seguro. O Suporte de proteção de dados da Quest não pode recuperar uma senha. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais máquinas protegidas, você não poderá recuperar os dados caso perca a frase de acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso. Usado para confirmar a entrada da frase de acesso.

20. Opcionalmente, na página **Criptografia**, para criptografar todos os dados transportados em uma rede, selecione **Criptografar os dados transportados em uma rede**. Essa opção é ativada por padrão; portanto, se não quiser criptografar dados dessa forma, desmarque essa opção.
21. Clique em **Concluir** para salvar e aplicar suas definições.

    Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.

Como proteger diversas máquinas manualmente

Use este procedimento para especificar manualmente detalhes de várias máquinas que você deseja proteger simultaneamente usando o software do agente. Os detalhes identificam cada máquina na rede com exclusividade e incluem informações de conexão e credenciais. Essa abordagem é muitas vezes usada para proteger máquinas Linux. No entanto, com este processo, você pode proteger somente máquinas Windows, somente máquinas Linux ou uma combinação de ambas.

1. No Console do Rapid Recovery Core, clique no menu suspenso **Proteger** e, em seguida, clique em **Proteger diversas máquinas**.

   O Assistente de proteção de diversas máquinas será exibido.
2. Na página **Bem-Vindo**, selecione uma das seguintes opções:
   - Típico
   - Avançado (exibir etapas opcionais)
3. Clique em **Avançar**.
4. Na página **Conexão** do assistente, na lista suspensa **Origem**, selecione **Manualmente**.
5. Clique em **Avançar**.
6. Na página **Selecionar máquinas**, para cada máquina que deseja proteger, insira os detalhes da máquina na caixa de diálogo. Pressione **Enter** para separar as informações de cada máquina que deseja adicionar. Use o formato `hostname::username::password::port`. A configuração de porta é opcional. A porta padrão para instalar o Agent em máquinas Windows ou Linux é 8006. Os exemplos incluem:

   ```
   10.255.255.255::administrator::&11@yYz90z
   Linux-host-00-2::administrator::p@$$w0rD::8006
   ```
7. Clique em **Avançar**.

   Se a página **Proteção** for exibida em seguida no Assistente de proteção de diversas máquinas, vá para a Etapa 11.

Se o software do agente ainda não tiver sido implementado nas máquinas que você deseja proteger ou se alguma das máquinas especificadas não puder ser protegida por outro motivo, as máquinas selecionadas aparecerão na página **Avisos**.

8. Como opção, na página **Avisos de máquinas**, você pode confirmar qualquer máquina selecionando-a e depois clicando em **Confirmar** na barra de ferramentas.
9. Como opção, na página **Avisos de máquinas**, selecione **Após a instalação do Agent, reiniciar as máquinas automaticamente**.

   NOTE: A Quest recomenda esta opção. Reinicie as máquinas agente antes de protegê-las. A reinicialização garante que o serviço do agente está em execução e que o módulo de kernel adequado seja usado para proteger a máquina, se relevante.

10. Se o status indicar que a máquina está acessível, clique em **Avançar** para instalar o software Agent.

    A página **Proteção** é exibida.

11. Opcionalmente, na página **Proteção**, se você quiser um nome que não seja o endereço IP para ser exibido no Rapid Recovery Core Consolepara essa máquina protegida, digite um nome na caixa de diálogo no campo **Nome de exibição**.

    Você pode inserir até 64 caracteres. Não use os caracteres especiais descritos no tópico . Além disso, não inicie o nome de exibição com nenhuma das combinações de caracteres descritas no tópico .

12. Selecione as configurações de programação de proteção adequadas, como descrito a seguir:

    - Para usar a programação de proteção padrão, na opção Definições de programação, selecione **Proteção padrão (instantâneos de todos os volumes a cada hora)**.

    Na programação de proteção padrão, o Core gera snapshots de todos os volumes na máquina protegida a cada hora. Para alterar as definições de proteção a qualquer momento depois de fechar o assistente, o que inclui a seleção dos volumes a serem protegidos, vá para a página **Resumo** da máquina protegida específica.

    - Para definir uma programação de proteção diferente, na opção Definições de programação, selecione **Proteção personalizada**.

13. Prossiga com a configuração da seguinte maneira:

    - Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção padrão tiver sido especificada, e se houver um repositório, clique em **Concluir** para confirmar suas escolhas, fechar o assistente e proteger a máquina especificada.
    - Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção padrão tiver sido especificada, e se houver um repositório, clique em **Avançar** e vá para a Etapa 16 para criar um repositório.
    - Se uma configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** e continue na etapa seguinte para escolher os volumes a proteger.
    - Se você tiver selecionado uma configuração avançada no Assistente de proteção de máquina e especificado a proteção padrão, clique em **Avançar** e continue para a Etapa 16 para ver as opções de repositório e criptografia.
    - Se a configuração Avançado tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** e continue na etapa seguinte para escolher os volumes a proteger.

    Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.

14. Na página **Volumes de proteção**, selecione os volumes que deseja proteger. Se você não deseja incluir na proteção algum volume relacionado, clique na coluna Verificar para limpar a seleção. Depois, clique em **Avançar**.

NOTE: Normalmente, é uma boa prática proteger, no mínimo, o volume Reservado pelo sistema e o volume em que se encontra o sistema operacional (normalmente a unidade C).

15. Na página **Programa de proteção**, defina um programa de proteção personalizado e clique em **Avançar**. Para obter detalhes sobre a definição de uma programação de proteção personalizada, consulte Criar programações de proteção personalizada no Modo Simples.

    Se as informações de repositório já estiverem configuradas e você tiver selecionado a opção Avançado na Etapa 1, a página Criptografia é exibida. Vá para a Etapa 19.

16. Na página **Repositório**, faça o seguinte:

    - Se você já tiver um repositório e quiser armazenar os dados dessa máquina para proteção no repositório existente, faça o seguinte:

      1. Selecione **Utilize um repositório existente**.
      2. Selecione um repositório existente na lista.
      3. Clique em **Avançar**.

      A página **Criptografia** é exibida. Passe à Etapa 19 para definir criptografia como opção.

    - Se deseja criar um repositório, clique na página **Repositório**, insira as informações descritas na tabela a seguir e, em seguida, clique em **Avançar** ou em **Concluir**, conforme apropriado.

Tabela 73. Configurações do repositório

Caixa de texto	Descrição
Nome	Insira o nome de exibição do repositório. Por padrão, essa caixa de texto consiste na palavra Repositório e um número, que corresponde ao número de repositórios neste Core. Por exemplo, se este for o primeiro repositório, o nome padrão é Repositório 1. Altere o nome conforme a necessidade. Nomes de repositório devem conter entre 1 e 40 caracteres alfanuméricos, incluindo espaços. Não use ou .
Local	Insira o local para armazenar os dados protegidos. Esse volume deve ser um local de armazenamento principal. A localização pode ser local (uma unidade no Core) ou pode ser uma unidade de rede de compartilhamento CIFS. Para um compartilhamento CIFS, o caminho deve começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido. **CAUTION: Defina uma pasta dedicada na raiz do local de armazenamento do seu repositório. Não especifique o local da raiz. Por exemplo, use `E:\Repository\`, e não `E:\`. Se o repositório que você está criando nessa etapa for removido mais tarde, todos os arquivos no local de armazenamento do seu repositório serão excluídos. Se você definir o local de armazenamento na raiz, todos os outros arquivos no volume (por exemplo: `E:\`) são excluídos, o que poderia resultar em uma perda de dados catastrófica.** Por exemplo, digite `X:\Repository\Data`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Digite um nome de usuário para um usuário com acesso administrativo. Essa informação é necessária somente quando o local do repositório especificado é um caminho da rede.

Caixa de texto	Descrição
Senha	Digite a senha para o usuário com acesso administrativo. Essa informação é necessária somente quando o local do repositório especificado é um caminho da rede.
Caminho de metadados	Insira o local para armazenar os metadados protegidos. Por exemplo, digite `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

17. Na página **Configuração de repositório**, configure a quantidade de espaço em disco a ser alocada para o repositório. A Quest recomenda reservar 20% do volume para metadados, que é o padrão. Opcionalmente, usando o controle deslizante ou o campo **Tamanho**, você pode alocar mais ou menos espaço no volume para o repositório.
18. Opcionalmente, se você deseja exibir e inserir informações detalhadas sobre as configurações do local de armazenamento, selecione **Mostrar opções avançadas** e ajuste as configurações conforme descrito na tabela a seguir. Para ocultar essas opções, desmarque a opção **Exibir opções avançadas**. Ao concluir a configuração do repositório, clique em **Avançar** ou em **Concluir**, conforme apropriado.

Tabela 74. Detalhes da Configuração de armazenamento

Caixa de texto	Descrição
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é 512.
Bytes por registro	Especifique a média de bytes por registro. O valor padrão é 8192.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Em • Desligar • Sincronizar Se definido como Ligado, que é o padrão, o Windows controla o armazenamento em cache. Isso é apropriado para o Windows 10 e para versões do Windows Server 2012 e posterior. **NOTE:** Definir a política de cache de gravação como Ligado pode resultar em desempenho mais rápido. Se você estiver utilizando o Windows Server 2008 R2 SP2, a recomendação de configuração será Desativado. Se configurado como Desativado, o Rapid Recovery controla o armazenamento em cache. Se definido como Sincronizar, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.

Se você selecionar a opção **Avançado** Etapa 1, a página **Criptografia** é exibida.

19. Opcionalmente, na página **Criptografia**, se você deseja usar chaves de criptografia para os dados armazenados no repositório, selecione **Criptografar dados em repouso em um repositório** e, em seguida, execute uma das seguintes ações:

    - Para selecionar uma chave de criptografia existente a ser aplicada a todos os novos dados armazenados no repositório, selecione **Criptografar dados usando criptografia baseada no Core com uma chave existente**, e, no menu suspenso **Selecionar chave de criptografia**, selecione a chave de criptografia.
    - Para definir uma nova chave de criptografia neste momento a ser aplicada a todos os futuros dados armazenados no repositório, selecione **Criptografar dados usando criptografia baseada no Core com uma nova chave**, e, em seguida, digite as informações referentes à chave, conforme descrito na tabela abaixo:

Tabela 75. Definir nova chave de criptografia

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia. Os nomes de chaves de criptografia devem ter entre 1 e 64 caracteres alfanuméricos. Não use caracteres proibidos ou frases proibidas.
Descrição	Insira um comentário descritivo para a chave de criptografia. Essas informações aparecem no campo Descrição ao visualizar uma lista de chaves de criptografia no Rapid Recovery Core Console. As descrições podem conter até 254 caracteres. A melhor prática é evitar o uso de caracteres proibidos e frases proibidas.
Senha	Insira a frase de acesso usada para controlar o acesso. A melhor prática é evitar o uso de caracteres proibidos. Armazene a frase de acesso em um local seguro. O Suporte de proteção de dados da Quest não pode recuperar uma senha. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais máquinas protegidas, você não poderá recuperar os dados caso perca a frase de acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso. Usado para confirmar a entrada da frase de acesso.

20. Opcionalmente, na página **Criptografia**, para criptografar todos os dados transportados em uma rede, selecione **Criptografar os dados transportados em uma rede**. Essa opção é ativada por padrão; portanto, se não quiser criptografar dados dessa forma, desmarque essa opção.
21. Clique em **Concluir** para salvar e aplicar suas definições.

    Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.

O software do agente do Rapid Recovery é implantado nas máquinas especificadas, se necessário, e as máquinas são adicionadas à proteção no Core.

Monitorar a proteção de várias máquinas

É possível monitorar o progresso à medida que o Rapid Recovery aplica as programações e políticas de proteção às máquinas.

1. No Rapid Recovery Core Console, navegue até a página inicial do Rapid Recovery e clique em  (Eventos).

   A página **Eventos** é exibida, dividida em Tarefas, Alertas e Eventos. Conforme os volumes são transferidos, o status, as horas de início e término aparecem no painel de Tarefas.

   Também é possível filtrar as tarefas por status (ativa, em espera, concluída, em fila e com falha). Para obter mais informações, consulte Visualizar tarefas.

   NOTE: Para ver apenas as tarefas que estão aguardando execução, selecione o ícone de Tarefas em espera.

   À medida que cada máquina protegida é adicionada, um alerta é registrado, que lista se a operação foi bem-sucedida ou se erros foram registrados. Para obter mais informações, consulte Visualizar alertas.

   Para obter informações sobre visualização de todos os eventos, consulte Ver um diário de todos os eventos registrados.

Ativar o suporte a aplicativos

Depois que uma VM é colocada sob proteção sem agente, você pode suportar o aplicativo Exchange ou SQL instalado nessa máquina.

Antes de começar, os pré-requisitos a seguir devem ser atendidos.

- **Proteger a VM com o Rapid Recovery Core.** A opção para ativar o suporte a aplicativos não está disponível durante a processo de proteção. O botão para ativar essa funcionalidade é exibido em várias páginas da interface do usuário depois que a máquina SQL ou Exchange é colocada sob proteção. Para obter mais informações, consulte Proteger máquinas virtuais vCenter/ESXi usando a proteção sem agente ou Proteger máquinas virtuais Hyper-V usando a proteção sem agente.
- **Ativar o remoto acesso ao WMI.** Para permitir o acesso ao WMI, você deve instalar e configurar o Windows Remote Management na máquina virtual (VM) de destino. Para obter mais informações, consulte o artigo da Base de Dados de Conhecimento Microsoft em https://msdn.microsoft.com/en-us/library/aa384372(v=vs.85).aspx.
- **Conceder direitos administrativos remotamente aos usuários locais.** Configure LocalAccountTokenFilterPolicy executando o seguinte prompt de comando administrativo:

```
winrm quickconfig
```

- **Obter autorização de acesso ao namespace raiz do WMI.** Para que o Core possa se conectar aos aplicativos sem o Agent, a VM deve permitir tráfego de rede de entrada nas portas TCP 135 e 445, e nas portas dinamicamente atribuídas 1024 a 1034.
- **Permitir o acesso remoto ao SQL Server e o Exchange.** Esse pré-requisito varia de acordo com o aplicativo para o qual você deseja oferecer suporte.
  - **SQL:** Configure o Firewall do Windows abrindo as portas 1433 e 1434.
  - **Exchange:** Abra as portas TCP e UDP 389.
- **Integrar o convidado ao host.** A integração é feita por meio da instalação do pacote de otimização específico para o hipervisor:
  - Para VMs ESXi, use as **Ferramentas VMware**, que são necessários para a proteção de VM ESXi sem agente.
  - Para o Hyper-V, use o pacote **Serviços de Integração**, que é pré-instalado na maioria dos sistemas operacionais Windows Server.

Conclua as etapas a seguir para ativar o suporte a aplicativos para VMs protegidas sem agente.

1. No Core Console, vá para a página **Machines** (Máquinas).
2. Siga umas destas etapas:
   - Para ativar o suporte a aplicativos para uma VM, clique no menu **Actions** (Ações) dessa VM e depois clique em **Enable application support** (Ativar o suporte a aplicativos).
   - Para ativar o suporte a aplicativos para várias VMs ao mesmo tempo, selecione as VMs, clique no menu suspenso **Application Support** (Suporte a aplicativos) e depois clique em **Enable application support** (Ativar o suporte a aplicativos).
3. Na janela **Edit Application Support** (Editar suporte a aplicativos), digite as credenciais da VM.

Um ícone verde aparecerá ao lado do nome da máquina protegida para a qual o suporte a aplicativos está ativado.

Se quiser adicionar credenciais do aplicativo, você pode fazer isso clicando em **SQL** ou **Exchange** na parte superior da página **Resumo** da máquina específica.

Definições e funções para servidores protegidos do Exchange

Se você estiver protegendo um Microsoft Exchange Server no seu Core, há configurações adicionais que você pode configurar no Rapid Recovery Core Console, e existem funções adicionais que você pode executar.

Uma configuração única, **Habilitar a verificação de capacidade de montagem automática**, está disponível no Console do Core relacionado ao Exchange Server. Se esse recurso estiver ativado, as verificações de capacidade de montagem do servidor do Exchange são conduzidas automaticamente. Esta configuração estará disponível quando o status da máquina protegida estiver verde (ativo) ou amarelo (pausado).

Para obter mais informações, consulte Sobre verificações de montabilidade do banco de dados no Exchange.

Você também pode executar uma verificação de capacidade de montagem sob demanda, a partir do painel de Pontos de recuperação em uma máquina protegida do Exchange server. Para obter mais informações, consulte Forçar uma verificação de capacidade de montagem de um banco de dados do Exchange.

A seguir, temos funções que você pode executar para um Exchange server protegido pelo Core.

- **Especificar credenciais do Exchange Server**. O Rapid Recovery Core permite que você defina credenciais de forma que o Core possa autenticar no Exchange Server a fim de obter informações.

Para obter informações sobre a definição de credenciais para os Exchange servers, consulte Definir credenciais para uma máquina do Exchange Server.

- **Registros truncados do Exchange**. Quando você forçar truncamento de logs do Exchange server, este processo identifica o espaço disponível e retoma espaço no Exchange server protegido.

  Para obter mais informações sobre o truncamento dos logs do Exchange server em demanda, consulte Forçar o truncamento de log para uma máquina Exchange. Este processo também pode ser executado como parte dos trabalhos noturnos.

- **Forçar uma verificação de capacidade de montagem de um database do Exchange**. Esta função verifica se os databases do Exchange são montáveis, a fim de detectar a corrupção e alertar os administradores para que todos os dados do Exchange server possam ser recuperados com sucesso.

  Para obter mais informações sobre forçar uma verificação de capacidade de montagem sob demanda, consulte Forçar uma verificação de capacidade de montagem de um banco de dados do Exchange. Você também pode forçar uma verificação de capacidade de montagem para ocorrer automaticamente após cada snapshot. Para obter mais informações sobre verificação de capacidade de montagem, consulte Sobre verificações de montabilidade do banco de dados no Exchange.

- **Forçar uma verificação de soma de verificação de pontos de recuperação do Exchange Server**. Esta função verifica a integridade de pontos de recuperação contendo arquivos de database do Exchange.

  Para obter mais informações sobre forçar uma verificação de soma de verificação sob demanda, consulte Forçar uma verificação de soma de verificação dos arquivos do banco de dados do Exchange.

Você pode truncar logs do Exchange e forçar uma verificação de soma de verificação, como parte dos trabalhos noturnos. Para obter mais informações sobre tarefas que você pode programar como trabalhos noturnos, consulte Noções básicas sobre trabalhos noturnos. Para obter informações sobre configuração de trabalhos noturnos, consulte Configurar trabalhos noturnos para o Core.

Definir credenciais para uma máquina do Exchange Server

Para definir as credenciais de login, um Exchange Server deve estar presente em um volume protegido. Se o Rapid Recovery não detectar a presença de um Exchange Server, a função Definir credenciais não será exibida no Core Console.

Assim que você proteger os dados em um Microsoft Exchange Server, você poderá definir as credenciais de login no Rapid Recovery Core Console.

Conclua as etapas deste procedimento para definir as credenciais de cada Exchange Server.

1. Na área de navegação à esquerda do Rapid Recovery Core Console, selecione a máquina protegida do Exchange Server em relação à qual você deseja definir credenciais.

   A página **Resumo** é exibida para o Exchange Server protegido.

2. Na página **Resumo**, nos links na parte superior da página clique na seta apontada para baixo à direita do menu do Exchange e, no menu suspenso resultante, selecione **Definir credenciais**.

   A caixa de diálogo **Editar credenciais do Exchange** do Exchange Server protegido é exibida.

3. Na caixa de diálogo **Editar credenciais do Exchange**, insira suas credenciais como a seguir:
   a. No campo de texto **Nome de usuário**, insira o nome de usuário com permissões para o Exchange Server, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
   b. No campo **Senha**, insira a senha associada ao nome de usuário especificado para se conectar ao Exchange Server.
   c. Clique em **OK** para confirmar as configurações e feche a caixa de diálogo.

Forçar o truncamento de log para uma máquina Exchange

Para forçar o truncamento de log, um banco de dados do Exchange deve estar presente em um volume protegido. Se o Rapid Recovery não detecta a presença de um banco de dados, a função de verificação de truncamento de log não é exibida no Core Console.

Quando você força o truncamento de log em um Exchange Server protegido, o tamanho dos logs é reduzido. Execute as etapas deste procedimento para forçar o truncamento de log conforme a demanda.

1. Na área de navegação esquerda do Rapid Recovery Core Console, selecione o Exchange server protegido para o qual deseja forçar o truncamento de log

   A página **Resumo** da máquina protegida é exibida.
2. Na parte superior da página, clique no menu suspenso **Exchange** e selecione **Forçar truncamento de log**.
3. Na caixa de diálogo resultante, clique para confirmar que você deseja forçar truncamento de log.

   A caixa de diálogo é fechada. O sistema inicia o truncamento dos logs do Exchange server. Se os alertas do sistema estiverem ativados para este tipo de evento, será exibida uma mensagem indicando que o truncamento de log foi iniciado.

Sobre verificações de montabilidade do banco de dados no Exchange

Ao usar o Rapid Recovery para fazer backup de Microsoft Exchange Servers, poderão ser feitas verificações de montabilidade em todos os bancos de dados Exchange após cada instantâneo. Esse recurso de detecção de corrupção alerta os administradores sobre possíveis falhas e garante que todos os dados nos Exchange servers sejam recuperados com êxito em caso de falha.

Para ativar ou desativar esse recurso, vá para o menu **Configurações** e defina a opção **Habilitar a verificação de capacidade de montagem automática** como **Sim** ou **Não**, respectivamente. Para obter mais informações sobre como modificar as configurações de uma máquina protegida, consulte Visualização e modificação das definições de máquina protegida.

Verificações de capacidade de montagem não são parte das configurações noturnas. No entanto, se a verificação de capacidade de montagem automática estiver ativada e se a o opção Truncar logs do Exchange estiver ativada, a verificação de capacidade de montagem é acionada depois da conclusão do truncamento de log.

Você também pode executar uma verificação de capacidade de montagem sob demanda do painel **Pontos de recuperação** em uma máquina protegida do Exchange server. Para obter mais informações, consulte Forçar uma verificação de capacidade de montagem de um banco de dados do Exchange.

NOTE: As verificações de montabilidade somente se aplicam ao Microsoft Exchange Server 2007, 2010, 2013 e 2016. Além disso, a conta de serviço do Rapid Recovery Agent deve ter a função de Administrador organizacional atribuída a ela no Exchange.

Forçar uma verificação de capacidade de montagem de um banco de dados do Exchange

Para forçar uma verificação de capacidade de montagem, um banco de dados do Exchange deve estar presente em um volume protegido. Se o Rapid Recovery não detectar a presença de um banco de dados, a função de verificação de capacidade de montagem não será exibida no Core Console.

Execute as etapas deste procedimento para forçar o sistema a realizar uma verificação de montabilidade de um ponto específico de recuperação do Exchange Server sob demanda.

1. Na área de navegação esquerda do Rapid Recovery Core Console, selecione a máquina protegida do Exchange server em relação à qual você deseja forçar a verificação de capacidade de montagem e clique no menu **Pontos de recuperação**.
2. Role o painel **Pontos de recuperação** para baixo.
3. Percorra os pontos de recuperação para encontrar o ponto de recuperação desejado. Opcionalmente, clique na seta ▸ ao lado de um ponto de recuperação na lista para expandir a visualização.

   Nas informações expandidas do ponto de recuperação, você poderá ver os volumes incluídos no ponto de recuperação.
4. No painel **Pontos de recuperação**, na fileira que representa o ponto de recuperação correto, clique em  e, no menu suspenso, selecione **Forçar verificação de capacidade de montagem**.
5. Na caixa de diálogo resultante, clique para confirmar que você deseja forçar uma verificação de capacidade de montagem.

   A caixa de diálogo é fechada. O sistema realiza a verificação de montabilidade. Se alertas do sistema estiverem ativados para esse tipo de evento, você verá uma mensagem indicando que a verificação de capacidade de montagem foi iniciada.

Para obter instruções sobre como visualizar o status da verificação de capacidade de montagem, consulte Como exibir eventos usando tarefas, alertas e páginas de diário.

Forçar uma verificação de soma de verificação dos arquivos do banco de dados do Exchange

Para forçar uma verificação de soma de verificação, um banco de dados do Exchange deve estar presente em um volume protegido. Se o Rapid Recovery não detecta a presença de um banco de dados, a função de verificação de soma de verificação não é exibida no Core Console.

Execute as etapas deste procedimento para forçar o sistema a realizar uma verificação de soma de verificação de um ponto específico de recuperação do Exchange Server.

1. Na área de navegação esquerda do Rapid Recovery Core Console, selecione o Exchange server protegido para o qual deseja forçar a verificação de soma de verificação e clique no menu **Pontos de recuperação**.

   A página **Pontos de recuperação** é exibida para o Exchange server protegido.
2. Role o painel **Pontos de recuperação** para baixo.
3. Percorra os pontos de recuperação para encontrar o ponto de recuperação desejado. Opcionalmente, clique na seta ▸ ao lado de um ponto de recuperação na lista para expandir a visualização.

Nas informações expandidas do ponto de recuperação, você poderá ver os volumes incluídos no ponto de recuperação.

4. No painel **Pontos de recuperação**, na fileira que representa o ponto de recuperação correto, clique em  e no menu suspenso, selecione **Forçar verificação de soma de verificação**.
5. Na caixa de diálogo resultante, clique para confirmar que você deseja forçar uma verificação de soma de verificação.

   A caixa de diálogo é fechada. O sistema realiza a verificação de soma de verificação. Se os alertas do sistema estiverem ativados para este tipo de evento, será exibida uma mensagem indicando que a verificação de soma de verificação foi iniciada.

Para obter instruções sobre como visualizar o status da verificação de soma de verificação, consulte Como exibir eventos usando tarefas, alertas e páginas de diário.

Definições e funções para servidores SQL protegidos

Se você estiver protegendo um servidor Microsoft SQL no seu Core, há definições adicionais que você pode configurar no Console do Rapid Recovery Core, e existem funções adicionais que você pode executar.

Uma única definição, **Capacidade de anexação**, está disponível no Console do Core relacionada ao SQL Server.

O Rapid Recovery Core permite que você execute uma verificação de capacidade de anexação do SQL para verificar a integridade de pontos de recuperação contendo SQL databases. Esta ação verifica a consistência dos SQL databases e garante que todos os arquivos que suportam MDF (dados) e LDF (log) estão disponíveis no snaphot de backup.

Em versões anteriores, as verificações de capacidade de anexação do SQL solicitaram historicamente uma versão licenciada do SQL Server na máquina Core. O Rapid Recovery Core agora fornece a capacidade de executar as verificações de capacidade de anexação do SQL a partir de uma instância do SQL Server no Core ou a partir de uma versão licenciada do SQL Server na máquina protegida de um SQL Server.

As definições da capacidade de anexação permitem que você especifique qual versão licenciada do SQL Server é usada para executar esta verificação. Para obter mais informações sobre a configuração de definições da capacidade de anexação, consulte Gerenciar definições da capacidade de anexação do SQL.

Para obter mais informações sobre a capacidade de anexação do SQL, consulte Sobre a capacidade de anexação do SQL.

A seguir, temos funções que você pode executar para um SQL server protegido pelo Core.

- **Especificar as credenciais do SQL Server**. O Rapid Recovery Core permite que você defina credenciais de forma que o Core possa autenticar no SQL server a fim de obter informações. Você pode definir as credenciais para uma única máquina protegida do SQL Server, ou definir as credenciais padrão para todos os SQL Servers protegidos.

  Para obter informações sobre a definição de credenciais para SQL servers, consulte Definir credenciais para uma máquina SQL Server.

- **Truncar logs de SQL**. Quando você forçar truncamento de logs do SQL Server, este processo identifica o espaço disponível no servidor protegido. Este processo não recupera nenhum espaço.

  Para obter mais informações sobre o truncamento dos logs do SQL server sob demanda, consulte Forçar truncamento de log para uma máquina SQL.

- **Forçar uma verificação de capacidade de anexação de um SQL Server**. Esta função verifica a consistência dos SQL databases e garante que todos os arquivos que suportam MDF (dados) e LDF (log) estão disponíveis no snaphot de backup.

Para obter mais informações sobre forçar uma verificação de capacidade de anexação para SQL servers sob demanda, consulte Forçar uma verificação de capacidade de anexação do SQL Server.

Além de especificar credenciais, cada uma das funções descritas na lista anterior pode ser realizada sob demanda, e também pode ser configurada para ocorrer como parte dos trabalhos noturnos realizados para o Core. Para obter mais informações sobre tarefas que você pode programar como trabalhos noturnos, consulte Noções básicas sobre trabalhos noturnos. Para obter informações sobre configuração de trabalhos noturnos, consulte Configurar trabalhos noturnos para o Core.

Definir credenciais para uma máquina SQL Server

Você deve adicionar a máquina do SQL Server para proteção no Rapid Recovery Core antes de realizar esse procedimento. Para obter mais informações sobre a proteção de máquinas, consulte Proteção de uma máquina.

Assim que você proteger os dados em uma máquina do Microsoft SQL Server. você poderá definir as credenciais de login para uma instância única ou para todos os SQL Servers no Rapid Recovery Core Console.

Conclua as etapas deste procedimento para definir as credenciais de cada SQL Server.

1. Na área de navegação à esquerda do Rapid Recovery Core Console, selecione a máquina protegida do SQL Server em relação à qual você deseja definir credenciais.

   A página **Resumo** é exibida para a máquina protegida do SQL Server.

2. Na página **Resumo**, nos links na parte superior da página clique na seta apontada para baixo ▾ à direita do menu do SQL e, no menu suspenso resultante, escolha uma das seguintes opções:

   - Se desejar definir credenciais padrão para todas as instâncias do SQL Server database, clique em **Definir credenciais padrão para todas as instâncias**, e na caixa de diálogo **Editar credenciais padrão**, faça o seguinte:

     1. No campo de texto **Nome de usuário**, insira o nome de usuário com permissões para todos os SQL Servers associados, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
     2. No campo de texto **Senha**, insira a senha associada ao nome de usuário especificado para se conectar ao SQL Server.
     3. Clique em **OK** para confirmar as configurações e feche a caixa de diálogo.

   - Se desejar definir credenciais para uma instância do SQL Server database, clique no nome de exibição da máquina protegida do SQL Server e, na caixa de diálogo **Editar credenciais de instância**, faça o seguinte:

     1. Selecione o tipo de credencial (Padrão, Windows ou SQL)
     2. No campo de texto **Nome de usuário**, insira o nome de usuário com permissões para o SQL Server, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
     3. No campo de texto **Senha**, insira a senha associada ao nome de usuário especificado para se conectar ao SQL Server.
     4. Clique em **OK** para confirmar as configurações e feche a caixa de diálogo.

Forçar truncamento de log para uma máquina SQL

O truncamento de log está disponível para máquinas que utilizam o SQL Server. Execute as etapas deste procedimento para forçar o truncamento de log.

NOTE: Quando realizado em uma máquina com SQL, o truncamento identifica o espaço livre em um disco, mas não reduz o tamanho dos logs.

1. Na área de navegação á esquerda do Rapid Recovery Core Console, selecione a máquina em que você deseja forçar o truncamento de log.

   A página **Resumo** é exibida para a máquina protegida.
2. Na página **Resumo** (ou em qualquer página para essa máquina protegida), na parte superior da página, clique no menu suspenso **SQL** e selecione **Forçar truncamento de log**.
3. Clique em **Sim** para confirmar que deseja forçar o truncamento de log.

Sobre a capacidade de anexação do SQL

O recurso de capacidade de anexação do SQL permite que o Rapid Recovery Core conecte os arquivos mestres do banco de dados (arquivos .MDF) e arquivos de log do banco de dados (arquivos .LDF) a um snapshot de um SQL Server protegido. O snapshot é capturado usando uma instância local do Microsoft SQL Server.

Assuntos relevantes para usuários Rapid Recovery que protegem máquinas do SQL Server incluem qual instância do SQL Server executa a capacidade de anexação e o método de execução da anexação do SQL (sob demanda ou como parte dos trabalhos noturnos).

O teste da capacidade de anexação permite que o Core verifique a consistência dos bancos de dados SQL e garanta que todos os arquivos MDF e LDF estejam disponíveis no snapshot de backup.

As verificações da capacidade de anexação podem ser executadas sob demanda para pontos de recuperação específicos ou como parte de um trabalho noturno.

Para executar a Verificação de capacidade de anexação do SQL sob demanda, consulte Forçar uma verificação de capacidade de anexação do SQL Server. Para executar a capacidade de anexação do SQL uma vez por dia em uma hora especificada para as suas operações de trabalhos noturnos, ative a opção **Verificar anexação dos bancos de dados SQL** em trabalhos noturnos. Para obter mais informações sobre como configurar trabalhos noturnos no Core, consulte Configurar trabalhos noturnos para o Core. Para obter mais informações sobre como configurar trabalhos noturnos em uma máquina específica (neste caso, um SQL Server protegido), consulte Personalizar trabalhos noturnos para uma máquina protegida.

Em versões anteriores, a capacidade de anexação do SQL exigia que uma instância local do Microsoft SQL Server fosse instalada e configurada na máquina do Core. Agora, o Rapid Recovery Core permite que você escolha executar a verificação de capacidade de anexação em uma instância do SQL Server no Core ou em uma instância do SQL Server em uma máquina protegida do SQL Server. Essa instância precisa ser uma versão totalmente licenciada do SQL Server adquirida da Microsoft ou por meio de um revendedor licenciado. A Microsoft não permite o uso de licenças SQL passivas.

Qualquer instância do SQL Server que você especificar é usada para todas as verificações de capacidade de anexação. A capacidade de anexação é sincronizada entre as configurações do Core e os trabalhos noturnos. Por exemplo, se você especificar o uso da instância do SQL Server Core para trabalhos noturnos, as verificações de capacidade de anexação sob demanda também usarão o Core. Por outro lado, se você especificar o uso de uma instância do SQL Server em uma máquina protegida específica, todas as verificações de capacidade de anexação noturnas e sob demanda usarão a instância local da máquina protegida.

Selecione a instância do SQL Server para usar como parte das configurações do Core global. Para obter mais informações, consulte Gerenciar definições da capacidade de anexação do SQL.

NOTE: Executar a verificação de capacidade de anexação de uma máquina protegida do SQL Server exige que o Software do agente Rapid Recovery esteja instalado nesse servidor. A proteção sem agente não é suportada para a capacidade de anexação do SQL.

A capacidade de anexação no Rapid Recovery suporta SQL Server 2005, 2008, 2008 R2, 2012 e 2014. À conta usada para realizar o teste deve ser concedida a função sysadmin na instância do SQL Server.

O formato de armazenamento em disco do SQL Server é o mesmo em ambientes de 64 e 32 bits, e a capacidade de anexação funciona em ambas as versões. Um banco de dados separado da instância do server

que está sendo executado em um ambiente pode ser anexado em uma instância de server que é executado em outro ambiente.

NOTE: A versão do SQL Server no Core deve ser igual ou mais recente que aquela em todas as máquinas protegidas com o SQL Server instalado.

Forçar uma verificação de capacidade de anexação do SQL Server

Para forçar uma verificação de capacidade de anexação, um SQL database deve estar presente em um volume protegido. Se o Rapid Recovery não detectar a presença de um banco de dados, a função de verificação de capacidade de anexação não será exibida no Core Console.

Execute as etapas deste procedimento para forçar o sistema a realizar uma verificação de capacidade de anexação de um ponto específico de recuperação do SQL Server.

1. Na área de navegação esquerda do Rapid Recovery Core Console, selecione a máquina protegida do SQL Server em relação à qual você deseja forçar a verificação de capacidade de anexação e clique no menu **Pontos de recuperação**.
2. Role o painel **Pontos de recuperação** para baixo.
3. Percorra os pontos de recuperação para encontrar o ponto de recuperação desejado. Opcionalmente, clique na seta ▸ ao lado de um ponto de recuperação na lista para expandir a visualização.

   Nas informações expandidas do ponto de recuperação, você poderá ver os volumes incluídos no ponto de recuperação.
4. No painel **Pontos de recuperação**, na fileira que representa o ponto de recuperação correto, clique em  e no menu suspenso, selecione **Forçar verificação de capacidade de anexação**.
5. Na caixa de diálogo resultante, clique para confirmar que você deseja forçar uma verificação de capacidade de anexação.

   A caixa de diálogo é fechada. O sistema realiza a verificação de capacidade de anexação.

Para obter instruções sobre como visualizar o status da verificação de capacidade de anexação, consulte Como exibir eventos usando tarefas, alertas e páginas de diário.

Gerenciar máquinas protegidas

Esta seção descreve como visualizar, configurar e gerenciar as máquinas protegidas em seu ambiente do Rapid Recovery.

Sobre o gerenciamento de máquinas protegidas

Você pode gerenciar máquinas protegidas no Rapid Recovery Core Console, incluindo as seguintes tarefas:

- Você pode ver as máquinas protegidas do Rapid Recovery Core Console usando as opções descritas no tópico .
- Você pode configurar as definições para uma determinada máquina, que substituem as configurações padrão do Core. Algumas tarefas de configuração incluem alterar as configurações do host ou VM do hipervisor, acessar informações do sistema, modificar as configurações de transferência, personalizar trabalhos noturnos ou configurar notificações para eventos. Para obter mais informações, consulte Configurar as definições da máquina.
- Você pode remover uma máquina ou cluster da proteção, ver as informações de licença de uma máquina protegida ou diagnosticar problemas vendo o arquivo de log de uma máquina protegida. Para obter mais informações sobre estas e outras tarefas, consulte Gerenciar máquinas.
- Você pode visualizar e gerenciar os dados salvos no Core. Para obter mais informações, consulte Gerenciar snapshots e pontos de recuperação.

Visualizar máquinas protegidas

A partir da página **Início** do Rapid Recovery Core Console, na visualização Tabelas de resumo, você poderá ver informações de resumo de quaisquer máquinas protegidas pelo Core no painel Máquinas protegidas.

NOTE: Um agente de software atua em nome do usuário para executar ações específicas. As máquinas protegidas também são chamadas de agentes, porque executam o software Rapid Recovery Agent para facilitar a criação de cópias de segurança e a replicação de dados no Rapid Recovery Core.

Você pode ver o status, o nome de exibição de cada máquina, o repositório que ela utiliza, a data e a hora do último instantâneo, quantos pontos de recuperação existem no repositório para a máquina e a quantidade total de espaço de armazenamento que os instantâneos usam no repositório.

Para gerenciar os aspectos da máquina protegida, comece navegando até a máquina que você deseja ver, configurar ou gerenciar. Na página **Início**, há três maneiras de navegar até uma máquina protegida:

- Você pode clicar no endereço IP ou nome de exibição de qualquer máquina protegida do painel Máquinas protegidas. Isso leva você para a página Resumo da máquina protegida selecionada.
- Na área de navegação à esquerda, você pode clicar no título do menu **Máquinas protegidas**. A página **Protected Machines** (Máquinas protegidas) aparece. Nessa página, você pode ver informações

resumidas sobre cada máquina. Para ver uma descrição detalhada dessa página, consulte Visualização das informações de resumo de uma máquina protegida.

- Na área de navegação à esquerda, no menu Máquinas protegidas, você pode clicar no endereço IP ou nome de exibição de qualquer máquina protegida. Isso leva você para a página **Resumo** da máquina protegida selecionada. Para ver uma descrição detalhada dessa página, consulte Visualização das informações de resumo de uma máquina protegida.

Visualizar informações de resumo de cluster

Execute as etapas deste procedimento para visualizar as informações de resumo de um cluster, incluindo informações sobre o quórum associado ao cluster.

1. No Rapid Recovery Core Console, em Máquinas protegidas, clique no cluster que você deseja visualizar.

   A página Resumo da máquina é exibida.
2. Na página Resumo, você pode visualizar informações como nome do cluster, tipo de cluster, tipo de quórum (se aplicável) e caminho do quórum (se aplicável). Essa página também mostra informações de relance sobre os volumes nesse cluster, incluindo o tamanho e programação de proteção. Se aplicável, também é possível visualizar informações do SQL Server ou Exchange Server para um cluster diferente.
3. Para visualizar as informações mais recentes, clique em **Atualizar**.

Para obter informações sobre visualização de informações de resumo e status de uma máquina ou nó individual no cluster, consulte .

Configurar as definições da máquina

Depois de ter protegido uma máquina no Rapid Recovery Core, você pode facilmente visualizar e modificar as definições que determinam o comportamento da máquina protegida. Quando você modifica as configurações de uma máquina específica, essas configurações substituem o comportamento definido no nível do Core.

Você pode visualizar e configurar as seguintes definições da máquina no Rapid Recovery Core Console:

- **Geral**. Os parâmetros de configuração gerais da máquina incluem nome de exibição, nome de host, porta, chave de criptografia, repositório e links para um host do hipervisor. Para obter mais informações sobre a configuração das definições gerais de uma máquina, consulte Visualização e modificação das definições de máquina protegida.
- **Trabalhos noturnos**. O subconjunto de definições de trabalhos noturnos do Core mostrado para uma máquina protegida específica permite suplantar as definições de trabalho noturno definidas no nível do Core. Isso inclui rollup, o que permite gerenciar a política de retenção. Algumas definições podem variar de acordo com o tipo da máquina protegida.
- **Definições de transferência.** Definições específicas para gerenciar os processos de transferência de dados da máquina protegida selecionada. Para obter mais informações sobre os tipos de transferência de dados afetados por essas definições, consulte Sobre a modificação das definições da transferência.
- **Gravadores excluídos**. Essas definições permitem excluir gravadores. Elas são específicas para a máquina. Um gravador é uma API específica publicada pela Microsoft para permitir que outros componentes de software participem do uso de Microsoft Volume Shadow Services (VSS). Cada gravador do Rapid Recovery que participa dos snapshots de volume está listado nas definições Gravadores excluídos. Caso um gravador esteja interferindo com ou impedindo o sucesso das transferências de backup, ele pode ser desativado individualmente. A Quest recomenda não mexer nessas definições a menos que um representante do Suporte de proteção de dados da Quest oriente você a fazer isso.
- **Detalhes da licença**. São detalhes sobre a licença de uma máquina protegida específica. Essas definições mostram informações do Core e do Portal de licenças do Portal de licenças do Rapid Recovery. Essas definições são apenas leitura. Para alterar essas definições, atualize suas informações de licença

entre o Core e o portal de licenças. Consulte seu administrador de licenças para obter detalhes. Para obter mais informações, consulte o *Guia do usuário do portal de licenças do Rapid Recovery*.

O procedimento para visualizar ou alterar as definições no nível da máquina é idêntico para geral, gravadores excluídos e detalhes da licença. Para obter mais informações, consulte Visualização e modificação das definições de máquina protegida.

O procedimento para modificar os trabalhos noturnos de uma máquina é diferente. Para obter mais informações sobre a configuração das definições de trabalhos noturnos de uma máquina, consulte Personalizar trabalhos noturnos para uma máquina protegida.

Em alguns casos, pode ser preciso ajustar a taxa de transferência de dados de uma máquina protegida. Para obter mais informações, consulte Sobre a modificação das definições da transferência.

Visualização e modificação das definições de máquina protegida

As definições da máquina ajudam a determinar o comportamento de uma máquina protegida pelo Core. Quando você modifica as configurações de uma máquina específica, essas configurações substituem o comportamento definido no nível do Core.

Da mesma forma, um host virtual Hyper-V protegido tem diferentes configurações de máquina em comparação com as máquinas virtuais que gerencia. Para obter mais informações, consulte Visualização das informações de resumo de um host.

Execute as etapas descritas neste procedimento para ver e modificar as definições gerais, de transferência, de gravadores excluídos e de licenciamento de uma máquina protegida.

NOTE: Para ver e modificar definições de trabalho noturno, consulte Personalizar trabalhos noturnos para uma máquina protegida.

1. No Rapid Recovery Core Console, no menu Máquinas protegidas, clique no endereço IP ou no nome da máquina para a máquina que você quer exibir ou modificar.

   A página **Resumo** da máquina selecionada será exibida.
2. Clique no menu **Definições**.

   A página **Definições** será exibida, mostrando as configurações da máquina selecionada. Opcionalmente, para mostrar categorias de definição em qualquer lugar na página, clique no hiperlink adequado no lado esquerdo da página.

   Quando você clica em uma configuração que deseja alterar, essa configuração se torna um controle editável. Execute um dos seguintes:

   - Quando o controle for um menu suspenso, clique na seta para baixo para listar as opções e selecione a opção desejada no menu.
   - Quando o controle for um campo de texto, digite um valor.
   - Quando a opção exibe **Sim** ou **Não**, clique no valor, que é substituído por uma caixa de seleção. Para uma configuração de Sim, marque a caixa de seleção. Para um valor Não, desmarque a caixa de seleção.
   - Quando a opção exibe um valor temporal (por exemplo, mostrando horas, minutos e segundos), você pode clicar em cada componente e digitar um novo valor ou usar as setas para cima e para baixo para selecionar novos valores.

   Para cada definição, quando estiver satisfeito com suas alterações, clique na ✓ para confirmar e salvar a alteração e sair do modo de edição, ou clique em ✕ para sair do modo de edição sem salvar.
3. Para modificar as definições gerais de uma máquina, clique na definição adequada e digite as informações de configuração, conforme descrito na tabela a seguir.

Tabela 76. Definições gerais de uma máquina protegida

Caixa de texto	Descrição
Nome de exibição	Insira um nome de exibição para a máquina. Esse é o nome da máquina protegida que será exibido no Rapid Recovery Core Console. Você pode inserir até 64 caracteres. Por padrão, esse é o nome de host da máquina. Se necessário, é possível mudá-lo para algo mais amigável. Não use ou .
Nome do host	Este é o nome da máquina protegida como aparece nos metadados da máquina. **NOTE:** Não altere essa configuração, pois fazer isso pode interromper a conexão entre a máquina protegida e o Core.
Repositório	Esta configuração só é exibida para clusters Hyper-V protegidos que oferecem suporte a discos rígidos virtuais compartilhados. Exibe o repositório configurado no Rapid Recovery Core em que pontos de recuperação de discos rígidos virtuais compartilhados com o cluster Hyper-V protegido são armazenados.
Porta	Insira um número de porta para a máquina. A porta é usada pelo serviço Rapid Recovery Core para se comunicar com essa máquina. A porta padrão é 8006.
Chave de criptografia	Se você quiser que a chave de criptografia definida para esse Rapid Recovery Core seja aplicada aos dados de todos os volumes nessa máquina protegida, especifique a chave de criptografia aqui. A chave deve estar desbloqueada. Se não existe uma chave de criptografia, você pode adicionar uma. Para obter mais informações sobre o gerenciamento de chaves de criptografia, consulte Gerenciar chaves de criptografia. Se os volumes dessa máquina protegida estiverem criptografados, você pode alterar para uma chave de criptografia diferente. Alternativamente, você pode desassociar uma chave de criptografia selecionando **(nenhuma)** no menu suspenso **Chave de criptografia**. **NOTE:** Após aplicar uma chave de criptografia, alterar uma chave ou desassociar uma chave de uma máquina protegida, o Rapid Recovery gera uma nova imagem de base no próximo snapshot programado ou forçado.
Repositório	Selecione um repositório para os pontos de recuperação. Exibe o repositório configurado no Rapid Recovery Core no qual devem ser armazenados os dados dessa máquina. O volume do repositório pode ser local (no armazenamento conectado ao servidor do Core) ou em um volume de um local compartilhado CIFS. **NOTE:** As Definições do repositório nesta página podem ser alteradas apenas se não houver pontos de recuperação ou se o repositório anterior estiver ausente.
Hipervisor	Esta configuração só é exibida para máquinas virtuais. O valor desta configuração indica se a máquina virtual selecionada está associada como filho de um host de hipervisor protegido. • Se você ver o endereço IP ou o nome de exibição de um host protegido, a associação existe. Esse resultado indica que a máquina protegida não está consumindo uma licença de seu pool de licenças disponível. • Se você deseja remover a associação, clique no endereço IP ou no nome de exibição do host de hipervisor, selecione **Não vinculado** no menu suspenso e

Caixa de texto	Descrição
	clique na marca de verificação para confirmar a alteração. Posteriormente, esta VM protegida consumirá uma licença do pool. • Se você ver "Não vinculado", a máquina atualmente não está associada ao Core como uma máquina virtual em um host protegido e consome uma licença do pool. Se você deseja salvar uma licença e o host é protegido por agente, você pode associá-lo clicando em **Não vinculado**, e selecionar o host no menu suspenso.
Versão do SO	Esta configuração só é exibida para máquinas virtuais convidadas associadas a um host de hipervisor protegido. Em geral, o Rapid Recovery detecta e exibe o sistema operacional em execução na máquina virtual protegida.

4. Para modificar as definições de trabalho noturno de uma máquina protegida, consulte Personalizar trabalhos noturnos para uma máquina protegida.
5. Para modificar as definições do Exchange de um Exchange Server, na seção Definições do Exchange Server, clique em **Habilitar a verificação de capacidade de montagem automática** e faça o seguinte:
   - Para habilitar a verificação de capacidade de montagem automática, marque a caixa de seleção e clique em ✔.
   - Para desabilitar a verificação de capacidade de montagem automática, desmarque a caixa de seleção e clique em ✖.

   Para obter mais informações sobre a verificação de capacidade de montagem automática, consulte Sobre verificações de montabilidade do banco de dados no Exchange.
6. Para modificar as definições de transferência de uma máquina, clique na definição adequada e digite as informações de configuração, conforme descrito na tabela a seguir.

   NOTE: Para obter informações conceituais sobre as definições da transferência, consulte Sobre a modificação das definições da transferência.

Tabela 77. Definições da transferência de uma máquina protegida

Caixa de texto	Descrição
Restaurar padrão	Esse comando restaura todas as definições da transferência para as definições padrão do sistema.
Prioridade	Define a prioridade de transferência entre máquinas protegidas. Permite atribuir prioridade por comparação com outras máquinas protegidas. Selecione um número de 1 a 10, sendo 1 a maior prioridade. A definição padrão estabelece uma prioridade de 5. **NOTE:** A prioridade é aplicada às transferências que estão na fila.
Máximo de fluxos simultâneos	Define o número máximo de links TCP enviados para o Core para serem processados em paralelo para cada máquina protegida em um Repositório de DVM. **NOTE:** A Quest recomenda definir esse valor em 8. Se houver perda de pacotes, tente aumentar essa definição.
Máximo de gravações simultâneas	Define o número máximo de ações simultâneas de gravação em disco por conexão de máquina protegida.

Caixa de texto	Descrição
	NOTE: A Quest recomenda defini-lo com o mesmo valor selecionado para Máximo de fluxos simultâneos. Se houver perda de pacotes, defina um valor ligeiramente mais baixo; por exemplo, se Máximo de fluxos simultâneos for 8, mude este para 7.
Usar o Número máximo de novas tentativas padrão do Core	Selecione essa opção para usar o número de tentativas padrão para cada máquina protegida, se algumas das operações não forem concluídas.
Tamanho máximo do segmento	Especifica a maior quantidade de dados, em bytes, que um computador pode receber em um único segmento TCP. A definição padrão é 4194304. Não altere essa definição padrão, a menos que tenha sido orientado por um representante do suporte da Quest.
Profundidade máxima da fila de transferência	Especifica a quantidade de comandos que podem ser enviados simultaneamente. A definição padrão é 64. É possível ajustá-la para um número maior se o seu sistema possuir um número elevado de operações simultâneas de entrada/saída.
Leituras pendentes por fluxo	Especifica quantas operações de leitura em fila serão armazenadas no back-end. Essa definição ajuda a controlar o enfileiramento de máquinas protegidas. A definição padrão é 0.
Porta do server de dados de transferência	Define a porta para transferências. A definição padrão é 8009.
Tempo limite de transferência	Especifica em minutos e segundos o tempo a permitir que um pacote permaneça estático sem transferência.
Tempo limite de snapshot	Especifica em minutos e segundos o tempo máximo a aguardar para tirar um snapshot.
Tempo limite da limpeza dos snapshots	Especifica o tempo máximo do processo de exclusão de snapshots VSS em uma máquina protegida, em minutos e segundos.
Tempo limite de leitura da rede	Especifica em minutos e segundos o tempo máximo a aguardar por uma conexão de leitura. Se a leitura de rede não puder ser realizada naquele tempo, a operação será tentada novamente.
Tempo limite de gravação da rede	Especifica o tempo máximo em segundos a aguardar por uma conexão de gravação. Se a gravação de rede não puder ser realizada naquele tempo, a operação será tentada novamente.
Criptografar dados de instantâneo	Especifica se os dados transportados entre a máquina protegida e o Core são criptografados. Essa opção é ativada por padrão. Esta configuração se aplica a dados em trânsito pela rede. Quando esta opção está ativada, todos os dados de instantâneo transportados para um repositório DVM são criptografados.

Caixa de texto	Descrição
	NOTE: A Quest recomenda definir esse parâmetro como Sim quando os dados entre o Core e as máquinas protegidas devem passar pela rede pública ou por redes não confiáveis, como a Internet.

7. Para modificar as configurações de gravações excluídas, clique na configuração apropriada e, em seguida, selecione um gravador se quiser excluí-lo.

   NOTE: Como os gravadores que aparecem na lista são específicos para a máquina que você está configurando, você não verá todos os gravadores em sua lista.

8. Os detalhes da licença de uma máquina protegida são apenas leitura. As informações de detalhes da licença são descritas na tabela a seguir.

Tabela 78. Detalhes da licença de uma máquina protegida

Caixa de texto	Descrição
Data de expiração	Indica a data de expiração da licença para a máquina protegida selecionada.
Status da licença	Indica o status atual da licença para a máquina protegida selecionada.
Tipo de licença	Indica o tipo de licença para a máquina protegida selecionada.
Tipo de agente	Indica se a máquina protegida atual é um agente físico ou virtual.

See also: Alterar as configurações para um host ou nó Hyper-V
See also: Alterar as configurações para uma máquina virtual protegida Hyper-V
See also: Alterar as configurações do vSphere para uma máquina virtual protegida VMware

Alterar as configurações para um host ou nó Hyper-V

Este procedimento se aplica a hosts ou nós Hyper-V que usam o Rapid Snap for Virtual do Rapid Recovery (proteção sem agente) para proteger máquinas virtuais (VMs).

Um host Hyper-V que está usando o Rapid Snap for Virtual (proteção sem agente) para proteger VMs é indicado na área de navegação à esquerda pelo ícone de host  . As configurações de um host Hyper-V com máquinas virtuais protegidas sem agente não são iguais a de uma máquina protegida típica. Todas as alterações feitas nas configurações de um host se aplicam às VMs nesse host.

1. No Core Console, em Máquinas protegidas na área de navegação à esquerda, clique no host Hyper-V cujas configurações você deseja alterar.

   A página **Resumo** do host é aberta.

2. Na barra de menus do host, clique em **Configurações**.

   A página **Configurações** é aberta.

3. Em **Geral**, clique na configuração que você deseja alterar.

   A definições selecionada se tornará editável, como um campo de texto ou um menu suspenso.

4. Insira as informações de configuração conforme descrito na tabela a seguir.

Tabela 79. Informações sobre as configurações gerais

Caixa de texto	Descrição
Nome de exibição	O nome da máquina protegida que será exibido no Rapid Recovery Core Console. Você pode inserir até 64 caracteres. Por padrão é o nome de host da máquina. Se necessário, é possível alterar o nome de exibição para algo mais amigável. Não use ou .
Nome do host	O nome da máquina protegida como aparece nos metadados da máquina. **NOTE:** Não altere essa configuração, pois fazer isso pode interromper a conexão entre a máquina protegida e o Core.

5. Em **Fila de transferência**, para alterar o número de trabalhos de transferência que podem ocorrer no host de cada vez, clique na configuração para **Quantidade máxima de transferências simultâneas**.

   NOTE: Para obter um melhor desempenho, é recomendado que a quantidade máxima de transferências simultâneas para o host ou nó Hyper-V seja definida como 1, que é a configuração padrão.

6. Em **Trabalhos noturnos**, para alterar as configurações dos trabalhos noturnos disponíveis, clique em **Alterar**.

   A janela **Trabalhos noturnos** é exibida.

7. Insira as informações de configuração conforme descrito na tabela a seguir.

Tabela 80. Informações sobre configurações de trabalhos noturnos

Caixa de texto	Descrição
Limpar as chaves de registro órfãs no host Hyper-V protegido	Remove os arquivos desnecessários do registro que resulta de anexar e desanexar discos virtuais durante transferências de dados.
Verificar a integridade dos pontos de recuperação	Realiza uma verificação de integridade de cada ponto de recuperação criado para as máquinas virtuais no host Hyper-V.

8. Clique em **OK**.
9. Em **Proteção automática**, para determinar proteger automaticamente novas máquinas virtuais quando elas forem adicionadas ao host Hyper-V, clique na configuração para **Proteger automaticamente novas máquinas virtuais**.

Alterar as configurações para uma máquina virtual protegida Hyper-V

Este procedimento se aplica às máquinas virtuais (VMs) Hyper-V que são protegidas usando o Rapid Snap for Virtual do Rapid Recovery (proteção sem agente).

Uma VM Hyper-V que está sendo protegida pelo Rapid Snap for Virtual (proteção sem agente) é indicada na área de navegação à esquerda pelo ícone de host . As configurações de uma VM Hyper-V sem agente são iguais a de uma máquina protegida típica, com exceção da seção Hyper-V na parte inferior da página Configurações. A seguinte tarefa fornece instruções para apenas as configurações da seção

Hyper-V. Para todas as demais definições da máquina protegida, consulte Visualização e modificação das definições de máquina protegida.

1. Na área de navegação esquerda do Core Console, em **Máquinas protegidas**, clique na VM Hyper-V cujas configurações você deseja alterar.

   A página **Resumo** da VM é aberta.
2. Na barra de menus do host, clique em **Configurações**.

   A página **Configurações** é aberta.
3. Na lista no lado esquerdo, clique em **Hyper-V**.

   A definições selecionada se tornará editável, como um campo de texto ou um menu suspenso.
4. Em **Hyper-V**, clique em **Configuração de instantâneo**.

   A definição selecionada se tornará editável como um menu suspenso.
5. No menu suspenso, selecione uma das opções descritas na tabela a seguir.

Tabela 81. Informações sobre as definições do Hyper-V

Caixa de texto	Descrição
Tente criar um instantâneo VSS durante a primeira transferência; se ela falhar, crie um ponto de verificação	Se o instantâneo VSS for bem-sucedido, o ponto de recuperação estará em um estado consistente com o aplicativo. Se o instantâneo VSS falhar e um ponto de verificação for criado, o ponto de recuperação estará em um estado consistente de falha.
Não cria um instantâneo VSS durante a transferência	Gera um ponto de recuperação em um estado consistente de falha.
Use somente instantâneos VSS durante transferências. Se a criação de um instantâneo VSS falhar, toda a transferência falhará	Gera apenas pontos de recuperação consistentes com o aplicativo. Se o instantâneo VSS falhar, nenhum ponto de recuperação é gerado.

Alterar as configurações do vSphere para uma máquina virtual protegida VMware

Este procedimento se aplica às máquinas virtuais (VMs) VMware ESXi que são protegidas usando o Rapid Snap for Virtual (proteção sem agente).

As configurações de uma máquina virtual VMware que é protegida sem agente incluem as mesmas configurações que são usadas para uma máquina protegida típica, com uma exceção. A seção **vSphere** da página **Configurações** inclui as configurações que se aplicam somente a máquinas virtuais VMware protegidas sem agente. A seguinte tarefa fornece instruções para apenas a seção **vSphere** da página **Configurações**. Para todas as demais definições da máquina protegida, consulte Visualização e modificação das definições de máquina protegida.

1. No Core Console, em Máquinas protegidas na área de navegação à esquerda, clique no host Hyper-V cujas configurações você deseja alterar.

   A página **Resumo** do host é aberta.
2. Na barra de menus do host, clique em **Configurações**.

   A página **Configurações** é aberta.
3. Na lista no lado esquerdo, clique em **vSphere**.

A definições selecionada se tornará editável, como um campo de texto ou um menu suspenso.

4. Em **vSphere**, clique na configuração que você deseja alterar.

   A definições selecionada se tornará editável, como um campo de texto ou um menu suspenso.

5. Insira as informações de configuração conforme descrito na tabela a seguir.

Tabela 82. Informações sobre as configurações do vSphere

Caixa de texto	Descrição
Permitir que o Rapid Recovery exclua o usuário criado no VMware	A definição padrão é Não.
Permitir a transferência de volumes com capacidade usada inválida	A definição padrão é Sim.
Permitir instantâneos fechados	A definição padrão é Sim.

Sobre a modificação das definições da transferência

No Rapid Recovery, é possível modificar as definições para gerenciar os processos de transferência de dados para uma máquina protegida. As definições de transferência descritas nesta seção são configuradas no nível de máquina protegida. Para fazer transferências no nível do Core, consulte Modificar definições de fila de transferência.

Há três tipos de transferências no Rapid Recovery:

- **Snapshot.** Faz a cópia de segurança de dados na sua máquina protegida. São possíveis dois tipos de snapshots: a imagem de base de todos os dados protegidos e um snapshot incremental de dados atualizados desde o último snapshot. Esse tipo de transferência cria pontos de recuperação que são armazenados no repositório associado ao Core. Para obter mais informações, consulte Gerenciar snapshots e pontos de recuperação.
- **Exportação de máquina virtual**. Cria uma máquina virtual (VM) a partir de um ponto de recuperação, contendo todos os dados da cópia de segurança da máquina protegida, bem como o sistema operacional e os drivers e dados associados para garantir que a VM seja inicializável. Para obter mais informações, consulte Exportação da VM.
- **Restaurar**. Restaura as informações de cópia de segurança para uma máquina protegida. Para obter mais informações, consulte Sobre restauração de volumes a partir de um ponto de recuperação.

  NOTE: O volume inteiro é sempre regravado durante a restauração de sistemas Windows usando partições do sistema EFI.

A transferência de dados no Rapid Recovery envolve a transmissão de um volume de dados ao longo de uma rede, das máquinas protegidas para o Core. No caso de replicação, a transferência também ocorre do Core de origem ou fonte para o Core de destino.

A transferência de dados pode ser otimizada para seu sistema por meio de determinadas definições de opções de desempenho. Essas definições controlam o uso de largura de banda de dados durante o processo de criação

de cópia de segurança de máquinas protegidas, exportação de VM ou restauração. Estes são alguns fatores que afetam o desempenho da transferência de dados:

- Número de transferências simultâneas de dados de agentes
- Número de fluxos simultâneos de dados
- Quantidade de alterações de dados no disco
- Largura de banda de rede disponível
- Desempenho do subsistema do disco do repositório
- Quantidade de memória disponível para armazenamento em buffer dos dados

É possível ajustar as opções de desempenho para melhor atender às suas necessidades de negócios e fazer o ajuste do desempenho com base em seu ambiente. Para obter mais informações, consulte Estrangulamento da velocidade de transferência.

Estrangulamento da velocidade de transferência

Ao transferir dados de backup ou pontos de recuperação replicados entre máquinas protegidas e Cores através da rede, você pode intencionalmente reduzir a velocidade da transferência. Esse processo é conhecido como estrangulamento.

Ao estrangular a velocidade de transferência, você limita a quantidade de largura de banda de rede dedicada à transferência de arquivos do Rapid Recovery. Ao configurar a replicação, por exemplo, o estrangulamento pode reduzir a possibilidade da transferência de pontos de recuperação anteriores ao Core replicado consumir toda a largura de banda da rede.

> **CAUTION: O estrangulamento da velocidade de transferência nem sempre é necessário ou recomendado. Essas informações são fornecidas para oferecer ideias para uma possível solução de problemas de desempenho em seu ambiente Rapid Recovery. Por exemplo, algumas vezes o estrangulamento resolver problemas relacionados a falhas de transferência repetidas ou lentidão da rede causados pela transferência de uma quantidade substancial de dados para seus Cores protegidos ou replicados.**

Há vários fatores envolvidos na determinação da melhor abordagem para o estrangulamento. O tipo de máquina protegida é um fator-chave. Por exemplo, um Microsoft Exchange Server ocupado tem uma taxa de alteração muito mais alta que um servidor Web legado raramente usado.

As capacidades de entrada e saída dos volumes de armazenamento em suas máquinas protegidas também podem contribuir para uma eficiência maior ou menor.

A velocidade da rede é outro fator crítico, com muitas variáveis. O backbone de rede usado (como 1 GbE versus 10 GbE), a arquitetura, a configuração, o uso intencional do agrupamento de NIC e mesmo o tipo de cabo usado podem afetar a velocidade de transferência da rede. Se o ambiente tiver uma rede de longa distância mais lenta e se os trabalhos de transferência de backup ou replicação falharem, considere o estrangulamento da velocidade de transferência usando algumas dessas definições.

Em última análise, o processo de estrangulamento da rede envolve tentativa e erro. A Quest recomenda que você ajuste e teste suas definições de transferência e as reveja periodicamente para garantir que suas definições continuam a atender suas necessidades.

O ajuste da velocidade de transferência deve ser realizado nas máquinas individualmente. No Core Console, navegue até uma máquina específica, selecione Definições e ajuste a velocidade de transferência. Para obter informações específicas sobre como visualizar e alterar essas definições, consulte Visualização e modificação das definições de máquina protegida.

Esse tópico também inclui uma descrição de cada definição usada para o estrangulamento da transferência. Essas descrições podem ser úteis para determinar quais definições você deve testar primeiro.

As quatro definições principais envolvidas no estrangulamento da velocidade de transferência são descritas na tabela a seguir:

Definição no nível da máquina	Definições padrão	Definição de limitação sugerida
Máximo de fluxos simultâneos	8	4
Máximo de gravações simultâneas	8	4
Tamanho máximo do segmento	4194304	2097152
Leituras pendentes por fluxo	0	Iniciar em 24

A Quest recomenda ajustar e testar as outras definições antes de alterar a definição padrão para leituras pendentes por fluxo, a menos que um representante do Quest Support tenha orientado você a fazer isso. Ao ajustar e testar esta definição, comece com um valor de 24.

Quando você especifica limitações para os parâmetros de transferência da máquina protegida, estas limitações são aplicadas por trabalho. Se dois trabalhos de transferência ocorrerem simultaneamente ou se sobrepuserem, o uso da largura de banda dobra. Se quatro trabalhos de transferência da rede se sobrepuserem, o uso da largura de banda quadruplica, e assim por diante.

Personalizar trabalhos noturnos para uma máquina protegida

Os trabalhos noturnos podem ser configurados no nível do Core ou no nível da máquina. Quando trabalhos noturnos são definidos no nível do Core, as alterações são aplicadas a todas as máquinas relevantes protegidas por esse Core. As alterações feitas nos trabalhos noturnos no nível da máquina substituem as alterações feitas no nível do Core e se aplicam às máquinas especificadas.

Para obter uma lista de todos os trabalhos noturnos, incluindo descrições e o escopo disponível para cada um, consulte o tópico Noções básicas sobre trabalhos noturnos.

Execute as etapas do procedimento a seguir para realizar alterações em trabalhos noturnos em uma única máquina protegida.

1. No Rapid Recovery Core Console, no menu Máquinas, clique no endereço IP ou no nome da máquina para a qual você quer personalizar os trabalhos noturnos.

   A página **Resumo** da máquina selecionada é exibida.
2. Clique no menu **Definições**.

   A página **Definições** é exibida, mostrando os parâmetros de configuração da máquina selecionada.
3. Opcionalmente, clique no link **Trabalhos noturnos** para descer na página **Definições** e visualizar todas as definições de trabalhos noturnos.
4. Sob o título Trabalhos noturnos, clique em **Change** (Alterar).

   A caixa de diálogo **Nightly Jobs** (Tarefas noturnas) é mostrada.
5. Na caixa de diálogo **Trabalhos noturnos**, selecione os trabalhos que você deseja executar à noite ou desmarque as opções que deseja omitir para essa máquina.

   NOTE: As opções podem variar por máquina. Por exemplo, uma máquina protegida que utiliza o Exchange Server pode incluir as opções Verificar a soma de verificação dos bancos de dados do Exchange e Truncar logs do Exchange.

NOTE: Para obter informações sobre a definição **Rollup**, incluindo a definição de uma política de retenção personalizada, consulte Personalizar as definições de política de retenção de uma máquina protegida.

6. Clique em **OK**.

NOTE: Os resultados desse procedimento aplicam-se apenas à máquina protegida selecionada. Para serem aplicados em outro local, repita o procedimento para cada máquina que desejar personalizar. Para alterar as configurações de trabalho noturno para todas as máquinas protegidas por um Core, consulte Configurar trabalhos noturnos para o Core.

Visualização das informações do sistema de uma máquina protegida

O Rapid Recovery Core Console oferece acesso fácil às informações do sistema sobre as máquinas protegidas no Core.

Ao visualizar as informações do sistema para uma máquina protegida específica, o painel **Informações do sistema** inclui informações gerais sobre a máquina protegida, incluindo sua relação com o Core e o repositório. O painel **Volumes** lista as informações sobre os volumes de armazenamento da máquina do Core. O painel **Conexões do mecanismo de reprodução** mostra os volumes de todas as máquinas que estão sendo protegidas.

Execute as etapas deste procedimento para visualizar as informações detalhadas do sistema de uma máquina protegida.

1. Navegue até o Rapid Recovery Core Console e, no menu de máquinas protegidas da área de navegação à esquerda, clique no nome de uma máquina protegida.

   A página **Resumo** da máquina protegida selecionada é exibida.
2. Na página **Resumo**, na parte inferior do painel **Resumo**, clique em **Informações do sistema**.
3. Na página **Informações do sistema**, você pode visualizar os seguintes detalhes sobre a máquina protegida selecionada.
   - **Informações do sistema.** Isso inclui o nome do host, a versão do SO, a memória física, o nome de exibição, o nome de domínio totalmente qualificado e o tipo de máquina virtual (se aplicável).
   - **Volumes**. Isso inclui o nome do volume, ID do dispositivo, sistema de arquivos, capacidade formatada e capacidade utilizada.
   - **Processadores**. Isso inclui a arquitetura, o número de cores e threads, a velocidade de clock e a descrição.
   - **Adaptadores de rede**. Isso inclui o tipo de adaptador de rede e a velocidade.
   - **Endereços IP**. Isso inclui o endereço IP e a família.

Gerenciar máquinas

Esta seção descreve as diferentes tarefas que você pode executar para gerenciar suas máquinas protegidas.

- Remover uma máquina
- Remover um cluster da proteção
- Visualizar informações de licença em uma máquina
- Download e visualização do arquivo de log de uma máquina protegida
- Converter um nó de cluster protegido em uma máquina protegida

Remover uma máquina

Ao remover uma máquina da proteção no Rapid Recovery Core, você tem duas opções: manter os pontos de recuperação salvos até o momento no Core ou removê-los.

Se você mantiver a pontos de recuperação, terá o que é conhecido como máquina “apenas pontos de recuperação”. As operações de restauração e montagem continuarão disponíveis nos pontos de recuperação capturados da máquina quando ela estava sob proteção. No entanto, os backups da máquina protegida não continuarão.

Se você remover os pontos de recuperação, essa ação excluirá do Rapid Recovery Core todos os dados de instantâneos da máquina anteriormente protegida.

Execute as etapas do procedimento a seguir para remover uma máquina da proteção no seu ambiente do Rapid Recovery.

1. No Rapid Recovery Core Console, no painel de navegação à esquerda, em Máquinas protegidas, clique na máquina que você deseja remover.
2. Na página **Resumo** da respectiva máquina, clique em **Remover máquina**.
3. Na caixa de diálogo, se você quiser excluir também todos os pontos de recuperação dessa máquina do repositório, selecione **Remover com pontos de recuperação**.
4. Para confirmar a sua escolha e remover a máquina, clique em **Sim**.

   CAUTION: Se você excluir pontos de recuperação, não será mais possível restaurar os dados dessa máquina.

   O Rapid Recovery remove a máquina da proteção e cancela todas as tarefas ativas da máquina.

Remover um cluster da proteção

Execute as etapas do procedimento a seguir para remover um cluster da proteção.

1. No Rapid Recovery Core Console, em Máquinas protegidas, clique no cluster que deseja remover.
2. Na página **Resumo do cluster**, clique em **Remover cluster**.
3. Opcionalmente, na caixa de diálogo, para remover todos os pontos de recuperação atualmente armazenados para esse cluster a partir do repositório, selecione **Remover com pontos de recuperação**.

   CAUTION: Se você excluir pontos de recuperação, não será mais possível restaurar os dados desse cluster.
4. Na caixa de diálogo, clique em **Sim** para confirmar.

Remover nós de cluster da proteção

Execute as etapas dos procedimentos a seguir para remover nós de cluster da proteção.

Se quiser apenas remover um nó do cluster, consulte Converter um nó de cluster protegido em uma máquina protegida.

1. No Rapid Recovery Core Console, em Máquinas protegidas, clique no nó do cluster que você deseja remover.
2. Na página **Resumo do nó**, clique em **Remover máquina**.

   A caixa de diálogo Remover nó é exibida.
3. Opcionalmente, na caixa de diálogo, para remover todos os pontos de recuperação atualmente armazenados para esse cluster a partir do repositório, selecione **Remover com pontos de recuperação**.

   CAUTION: Se você excluir pontos de recuperação, não será mais possível restaurar os dados dos nós de cluster.
4. Na caixa de diálogo, clique em **Sim** para confirmar.

Remover todos os nós de um cluster da proteção

Execute as etapas deste procedimento para remover todos os nós em um cluster da proteção.

CAUTION: Se você remover todos os nós do cluster, o cluster também será removido.

1. No Rapid Recovery Core Console, em Máquinas protegidas, clique no cluster cujos nós você deseja remover.
2. Na página **Resumo** para o cluster, clique em **Nós protegidos**.
3. Na página **Nós Protegidos**, selecione todos os nós.
4. No menu suspenso **Remover máquinas**, selecione uma das opções descritas na tabela a seguir.

Tabela 83. Opções de Remover nós

Opção	Descrição
Remover e manter pontos de recuperação	Para manter todos os pontos de recuperação atualmente armazenados deste cluster.
Remover pontos de recuperação	Para remover do repositório todos os pontos de recuperação atualmente armazenados deste cluster. **CAUTION: Se você excluir pontos de recuperação, não será mais possível restaurar os dados desse cluster.**

5. Na caixa de diálogo Excluir nós, clique em **Sim** para confirmar.

Visualizar informações de licença em uma máquina

Você pode visualizar as informações de status da licença do status da licença Rapid Recovery instalado em uma máquina protegida.

1. No Rapid Recovery Core Console, em Máquinas protegidas, clique na máquina que você deseja modificar.

A página **Resumo** da máquina de seleção é exibida.

2. Clique no menu **Definições**.

   A página **Definições** é exibida, mostrando os parâmetros de configuração da máquina selecionada.

3. Clique no link **Aplicação de licença** para rolar a página Definições a fim de exibir definições de aplicação de licença específicas de máquina.

   Aparece a tela Status e apresenta os detalhes sobre a aplicação de licença do produto.

Download e visualização do arquivo de log de uma máquina protegida

Se você encontrar erros ou problemas com uma máquina protegida, poderá baixar os logs da máquina para visualizá-los ou compartilhá-los com seu representante do Quest Support.

1. Na área de navegação à esquerda do Core Console, no menu Máquinas protegidas, clique na seta para expandir o menu sensível ao contexto da máquina protegida relevante. Role para baixo até **Mais**, expanda esse menu e selecione  **Log do agente**.

   A página **Baixar log do agente** é mostrada.

2. Na página **Baixar log do agente**, clique em  **Clique aqui para começar o download**.
3. Na caixa de diálogo **Abrindo AgentAppRecovery.log**, realize um dos procedimentos a seguir:

   - Para abrir o arquivo de log, selecione **Abrir com** e um aplicativo (como Bloco de Notas) para visualizar o arquivo de log com base em texto e, por fim, clique em **OK**.

     O arquivo **AgentAppRecovery.log** é aberto no aplicativo selecionado.

   - Para salvar o arquivo localmente, selecione **Salvar arquivo** e clique em **OK**.

     O arquivo **AgentAppRecovery.log** é salvo na sua pasta Downloads. Ele pode ser aberto usando-se qualquer editor de texto.

See also: Como baixar e exibir o arquivo de log do Core
See also: Download e visualização do arquivo de log de uma máquina protegida

Converter um nó de cluster protegido em uma máquina protegida

No Rapid Recovery, converter um nó do cluster protegido em uma máquina protegida, de modo que ela ainda seja gerenciada pelo Core, mas não faça mais parte do cluster. Isso é útil, por exemplo, se você precisar remover do cluster o nó de cluster, mas ainda mantê-lo protegido.

1. No Rapid Recovery Core Console, navegue até o cluster que contém a máquina a ser convertida e clique em **Nós protegidos**.
2. Na página **Nós protegidos**, a partir do nó específico que deseja converter, clique no menu suspenso Ações e selecione **Converter para agente**.
3. Para adicionar a máquina de volta ao cluster, selecione-a e depois, na página Resumo do menu Ações, selecione **Converter para nó do cluster** e clique em **Sim** para confirmar a ação.

Noções básicas sobre grupos personalizados

O Rapid Recovery Core mostra um menu Máquinas protegidas na área de navegação à esquerda. Ele inclui todas as máquinas ou clusters de servidores adicionados para proteção no seu Rapid Recovery Core. Outros menus poderão ser exibidos dentro deste, se você incluiu esses objetos no seu Core. Da mesma forma, você pode criar um grupo personalizado, o que exibe como o último tipo de menu na área de navegação à esquerda.

O principal benefício de um grupo personalizado é a habilidade de agrupar os objetos do Core em um contêiner lógico. Isso pode ajudá-lo a organizar e gerenciar objetos do Core para um objetivo específico (por exemplo, por organização, centro de custo, departamento, região geográfica e assim por diante).

O ato de criar um grupo sempre adiciona um membro do grupo (por exemplo, uma máquina protegida ou cluster de servidores, uma máquina replicada ou uma máquina somente de pontos de recuperação) ao novo grupo personalizado. O objeto adicionado é determinado pelo seu ponto de origem, quando você cria o grupo. O ideal é, então, adicionar mais membros ao grupo. Depois disso, você pode realizar ações de grupo que se apliquem a todos os membros semelhantes desse grupo personalizado, conforme descrito em Realizar ações de grupo.

Os grupos personalizados podem incluir máquinas protegidas, clusters de servidores, máquinas replicadas e máquinas somente de ponto de recuperação. Os clusters de servidores se comportam da mesma maneira que as máquinas protegidas, exceto que um cluster de servidores e seus nós se comportam como uma única entidade. Se você tentar adicionar um nó de um cluster de servers a um grupo, todo o cluster será adicionado.

Um grupo personalizado pode conter membros semelhantes ou diferentes. Para grupos de membros semelhantes, todas as ações do grupo se aplicam a todos os membros do grupo. Por exemplo, se você forçar um snapshot para um grupo personalizado de máquinas protegidas, será feito um backup de máquina. Para grupos com membros diferentes (por exemplo, máquinas protegidas e replicadas), se você aplicar uma ação de grupo como forçar a replicação, ela se aplicará apenas às máquinas replicadas.

É possível criar um ou mais grupos. Uma única máquina protegida ou replicada pode ser incluída em um ou mais grupos. Dessa forma, é possível agrupar máquinas em seu core da forma que você escolher e executar ações nesse grupo específico.

Cada grupo personalizado aparece na área de navegação à esquerda, com um rótulo que você atribuir. Os grupos com máquinas protegidas padrão aparecem em primeiro lugar no grupo personalizado; as máquinas replicadas serão mostradas abaixo das máquinas protegidas, se for o caso. Se houver alguma máquina somente de ponto de recuperação, ela será listada abaixo das máquinas replicadas.

Na área de navegação à esquerda, cada objeto protegido no Core aparece no seu próprio menu. Os grupos personalizados aparecem no final desses menus.

Incluir uma máquina em um grupo não a remove de seu local original. Por exemplo, se você tiver três máquinas protegidas chamadas Agente1, Agente2 e Agente3 e adicionar o Agente1 ao GrupoPersonalizado1, o Agente1 aparecerá em ambos os locais.

See also: Criar grupos personalizados
See also: Modificar nomes de grupos personalizados
See also: Remover grupos personalizados
See also: Realizar ações de grupo
See also: Visualizar todas as máquinas de um grupo personalizado em uma página

Criar grupos personalizados

Ao rolar o cursor sobre o nome de qualquer máquina no menu Máquinas protegidas ou Máquinas replicadas, verá uma seta que abre um menu suspenso. Nesse menu, é possível criar um rótulo personalizado.

Use o procedimento abaixo para criar um grupo personalizado.

1. Navegue até o Rapid Recovery Core Console.
2. No menu Máquinas protegidas, máquinas replicadas ou máquinas apenas de pontos de recuperação, faça o seguinte:
    a. Coloque o cursor sobre uma máquina no menu.
    b. Clique no menu suspenso dessa máquina.
    c. Role e selecione **Rotulado como** e clique em **Novo rótulo**.

    A caixa de diálogo **Criar rótulo** é exibida.
3. No campo **Nome**, digite um rótulo adequado para o seu grupo personalizado.

    Use um nome descritivo, que comunique a finalidade do grupo. Por exemplo, para agrupar máquinas protegidas, máquinas replicadas e máquinas apenas de pontos de recuperação por departamento, digite `Departamento de contabilidade`. Posteriormente, é possível renomear o grupo.

    NOTE: Os rótulos precisam ter 50 caracteres ou menos. Você pode incluir um único espaço entre as palavras. Você precisa fornecer um rótulo para o seu grupo personalizado.
4. Quando estiver satisfeito com o nome do rótulo, clique em **OK**.

    A caixa de diálogo é fechada e o grupo personalizado é mostrado como o último elemento na área de navegação esquerda.
5. Opcionalmente, você pode adicionar outras máquinas protegidas, máquinas replicadas ou máquinas apenas de ponto de recuperação a esse grupo. Opcionalmente, para adicionar outros agentes a esse grupo, navegue até o nome do agente no menu apropriado, clique no menu suspenso para abri-lo, role para baixo e selecione **Rotulado como**. Depois, clique no nome do grupo personalizado.

    Agora você pode realizar ações de grupo nesse grupo. Para obter mais informações, consulte Realizar ações de grupo.

Modificar nomes de grupos personalizados

Ao modificar o nome de um grupo personalizado, apenas o rótulo é alterado. Os nomes das máquinas continuam os mesmos.

Use o procedimento abaixo para modificar o nome de um grupo personalizado.

1. Navegue até o Rapid Recovery Core Console.
2. No menu Máquinas protegidas, role o cursor sobre o grupo personalizado que deseja modificar.
3. Clique no menu suspenso desse grupo e clique em **Editar**.

    A caixa de diálogo **Editar rótulo** será exibida; nessa caixa, o nome do grupo personalizado torna-se editável.
4. No campo **Nome**, atualize o texto ou exclua o texto do rótulo existente e digite um novo rótulo ou o seu grupo personalizado.

    Use um nome descritivo, que comunique a finalidade do grupo. Por exemplo, para agrupar as máquinas protegidas, máquinas replicadas e máquinas apenas de ponto de recuperação por região geográfica, digite `Tóquio`. Posteriormente, é possível renomear o grupo.

    NOTE: Os rótulos precisam ter 50 caracteres ou menos. Você pode incluir um único espaço entre as palavras. Você precisa fornecer um rótulo para o seu grupo personalizado.
5. Quando estiver satisfeito com o nome do rótulo, clique em **OK**.

    A caixa de diálogo é fechada e o grupo personalizado modificado é exibido como o último elemento da área de navegação à esquerda.
6. Opcionalmente, você pode adicionar outras máquinas protegidas, máquinas replicadas ou máquinas apenas de ponto de recuperação a esse grupo. Opcionalmente, para adicionar outros agentes a esse

grupo, navegue até o nome do agente no menu apropriado, clique no menu suspenso para abri-lo, role para baixo e selecione **Rotulado como**. Depois, clique no nome do grupo personalizado.

Remover grupos personalizados

Quando um grupo personalizado é removido, ele é excluído do menu Máquinas protegidas. As máquinas que estavam no grupo não são removidas e ainda podem ser encontradas no menu padrão apropriado.

Use o procedimento abaixo para remover um grupo personalizado.

1. Navegue até o Rapid Recovery Core Console.
2. No menu Máquinas protegidas, role o cursor sobre o grupo personalizado que deseja remover.
3. Clique no menu suspenso desse grupo e clique em **Remover rótulo**.

   Aparece uma mensagem pedindo confirmação para a remoção do grupo.
4. Confirmar a remoção do grupo personalizado.

   A caixa de diálogo é fechada e o grupo personalizado é removido da área de navegação.

Realizar ações de grupo

É possível realizar ações de grupo em qualquer grupo que apareça na área de navegação à esquerda do Rapid Recovery Core Console. Se o grupo contiver membros diferentes (por exemplo, máquinas replicadas e máquinas de apenas pontos de recuperação), as ações solicitadas serão realizadas apenas nos membros do grupo relevantes.

Use o procedimento abaixo para realizar ações de grupo em um grupo personalizado.

1. Navegue até o Rapid Recovery Core Console.
2. No menu Máquinas protegidas, role o cursor sobre o grupo personalizado no qual deseja realizar uma ação de grupo.
3. Clique no menu suspenso desse grupo e selecione uma ação, como a seguir:
   - Para forçar um snapshot incremental ou uma imagem de base de todas as máquinas protegidas, clique em **Forçar snapshot** ou em **Forçar imagem de base**, conforme o caso.
   - Para pausar a proteção de todas as máquinas protegidas no grupo, clique em **Pausar proteção** e especifique os parâmetros de retomada.
   - Para retomar a proteção de todas as máquinas protegidas no grupo cuja proteção tenha sido pausada, clique em **Retomar proteção** e confirme que deseja retomar.
   - Para atualizar as informações de todos os objetos no grupo, clique em **Atualizar metadados**.
   - Para pausar a replicação de todas as máquinas replicadas nesse grupo, em Replicação, clique em **Pausar**.
   - Para retomar a replicação de todas as máquinas replicadas nesse grupo cuja replicação tenha sido pausada, em Replicação, clique em **Retomar**.
   - Para forçar a replicação de todas as máquinas replicadas nesse grupo, em Replicação, clique em **Forçar**.
   - Para remover a replicação de todas as máquinas replicadas nesse grupo, em Replicação, clique em **Remover**.
   - Para remover as máquinas de apenas pontos de recuperação deste Core e descartar os pontos de recuperação, em Apenas pontos de recuperação, clique em **Remover pontos de recuperação**.
   - Apenas para grupos personalizados, para modificar o rótulo deles, selecione **Editar**.
   - Apenas para grupos personalizados, para remover o grupo personalizado do menu de navegação, selecione **Remover rótulo**.

See also: Forçar um snapshot
See also: Forçar a replicação
See also: Pausar e retomar a replicação
See also: Pausar e retomar a proteção
See also: Remover replicação de entrada do Core de destino
See also: Modificar nomes de grupos personalizados
See also: Remover grupos personalizados

Visualizar todas as máquinas de um grupo personalizado em uma página

Clique no nome de um grupo personalizado para ver a página Máquinas que relaciona todas as máquinas nesse grupo personalizado. É possível então realizar algumas funções em todas as máquinas a partir do menu Ações ou realizar funções individualmente selecionando os comandos de cada máquina individual.

Instantâneos e pontos de recuperação

Esta seção descreve como usar e gerenciar os instantâneos e os pontos de recuperação gerados pelo Rapid Recovery. Contém informações sobre montagem, exibição e imposição, bem como migração e exclusão de pontos de recuperação.

Gerenciar snapshots e pontos de recuperação

Um ponto de recuperação é uma coleção de snapshots tirados de volumes de disco individuais e armazenados no repositório. Os snapshots capturam e armazenam o estado de um volume de disco em determinado momento, enquanto os aplicativos que geram os dados ainda estão em uso. No Rapid Recovery, é possível forçar um instantâneo, pausar temporariamente os instantâneos e visualizar as listas de pontos de recuperação atuais no repositório, além de excluí-los se necessário. Os pontos de recuperação são utilizados para restaurar as máquinas protegidas ou para montar um sistema de arquivos local.

Os instantâneos capturados pelo Rapid Recovery são feitos no nível do bloco e reconhecem o aplicativo. Isso significa que todas as transações abertas e os logs de transação contínua são concluídos e os caches são descarregados em disco antes da criação do snapshot.

O Rapid Recovery usa um driver de filtro de volume de baixo nível, que se anexa aos volumes montados e depois rastreia todas as alterações no nível de bloco para o próximo instantâneo iminente. O Microsoft Volume Shadow Services (VSS) é usado para facilitar snapshots consistentes de falhas de aplicativos.

Ver a página de pontos de recuperação de uma máquina protegida

Conclua as etapas do procedimento a seguir para ver a lista completa de ponto de recuperação de uma máquina protegida.

NOTE: Se você estiver protegendo dados a partir de um cluster de servers DAG ou CCR, os pontos de recuperação associados não aparecerão no nível de cluster. Estarão visíveis apenas no nível de nó ou máquina.

1. No Rapid Recovery Core Console, navegue até a máquina protegida da qual deseja visualizar os pontos de recuperação.
2. No menu na parte superior da página, clique em **Pontos de recuperação**.

   A página **Pontos de recuperação** é exibida, mostrando um painel de resumo dos pontos de recuperação e um painel de pontos de recuperação.

   Você pode visualizar informações resumidas sobre os pontos de recuperação da máquina conforme a descrição na tabela a seguir.

Tabela 84. Informações resumidas do ponto de recuperação

Informações	Descrição
Total de pontos de recuperação	Lista o número total de pontos de recuperação salvos no repositório para esta máquina.
Total de dados protegidos	Indica a quantidade de espaço de armazenamento usado no repositório para esses pontos de recuperação.
Repositório	Mostra o nome do repositório no qual esses pontos de recuperação estão armazenados.
Status do repositório	Exibe graficamente a quantidade de espaço consumido pelos pontos de recuperação. Mostra a porcentagem do repositório usado, a quantidade de espaço e o espaço total do repositório. Clique no gráfico para ver a quantidade de espaço restante.

Você pode visualizar informações sobre os pontos de recuperação da máquina conforme a descrição na tabela a seguir.

Tabela 85. Informações do ponto de recuperação

Informações	Descrição
Ícone	Representação gráfica de um ponto de recuperação ou, se expandido, um volume dentro do ponto de recuperação . Os pontos de recuperação mostram uma seta para a direita indicando que detalhes podem ser expandidos.
Criptografado	Indica se o ponto de recuperação é criptografado.
Status	Indica o status atual do ponto de recuperação.
Conteúdo	Relaciona os volumes incluídos no ponto de recuperação. • Clique em (Informações) para ver o uso de espaço e o sistema de arquivos. • Para servidores Exchange, clique em para exibir informações sobre o servidor.
Tipo	Define um ponto de recuperação como uma imagem de base ou um snapshot (diferencial) incremental.
Data de criação	Exibe a data em que o ponto de recuperação foi criado.
Tamanho	Exibe a quantidade de espaço que o ponto de recuperação consome no repositório.
•••	O menu suspenso [Mais] permite que você execute determinadas funções para o ponto de recuperação selecionado.

3. Opcionalmente, expanda um ponto de recuperação para ver os volumes protegidos.

Referências relacionadas

See also: Como ver pontos de recuperação para uma máquina

Noções básicas sobre os indicadores de status do ponto de recuperação

Após a captura de um ponto de recuperação de um SQL ou Exchange Server protegido, o aplicativo exibe um indicador de status da cor correspondente na grade Ponto de Recuperação. Essa grade é exibida no painel **Pontos de recuperação** durante a exibição dos pontos de recuperação de uma máquina específica. A cor exibida se baseia nas definições de verificação da máquina protegida e no sucesso ou na falha dessas verificações, conforme descrito nas tabelas a seguir.

NOTE: Para obter mais informações sobre como exibir pontos de recuperação, consulte Ver a página de pontos de recuperação de uma máquina protegida.

Cores de status do ponto de recuperação para bancos de dados do Exchange

A tabela a seguir lista os indicadores de status exibidos para os bancos de dados do Exchange.

Tabela 86. Indicadores de status do banco de dados do Exchange

Cor do status	Descrição
Branco	Indica que um banco de dados do Exchange não é detectado dentro do ponto de recuperação, do volume ou do grupos de volumes.
Amarelo	Indica que as verificações de montabilidade do banco de dados do Exchange ainda não foram executadas.
Vermelho	Indica que as verificações de capacidade de montagem ou soma de verificação falharam em pelo menos um banco de dados.
Verde	Indica que o ponto de recuperação contém um ou mais bancos de dados e que as verificações de capacidade de montagem estão ativadas e que a verificação de capacidade de montagem ou que a verificação de soma de verificação foi aprovada.

Cores de status do ponto de recuperação para bancos de dados SQL

A tabela a seguir lista os indicadores de status exibidos para bancos de dados SQL.

Tabela 87. Indicadores de status do banco de dados SQL

Cor do status	Descrição
Branco	Indica que um banco de dados SQL não é detectado dentro do ponto de recuperação, do volume ou do grupos de volumes.
Amarelo	O banco de dados SQL estava offline, indicando que as verificações de capacidade de anexação não eram possíveis e não foram realizadas.
Vermelho	Indica que a verificação de capacidade de anexação falhou ou que o banco de dados SQL está offline.
Verde	Indica que a verificação da capacidade de anexação passou no teste.

NOTE: Pontos de recuperação que não tenham um banco de dados Exchange ou SQL associados são exibidos com um indicador de status branco. Em situações em que existem bancos de dados do Exchange e SQL para o ponto de recuperação, o indicador de status mais grave é exibido para o ponto de recuperação.

Montar um ponto de recuperação

No Rapid Recovery, você pode montar um ponto de recuperação para uma máquina Windows para acessar dados armazenados por meio de um sistema de arquivos local.

NOTE: Para montar um ponto de recuperação do Linux com o utilitário `local_mount`, consulte Montar um volume de ponto de recuperação em máquina Linux.

NOTE: Ao montar pontos de recuperação a partir dos dados restaurados de uma máquina que tem a deduplicação de dados ativada, você também deverá ativar a deduplicação no servidor Core.

1. No Rapid Recovery Core Console, navegue até a máquina que deseja montar em um sistema de arquivos local.

   A página **Resumo** da máquina protegida selecionada é exibida.

2. Clique no menu **Pontos de recuperação**.

   A página **Pontos de recuperação** da máquina selecionada é exibida.

3. Opcionalmente, no painel **Pontos de recuperação**, na lista de pontos de recuperação, clique no símbolo de seta para a direita para expandir os detalhes do ponto de recuperação, mostrando os volumes incluídos no ponto de recuperação.

4. Na linha do ponto de recuperação que você deseja montar, clique em e, no menu suspenso, selecione **Montagem**.

   O **Assistente de montagem** é exibido, mostrando a página **Volumes**.

5. Na página **Volumes**, selecione cada volume do ponto de recuperação que você deseja montar e depois clique em **Avançar**.

   A página **Opções de montagem** do Assistente de montagem é exibida.

6. Na página **Opções de montagem**, edite as definições de montagem de um ponto de recuperação, conforme descrito na tabela a seguir.

Tabela 88. Definições das Opções de montagem

Opção	Descrição
Pasta local	Especifique o caminho usado para acessar o ponto de recuperação montado. Por exemplo, selecione `C:\ProgramData\AppRecovery\MountPoints\MountPoint1`.
Tipo de montagem	Especifique a maneira de acessar os dados do ponto de recuperação montado: • Apenas leitura • Apenas leitura com gravações anteriores • Gravável
Criar um compartilhamento do Windows	Como opção, marque esta caixa de seleção para especificar se o ponto de recuperação montado pode ser compartilhado e defina os direitos de acesso a ele, incluindo o nome de compartilhamento e os grupos permitidos.

Opção	Descrição
para essa montagem	

7. Clique em **Concluir** para montar o ponto de recuperação.

   NOTE: Se quiser copiar diretórios ou arquivos de um ponto de recuperação montado para outra máquina Windows, você pode usar o Windows Explorer para copiá-los com as permissões padrão ou permissões de acesso dos arquivos originais. Para obter detalhes, consulte Restaurar um diretório ou arquivo usando o Windows Explorer a Restaurar um diretório ou arquivo e preservar as permissões usando o Windows Explorer.

8. Como opção, enquanto a tarefa estiver em andamento, você poderá visualizar seu progresso no menu suspenso **Tarefas em execução** no Core Console ou visualizar informações detalhadas na página **Eventos**. Para obter mais informações sobre o monitoramento de eventos do Rapid Recovery, consulte Como exibir eventos usando tarefas, alertas e páginas de diário.

Desmontar pontos de recuperação

Execute as etapas deste procedimento para desmontar pontos de recuperação montados no Core.

NOTE: Ao desmontar um ponto de recuperação montado remotamente, a ação é denominada desconectar.

1. No Rapid Recovery Core Console, na barra de ícones, clique em (Mais) e selecione **Mounts** (Montagens).

   A página **Montagens** aparece. Há um painel para montagens locais (pontos de recuperação montados no Core) e outro para montagens remotas (pontos de recuperação montados usando o Local Mount Utility). Em cada painel, os respectivos pontos de recuperação montados aparecem em uma lista.

2. Para desmontar montagens locais, no painel **Montagens locais**, faça o seguinte:
   a. Selecione o ponto ou os pontos de montagem locais que você quer desmontar.
   - Para desmontar todos os pontos de recuperação, clique na caixa de verificação na barra de título da tabela Montagens locais para selecionar todos os pontos de montagem.
   - Para desmontar um ou mais pontos de recuperação, clique na caixa de verificação na primeira coluna de cada linha representando o ponto de montagem que você deseja desconectar.

   b. Clique em **Dismount** (Desmontar).

   Uma caixa de diálogo de confirmação é exibida.

   c. Clique para confirmar que você quer desmontar os pontos de recuperação selecionados.

   Os pontos de recuperação locais são desmontados.

   NOTE: Se os alertas do sistema estiverem habilitados, você pode ver um alerta de que os pontos de montagem adequados estão sendo desmontados.

3. Para desconectar pontos de recuperação montados remotamente, no painel **Remote Mounts** (Montagens remotas), faça o seguinte:
   a. Selecione o ponto ou os pontos de montagem remota que você quer desconectar.
   - Para desconectar todos os pontos de recuperação, clique na caixa de verificação na barra de título da tabela Montagem remota para selecionar todos os pontos de montagem.
   - Para desconectar um ou mais pontos de recuperação, clique na caixa de verificação na primeira coluna de cada linha representando o ponto de montagem que você deseja desconectar.

b. Clique em **Disconnect** (Desconectar).

Uma caixa de diálogo de confirmação é exibida.

c. Clique para confirmar que você quer desconectar os pontos de recuperação selecionados.

Os pontos de recuperação locais são desconectados.

NOTE: Se os alertas do sistema estiverem habilitados, você pode ver um alerta de que os pontos de montagem adequados estão sendo desconectados.

4. Confirme se os pontos de recuperação montados anteriormente não aparecem mais na lista de montagens locais ou de montagens remotas, conforme apropriado.

Trabalhar com pontos de recuperação do Linux

O método recomendado e compatível de montar e desmontar pontos de recuperação em uma máquina Linux protegida é usar o utilitário **local_mount**.

Os procedimentos apresentados abaixo tratam especificamente do uso do local_mount para montar e desmontar pontos de recuperação do Linux.

NOTE: Para gerenciar pontos de recuperação do Linux de outras maneiras, consulte Gerenciar snapshots e pontos de recuperação, pois todas as outras atividades de gerenciamento podem ser realizadas no Core Console.

- Montar um volume de ponto de recuperação em máquina Linux
- Desmontar um ponto de recuperação em uma máquina Linux

Montar um volume de ponto de recuperação em máquina Linux

Com o utilitário local_mount no Rapid Recovery, você pode montar um volume remotamente de um ponto de recuperação como um volume local em uma máquina Linux.

NOTE: Ao realizar este procedimento, não tente montar pontos de recuperação na pasta /tmp, que contém os arquivos aavdisk.

1. Crie um novo diretório para montar o ponto de recuperação (por exemplo, pode usar o comando `mkdir`).
2. Confirme se o diretório existe (por exemplo, usando o comando `ls`).
3. Execute o utilitário local_mount do Rapid Recovery como raiz ou como superusuário, por exemplo:

   ```
   sudo local_mount
   ```
4. No prompt de montagem do Rapid Recovery, digite o comando a seguir para listar as máquinas protegidas.

   ```
   lm
   ```
5. Quando solicitado, digite o endereço IP ou nome do host do servidor do Rapid Recovery Core.
6. Insira as credenciais de login do server do Core, ou seja, o nome de usuário e a senha.

   Será exibida uma lista das máquinas que estão protegidas pelo servidor do Rapid Recovery. Cada máquina é identificada por: número de item de linha, host/endereço IP e número de ID da máquina.

Por exemplo: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba

7. Insira o seguinte comando para relacionar os pontos de recuperação que estão disponíveis para uma máquina especificada:

   ```
   lr <line_number_of_machine>
   ```

   NOTE: Observe que você também pode inserir o número de ID da máquina neste comando em vez do número do item de linha.

   É exibida uma lista com os pontos de recuperação de base e incrementais da máquina. Essa lista inclui o número do item de linha, o carimbo de data e hora, o local do volume, o tamanho do ponto de recuperação e número de ID do volume, que termina com um número de sequência para identificar o ponto de recuperação.

   Por exemplo, 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2

8. Insira o seguinte comando para selecionar e montar o ponto de recuperação especificado no ponto/caminho de montagem especificado.

   ```
   m <volume_recovery_point_ID_number> <volume-letter> [flag] <path>
   ```

   O sinalizador no comando determina como montar o ponto de recuperação. Você pode usar uma das opções a seguir:

   - [r] - montar apenas leitura (padrão). Este sinalizador permite montar um ponto de recuperação, mas não alterá-lo.
   - [w] - montar gravável. Este sinalizador permite montar um ponto de recuperação e alterá-lo.
   - [v] - montar com gravações anteriores. O sinalizador "v" permite montar o ponto de recuperação e incluir alterações que tenham sido feitas durante a montagem gravável anterior mas não estejam presentes no ponto de recuperação.
   - [n] - não montar nbd em <path>. Um nbd (dispositivo de bloco de rede) estabelece uma conexão de socket entre o Core e a máquina protegida quando você realiza uma montagem local. Este sinalizador permite montar o ponto de recuperação sem montar o nbd, o que é útil caso você queira verificar manualmente o sistema de arquivos do ponto de recuperação.

     NOTE: Você também pode especificar um número de linha no comando em vez do número de ID do ponto de recuperação para identificar o ponto de recuperação. Nesse caso, você usaria o número de linha da máquina (da saída de lm), seguido do número da linha do ponto de recuperação e letra de volume, seguido do caminho, como neste exemplo: m <machine_line_number> <recovery_point_line_number> <volume_letter> <path>. Por exemplo, se o resultado de `lm` relacionar três máquinas protegidas e você digitar o comando `lr` para o número 2 e montar o volume b do ponto de recuperação 23 em /tmp/mount_dir, o comando será:

     ```
     m 2 23 b /tmp/mount_dir
     ```

     NOTE: Se você estiver montando um volume BTRFS de um sistema operacional compatível (consulte o tópico “Matriz de compatibilidade e instalação do sistema operacional do Rapid Recovery versão 6.1” no Guia de instalação e atualização do Rapid Recovery), você precisa incluir o seguinte parâmetro:

     ```
     mount -o nodatasum,device=/dev/xxx /dev/xxx /mnt/yyy
     ```

9. Para confirmar se a montagem foi bem-sucedida, insira o seguinte comando, que deve listar o volume remoto anexado:

   ```
   l
   ```

Desmontar um ponto de recuperação em uma máquina Linux

Complete as etapas neste procedimento para desmontar um ponto de recuperação em uma máquina Linux.

1. Execute o utilitário local_mount do Rapid Recovery como raiz ou como superusuário, por exemplo:
   ```
   sudo local_mount
   ```
2. No prompt de montagem do Rapid Recovery, digite o comando a seguir para listar as máquinas protegidas.
   ```
   lm
   ```
3. Quando solicitado, digite o endereço IP ou nome do host do servidor do Rapid Recovery Core Core.
4. Insira as credenciais de login (nome de usuário e a senha) do server do Core.

   Será exibida uma lista das máquinas que estão protegidas pelo servidor do Rapid Recovery Core.
5. Insira o seguinte comando para relacionar os pontos de recuperação que estão disponíveis para uma máquina especificada:
   ```
   lr <line_number_of_machine>
   ```
   NOTE: Observe que você também pode inserir o número de ID da máquina neste comando em vez do número do item de linha.

   Uma lista exibe e inclui os pontos de recuperação de base e incremental da máquina. Essa lista inclui um número de item de linha, data e carimbo de data e hora, localização do volume, tamanho de ponto de recuperação e número de ID do volume que inclui um número de sequência no fim, que identifica o ponto de recuperação.

   Por exemplo: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2
6. Execute o comando `l or list` para obter uma lista dos dispositivos Network Block Device (NBD). Se você montar um ponto de recuperação, receberá um caminho para o NBD-device depois de executar o comando `l or list`.
7. Insira o seguinte comando para desmontar um ponto de recuperação:
   ```
   unmount <path_of_nbd-device>
   ```
8. Execute o comando `l or list` para garantir que a desmontagem do ponto de recuperação foi bem-sucedida.

Forçar um snapshot

Forçar um snapshot permite forçar uma transferência de dados para a máquina protegida atual. Ao forçar um snapshot, a transferência começa imediatamente ou é adicionada à fila se outros trabalhos estiverem em execução.

Você pode escolher entre dois tipos de snapshots.

Se você selecionar um snapshot incremental e não houver nenhum ponto de recuperação anterior, uma imagem de base é capturada. Forçar um snapshot não altera o horário de qualquer snapshot programado.

NOTE: O Rapid Recovery suporta Window 8, Windows 8.1, Windows Server 2012, Windows Server 2012 R2 e Windows Server 2016 para transferências de base e incrementais.

- Uma imagem de base é um snapshot de todos os dados nos volumes selecionados da máquina.
- Um snapshot incremental captura todos os dados que foram alterados desde o último snapshot.

1. No Rapid Recovery Core Console, navegue até a máquina ou cluster com o ponto de recuperação no qual deseja forçar um snapshot.
2. Na página Resumo, no painel Resumo, clique em **Forçar snapshot**.

   A caixa de diálogo Forçar snapshot é mostrada.
3. Na caixa de diálogo Forçar snapshot, na caixa de seleção, clique em um ou mais volumes ou grupos de proteção.
4. Clique em **Forçar snapshot** ou Forçar imagem de base, respectivamente.
5. Se você tiver selecionado uma imagem de base, clique para confirmar que você quer capturar uma imagem de base.

   Uma imagem de base pode levar uma quantidade de tempo significativa, com base na quantidade de dados dos volumes que você quer incluir no backup.
   O snapshot selecionado é colocado na fila e começa assim que outros trabalhos forem concluídos.

Remover pontos de recuperação

Você pode remover facilmente os pontos de recuperação para uma determinada máquina do repositório. Ao excluir pontos de recuperação no Rapid Recovery, você pode especificar uma das opções a seguir.

- **Excluir todos os pontos de recuperação**. Remove todos os pontos de recuperação para a a máquina protegida selecionada do repositório.
- **Excluir um intervalo de pontos de recuperação**. Remove todos os pontos de recuperação em um intervalo especificado antes do atual, até e incluindo a imagem base, que corresponde a todos os dados na máquina, assim como todos os pontos de recuperação após o atual até a próxima imagem de base.

NOTE: Não é possível recuperar os pontos de recuperação que você excluiu. Se você precisar dos dados armazenados nos pontos de recuperação, considere arquivar os dados primeiro.

1. No Rapid Recovery Core Console, no menu **Máquinas protegidas**, clique no nome ou endereço IP da máquina para a qual você quer visualizar e remover pontos de recuperação.

   A visualização Resumo da máquina protegida selecionada é exibida.
2. Ao lado do nome ou endereço IP da máquina, clique no menu **Pontos de recuperação**.

   A página **Pontos de recuperação** da máquina selecionada é exibida.
3. Role o painel **Pontos de recuperação** para baixo.

   As opções aparecem sob o título painel, incluindo Atualizar, Excluir intervalo e Excluir tudo.
4. Para excluir todos os pontos de recuperação armazenados atualmente, sob o título do painel Pontos de recuperação, clique em **Excluir tudo** e, na caixa de diálogo de confirmação, clique para confirmar a exclusão.
5. Para excluir um conjunto de pontos de recuperação em um intervalo de dados específico, faça o seguinte:
   a. Sob o título do painel Pontos de recuperação, clique em **Excluir intervalo**.

   A caixa de diálogo **Excluir pontos de recuperação dentro do intervalo** é exibida.

   b. Na caixa de diálogo **Excluir pontos de recuperação dentro do intervalo**, no campo **De**, selecione a data e hora a partir da qual você quer começar a excluir os pontos de recuperação.
   c. No campo **Até**, selecione a data e a hora que definem os últimos pontos de recuperação que você deseja excluir.
   d. Clique em **Excluir**.
   e. Na caixa de diálogo de confirmação, clique para confirmar a exclusão.

Excluir uma cadeia de pontos de recuperação órfãos

Um ponto de recuperação órfão é um snapshot incremental que não está associado a uma imagem de base. Snapshots subsequentes continuam a se acumular sobre esse ponto de recuperação. No entanto, sem a imagem de base, os pontos de recuperação resultantes são incompletos e é improvável que contenham os dados necessários para concluir uma recuperação. Esses pontos de recuperação são considerados parte da cadeia de pontos de recuperação órfãos. Se essa situação ocorrer, a melhor solução é excluir a cadeia e criar uma nova imagem de base.

Para obter mais informações sobre como forçar uma imagem de base, consulte Forçar um snapshot.

1. No Rapid Recovery Core Console, navegue para a máquina protegida cuja cadeia do ponto de recuperação você deseja excluir.
2. No menu na parte superior da página, clique em **Pontos de recuperação**.
3. No painel Pontos de recuperação, expanda o ponto de recuperação órfão.

   Esse ponto de recuperação é chamado, na coluna Tipo, de “Incremental, Órfão”.
4. A seguir, em Ações, clique em **Excluir**.

   Aparece a janela Excluir pontos de recuperação.
5. Na janela Excluir pontos de recuperação, clique em **Sim**.

> **CAUTION: Excluir esse ponto de recuperação exclui toda a cadeia de pontos de recuperação, incluindo os pontos de recuperação incremental que ocorrem antes ou depois dela, até a próxima imagem de base. Essa operação não pode ser desfeita.**
>
> **CAUTION: A cadeia de pontos de recuperação órfãos é excluída.**

Como migrar pontos de recuperação para um repositório diferente

Caso queira remover os pontos de recuperação de uma máquina protegida de um repositório sem excluí-los, você pode migrá-los para um repositório diferente usando esse procedimento. Esse processo envolve o arquivamento de pontos de recuperação do repositório de origem e, em seguida, a importação do arquivo para o repositório de destino.

Por exemplo, você pode realizar esse procedimento caso o repositório existente esteja cheio ou caso as necessidades mudem e você queira proteger uma máquina usando um Core e um repositório diferentes.

CAUTION: Caso o repositório tenha sido atualizado anteriormente do AppAssure **5.3 ou 5.4 e usado replicação, a** Quest **recomenda realizar o Trabalho de verificar o repositório em cada repositório nesse Core de destino antes da migração. A realização desse trabalho impedirá a cópia de eventuais irregularidades nos dados para o novo repositório de destino. O Trabalho de verificar o repositório só permanece disponível na UI caso seja aplicável ao Core, e pode demorar um tempo substancial para ser executado. Para obter mais informações sobre este trabalho, consulte Sobre como verificar a integridade dos repositórios DVM. Para obter mais informações sobre como executar este trabalho, consulte Executar uma verificação de integridade em um repositório DVM.**

1. No Rapid Recovery Core Console, pause a proteção da máquina protegida ou das máquinas cujos pontos de recuperação você deseja migrar. Para obter mais informações, consulte Pausar e retomar a proteção.
2. Cancele todas as operações atuais da máquina protegida ou das máquinas cujos pontos de recuperação você deseja migrar, ou aguarde a conclusão de todas elas.
3. Arquive os pontos de recuperação das máquinas que você pausou. Para obter mais informações, consulte Criar um arquivo.
4. Após o arquivamento e a verificação do arquivo, remova os pontos de recuperação existentes da máquina protegida que você deseja migrar. Para obter mais informações, consulte Remover pontos de recuperação.

   NOTE: Sem remover os pontos de recuperação existentes, você não pode alterar repositórios de uma máquina protegida.
5. Crie um novo repositório para os pontos de recuperação migrados ou verifique se existe um novo repositório de destino. Para obter mais informações, consulte Criar um repositório de DVM.
   - Caso você queira utilizar um repositório existente, passe à Etapa 6.
6. Altere o repositório de cada máquina que você pausou concluindo as etapas a seguir:
   a. No Core Console, clique na máquina protegida na árvore de navegação.
   b. Na página **Resumo** da máquina protegida, clique em **Definições**.
   c. Na página **Definições**, no painel **Geral**, clique na lista suspensa **Repositório** e selecione o nome do repositório criado na Etapa 4.
      - Se quiser usar um repositório existente, selecione o nome de um repositório.

        NOTE: Ao migrar pontos de recuperação para um repositório existente, certifique-se de que o repositório possui espaço livre suficiente para conter os pontos de recuperação migrados.
   d. Clique em **OK**.
7. Retome a proteção das máquinas que você pausou. Para obter mais informações, consulte Pausar e retomar a proteção.
8. Gere uma nova imagem de base de cada máquina protegido que você moveu. Para obter mais informações, consulte Forçar um snapshot e use Forçar imagem de base.
9. Importe os dados arquivados das máquinas que você deseja migrar. Para obter mais informações, consulte Importação de um arquivo.

Replicação

Este capítulo descreve como configurar e gerenciar a replicação de dados protegidos de um Core de origem do Rapid Recovery para um Core de destino do Rapid Recovery para recuperação após desastres.

Replicação com Rapid Recovery

Esta seção fornece informações conceituais e de procedimentos para ajudá-lo a entender e configurar a replicação no Rapid Recovery.

Replicação é um processo de copiar pontos de recuperação de um Rapid Recovery Core e transmiti-los para outro Rapid Recovery Core visando a recuperação de desastres. O processo exige uma solução com pares de origem/destino entre dois ou mais Cores.

O Core de origem copia os pontos de recuperação de máquinas protegidas designadas e então transmite de modo assíncrono e contínuo os dados de snapshot para o Core de destino.

A menos que você altere o comportamento padrão ao definir um programa de replicação, o Core iniciará o trabalho de replicação imediatamente após conclusão de cada snapshot de backup, verificação de soma de verificação, verificação de montabilidade e verificação de capacidade de anexação. O truncamento de log de qualquer tipo também aciona um trabalho de replicação, assim como verifica a integridade dos pontos de recuperação ou de um banco de dados Oracle. Se uma dessas ações estiver incluída em trabalhos noturnos, a execução dos trabalhos noturnos também acionará um trabalho de replicação. Para obter mais informações, consulte Programar a replicação.

NOTE: Ao replicar dados de um cluster, você deve replicar todo o cluster. Por exemplo, se você selecionar um nó para ser replicado, o cluster é automaticamente selecionado. Da mesma forma, se você selecionar o cluster, todos os nós nesse cluster são também selecionados.

Para obter melhor segurança de dados, os administradores geralmente usam um Core de destino em uma localidade remota de recuperação de desastres. É possível configurar a replicação de saída para um data center de propriedade da empresa ou para uma localidade remota de recuperação de desastres (ou seja, um Core de destino "autogerenciado"). Ou é possível configurar a replicação de saída para um provedor de serviços gerenciados (MSP) terceirizado ou provedor de nuvem que hospede serviços de recuperação após desastres e cópia de segurança em um site externo. Ao replicar para um Core de destino de terceiros, é possível usar fluxos de trabalho incorporados que permitam solicitar conexões e receber notificações automáticas de feedback.

A replicação é gerenciada por máquina protegida. Qualquer máquina (ou todas as máquinas) protegida ou replicada em um Core de origem pode ser configurada para replicar em um Core de destino.

Os possíveis cenários de replicação incluem:

- **Replicação para uma localização local**. O Core de destino situa-se em um datacenter local ou localização no local e a replicação é sempre mantida. Nessa configuração, a perda do Core não impediria a recuperação.
- **Replicação para uma localização externa**. O Core de destino está localizado em uma instalação de recuperação após desastres externa para recuperação em caso de perda.
- **Replicação mútua**. Dois datacenters em locais diferentes, cada um contendo um Core, protegendo máquinas e atuando mutuamente como cópia de segurança externa para recuperação após desastres. Nesse cenário, cada Core replica as máquinas protegidas do Core localizado no outro datacenter.
- **Replicação hospedada e na nuvem**. Os parceiros MSP do Rapid Recovery mantêm vários Cores de destino em um datacenter ou uma nuvem pública. Em cada um desses Cores, o parceiro MSP permite que

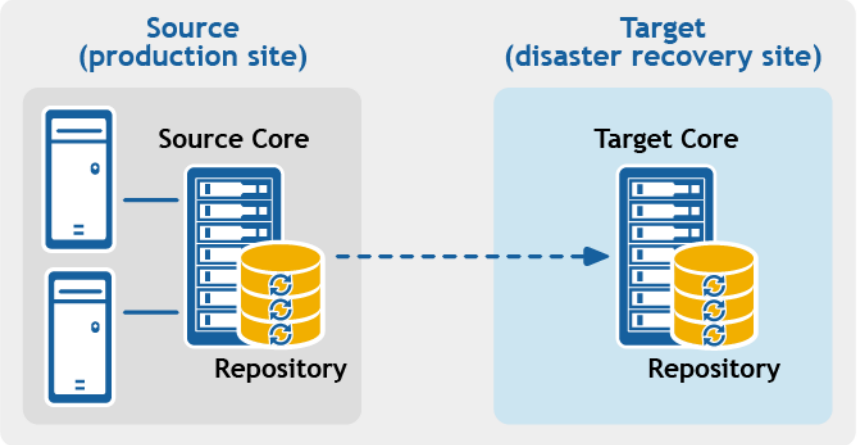
um ou mais dos seus clientes replique os pontos de recuperação a partir de um Core de origem no local do cliente para o Core de destino do MSP por uma taxa.

NOTE: Nesse cenário, os clientes têm acesso apenas aos seus próprios dados.

As possíveis configurações de replicação incluem:

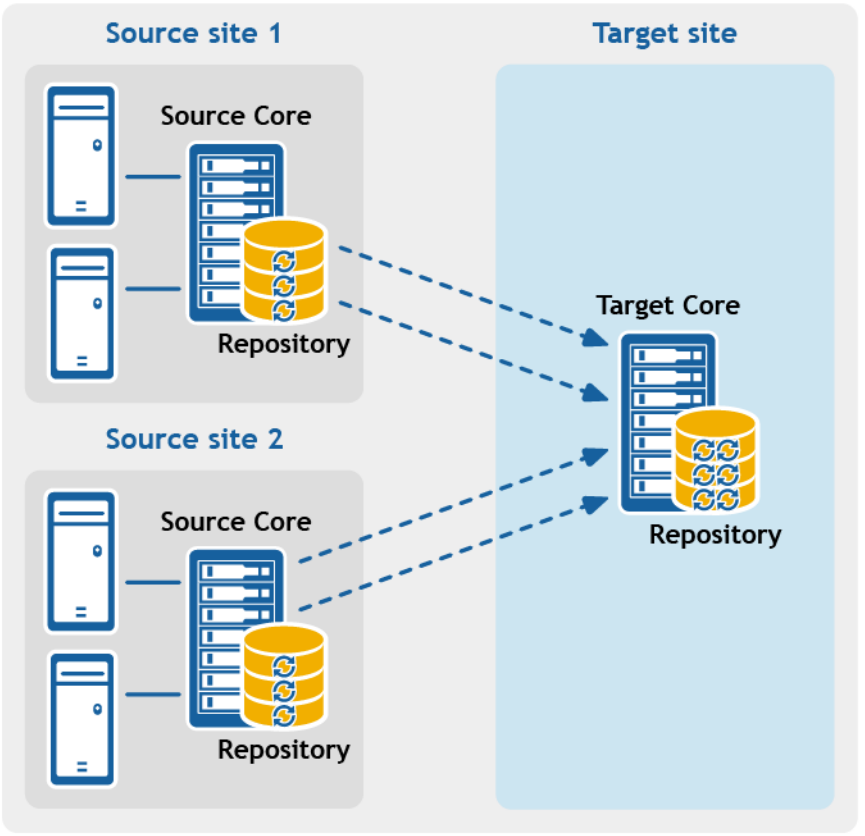
- **Replicação ponto-a-ponto**. Replica uma ou mais máquinas protegidas de um único Core de origem para um único Core de destino.

Figura 1. Configuração de replicação ponto-a-ponto



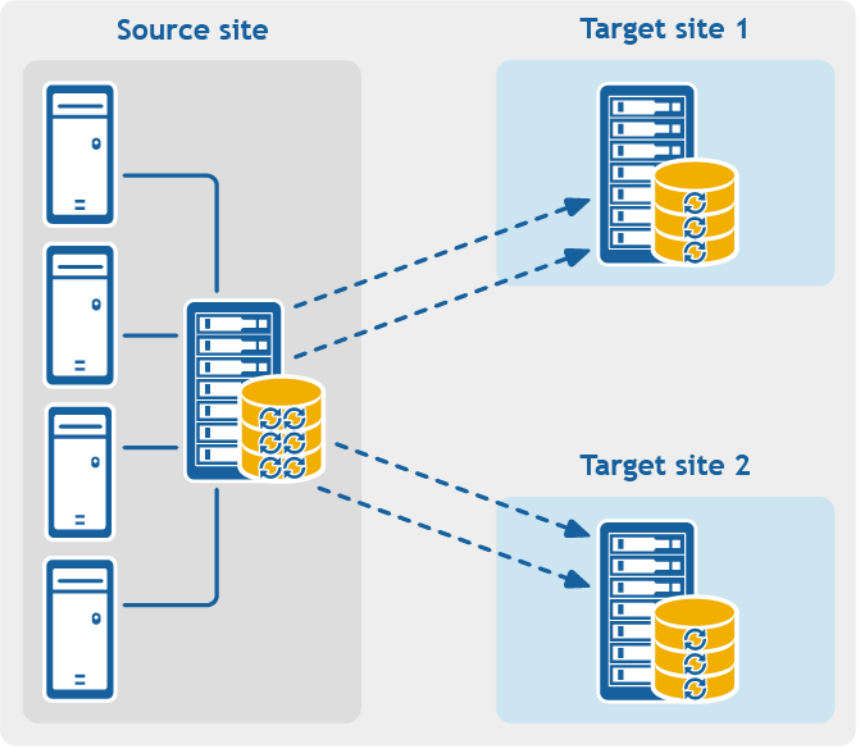
- **Replicação multiponto-a-ponto**. Replica máquinas protegidas de vários Cores de origem para um único Core de destino.

Figura 2. Configuração de replicação de multiponto-a-ponto



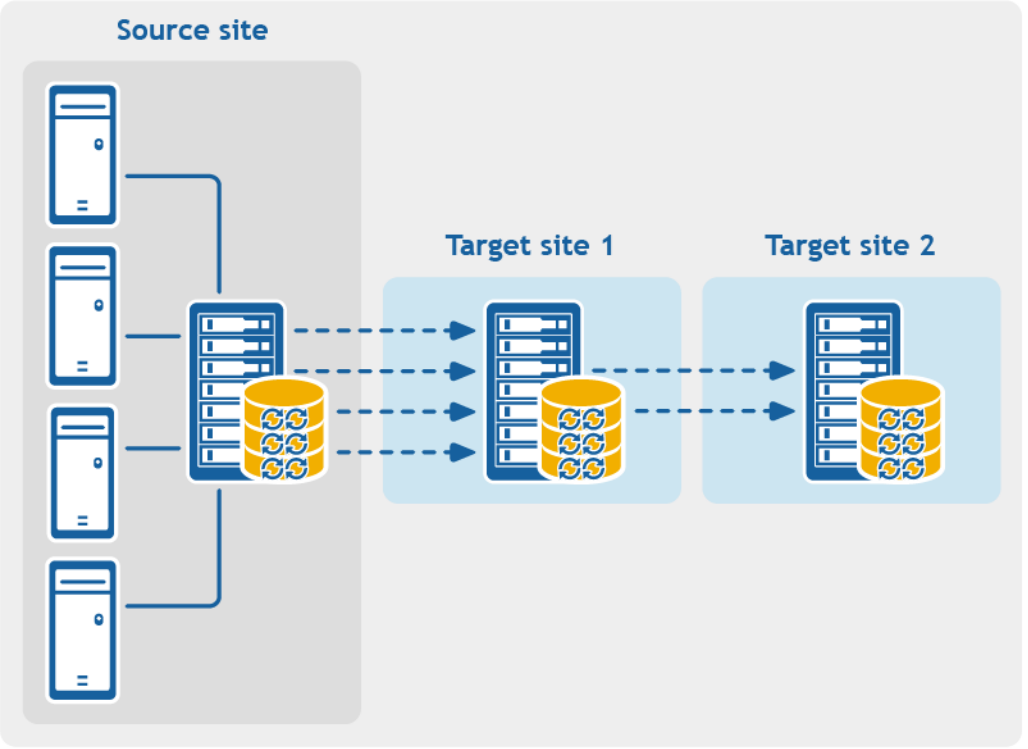
- **Replicação de ponto-a-multiponto**. Replica uma ou mais máquinas protegidas de um único Core de origem para mais de um Core de destino.

Figura 3. Configuração de replicação ponto-a-multiponto



- **Replicação de saltos múltiplos.** Replica uma ou mais máquinas protegidas de um Core de destino para outro Core de destino, produzindo opções e ativação adicional pós-falha ou recuperação no Core replicado.

Figura 4. Configuração de replicação de saltos múltiplos



Se estiver usando soluções de backup da série DL, o Core de destino para o qual você replicar deverá ter uma licença de software válida configurada. Esses appliances de hardware incluem uma licença de destino de replicação com a compra. Verifique a chave de licença na mensagem de e-mail de boas-vindas que você recebeu quando adquiriu o appliance. Para obter assistência, visite o site de Assistência de licenciamento em https://support.quest.com/contact-us/licensing ou envie um e-mail para license@quest.com.

Cadeias de pontos de recuperação e órfãos

O Rapid Recovery captura os snapshots de uma máquina protegida e salva os dados em um repositório como um ponto de recuperação. O primeiro ponto de recuperação salvo no Core é chamado de imagem de base. A imagem de base inclui o sistema operacional, os aplicativos e as configurações para cada volume que você seleciona para proteger, bem como todos os dados nesses volumes. Os backups sucessivos são snapshots incrementais, que consistem apenas em dados alterados nos volumes protegidos desde o último backup. A imagem de base e os snapshots incrementais formam uma cadeia completa de pontos de recuperação.

A partir de uma cadeia completa de pontos de recuperação, você pode restaurar os dados com facilidade e confiança, usando toda a faixa de opções de recuperação disponíveis para o Rapid Recovery. Essas opções incluem a restauração no nível do arquivo, no nível do volume e bare metal restore.

Uma vez que logicamente não é possível restaurar dados que não existem, no caso de uma cadeia incompleta de pontos de recuperação, você não poderá restaurar os dados no nível do volume ou realizar um bare metal restore. Nesses casos, você ainda poderá restaurar quaisquer dados existentes em um ponto de recuperação no nível do arquivo.

Se a informação que você deseja restaurar de um ponto de recuperação estiver em um backup prévio que não está disponível para o Core (um snapshot incremental ou imagem de base prévio), o ponto de recuperação será considerado órfão. Os pontos de recuperação órfãos são típicos em alguns cenários de replicação.

Por exemplo, quando você estabelece a replicação pela primeira vez, as suas opções para restaurar os dados dos pontos de recuperação replicados são limitadas. Até que todos os dados de backup do Core de origem sejam transmitidos ao Core de destino, criando cadeias completas de pontos de recuperação a partir dos órfãos, você pode realizar somente a restauração no nível do arquivo.

Quando a replicação começar

Por padrão, os trabalhos de transferência de replicação são automaticamente colocados em fila pelo Core, imediatamente depois da conclusão de cada transferência do backup programado regularmente. Portanto, a menos que o programa da replicação de uma máquina protegida seja personalizado, ele é baseado no programa padrão do snapshot de backup.

Quando você configurar uma replicação pela primeira vez, se houver um ou mais pontos de recuperação no Core de origem, o processo de replicação começará imediatamente, a menos que:

- Você selecione a opção para pausar a replicação inicialmente ou
- Você selecione a opção para usar uma unidade de seeding para realizar a transferência inicial.

Se você pausar a replicação inicialmente, ela começará quando você retomar a replicação explicitamente.

Se você configurar a replicação e especificar o uso de uma unidade de seeding, a replicação para o Core de destino começará com o próximo snapshot de backup regularmente programado.

NOTE: Você pode também forçar um backup da máquina protegida depois de estabelecer a replicação. Isso faz a replicação começar imediatamente depois que o snapshot da máquina protegida for concluído.

Se você especificar uma unidade de seeding ao configurar uma replicação, somente as futuras transferências de backup serão replicadas. Se você deseja que os pontos de recuperação existentes da máquina protegida original existam no Core de destino, precisará fazer o seeding dos dados da máquina protegida. Para fazer o seeding dos dados, crie uma unidade de seeding do Core de origem e, em seguida, consuma-a no Core de destino.

Você também pode personalizar o programa da replicação para uma máquina protegida. Por exemplo, se você usar o programa de proteção padrão de um backup por hora, poderá especificar que o Core de origem replique para o Core de destino em um programa diferente (por exemplo, uma vez por dia às 2AM).

Determinar suas necessidades e sua estratégia de seeding

Os tópicos a seguir discutem a restauração de dados replicados e se você precisa fazer o seeding dos dados do ponto de recuperação do Core de origem.

Quando o seeding de dados é necessário

Quando você estabelece a replicação pela primeira vez, a menos que especifique o uso de uma unidade de seeding, o Core de origem começa a transmitir todos os pontos de recuperação para as máquinas selecionadas para o Core de destino. A transmissão dos seus dados via rede pode levar um bom tempo. Os fatores envolvidos incluem a velocidade da rede, a robustez da arquitetura da rede e a quantidade de dados a serem transmitidos ao Core de destino. Por exemplo, se os dados de backup do Core de origem medirem 10GB e o link WAN transferir 24Mbps, a transferência pode demorar cerca de uma hora para ser concluída.

Com base na quantidade de informação que você deseja copiar para o Core de destino, a unidade de seeding pode adicionar até centenas ou milhares de gigabytes de dados. Muitas organizações optam por não consumir a

largura de banda de rede necessária e, em vez disso, preferem definir e consumir uma unidade de seeding. Para obter mais informações, consulte Considerações sobre desempenho para transferência de dados replicados.

Se você especificar o uso de uma unidade de seeding ao definir a replicação, apenas os pontos de recuperação salvos para o Core de origem depois de estabelecer a replicação serão replicados para o Core de destino. Os backups salvos no Core de origem antes do estabelecimento da replicação não estarão presentes no Core de destino até que você faça explicitamente o seeding dos dados, usando o processo a seguir.

Para evitar diminuir a velocidade da rede com uma transferência intensiva de dados históricos, faça o seeding dos dados do backup prévio para o Core de destino usando uma **unidade de seeding**. Uma unidade de seeding é um arquivo que **copia** um conjunto de imagens de base desduplicadas e snapshots incrementais do Core de origem. O arquivo da unidade de seeding contém o conjunto completo de pontos de recuperação prévios para as máquinas protegidas que você deseja replicar do Core de origem para o Core de destino.

Mova o arquivo da unidade de seeding para um volume de armazenamento, que depois você disponibiliza para o Core de destino. Em seguida, você **consome** a informação da unidade de seeding. Isso envolve anexar o volume com a imagem da unidade de seeding ao Core de destino e importar os dados para o repositório do Core Console. Esse processo repara os órfãos, unindo os snapshots incrementais replicados no Core de destino com as suas imagens de base para formar uma ou mais cadeias completas de pontos de recuperação. Esse processo é às vezes chamada de copiar-consumir.

O seeding dos dados do seu Core de origem nem sempre é necessário. Por exemplo:

- Se você estiver configurando a replicação para um novo Rapid Recovery Core, o seeding não será necessário.
- Se os dados de snapshots prévios não forem críticos para os seus dados replicados, e você precisa recuperar somente os dados salvos depois da configuração da replicação, o seeding não será necessário.

  NOTE: Nesse caso, a Quest recomenda capturar uma nova imagem de base imediatamente antes ou depois de configurar a replicação. Esta etapa garante a existência de uma cadeia completa de pontos de recuperação no Core de destino, a fim de restaurar dados no futuro.
- Se você capturou uma imagem de base imediatamente antes de configurar a replicação e precisa somente restaurar os dados capturados depois dessa data, o seeding não será necessário.
- Se você configurar a replicação sem especificar uma unidade de seeding, os dados do snapshot são transmitidos via rede do Core de origem para o Core de destino.

Se uma dessas situações aplicar-se a você, o seeding dos dados não será necessário. Nesses casos, a replicação pode ser concluída inteiramente no Core de origem.

Se você configurar a replicação para um Core com pontos de recuperação existentes e precisar restaurar no nível de volume, desejar realizar um BMR ou restaurar os dados de uma imagem de base prévia ou snapshot incremental, o seeding será necessário. Nessas situações, pense nas suas necessidades e na sua estratégia de seeding. Analise as informações sobre esse tópico e decida se fará o seeding para o Core de destino e qual abordagem usará.

Abordagens para o seeding dos dados

Se você deseja que as máquinas replicadas em um Core de destino tenham acesso aos dados salvos previamente no Core de origem, faça o seeding do Core de destino usando uma das seguintes abordagens:

1. **Faça o seeding para o Core de destino via conexão de rede.** Especifique o uso de uma unidade de propagação quando definir a replicação. Em seguida, você pode compartilhar a pasta que contém a unidade de propagação com o Core de destino e consumir o arquivo da unidade de propagação via rede. Para dados grandes ou conexões lentas, esse método de seeding pode levar uma quantidade substancial de tempo e consumir uma largura de banda substancial.

   NOTE: A Quest não recomenda a propagação de grandes quantidades de dados via conexão de rede. O seeding inicial envolve potencialmente quantidades de dados muito grandes, o que pode sobrecarregar uma conexão WAN típica.
2. **Transferir dados de backup do Core de origem usando a mídia de armazenamento físico.** Transfira o arquivo da unidade de seeding para um dispositivo de armazenamento externo removível e portátil.

Normalmente, essa abordagem é útil para grandes conjuntos de dados ou sites com conexões de rede lentas. Esse método de seeding exige a realização das seguintes etapas:

a. Crie um arquivo de seeding do Core de origem, salvando-o na mídia removível.
b. Transporte a unidade de seeding para o local físico do Core de destino.
c. Anexe a unidade ao Core de destino.
d. Consuma os dados da unidade de seeding para o repositório do Core de destino.

Ao replicar para um Core de terceiros, assim que a mídia for recebida pelo MSP, um representante do datacenter normalmente anexa a mídia e avisa-o quando ela estiver pronta para você consumir (ou importar) os dados do seeding para o Core.

NOTE: Uma vez que grandes quantidades de dados precisam ser copiadas para o dispositivo de armazenamento, recomenda-se o uso de uma conexão eSATA, USB 3.0 ou outra de alta velocidade. Se o tamanho total do arquivo de dados de seeding for superior ao espaço disponível na mídia removível, o arquivo pode ocupar vários dispositivos.

3. **Para Cores de origem e de destino armazenados em máquinas virtuais, transfira os dados de backup usando um disco rígido virtual.** Se o Core de origem e de destino estiverem em uma máquina virtual, você poderá definir e consumir uma unidade de seeding na mídia de armazenamento virtual. Esse método de seeding exige a realização das seguintes etapas:

a. Crie um arquivo da unidade de seeding do Core de origem, salvando-o em um volume de armazenamento virtual.
b. Retire o volume do Core de origem e anexe-o ao Core de destino.
c. Consuma os dados da unidade de seeding para o repositório do Core de destino.

NOTE: Embora a replicação de snapshots incrementais possa ocorrer entre os Cores de origem e destino antes do seeding terminar, os snapshots replicados transmitidos da origem para o destino permanecem órfãos até que os dados iniciais sejam consumidos e são combinados com as imagens de base replicadas.

Links relacionados

- Para obter detalhes do processo de consumo da unidade de seeding, consulte o tópico Consumo da unidade de propagação em um Core de destino.
- Para obter mais informações sobre pontos de recuperação órfãos, consulte Excluir uma cadeia de pontos de recuperação órfãos.
- Para obter informações sobre como preparar uma unidade de seeding, consulte Noções gerais sobre unidades de seeding, e Consumo da unidade de seeding em um Core de destino.

See also: Consumo da unidade de propagação em um Core de destino
See also: Excluir uma cadeia de pontos de recuperação órfãos

Considerações sobre desempenho para transferência de dados replicados

Se a largura da banda entre os Cores de origem e de destino não pode acomodar a transferência de pontos de recuperação armazenados, configure a replicação e especifique o uso de uma unidade de seeding. Este processo propaga o Core de destino com imagens base e pontos de recuperação do servidores selecionados protegidos no Core de origem. O processo de seeding pode ser executado a qualquer momento. Ele pode ser realizado como parte da transferência inicial de dados, que funciona como fundamento para replicações programadas regularmente. Você também pode propagar dados para uma máquina anteriormente replicada se a replicação foi pausada ou apagada. Nesse caso, a opção "Criar cadeias de ponto de recuperação" permitiria copiar os pontos de recuperação ainda não replicados para uma unidade de seeding.

Ao preparar-se para a replicação, considere os seguintes fatores:

- **Taxa de alteração.** A taxa de alteração é a taxa de acumulação da quantidade de dados protegidos. A taxa depende da quantidade de dados alterados em volumes protegidos e do intervalo de proteção dos volumes. Alguns tipos de máquinas normalmente têm uma taxa maior de alteração, como, por exemplo, um e-mail do Exchange server. Uma forma de reduzir a taxa de alteração é reduzir o intervalo de proteção.
- **Largura de banda.** A largura de banda é a velocidade de transferência disponível entre o Core de origem e o de destino. É vital que a largura de banda seja superior à taxa de alteração para que a replicação acompanhe os pontos de recuperação criados pelos snapshots. Devido à quantidade de dados transmitidos de um Core para outro, vários fluxos paralelos podem ser necessários para se obter velocidades por fio de uma conexão Ethernet de 1GB.

  NOTE: A largura da banda que os ISPs especificam é tipicamente a largura de banda total disponível. Todos os dispositivos na rede compartilham a largura de banda de saída. Certifique-se de que haja largura de banda livre suficiente para replicação a fim de acomodar a taxa de alteração.
- **Número de máquinas protegidas.** É importante considerar o número de máquinas protegidas pelo Core de origem e quantas você pretende replicar para o Core de destino. Você não precisa replicar cada máquina protegida no Core de origem; o Rapid Recovery permite que você replique por máquina protegida, portanto, você pode optar por replicar somente certas máquinas, se quiser. Se todas as máquinas protegidas em um Core de origem precisarem ser replicadas, a taxa de alteração será normalmente mais alta. Este fator é relevante se o largura da banda entre o Core de origem e o de destino não for suficiente para a quantidade e o tamanho dos pontos de recuperação que estão sendo replicados.

A taxa de alteração máxima por tipo de conexão WAN é mostrada na tabela abaixo com exemplos da largura de banda necessária por gigabyte para obter uma taxa de alteração razoável.

Tabela 89. Exemplos de largura de banda por gigabyte

Banda larga	Largura de banda	Taxa de alteração máxima
DSL	768 Kbps ou mais	330MB por hora
Cabo	1 Mbps ou mais	429MB por hora
T1	1,5 Mbps ou mais	644MB por hora
Fibra	20 Mbps ou mais	8,38GB por hora

NOTE: Para obter resultados ideais, siga as recomendações apresentadas na lista na tabela anterior.

Se um link falhar durante a transferência de dados, a replicação é retomada a partir do ponto de falha anterior da transferência (assim que a funcionalidade do link for restaurada).

Dependendo da configuração de rede, a replicação pode ser um processo demorado. Certifique-se de que você tenha largura da banda suficiente para acomodar a replicação, outras transferências do Rapid Recovery como backups, e quaisquer outros aplicativos importantes que você precisa executar.

Se você tiver problemas com a transferência de dados pela rede, particularmente para algumas máquinas protegidas ou replicadas, considere ajustar a taxa de transferência de dados para tais máquinas. Para obter mais informações, consulte Sobre a modificação das definições da transferência e Estrangulamento da velocidade de transferência.

Sobre replicação e pontos de recuperação criptografados

Embora a unidade de propagação não contenha cópias de segurança do registro e dos certificados do Core de origem, ela conterá as chaves de criptografia do Core de origem se os pontos de recuperação que estão sendo replicados da origem para o destino estiverem criptografados. Os pontos de recuperação replicados permanecem criptografados depois de transmitidos para o Core de destino. Os proprietários ou administradores do Core de destino precisam da frase de acesso para recuperar os dados criptografados.

Sobre políticas de retenção para replicação

As políticas de retenção nos Cores de origem e de destino não são sincronizadas. Rollup e exclusão sob demanda são executadas de forma independente em cada Core na ação inicial, bem como durante os trabalhos noturnos.

Para obter mais informações sobre as políticas de retenção, consulte Gerenciar políticas de retenção.

Ver a replicação de entrada e saída

Se você clicar no ícone **Replicar** da barra de ícones, a página **Replication** (Replicação) será exibida. Essa página fornece noções básicas sobre a replicação, no escopo deste Core. Ela inclui dois painéis:

- O painel **Replicação de saída** lista as máquinas protegidas neste Core que são replicadas em outro Core.
- O painel **Replicação de entrada** lista as máquinas replicadas neste Core e o Core de origem do qual essas máquinas são replicadas.

Esta seção descreve as informações mostradas nesses painéis.

As informações sobre a replicação de saída deste Rapid Recovery são descritas na tabela a seguir.

Tabela 90. Informações sobre a replicação de saída

Elemento de UI	Descrição
Selecione um item	Para cada fila na tabela de resumo, você pode marcar a caixa de seleção para realizar ações na lista de opções do menu acima da tabela.
Tipo	Mostra o tipo de máquina. Você pode expandir um Core de destino para mostrar máquinas replicadas individuais.
Indicador de status	Status da replicação. Círculos coloridos na coluna Status mostram se uma máquina replicada está online ou inacessível. Quando você passa o cursor sobre o círculo colorido, a condição de status é exibida. As condições de status são verde (replicação estabelecida e online), amarelo (replicação pausada), vermelho (erro de autenticação) e cinza (offline ou inacessível).
Nome da replicação	O nome de exibição da máquina do Core para a qual as máquinas deste Core de origem serão replicadas.
Máquinas	Lista o número de máquinas replicadas no Core de destino selecionado.

Elemento de UI	Descrição
Sincronizar	A data e a hora da última transferência de replicação para o Core de destino.
•••	Quando você clica no menu suspenso Mais nessa coluna, visualiza uma lista de ações que afetam a relação da replicação específica.

Você pode realizar ações em dois ou mais Cores de destino listados na grade de Replicação de saída. Para realizar ações em vários Cores de destino, marque a caixa de seleção de cada Core na grade e, no menu acima da grade, selecione a ação que deseja realizar. Você pode realizar as ações descritas na tabela a seguir.

Tabela 91. Ações globais disponíveis no painel Replicação de saída

Elemento de UI	Descrição
Adicionar Core de destino	Permite definir outro Core de destino para as máquinas replicadas protegidas neste Core de origem.
Atualizar	Atualiza as informações mostradas na tabela.
Forçar	Força a replicação.
Pausar	Pausa a replicação estabelecida.
Retomar	Retoma a replicação pausada.
Copiar	Abre o assistente de replicação, permitindo copiar os pontos de recuperação existentes para as máquinas protegidas selecionadas para uma unidade de seeding.
Excluir	Exclui a replicação de saída.
Unidades de propagação	Essa opção de menu aparece se os dados foram copiados para uma unidade de seeding ao configurar a replicação. Exibe informações sobre o arquivo de unidade de seeding, incluindo os dados e a hora em que a unidade foi salva. Menus minimizáveis indicam o Core de destino e as máquinas protegidas das quais os arquivos da unidade de seeding foram gerados.
•••	Quando você clica no menu suspenso Mais nessa coluna, visualiza uma lista de ações que afetam a relação da replicação específica.

As informações sobre a replicação de entrada de outro Core são descritas na tabela a seguir.

Tabela 92. Informações sobre a replicação de entrada

Elemento de UI	Descrição
Selecione um item	Para cada fila na tabela de resumo, você pode marcar a caixa de seleção para realizar ações na lista de opções do menu acima da tabela.
Tipo	Mostra o tipo de máquina. Você pode expandir um Core de origem para mostrar máquinas replicadas individuais.
Indicador de status	Status da replicação. Círculos coloridos na coluna Status mostram se uma máquina replicada está online ou inacessível. Quando você passa o cursor sobre o círculo colorido, a condição de status é exibida. As condições de status são verde (replicação

Elemento de UI	Descrição
	estabelecida e online), amarelo (replicação pausada), vermelho (erro de autenticação) e cinza (offline ou inacessível).
Nome da replicação	O nome de exibição da máquina do Core de origem que contém as máquinas protegidas que são replicadas neste Core de destino. Esse nome também pode ser especificado ao estabelecer a replicação no Core de origem usando o Assistente de replicação.
Máquinas	Lista o número de máquinas protegidas no Core de origem que são replicadas para este Core de destino.
Sincronizar	A data e a hora da última transferência de replicação do Core de origem.
	Quando você clica no menu suspenso Mais nessa coluna, visualiza uma lista de ações que afetam a relação da replicação específica.

Você pode realizar ações em dois ou mais Cores de origens listados na grade de Replicação de entrada. Para realizar ações em vários Cores de origem, marque a caixa de seleção de cada Core na grade e, no menu acima da grade, selecione a ação que deseja realizar. Você pode realizar as ações descritas na tabela a seguir.

Tabela 93. Ações globais disponíveis no painel Replicação de entrada

Elemento de UI	Descrição
Atualizar	Atualiza as informações mostradas na tabela.
Forçar	Força a replicação.
Pausar	Pausa a replicação estabelecida.
Retomar	Retoma a replicação pausada.
Excluir	Exclui a replicação de entrada.

Configurar a replicação

Para replicar os dados usando o Rapid Recovery, é preciso configurar as cores de origem e de destino para a replicação. Depois de configurar a replicação, você pode replicar dados de máquina protegida, monitorar e gerenciar a replicação e realizar a recuperação.

NOTE: Ao replicar dados de um cluster, você deve replicar todo o cluster. Por exemplo, se você selecionar um nó para ser replicado, o cluster é automaticamente selecionado. Da mesma forma, se você selecionar o cluster, todos os nós nesse cluster são também selecionados.

A replicação no Rapid Recovery envolve executar as seguintes operações:

- Definir um repositório no core de destino. Para obter mais informações sobre adicionar um repositório ao core de destino, consulte Criar um repositório de DVM.
- Configurar a replicação autogerenciada. Para obter mais informações sobre replicar em um core de destino autogerenciado, consulte Replicar para um Core de destino autogerenciado.
- Configurar a replicação de terceiros. Para obter mais informações sobre replicar em um core de destino de terceiros, consulte Replicar para um Core de destino de terceiros.
- Replicar uma máquina protegida existente. Para obter mais informações sobre replicação de uma máquina já protegida pelo Core de origem, consulte Adicionar uma máquina a uma replicação existente.
- Consumir a unidade de seeding. Para obter mais informações sobre consumir dados da unidade de seeding no core de destino, consulte Consumo da unidade de propagação em um Core de destino.
- Definir a prioridade de replicação de uma máquina protegida. Para obter mais informações sobre priorização da replicação de máquinas protegidas, consulte Definir a prioridade de replicação de uma máquina protegida.
- Definir uma programação de replicação para uma máquina protegida. Para obter mais informações sobre a definição de uma programação de replicação, consulte Programar a replicação.
- Monitorar replicação conforme necessário. Para obter mais informações sobre monitoramento de replicação, consulte Ver a replicação de entrada e saída
- Gerenciar as definições de replicação conforme necessário. Para obter mais informações sobre gerenciamento das definições de replicação, consulte Gerenciar definições de replicação.
- Recuperar dados replicados em caso de desastre ou perda de dados. Para obter mais informações sobre a recuperação de dados replicados, consulte Recuperar dados replicados.

Replicar para um Core de destino autogerenciado

Essa configuração se aplica à replicação para localização externa e à replicação mútua. As etapas a seguir são pré-requisitos:

- O Rapid Recovery Core deve ser instalado em todas as máquinas de origem e de destino.
- Se você estiver configurando o Rapid Recovery para replicação multiponto a ponto, será preciso realizar essa tarefa em todos os Cores de origem e no Core de destino único. Para obter descrições destas configurações de replicação, consulte Replicação.
- Se você precisar criar uma unidade de seeding para transferi-la para um volume de armazenamento removível físico para executar a transferência inicial de pontos de recuperação existentes, você precisa ter um dispositivo de armazenamento portátil preparado. Você também precisa ter acesso físico à máquina do Core de origem, para anexar a unidade para copiar o arquivo da unidade de seeding.
- Se você estiver usando uma unidade de seeding em um Core de destino autogerenciado, você ou um administrador confiável deve ter acesso físico ao Core de destino.

Um Core de destino autogerenciado é um Core ao qual você tenha acesso. Por exemplo, um Core autogerenciado frequentemente é gerenciado por sua empresa em locais externos, ou é hospedado em um local geográfico diferente do Core de origem. A replicação pode ser executada totalmente no Core de origem, a menos que você escolha executar a propagação dos seus dados usando uma unidade de seeding. Nesses casos, você precisa criar uma unidade de seeding usando este procedimento, e posteriormente anexar a unidade de seeding ao Core de destino para consumir os dados do ponto de recuperação arquivados. Para obter mais informações, consulte Determinar suas necessidades e sua estratégia de seeding.

Execute as etapas do procedimento a seguir para configurar seu Core de origem a fim de replicar em um Core de destino autogerenciado.

1. Navegue até o Rapid Recovery Core Console do Core de origem.
2. Na barra de botões, clique em **Replicar**.

   O **Assistente de replicação** será exibido.
3. Na página **Core de destino** do Assistente de replicação, se você estiver estabelecendo a replicação com um Core de destino que tenha sido emparelhado com este Core de origem anteriormente, selecione **Usar um Core de destino existente**e, em seguida, selecione o Core de destino adequado na lista suspensa. Pule para a etapa 5.
4. Na página **Core de destino** do Assistente de replicação, se você estiver estabelecendo a replicação com um Core de destino a partir deste Core de origem pela primeira vez, selecione **Tenho meu próprio Core de destino**, e, em seguida, digite as informações, conforme descrito na tabela a seguir.

Tabela 94. Informações do Core de destino

Caixa de texto	Descrição
Nome do host	Insira o nome do host ou o endereço IP da máquina do Core na qual está replicando.
Porta	Insira o número da porta pela qual o Rapid Recovery Core se comunicará com a máquina. O número de porta padrão é 8006.
Nome de usuário	Insira o nome de usuário para acessar a máquina.
Senha	Insira a senha para acessar a máquina.

5. Clique em **Avançar**.

   NOTE: Se não existir repositório no Core de destino, aparecerá um aviso informando que o Core de origem pode ser pareado ao de destino, mas você não poderá replicar agentes (máquinas protegidas) para esse local até que um repositório seja estabelecido. Para obter informações sobre como configurar um repositório para um Core, consulte Criar um repositório de DVM.
6. Na página **Solicitar**, digite um nome para essa configuração de replicação, por exemplo, SourceCore1. Este é o nome de exibição usado para o painel de Replicação de entrada na página de Replicação do Core de destino.
7. Clique em **Avançar**.
8. Na página **Máquinas protegidas**, selecione as máquinas protegidas que deseja replicar e use as listas suspensas na coluna Repositório para selecionar um repositório para cada máquina protegida.
9. Se desejar realizar o processo de propagação para a transferência dos dados de base, execute as seguintes etapas. Se você não quiser semear os dados, vá para a próxima etapa.

   NOTE: Uma vez que grandes quantidades de dados precisam ser copiadas para o dispositivo de armazenamento portátil, a Quest recomendada utilizar uma conexão eSATA, USB 3.0 ou outra de alta velocidade nesse dispositivo.

   a. Na página **Máquinas protegidas** do Assistente de replicação, selecione **Usar uma unidade de seeding para realizar a transferência inicial**.

   - Se já tiver uma ou mais máquinas protegidas replicando para um Core de destino, você poderá incluí-las na unidade de seeding selecionando a opção **Incluir os pontos de recuperação já replicados na unidade de propagação**.
   - Se não quiser que a replicação comece imediatamente após a conclusão desse procedimento, selecione **Pausar replicação inicialmente**.

NOTE: Se você selecionar essa opção, a replicação não começará até que você retome-o explicitamente. Para obter mais informações, consulte Pausar e retomar a replicação.

b. Clique em **Avançar**.

c. Na página **Local da unidade de seeding** do assistente de replicação, use a lista suspensa do **Tipo de local** para selecionar entre os seguintes tipos de destino:

- Local
- Rede
- Nuvem

d. No campo Local, digite os detalhes para o arquivo da unidade de seeding conforme descrito na tabela a seguir com base no tipo de local selecionado na Etapa c.

Tabela 95. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Usado para definir o caminho do local onde você deseja que o arquivo da unidade de seeding resida, por exemplo, `D:\work\archive`.
Rede	Local de saída	Insira a localização para a saída. Usado para definir o caminho do local onde você deseja que o arquivo da unidade de seeding resida, por exemplo, `\\servername\sharename`.
	Nome de usuário	Insira um nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTE:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é Rapid-Recovery-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

e. Clique em **Avançar**.

f. Na página **Opções da unidade de seeding** do Assistente de replicação, insira as informações conforme descrito na tabela a seguir.

Tabela 96. Opções da unidade de propagação

Item	Descrição
Tamanho máximo	Grandes arquivos de dados podem ser divididos em vários segmentos. Selecione o tamanho máximo do segmento que deseja reservar para criar a unidade de seeding efetuando uma das seguintes ações: • Selecione **Destino Inteiro** para reservar todo o espaço disponível no caminho fornecido na página Local da unidade de seeding para uso futuro. Por exemplo, se o local for `D:\work\archive`, todo o espaço disponível na unidade D: será reservado se necessário para copiar a unidade de seeding, mas ele não será reservado imediatamente depois de iniciar o processo de cópia. • Selecione a caixa de texto, insira uma quantidade e depois selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar. O padrão é 250MB.
Reciclar ação	Caso o caminho já tenha uma unidade de seeding, selecione uma das seguintes opções: • **Não reutilizar**. Não substituir ou apagar quaisquer dados de propagação existentes no local. Se o local não estiver vazio, a gravação da unidade de seeding falhará. • **Substituir esse Core**. Substitui quaisquer dados de propagação preexistentes pertencentes a este core, porém deixando os dados de outros cores intactos. • **Apagar completamente**. Apaga todos os dados do diretório antes de gravar a unidade de seeding.
Comentários	Insira um comentário descrevendo a unidade de seeding.
Adicionar todos os agentes à unidade de seeding	Selecione essa opção para replicar todas as máquinas protegidas no Core de origem usando a unidade de propagação. Essa opção é selecionada por padrão.
Construir cadeias de pontos de recuperação (corrigir órfãos)	Selecione esta opção para replicar toda a cadeia do ponto de recuperação na unidade de seeding. Esta opção acrescenta alguns pontos de recuperação já replicados à unidade de seeding, impedindo que ocorram órfãos. Essa opção é selecionada por padrão. **NOTE:** A propagação típica no AppAssure 5.4 replica apenas o último ponto de recuperação na unidade de propagação, o que reduz a quantidade de tempo e espaço necessária para a criação da unidade de propagação. A opção de criar cadeias de ponto de recuperação na unidade de propagação exige espaço suficiente na unidade para armazenar os últimos pontos de recuperação das máquinas protegidas especificadas e pode aumentar o tempo necessário para concluir a tarefa.

g. Execute um dos seguintes:

- Se você tiver desmarcado a caixa de seleção **Adicionar todos os agentes à unidade de seeding**, clique em **Avançar**.
- Se você selecionou **Adicionar todos os agentes à unidade de seeding**, vá para a Etapa 10.

10. Clique em **Concluir**.
11. Caso você tenha criado uma unidade de seeding, envie-a para o Core de destino.

    O emparelhamento do Core de origem com o de destino está concluído.

A menos que você tenha selecionado a opção para pausar inicialmente a replicação, o processo de replicação começa imediatamente.

1. Se você selecionou a opção para usar uma unidade de seeding, a replicação produz pontos de recuperação órfãos no Core de destino até que a unidade de seeding seja consumida e forneça as imagens de base necessárias.
2. Se você especificou o uso do uma unidade, transfira o arquivo da unidade de seeding para um volume (pasta compartilhada, disco virtual ou unidades de armazenamento removíveis). Em seguida, consumir a unidade de seeding.

See also: Adicionar uma conta de nuvem
See also: Criar um repositório de DVM
See also: Replicação com Rapid Recovery
See also: Determinar suas necessidades e sua estratégia de seeding
See also: Replicação

Replicar para um Core de destino de terceiros

Um Core de terceiros é um Core de destino gerenciado e mantido por um MSP. Replicar em um Core gerenciado por terceiros não exige que o cliente tenha acesso ao Core de destino.

O processo de replicação em um Core de terceiros envolve tarefas que devem ser executadas pelo cliente, bem como por terceiros. Depois de o cliente enviar uma solicitação de replicação no(s) Core(s) de origem, o MSP deve concluir a configuração do Core de destino, revisando a solicitação.

NOTE: Essa configuração se aplica a replicação hospedada e na nuvem. O Rapid Recovery Core deve ser instalado em todas as máquinas do Core de origem. Se estiver configurando o Rapid Recovery para a replicação Multiponto a ponto, você precisará realizar essa tarefa em todos os Cores de origem.

Para replicar em um Core de destino gerenciado por terceiros, execute as seguintes tarefas:

- Enviar uma solicitação de replicação para um provedor de serviços terceirizado
- Revisar uma solicitação de replicação de um cliente
- Ignorar uma solicitação de replicação de um cliente

Enviar uma solicitação de replicação para um provedor de serviços terceirizado

Se você for um usuário final que assina um core gerenciado por terceiros, como um MSP, execute as etapas deste procedimento para enviar uma solicitação de replicação ao seu provedor de serviços de terceiros.

1. Navegar para o Rapid Recovery Core.
2. Na barra de botões do ícone, clique em **Replicate** (Replicar).

   O **Assistente de replicação** será exibido.
3. Na página **Core de destino** do Assistente de replicação, selecione **Eu possuo uma assinatura com um terceiro que oferece cópia de segurança em outro local e serviços de recuperação de desastres** e, em seguida, insira as informações conforme descrito na tabela a seguir.

Tabela 97. Informações sobre o Core de destino de terceiros

Caixa de texto	Descrição
Nome do host	Insira o nome de host, endereço IP ou FQDN da máquina de core de terceiros.
Porta	Insira o número da porta lhe foi fornecido pelo seu provedor de serviços de terceiros. O número de porta padrão é 8006.

- Se o Core que você deseja adicionar foi emparelhado com este core de origem anteriormente, você pode fazer o seguinte:
  1. Selecione **Usar um core de destino existente**.
  2. Selecione o core de destino na lista suspensa.
  3. Clique em **Avançar**.
  4. Pule para a Etapa 7.

4. Clique em **Avançar**.
5. Na página **Solicitação** do Assistente de replicação, insira as informações conforme descrito na tabela a seguir.

Tabela 98. Detalhes do Core de destino de terceiros

Caixa de texto	Descrição
Endereço de e-mail	Insira o endereço de e-mail associado à sua assinatura de serviço de terceiros.
ID do cliente (opcional)	Como opção, insira o ID do cliente que foi atribuído a você pelo provedor de serviços.

6. Clique em **Avançar**.
7. Na página **Máquinas protegidas** do Assistente de replicação, selecione as máquinas protegidas que deseja replicar no Core de terceiros.
8. Se desejar realizar o processo de propagação para a transferência dos dados de base, execute as seguintes etapas.

NOTE: Como grandes quantidades de dados precisam ser copiadas para o dispositivo de armazenamento portátil, recomenda-se o uso de uma conexão eSATA, USB 3.0 ou outra de alta velocidade com o dispositivo.

   a. Na página **Máquinas protegidas** do Assistente de replicação, selecione **Usar uma unidade de seeding para realizar a transferência inicial**.

   - Se já tiver uma ou mais máquinas protegidas replicando para um Core de destino, você poderá incluí-las na unidade de propagação selecionando a opção **Incluir os pontos de recuperação já replicados na unidade de seeding**.

   b. Clique em **Avançar**.
   c. Na página **Local da unidade de seeding** do Assistente de replicação, use a lista suspensa do tipo de **Local** para selecionar entre os seguintes tipos de destino:

   - Local
   - Rede
   - Nuvem

   d. Digite os detalhes para o arquivamento conforme descrito na tabela a seguir com base no tipo de local selecionado na Etapa c.

Tabela 99. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Usado para definir o caminho do local onde você deseja que o arquivo da unidade de seeding resida, por exemplo, `D:\work\archive`.
Rede	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, `\\servername\sharename`.
	Nome de usuário	Insira um nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTE:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é Rapid-Recovery-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

e. Clique em **Avançar**.

f. Na página **Opções da unidade de seeding** do Assistente de replicação, insira as informações conforme descrito na tabela a seguir.

Tabela 100. Opções da unidade de propagação

Item	Descrição
Tamanho máximo	Grandes arquivos de dados podem ser divididos em vários segmentos. Selecione a quantidade máxima de espaço que você deseja reservar para criar a unidade de seeding efetuando uma das seguintes ações: • Selecione **Destino inteiro** para reservar todo o espaço disponível no caminho fornecido na página Local da unidade de seeding (por exemplo, se o local for D: \work\archive, todo o espaço disponível na unidade D: será reservado). • Selecione a caixa de texto em branco, insira uma quantidade e depois selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar.

Item	Descrição
Reciclar ação	Caso o caminho já tenha uma unidade de seeding, selecione uma das seguintes opções: • **Não reutilizar**. Não substituir ou apagar quaisquer dados de propagação existentes no local. Se o local não estiver vazio, a gravação da unidade de seeding falhará. • **Substituir esse Core**. Substitui quaisquer dados de propagação preexistentes pertencentes a este core, porém deixando os dados de outros cores intactos. • **Apagar completamente**. Apaga todos os dados do diretório antes de gravar a unidade de seeding.
Comentários	Insira um comentário descrevendo a unidade de seeding.
Adicionar todos os agentes à unidade de seeding	Selecione essa opção para replicar todas as máquinas protegidas no Core de origem usando a unidade de propagação. Essa opção é selecionada por padrão.
Criar cadeias de pontos de recuperação (corrigir órfãos)	Selecione esta opção para replicar toda a cadeia do ponto de recuperação na unidade de seeding. Essa opção é selecionada por padrão. **NOTE:** A propagação típica no AppAssure 5.4 replica apenas o último ponto de recuperação na unidade de propagação, o que reduz a quantidade de tempo e espaço necessária para a criação da unidade de propagação. A opção de criar cadeias de ponto de recuperação (RP) na unidade de propagação exige espaço suficiente na unidade para armazenar os últimos pontos de recuperação das máquinas protegidas especificadas e pode aumentar o tempo necessário para concluir a tarefa.

g. Execute um dos seguintes:

- Se você tiver desmarcado a caixa de seleção **Adicionar todos os agentes à unidade de seeding**, clique em **Avançar**.
- Se você selecionou **Adicionar todos os agentes à unidade de seeding**, vá para a Etapa 9.

h. Na página **Máquinas** do Assistente de replicação, selecione as máquinas protegidas que você deseja replicar no Core de destino usando a unidade de propagação.

9. Clique em **Concluir**.
10. Se tiver criado uma unidade de seeding, envie-a conforme indicado pelo seu provedor de serviços de terceiros.

Revisar uma solicitação de replicação de um cliente

Depois que um usuário final concluir o procedimento Enviar uma solicitação de replicação para um provedor de serviços terceirizado, uma solicitação de replicação será enviada do core de origem para o core de destino de terceiros. Como terceiro, você pode revisar a solicitação e aprová-la para começar a replicação para seu cliente, ou pode negá-la para impedir que a replicação ocorra.

Escolha entre as opções a seguir:

- Aprovar uma solicitação de replicação
- Negar uma solicitação de replicação

Aprovar uma solicitação de replicação

Execute o procedimento a seguir para aprovar uma solicitação de replicação em um core de destino de terceiros.

1. No Core de destino, navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Replicação).

   A página **Replicação** é exibida.
3. Na página **Replicação**, clique em **Solicitar (#)**.

   A seção **Pending Replication Requests** (Solicitações de replicação pendentes) é mostrada.
4. Em Solicitações de replicação pendentes, clique no menu suspenso ao lado da solicitação que deseja revisar e depois clique em **Revisar**.

   A janela **Revisar solicitações de replicação** é exibida.

   NOTE: As informações que aparecem na seção Identidade do core de origem dessa janela são determinadas pela solicitação executada pelo cliente.
5. Em Identidade do core de origem, realize um dos procedimentos a seguir:
   - Selecione **Replace an existing replicated Core** (Substituir um núcleo replicado existente) e, em seguida, selecione um núcleo na lista suspensa.
   - Selecione **Criar um novo Core de origem** e confirme se o Nome do Core, Endereço de e-mail do cliente e ID do cliente fornecidos estão corretos. Edite as informações conforme necessário.
6. Em Agentes, selecione as máquinas às quais se aplica a aprovação e use as listas suspensas na coluna Repositório para selecionar o repositório apropriado a cada máquina.
7. Como opção, na caixa de texto **Comentários** insira uma descrição ou mensagem para ser incluída na resposta ao cliente.
8. Clique em **Enviar resposta**.

   A replicação é aceita.

Negar uma solicitação de replicação

Execute as etapas do procedimento a seguir para negar uma solicitação de replicação enviada a um core de terceiros a partir de um cliente.

Para negar uma solicitação sem revisá-la, consulte Ignorar uma solicitação de replicação de um cliente.

1. No Core de destino, navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Replicação).

   A página **Replicação** é exibida.
3. Na página **Replicação**, clique em **Solicitar (#)**.

   A seção **Pending Replication Requests** (Solicitações de replicação pendentes) é mostrada.
4. Em Solicitações de replicação pendentes, clique no menu suspenso ao lado da solicitação que deseja revisar e depois clique em **Revisar**.

   A janela **Revisar solicitações de replicação** é exibida.
5. Clique em **Negar**.

   A replicação é negada. A notificação de negação é exibida sob Alertas na página Eventos do Core de origem.

Ignorar uma solicitação de replicação de um cliente

Como prestador de serviço de terceiros de um core de destino, você tem a opção de ignorar uma solicitação de replicação enviada por um cliente. Essa opção pode ser usada se a solicitação tiver sido enviada por engano ou se você quiser negar uma solicitação sem revisá-la.

Para obter mais informações sobre solicitações de replicação, consulte Revisar uma solicitação de replicação de um cliente.

Execute o procedimento a seguir para ignorar uma solicitação de replicação de um cliente.

1. No Core de destino, navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em  (Replicação).

   A página **Replicação** é exibida.
3. Na página **Replicação**, clique em **Solicitar (#)**.

   A seção **Pending Replication Requests** (Solicitações de replicação pendentes) é mostrada.
4. Em Solicitações de replicação pendentes, clique no menu suspenso ao lado da solicitação que deseja ignorar e depois clique em **Ignorar**.
5. Na caixa de diálogo **Ignorando solicitação**, clique em **Sim** para confirmar o comando.

   Uma notificação de que a solicitação foi ignorada é enviada ao Core de origem, e a solicitação é removida da página Replicação no Core de destino.

Adicionar uma máquina a uma replicação existente

Após o estabelecimento da replicação entre um Core de origem e um de destino, é possível adicionar novas máquinas protegidas para replicação no destino. Conclua as etapas do procedimento a seguir no Core de origem para adicionar uma nova máquina protegida a um Core de destino pareado para replicação.

Para obter mais informações sobre a replicação, consulte Replicação e Replicar para um Core de destino autogerenciado.

1. Navegue até o Console do Rapid Recovery Core do Core de origem.
2. Na barra de botões, clique em **Replicar**.

   O Assistente de replicação é aberto na página **Máquinas protegidas**.
3. Na página **Máquinas protegidas**, selecione as máquinas protegidas que deseja replicar e use as listas suspensas na coluna Repositório para selecionar um repositório para cada máquina protegida.
4. Se desejar realizar o processo de propagação para a transferência dos dados de base, execute as seguintes etapas:

   NOTE: Como grandes quantidades de dados precisam ser copiadas para o dispositivo de armazenamento portátil, recomenda-se o uso de uma conexão eSATA, USB 3.0 ou outra de alta velocidade com o dispositivo.

a. Na página **Máquinas protegidas** do Assistente de replicação, selecione **Usar uma unidade de seeding para realizar a transferência inicial**.

- Se já tiver uma ou mais máquinas protegidas replicando para um Core de destino, você poderá incluí-las na unidade de seeding selecionando a opção **Incluir os pontos de recuperação já replicados na unidade de propagação**.

b. Clique em **Avançar**.

c. Na página **Local da unidade de seeding** do assistente, use a lista suspensa do tipo de **Local** para selecionar entre os seguintes tipos de destino:

- Local
- Rede
- Nuvem

d. Digite os detalhes para o arquivamento conforme descrito na tabela a seguir com base no tipo de local selecionado na Etapa c.

Tabela 101. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, d:\work\archive.
Rede	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, \ \servername\sharename.
	Nome de usuário	Insira um nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTE:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é Rapid-Recovery-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

e. Clique em **Avançar**.

f. Na página **Opções da unidade de seeding** do assistente, insira as informações conforme descrito na tabela a seguir.

Tabela 102. Opções da unidade de propagação

Item	Descrição
Tamanho máximo	Grandes arquivos de dados podem ser divididos em vários segmentos. Selecione a quantidade máxima de espaço que você deseja reservar para criar a unidade de seeding efetuando uma das seguintes ações: • Selecione **Destino inteiro** para reservar todo o espaço disponível no caminho fornecido na página Local da unidade de seeding (por exemplo, se o local for D:\work\archive, todo o espaço disponível na unidade D: será reservado). • Selecione a caixa de texto em branco, insira uma quantidade e depois selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar.
Reciclar ação	Caso o caminho já tenha uma unidade de seeding, selecione uma das seguintes opções: • Não reutilizar. Não substituir ou apagar quaisquer dados de propagação existentes no local. Se o local não estiver vazio, a gravação da unidade de seeding falhará. • Substituir este Core. Substitui quaisquer dados de propagação preexistentes pertencentes a este core, porém deixando os dados de outros cores intactos. • Apagar completamente. Apaga todos os dados do diretório antes de gravar a unidade de seeding.
Comentários	Insira um comentário descrevendo a unidade de seeding.
Adicionar todos os agentes à unidade de seeding	Selecione essa opção para replicar todas as máquinas protegidas no Core de origem usando a unidade de propagação. Essa opção é selecionada por padrão.
Construir cadeias de pontos de recuperação (corrigir órfãos)	Selecione esta opção para replicar toda a cadeia do ponto de recuperação na unidade de seeding. Essa opção é selecionada por padrão. **NOTE:** A propagação típica no Rapid Recovery 5.4 replica apenas o último ponto de recuperação na unidade de seeding, o que reduz a quantidade de tempo e espaço necessária para a criação da unidade de seeding. A opção de criar cadeias de ponto de recuperação (RP) na unidade de propagação exige espaço suficiente na unidade para armazenar os últimos pontos de recuperação das máquinas protegidas especificadas e pode aumentar o tempo necessário para concluir a tarefa.

g. Execute um dos seguintes:

- Se você tiver desmarcado a caixa de seleção **Adicionar todos os agentes à unidade de seeding**, clique em **Avançar**.
- Se tiver selecionado **Adicionar todos os agentes à unidade de seeding**, vá para a Etapa 5.

h. Na página **Máquinas protegidas** do assistente, selecione as máquinas protegidas que você deseja replicar no Core de destino usando a unidade de seeding.

5. Clique em **Concluir**.

Consumo da unidade de propagação em um Core de destino

Execute o procedimento a seguir para consumir os dados do arquivo da unidade de propagação no Core de destino.

NOTE: Esse procedimento será necessário apenas se um arquivo da unidade de propagação tiver sido criado como parte de Replicar para um Core de destino autogerenciado ou Replicar para um Core de destino de terceiros.

1. Se a unidade de propagação tiver sido salva em um dispositivo de armazenamento portátil, como uma unidade USB, conecte a unidade ao Core de destino.
2. No Core de destino, abra o Rapid Recovery Core Console e, na barra de ícones, clique em (Replicação).

   A página **Replicação** é exibida.
3. Na página **Replicação**, em Replicação de entrada, clique no menu suspenso do Core de origem correto e selecione **Consumir**.

   A caixa de diálogo **Consumir** é exibida.
4. No campo **Tipo de local**, selecione uma das seguintes opções a partir da lista suspensa:
   - Local
   - Rede
   - Nuvem
5. Insira os detalhes do arquivo para arquivamento da unidade de propagação, como descrito na tabela, com base no tipo de local selecionado na Etapa 4.

Tabela 103. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Local	Local	Insira o caminho para o arquivo.
Rede	Local	Insira o caminho para o arquivo.
	Nome de usuário	Insira o nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira a senha para o caminho da rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTE:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.

Opção	Caixa de texto	Descrição
	Nome da pasta	Insira o nome da pasta na qual os dados arquivos estão salvos; por exemplo Rapid-Recovery-Arquivo-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

6. Clique em **Verificar arquivo**.

   O Core procura o arquivo.

   Depois de encontrar o arquivo, as seguintes caixas de texto serão exibidas na janela Consumir, pré-preenchidas com os dados coletados na Etapa 4, Etapa 5 e no arquivo. O Período exibe as datas dos pontos de recuperação mais antigos e mais novos contidos na unidade de seeding. Qualquer comentário inserido quando a unidade de seeding foi criada é importado automaticamente.

7. Na caixa de diálogo **Consumir**, em Agentes, selecione as máquinas em relação às quais você deseja consumir os dados.
8. Clique em **Consumir**.
9. Para monitorar o progresso do consumo de dados, clique na página Eventos.

Abandonar uma unidade de propagação

Se você for criar uma unidade de seeding com o intuito de consumi-la no Core de destino, mas posteriormente optar por não consumi-la, você pode abandonar a unidade de seeding.

Até que você abandone a unidade de seeding ou a consuma, um link para a unidade de seeding pendente permanecerá no painel de Replicação de saída no Core de origem.

Até que você transmita informações da unidade de seeding, os pontos de recuperação órfãos (que existem na máquina original protegida, mas não no Core de destino) não podem ser usados para restaurar dados.

CAUTION: Se você abandonar a unidade de seeding, os pontos originais de recuperação (definidos no arquivo da unidade de seeding) serão transmitidos pela rede para o Core de destino durante o próximo trabalho de replicação. A transmissão de antigos pontos de recuperação pela rede poderá reduzir consideravelmente a velocidade da rede, especialmente se houver muitos pontos de recuperação.

Execute as etapas do procedimento a seguir para abandonar uma unidade de seeding pendente.

NOTE: Abandonar a unidade de seeding no Console do Core não afeta o arquivo da unidade de seeding em seu local de armazenamento.

1. No Core de origem, abra o Rapid Recovery Core Console e, na barra de ícones, clique em (Replicação).

   A página **Replicação** é exibida.
2. Na página **Replicação**, no painel Replicação de saída, clique em **Unidades de seeding (#)**.

   No painel Replicação de saída, uma seção será exibida contendo informações sobre as unidades de seeding pendentes.
3. Opcionalmente, clique na seta para expandir o menu minimizado.

   As informações sobre as unidade de seeding pendentes, incluindo o Core de destino e o período dos pontos de recuperação incluídos na unidade de seeding.
4. Para o arquivo da unidade de propagação que você deseja abandonar, clique em (Mais opções) e selecione **Abandon** (Abandonar).
5. Na janela de confirmação, confirme que você quer abandonar a unidade de seeding.

   A unidade de seeding é removida.

Se não houver mais unidades de seeding no Core de origem, o link Unidades de seeding (#) e a seção Unidades de seeding pendentes serão removidos do painel Replicação de saída.

Gerenciar definições de replicação

O Rapid Recovery permite monitorar, programar e ajustar a replicação nos níveis global, de Core e de máquina protegida.

É possível editar as seguintes definições de replicação:

- Para programar trabalhos de replicação, consulte Programar a replicação.
- Para criar uma unidade de propagação de uma máquina protegida que já está pareada para replicação, consulte Usar a função Copiar para criar uma unidade de propagação
- Para monitorar o progresso de um trabalho de replicação, consulte Ver a replicação de entrada e saída.
- Para pausar ou retomar um trabalho de replicação em pausa, consulte Pausar e retomar a replicação.
- Para forçar a replicação de uma máquina protegida de entrada ou saída, consulte Forçar a replicação.
- Para gerenciar as definições de todos os cores de destino e procedimentos de replicação, consulte Gerenciar definições para replicação de saída.
- Para gerenciar as definições de um core de destino individual, consulte Alterar configurações de Core de destino.
- Para gerenciar as definições de prioridade de uma máquina protegida individual que está sendo replicada para um Core de destino, consulte Definir a prioridade de replicação de uma máquina protegida.

Programar a replicação

A menos que você altere o comportamento padrão ao definir um programa de replicação, o Core iniciará o trabalho de replicação imediatamente após conclusão de cada snapshot de backup, verificação de soma de verificação, verificação de capacidade de anexação e trabalhos noturnos

Você pode alterar o programa da replicação para reduzir a carga da rede.

Conclua as etapas do procedimento a seguir para definir um programa de replicação para qualquer máquina replicada.

1. No Core de destino, abra o Rapid Recovery Core Console e, na barra de ícones, clique em (Replicação).

   A página **Replicação** é exibida.

2. No painel Replicação de saída, no Core para o qual você deseja programar a replicação, clique em (Mais opções) e selecione **Programar**.

   A caixa de diálogo **Programa de replicação para [NomeCore]** é aberta.

3. Selecione uma das três opções a seguir:

   - **A todo o momento**. Replica após cada novo snapshot, verificação de soma de verificação e verificação de capacidade de anexação, e depois da conclusão de trabalhos noturnos.
   - **Diário (Iniciar replicação somente durante o período de tempo especificado)**. Começa a replicar apenas dentro do intervalo de tempo fornecido.

     1. Na caixa de texto **De**, digite o primeiro horário em que a replicação deve começar.
     2. Na caixa de texto **A**, digite o último horário em que a replicação deve começar.

NOTE: Se a replicação estiver em andamento quando terminar o tempo programado, o trabalho de replicação é concluído depois do período de tempo alocado.

- **Personalizado**. Começa replicar somente dentro do período fornecido, permitindo definir um período para os dias da semana e outro para os fins de semana.

  1. Ao lado de Dias da semana, na caixa de texto **De**, insira o primeiro horário em que a replicação deve ocorrer em um dia da semana. Depois, na caixa de texto **A**, insira o último horário em que a replicação deve ocorrer em um dia da semana.
  2. Ao lado de Fins de semana, na caixa de texto **De**, insira o primeiro horário em que a replicação deve ocorrer em fins de semana. Depois, na caixa de texto **A**, insira o último horário em que a replicação deve ocorrer em fins de semana.

4. Clique em **Salvar**.

   O programa é aplicado a todas as replicações do Core de destino selecionado.

Usar a função Copiar para criar uma unidade de propagação

Caso tenha optado por não criar uma unidade de propagação ao configurar a replicação, você pode criar uma unidade de propagação usando a função Copiar no menu suspenso da máquina protegida.

1. No Core de origem, abra o Rapid Recovery Core Console e, na barra de ícones, clique em (Replicação).

   A página **Replicação** é exibida.

2. Na página **Replicação**, no painel Replicação de saída, clique em para expandir o Core que protege a máquina para a qual você deseja criar uma unidade de propagação.

   A seleção expande-se para mostrar cada máquina protegida no Core especificado.

3. Clique na primeira linha da tabela para selecionar cada máquina para a qual deseja criar uma unidade de seeding.
4. No menu sob o painel Replicação de Saída, clique em **Copiar**.

   O **Assistente de replicação** é exibido.

5. Na página **Local da unidade de seeding** do assistente, use a lista suspensa **Local** para selecionar entre os seguintes tipos de destino:

   - Local
   - Rede
   - Nuvem

6. Digite os detalhes do arquivo da unidade de seeding conforme descrito na tabela a seguir, com base no tipo de local selecionado na etapa prévia.

Tabela 104. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, d:\work \archive.
Rede	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, \ \servername\sharename.

Opção	Caixa de texto	Descrição
	Nome de usuário	Insira um nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTE:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é Rapid-Recovery-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

7. Clique em **Avançar**.
8. Na página Opções da unidade de seeding, insira as informações conforme descrito na tabela a seguir.

Tabela 105. Opções da unidade de propagação

Item	Descrição
Tamanho máximo	Grandes arquivos de dados podem ser divididos em vários segmentos. Selecione a quantidade máxima de espaço que você deseja reservar para criar a unidade de seeding efetuando uma das seguintes ações: • Selecione **Destino inteiro** para reservar todo o espaço disponível no caminho fornecido na página Local da unidade de seeding (por exemplo, se o local for D:\work\archive, todo o espaço disponível na unidade D: será reservado). • Selecione a caixa de texto em branco, insira uma quantidade e depois selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar.
Reciclar ação	Caso o caminho já tenha uma unidade de seeding, selecione uma das seguintes opções: • **Não reutilizar.** Não substituir ou apagar quaisquer dados de propagação existentes no local. Se o local não estiver vazio, a gravação da unidade de seeding falhará. • **Substituir esse Core**. Substitui quaisquer dados de propagação preexistentes pertencentes a este core, porém deixando os dados de outros cores intactos. • **Apagar completamente**. Apaga todos os dados do diretório antes de gravar a unidade de seeding.
Comentários	Insira um comentário descrevendo a unidade de seeding.
Adicionar todos os agentes à unidade de seeding	Selecione essa opção para replicar todas as máquinas protegidas no Core de origem usando a unidade de propagação. Essa opção é selecionada por padrão.

Item	Descrição
Construir cadeias de pontos de recuperação (corrigir órfãos)	Selecione esta opção para replicar toda a cadeia do ponto de recuperação na unidade de seeding. Essa opção é selecionada por padrão. **NOTE:** O seeding típico no Rapid Recovery 5.4.x replicava somente o último ponto de recuperação para a unidade de seeding, o que reduzia o tempo e a quantidade de espaço necessários para criar a unidade de seeding. A opção de criar cadeias de ponto de recuperação na unidade de seeding exige espaço suficiente na unidade para armazenar os últimos pontos de recuperação das máquinas protegidas especificadas e pode aumentar o tempo necessário para concluir a tarefa.

9. Execute um dos seguintes:
   - Se você tiver desmarcado a caixa de seleção **Adicionar todos os agentes à unidade de seeding**, clique em **Avançar**.
   - Se você selecionou **Adicionar todos os agentes à unidade de seeding**, vá para a Etapa 10.
10. Na página **Máquinas protegidas** do assistente, selecione as máquinas protegidas para as quais deseja criar uma unidade de seeding.
11. Clique em **Concluir**.

Monitorar a replicação

Quando a replicação estiver configurada, você poderá monitorar o status das tarefas de replicação para os Cores de origem e destino. É possível atualizar as informações de status, visualizar detalhes de replicação, e muito mais.

1. No Core de origem, abra o Rapid Recovery Core Console e, na barra de ícones, clique em (Replicação).

   A página **Replicação** é exibida.
2. Nessa página, você pode ver informações e monitorar o status das tarefas de replicação conforme descrito na seguinte tabela.

Tabela 106. Tarefas de replicação

Seção	Descrição	Ações disponíveis
Unidades de propagação (#)	Depois de especificar o uso de uma unidades de propagação ao definir a replicação, um link de **Unidades de propagação (#)** será exibido no painel de Replicação de saída no Core de origem até você abandonar ou consumir a unidade. O número exibido indica quantas unidades de propagação estão pendentes. **NOTE:** Esse link não será exibido a menos que uma unidade de propagação esteja pendente. Clique nesse link para listar as unidades de propagação que foram gravadas, mas que ainda não consumidas pelo Core de destino. Ainda, expanda o menu que pode ser minimizado para exibir informações sobre unidades de	Na tarefa suspensa, clique em **Abandonar** para abandonar ou cancelar o processo de propagação.

Seção	Descrição	Ações disponíveis
	propagação pendentes, incluindo o Core de destino e a faixa de data dos pontos de recuperação incluídos na unidade de propagação.	
Replicação de saída	Lista todos os Cores de destino em relação aos quais o Core de origem está replicando. Inclui um indicador de estado, o nome do Core de destino, o número de máquinas sendo replicadas e o progresso de uma transmissão de replicação.	Em um Core de origem, no menu suspenso ... (Mais), você pode selecionar as seguintes opções: • **Detalhes.**Lista ID, URL, nome de exibição, estado, ID do cliente, endereço de e-mail e comentários do Core replicado. • **Alterar definições.** Lista o nome de exibição e permite editar o host e a porta do Core de destino. • **Programar.** Permite definir um programa personalizado para replicação nesse Core de destino. • **Adicionar máquinas.** Permite selecionar um host em uma lista suspensa, selecionar máquinas protegidas para replicação e criar uma unidade de propagação para a transferência inicial da nova máquina protegida. Opcionalmente, você pode incluir pontos de recuperação para máquinas já adicionada à replicação. • **Excluir.** Permite excluir a relação de replicação entre os Cores de origem e destino. Isso anulará toda a replicação nesse Core.
Replicação de entrada	Relaciona todas as máquinas de origem a partir das quais o destino recebe os dados replicados. Inclui o nome do Core remoto, estado, máquinas e progresso. Lista todos os Cores de origem partir dos quais o destino recebe os dados replicados. O nome de exibição dos Cores de origem listados é preenchido a partir do valor no Assistente de replicação ao definir a replicação. Inclui um indicador de estado, o nome do Core remoto e o progresso de uma transmissão de replicação.	Em um Core de destino, no menu suspenso ... (Mais), você pode selecionar as seguintes opções: • **Detalhes.** Lista o ID, nome de host, ID do cliente, endereço de e-mail e comentário do Core replicado. • **Consumir.** Consome os dados iniciais da unidade de seeding e os salva no repositório local. • **Excluir.** Permite excluir a relação de replicação entre os Cores de origem e destino. Isso anulará toda a replicação a partir desse Core.
Solicitações de replicação pendentes	Essas informações são aplicadas somente a provedores de serviços gerenciados. Quando um cliente clica no	No menu suspenso, clique em **Ignorar** para ignorar ou rejeitar a solicitação ou

Seção	Descrição	Ações disponíveis
	link **Solicitações** no painel de Replicação de entrada, uma seção de tabela de resumo é exibida, listando o ID do cliente, endereço de e-mail e nome de host da solicitação.	em **Revisar** para revisar a solicitação pendente.

Pausar e retomar a replicação

É possível pausar a replicação temporariamente para os Cores de origem (saída) ou de destino (entrada).

A opção para pausar a replicação só está disponível quando a replicação estiver ativa. A opção para retomar a replicação só está disponível se a replicação estiver pausado.

Execute as etapas do procedimento a seguir para pausar ou retomar a replicação.

1. Abra o Rapid Recovery Core Console e, na barra de ícones, clique em (Replicação).

   A página **Replicação** é exibida.
2. Para pausar a replicação para todas as máquinas replicadas, faça o seguinte:
   a. Clique na caixa de seleção na parte superior da tabela de resumo para selecionar o Core de origem ou de destino.
   b. Clique em **Pausar** no menu anterior ao da tabela de resumo.

   A replicação para todas as máquinas protegidas no Core selecionado será pausada.
3. Para pausar a replicação apenas para determinadas máquinas, faça o seguinte:
   a. Clique na seta à direita de qualquer Core.

   A vista expande-se para mostrar cada uma das máquinas protegidas do Core selecionado que estão sendo replicadas.
   b. Clique na primeira coluna para selecionar cada máquina para a qual você quer pausar a replicação. Clique em qualquer seleção novamente para limpar a caixa de seleção para as máquinas que você não quer pausar.
   c. Clique em **Pausar** no menu anterior ao da tabela de resumo.

   A replicação para as máquinas protegidas selecionadas será pausada.
4. Para retomar a replicação para todas as máquinas replicadas, faça o seguinte:
   a. Clique na caixa de seleção na parte superior da tabela de resumo para selecionar o Core de origem ou de destino.
   b. Clique em **Retomar** no menu na parte superior da tabela de resumo.

   A replicação para todas as máquinas protegidas no Core selecionado será retomada.
5. Para retomar a replicação apenas para determinadas máquinas, faça o seguinte:
   a. Clique na seta à direita de qualquer Core.

   A vista expande-se para mostrar cada uma das máquinas protegidas do Core selecionado que estão sendo replicadas.
   b. Clique na primeira coluna para selecionar cada máquina para a qual você quer retomar a replicação. Clique em qualquer seleção novamente para limpar a caixa de seleção para as máquinas que você não quer retomar.
   c. Clique em **Retomar** no menu na parte superior da tabela de resumo.

   A replicação para as máquinas protegidas selecionadas será retomada.

Forçar a replicação

A partir do Core de origem, você pode forçar a replicação a qualquer momento, em vez de aguardar por um trabalho de replicação na fila após um evento específico, como um backup ou verificação de capacidade de anexação.

Execute as etapas do procedimento a seguir para forçar a replicação a partir do Core de origem ou de destino.

1. No Core de origem, abra o Rapid Recovery Core Console e, na barra de ícones, clique em (Replicação).

   A página **Replicação** é exibida.

2. Execute um dos seguintes:

   - Para forçar a replicação em um Core de origem, no painel **Outgoing Replication** (Replicação de saída), selecione um Core e no menu na parte superior da tabela de resumo, clique em **Force** (Forçar).
   - Para forçar a replicação em um Core de destino, no painel **Incoming Replication** (Replicação de entrada), selecione um Core e no menu na parte superior da tabela de resumo, clique em **Force** (Forçar).

   A caixa de diálogo Forçar replicação será exibida.

3. Opcionalmente, se você quiser reparar qualquer cadeia de pontos de recuperação definida como órfã, selecione **restaurar apenas cadeias de Ponto de recuperação órfãs**.
4. Para confirmar, na caixa de diálogo Forçar replicação, clique em **(Sim)**.

   A caixa de diálogo é fechada e a replicação é forçada.

Gerenciar definições para replicação de saída

As alterações feitas nessas definições afetam a transferência de dados para todos os Cores de destino associados a esse Core de origem.

1. No Core de origem, abra o Rapid Recovery Core Console e, na barra de ícones, clique em (Replicação).

   A página **Replicação** é exibida.

2. No painel **Replicação de saída**, na parte superior da tabela de resumo, clique em (Definições).

   A caixa de diálogo **Definições de replicação** é exibida.

3. Na caixa de diálogo **Definições de replicação**, edite as definições de replicação, como descrito na tabela a seguir.

Tabela 107. Definições de replicação

Opção	Descrição
Duração do cache (segundos)	Especificar a quantidade de tempo entre cada solicitação de status de Core de destino feita pelo Core de origem.
Tempo limite da sessão de imagem do volume (minutos)	Especificar a quantidade de tempo que o Core de origem gasta tentando transferir uma imagem de volume para o Core de destino.

Opção	Descrição
Máximo de fluxos paralelos	Especificar o número de conexões de rede com uso simultâneo permitido por uma única máquina protegida para replicar os dados dessa máquina.
Velocidade máxima de transferência (MB/s)	Especificar o limite de velocidade para a transferência de dados replicados.
Tamanho máximo de transferência de dados (GB)	Especifique o tamanho máximo em GB para transferência de blocos de dados replicados.
Restaurar padrão	Selecione essa opção para alterar todas as definições de replicação para o padrão do sistema. **NOTE:** Tome nota de quaisquer configurações personalizadas antes de selecionar essa opção. Você não será solicitado a confirmar essa ação

4. Quando estiver satisfeito, clique em **Salvar** para salvar as definições de replicação e fechar a caixa de diálogo.

Alterar configurações de Core de destino

Você pode alterar as configurações de host e porta para Cores de destino individuais a partir do Core de origem.

1. No Core de origem, abra o Rapid Recovery Core Console e, na barra de ícones, clique em (Replicação). .

   A página **Replicação** é exibida.

   No painel **Replicação de saída**, a tabela de resumo inclui uma linha para cada Core de destino que foi configurado para replicar os pontos de recuperação a partir desse Core de origem.

2. Clique no menu suspenso (Configurações) do Core de destino que você deseja modificar e selecione **Change Settings** (Alterar configurações).

   A caixa de diálogo **Configurações** é exibida.

3. Edite uma das opções descritas na tabela a seguir.

Tabela 108. Configurações de Core de destino

Opção	Descrição
Host	Insira o host do Core de destino.
Porta	Insira uma porta para que o Core de destino use para comunicação com o Core de origem. **NOTE:** A porta padrão é 8006.

4. Clique em **Salvar**.

Definir a prioridade de replicação de uma máquina protegida

A prioridade da replicação determina quais trabalhos de replicação serão enviados para o Core em primeiro lugar. A priorização é definida ordenadamente, em uma escala de 1 a 10 na qual 1 é a primeira prioridade e 10 é a última prioridade. Quando você estabelece a replicação pela primeira vez para qualquer máquina, a sua prioridade é definida como 5. Você pode visualizar e alterar a prioridade no nível da máquina protegida no Core de origem.

Em alguns casos, é possível que alguns trabalhos de replicação sejam abandonados. Por exemplo, os trabalhos de replicação podem ser abandonados se o seu ambiente estiver enfrentando altas taxas incomuns de alteração ou se a rede não tiver largura de banda suficiente. Essa situação é particularmente provável se você definir os programas que limitam as horas em que a replicação ocorre no seu ambiente. Para obter mais informações sobre como definir a replicação programada, consulte Programar a replicação.

Para garantir que a replicação ocorra primeiro para as máquinas importantes, defina a prioridade dos servidores críticos com um menor número (entre 1 e 5). Defina a prioridade das máquinas menos importantes com um número maior (entre 6 e 10).

A definição da prioridade da replicação como 4 para qualquer máquina protegida garante que o trabalho de replicação dessa máquina inicie antes de uma máquina com a prioridade de replicação padrão de 5. Os trabalhos de replicação das máquinas com prioridade 3 são colocados em fila antes do 4 e assim por diante. Quanto menor o número da prioridade, mais cedo os trabalhos de replicação serão enviados. É fácil lembrar que a prioridade 1 é a mais importante. As máquinas com prioridade de replicação 1 são as primeiras a entrarem na fila para a replicação.

Conclua as etapas a seguir para editar as definições que priorizam a replicação de uma máquina protegida.

1. No Core de origem, abra o Rapid Recovery Core Console e, na barra de ícones, clique em (Replicação).

   A página **Replicação** é exibida.

2. No painel **Replicação de saída**, clique na seta à direita de qualquer Core de origem.

   A visualização expande para mostrar cada uma das máquinas protegidas desse Core de origem que estão sendo replicadas para o Core de destino designado.

3. Clique no menu suspenso (Mais) da máquina protegida que você deseja priorizar e clique em **Change Settings** (Alterar configurações).

   Uma caixa de diálogo será exibida.

4. Clique na lista suspensa **Prioridade** e selecione uma prioridade, de **1 (Mais alta)** a **10 (Mais baixa)**, com base nos seus requisitos.
5. Clique em **Salvar**.

   A caixa de diálogo é fechada e a prioridade da replicação para a máquina selecionada atualiza.

Remover replicação de saída do Core de origem

Conclua as etapas deste procedimento para remover uma ou mais máquinas protegidas da replicação no Core de origem.

1. No Core de origem, abra o Rapid Recovery Core Console e, na barra de ícones, clique em (Replicação).

A página **Replicação** é exibida.

No painel **Replicação de saída**, a tabela de resumo inclui uma linha para cada Core de destino que foi configurado para replicar os pontos de recuperação a partir desse Core de origem.

2. Opcionalmente, clique na seta à direita de qualquer Core de destino.

   A visualização expande para mostrar cada uma das máquinas protegidas desse Core de origem que estão sendo replicadas para o Core de destino designado.

3. Selecione as máquinas protegidas que deseja remover da replicação de saída como a seguir:

   - Para remover completamente a relação de replicação existente entre Core de origem e qualquer Core de destino, clique no menu suspenso (Mais) para qualquer Core de destino e selecione **Excluir**.
   - Para remover a replicação de saída para um subconjunto de máquinas no Core de destino especificado, expanda a visualização para exibir todas as máquinas sendo replicadas e marque a caixa de seleção de cada máquina replicada que deseja remover. Desmarque a caixa de seleção de qualquer máquina você deseja continuar replicando. Depois, no menu acima da tabela de resumo, clique em **Excluir**.

   Uma mensagem de confirmação será exibida, perguntando se você deseja remover as relações de replicação.

4. Na caixa de diálogo resultante, clique em **Sim** para confirmar a remoção.

Remover replicação de entrada do Core de destino

Conclua as etapas deste procedimento para remover uma ou mais máquinas protegidas da replicação no Core de destino.

NOTE: Você também pode remover a replicação de máquinas protegidas do painel de Replicação de saída na página Replicação do Core de origem. Para obter mais informações, consulte Remover replicação de saída do Core de origem

1. No Core de destino, abra o Rapid Recovery Core Console e, na barra de ícones, clique em (Replicação).

   A página **Replicação** é exibida. No painel de Replicação de entrada, a tabela de resumo inclui uma linha de cada Core de origem com máquinas protegidas que são replicadas por esse Core de destino.

2. Selecione as máquinas replicadas a serem removidas como a seguir:

   - Para excluir **todas** as máquinas replicadas do Core de origem para seu Core de destino, no painel Replicação de entrada, marque a caixa de seleção para esse Core.
   - Para excluir um subconjunto menor de máquinas do mesmo Core de origem, faça o seguinte:

     a. Clique na seta à direita do Core de origem.

   A visualização é expandida para exibir cada uma das máquinas do Core de origem selecionado que são replicadas em seu Core de destino.

     b. Marque a caixa de seleção de cada máquina replicada que deseja remover.

     c. Na linha principal do Core de origem selecionado, clique no menu suspenso (Mais) e selecione **Excluir**.

A caixa de diálogo **Remover replicação** é exibida.

3. Na caixa de diálogo **Remover replicação**, faça o seguinte:
   - Se desejar manter os pontos de recuperação replicados no Core de destino, remova a opção **Excluir pontos de recuperação existentes** .
   - Se desejar excluir todos os pontos de recuperação replicados dessa máquina, bem como remover o core de origem da replicação, selecione **Excluir pontos de recuperação existentes**.
4. Clique em **Sim** para confirmar a exclusão.

   WARNING: Se você selecionar essa opção, todos os pontos de recuperação nesse Core serão excluídos.

   As máquinas protegidas selecionadas no Core de origem são removidas da replicação nesse Core de destino. Opcionalmente, se você tiver selecionado a opção de excluir pontos de recuperação, eles serão removidos do repositório desse Core.

Recuperar dados replicados

A funcionalidade de replicação “Dia a dia” é mantida no Core de origem, enquanto apenas o Core de destino é capaz de executar as funções necessárias para a recuperação após desastres.

Para recuperação após desastres, o Core de destino pode usar os pontos de recuperação replicados para recuperar as máquinas protegidas. Você pode executar as seguintes opções de recuperação no Core de destino:

- **Montar pontos de recuperação**. Para obter mais informações, consulte Montar um ponto de recuperação.
- **Reverter para pontos de recuperação.** Para obter mais informações, consulte Sobre restauração de volumes a partir de um ponto de recuperação ou Restaurar volumes em uma máquina Linux usando a linha de comando.
- **Realizar uma exportação de máquina virtual (VM).** Para obter mais informações, consulte Exportação para máquinas virtuais usando o Rapid Recovery.
- **Realizar uma bare metal restore (BMR).** Para obter mais informações, consulte Realizar uma restauração sem sistema operacional para máquinas Windows.

Eventos

O Rapid Recovery Core inclui conjuntos predefinidos de eventos. Esses eventos podem ser usados para notificar os administradores de problemas críticos no Core ou sobre problemas com trabalhos relacionados a backups, exportação virtual, replicação e assim por diante.

Esta seção descreve como visualizar os eventos mostrados no Rapid Recovery Core Console. Você pode também aprender sobre os métodos de notificação de evento e a configuração, incluindo como configurar as notificações por e-mail. Por fim, você pode configurar as notificações para alterar por quanto tempo os logs de evento são mantidos e reduzir a notificação de eventos repetitivos.

Como exibir eventos usando tarefas, alertas e páginas de diário

No Core Console, você pode mostrar eventos do Core e ver eventos de uma máquina protegida ou replicada específica.

As páginas **Eventos** no Core Console exibem um registro de todos os eventos relacionados ao Rapid Recovery Core. Para acessar e exibir eventos do Core, clique em (Eventos).

As páginas **Eventos** de uma máquina replicada ou protegida específica exibem um log de eventos relacionados a essa máquina específica. Para acessar e mostrar eventos de uma máquina selecionada, clique no nome da máquina no menu Máquinas protegidas e, na página **Resumo** da máquina, clique no menu **Eventos**.

As páginas Eventos (no núcleo ou em uma determinada máquina) estão disponíveis em 3 visualizações: Tarefas, Alertas e Diário.Todos os itens mostrados em qualquer categoria são um evento. Essas visualizações permitem filtrar detalhes sobre diversos subconjuntos de eventos, conforme apropriado. A exibição padrão é mostrar as tarefas.

- Uma **tarefa** é um evento relacionado a um trabalho. Um **trabalho** é um processo que o Rapid Recovery Core precisa realizar. Cada trabalho tem um estado atual e uma hora e data de início e de término. Algumas tarefas são iniciadas manualmente ou programadas pelo usuário. Os exemplos incluem forçar um instantâneo, agendar um backup ou executar uma restauração a partir do ponto de recuperação. Outras tarefas são funções automáticas, como, por exemplo, executar trabalhos noturnos ou executar rollup usando a política de retenção padrão.
- Um **alerta** é um evento de prioridade, como um erro, uma advertência ou uma mensagem informativa importante. Se você solicitar notificações de qualquer evento específico, estas notificações serão mostradas no subconjunto Alertas.
- O **diário** mostra uma lista completa de todos os eventos registrados (para o Core ou para a máquina selecionada, conforme apropriado). Esta lista é mais abrangente, apresentando trabalhos, eventos de alta prioridade e eventos de prioridade mais baixa. Esta categoria inclui eventos passivos e não relacionados a um trabalho (como o Core iniciando com sucesso ou reportando o status do portal de licenças).

Conclua as etapas nos procedimentos a seguir para exibir tarefas, alertas ou todos os registros de todos os eventos:

- Visualizar tarefas
- Visualizar alertas
- Ver um diário de todos os eventos registrados
- Ver as tarefas em execução de qualquer página do Core Console
- Navegar entre tarefas, alertas e diário de eventos

Visualizar tarefas

Uma tarefa é um trabalho que o Rapid Recovery Core deve realizar, como transferir dados em uma cópia de segurança programada regular ou executar uma restauração a partir de um ponto de recuperação.

NOTE: Quando uma tarefa está em execução, ela é relacionada no menu suspenso **Tarefas em execução** no alto do Core Console. Clicar em uma tarefa em execução abre a caixa de diálogo **Monitorar tarefa ativa**. Aqui, você pode cancelar uma ou mais tarefas em execução. Para obter mais detalhes, consulte o tópico Ver as tarefas em execução de qualquer página do Core Console. Você também pode suspender o agendamento de tarefas futuras no Core. Isso é útil, por exemplo, ao executar upgrades do SO ou a manutenção do servidor. Para obter mais informações sobre essa função, consulte o tópico Suspender ou retomar tarefas agendadas.

Execute o procedimento a seguir para ver as tarefas especificamente do Rapid Recovery Core ou para ver as tarefas associadas a uma máquina específica.

1. Para ver todas as tarefas do Rapid Recovery Core, na barra de ícones, clique em (Eventos). A exibição padrão mostra todas as tarefas do Core.

   Se desejar visualizar as tarefas de uma máquina protegida específica, acesse a página **Resumo** da máquina especificada e clique no menu **Eventos**. A exibição padrão mostra todas as tarefas da máquina selecionada.

2. Como opção, para filtrar a lista de tarefas por palavra-chave, data inicial, data final ou qualquer combinação, faça o seguinte e, em seguida, pressione **Enter**:
   a. Para filtrar por palavra-chave, insira-a na caixa de texto **Pesquisar palavra-chave**.

   Por exemplo, você pode filtrar por palavras-chave como "executando," "arquivo", "exportar" ou "transferência".

   b. Para filtrar por data e hora inicial, insira-as utilizando uma das seguintes opções:

   - Na caixa de texto **De**, digite a data e hora no formato MM/DD/AAAA HH:MM AM/PM. Por exemplo, para pesquisar a partir do primeiro dia de janeiro de 2016 às 8h da manhã, insira 01/01/16 8:00 AM.
   - Para selecionar a data e a hora atuais, clique no widget **Calendário** na caixa de texto **De** e, em seguida, clique na data atual. A hora atual é exibida automaticamente.
   - Clique no widget **Calendário**, selecione a data e, em seguida, clique no widget Relógio e selecione o tempo desejado usando os controles. Clique fora do calendário para aceitar as alterações selecionadas.

   c. Para refinar ainda mais a lista de tarefas que aparece, você também pode definir uma data e hora final no mesmo formato.

   A lista de tarefas é filtrada imediatamente com base nos critérios selecionados.
3. Como opção, você pode filtrar as tarefas que aparecem na lista da seguinte forma:

Opção	Descrição
	Para ver somente as tarefas ativas, clique no ícone **Tarefas ativas**.
	Para ver somente as tarefas que estão na fila para serem executadas, clique no ícone **Tarefas em fila**.
	Para ver somente as tarefas que estão esperando para serem executadas, clique no ícone **Tarefas em espera**.
	Para ver somente as tarefas que foram concluídas, clique no ícone **Tarefas concluídas**.
	Para ver somente as tarefas com falha, clique no ícone **Tarefas com falha**.
	Para ver todos os eventos, incluindo os eventos de serviço do Core que, por padrão, não são exibidos, clique no ícone **Serviço**.

4. Para exportar a lista de tarefas, selecione um formato na lista e clique em **Exportar**. Na caixa de diálogo resultante, confirme a exportação e clique em **OK**.

   É possível exportar usando os seguintes formatos:

Tabela 109. Formatos de exportação

Os formatos de saída disponíveis pelos quais você pode fazer o download de um relatório.

Formato	Descrição
PDF	Formato portátil de documento (padrão formato de exportação)
HTML	Formato de página da Web
CSV	Valores separados por vírgula
XLS	Pasta de trabalho do Microsoft Excel 1997 - 2003
XLSX	Pasta de trabalho do Excel

   O arquivo do tipo selecionado é baixado para o local padrão no servidor Core.

5. Clique no ícone **Detalhes do trabalho** de qualquer tarefa para abrir uma nova janela com os detalhes da tarefa.

Tarefas relacionadas

See also: Visualizar tarefas
See also: Suspender ou retomar tarefas agendadas
See also: Visualizar alertas
See also: Ver um diário de todos os eventos registrados
See also: Ver as tarefas em execução de qualquer página do Core Console
See also: Navegar entre tarefas, alertas e diário de eventos

Ver as tarefas em execução de qualquer página do Core Console

Para executar este procedimento é preciso haver uma tarefa atualmente em execução no Rapid Recovery Core.

O Rapid Recovery oferece uma forma rápida de visualizar tarefas atualmente em execução no Core a partir de qualquer página do Core Console.

No lado direito da barra de botões está a fila de **Tarefas em execução**. Em resoluções de tela mais baixas, ou se a janela do navegador não estiver totalmente expandida, a fila pode aparece como um ícone  . Quando uma ou mais tarefas estão em execução, um número indicando o número de tarefas atualmente em execução no Core é mostrado ao lado da fila e o ícone se torna animado. Você pode clicar na fila para mostrar uma lista suspensa de tarefas em execução e executar as ações descritas no procedimento a seguir.

1. No Core Console, enquanto uma tarefa estiver em execução, clique em **Tarefas em execução** ou no ícone de tarefas em execução.

   Uma pequena caixa é exibida, mostrando o tipo de tarefas em execução e o progresso, e apresenta as opções para cancelar uma ou mais tarefas ou para ver mais detalhes.
2. Para cancelar uma ou mais tarefas em execução, execute uma das opções a seguir:
   - Para cancelar uma única tarefa, clique no **X** ao lado da descrição da tarefa.
   - Para cancelar todas as tarefas em execução, clique em **Cancelar tudo**.
3. Para ver mais detalhes sobre uma tarefa em execução, clique na descrição da tarefa.

   A janela **Monitorar tarefa ativa** é aberta e mostra detalhes como o andamento e a hora de início.

Tarefas relacionadas

See also: Visualizar tarefas
See also: Navegar entre tarefas, alertas e diário de eventos
See also: Suspender ou retomar tarefas agendadas

Suspender ou retomar tarefas agendadas

Para retomar o agendador do Core, primeiro ele deve ser pausado, conforme descrito na etapa 3.

O Core rastreia as tarefas com base em uma agenda. As transferências para backup, replicação e arquivamento podem ser agendadas; os relatórios podem ser gerados semanal ou mensalmente; e assim por diante. Quando chegar o momento de executar uma tarefa agendada, o trabalho será colocado em uma fila, e os trabalhos serão realizados consecutiva ou concomitantemente, conforme a prioridade. Esse recurso é conhecido como agendador do Core.

Agora os usuários podem notificar o Core para suspender o agendador. Quando suspenso, os trabalhos futuros que, de outra forma, seriam agendados automaticamente para serem executados no Core ficam retidos temporariamente em uma fila, e novas tarefas não são agendadas. Essa função é útil em situações como executar atualizações do sistema operacional, instalações de software ou manutenção no servidor do Core. Quando suspensa, os trabalhos se acumulam na fila, mas não começam até que a função do agendador do Core seja explicitamente retomada. Nesse meio tempo, uma faixa é exibida ao longo do Core Console indicando que o agendador do Core está em pausa.

NOTE: Esse recurso impede a execução de tarefas que seriam agendadas em breve. Para ver ou cancelar tarefas que já estão na fila sem suspender suas tarefas futuras, consulte o tópico Ver as tarefas em execução de qualquer página do Core Console.

Conclua as etapas a seguir para suspender ou retomar a função do agendador do Core.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Eventos).

A página **Tasks** (Tarefas) será exibida.

3. Para suspender a função do agendador do Core, faça o seguinte:
    a. Clique em **Suspender agendador**.
    b. Na caixa de diálogo, se você quiser cancelar todas as tarefas em execução e suspender as tarefas futuras, selecione **Cancel Active Tasks and Suspend** (Cancelar tarefas ativas e suspender).
    c. Para suspender somente futuras tarefas, clique em **Suspend** (Suspender).

    As tarefas serão suspensas, e uma faixa será exibida em todas as páginas do Core Console informando que todas as tarefas agendadas estão suspensas.

4. Para retomar as tarefas suspensas, na página **Tarefas**, clique em **Retomar agendador**.

NOTE: Quando o agendador estiver suspenso, você também pode clicar em **Resume** (Retomar) na faixa no topo da Core Console.

Tarefas relacionadas

See also: Ver as tarefas em execução de qualquer página do Core Console
See also: Visualizar tarefas
See also: Suspender ou retomar tarefas agendadas
See also: Visualizar alertas
See also: Ver um diário de todos os eventos registrados
See also: Navegar entre tarefas, alertas e diário de eventos

Visualizar alertas

Um alerta é uma notificação de prioridade de um evento. Todos os eventos para os quais você especificamente solicitou notificação aparecem na lista de alertas, juntamente com erros, avisos ou mensagens informativas importantes.

O Rapid Recovery Core é fornecido com um conjunto padrão de eventos que são organizados por ordem de prioridade como alertas. Você pode personalizar os eventos que aparecem como alertas, editando o grupo de notificação padrão (ou configurando um novo grupo de notificação). Além disso, para esses eventos que aparecem na página **Alertas**, você pode alterar os métodos utilizados para notificar você alterando as opções de notificação. Para obter mais informações sobre como alterar os eventos que aparecem como alertas ou sobre como alterar as opções de notificação, consulte o tópico Noções básicas sobre as notificações de eventos no Rapid Recovery.

Execute o procedimento a seguir para ver alertas especificamente do Rapid Recovery Core ou para ver alertas associados a uma máquina específica.

1. Para ver alertas do Rapid Recovery Core, na barra de ícones, clique em (Eventos). Clique no menu suspenso do lado direito do título da página Tarefas e selecione **Alertas**.

    Se você deseja visualizar os alertas de uma máquina protegida específica, navegue até a página **Resumo** da máquina especificada, clique no menu **Eventos** e clique em **Alertas**.

    A lista de eventos é filtrada para exibir apenas os alertas importantes do Core ou da máquina selecionada.

2. Como opção, para filtrar a lista dos alertas importantes por data inicial, data final, descrição da mensagem de alerta ou qualquer combinação, faça o seguinte:
    a. Para filtrar por categoria de alerta (erros, mensagens informativas ou avisos), clique no menu suspenso de status e selecione uma ou mais condições de status. As opções de filtro de categoria de alerta são erros, mensagens informativas e avisos, ou qualquer combinação das três.

b. Para filtrar por data e hora inicial, insira-as utilizando uma das seguintes opções:

- Na caixa de texto **De**, digite a data e hora no formato MM/DD/AAAA HH:MM AM/PM. Por exemplo, para pesquisar a partir do primeiro dia de janeiro de 2016 às 8h da manhã, insira 01/01/16 8:00 AM.
- Para selecionar a data e a hora atuais, clique no widget **Calendário** na caixa de texto **De** e, em seguida, clique na data atual. A hora atual é exibida automaticamente.
- Clique no widget **Calendário**, selecione a data e, em seguida, clique no widget Relógio e selecione o tempo desejado usando os controles. Clique fora do calendário para aceitar as alterações selecionadas.

c. Para filtrar por descrição da mensagem de alerta, insira a descrição na caixa de texto **Pesquisar mensagem**.

Por exemplo, para ver apenas alertas relacionados aos agentes, digite "agente" para ver alertas relacionados às transferências, digite "transferência" e assim por diante.

d. Para refinar ainda mais a lista de alertas exibida, você também pode definir uma data e hora final no mesmo formato.

A lista de alertas é filtrada imediatamente com base nos critérios selecionados.

3. De forma opcional, se você quiser remover todos os alertas, clique em **Descartar tudo**.

Tarefas relacionadas

See also: Configurar grupos de notificação
See also: Visualizar tarefas
See also: Suspender ou retomar tarefas agendadas
See also: Visualizar alertas
See also: Ver um diário de todos os eventos registrados
See also: Ver as tarefas em execução de qualquer página do Core Console
See also: Navegar entre tarefas, alertas e diário de eventos

Referências relacionadas

See also: Noções básicas sobre as notificações de eventos no Rapid Recovery

Ver um diário de todos os eventos registrados

O diário mostra a lista de todos os eventos registrados. Esta lista é abrangente, incluindo os eventos relacionados a trabalho e eventos não relacionados a trabalho. Inclui eventos específicos para os quais você solicitou uma notificação. O diário também mostra uma lista de eventos passivos e eventos de status do Core, do portal de licenças, e assim por diante.

NOTE: Se o seu ambiente estiver definido para utilizar a redução de repetição, alguns eventos repetidos podem não ser registrados toda vez que o evento ocorrer. Para obter mais informações sobre esse recurso, consulte Sobre redução de repetição

Execute o procedimento a seguir para ver um diário de todos os eventos do Rapid Recovery Core ou para ver alertas associados a uma máquina específica.

1. Para ver um diário de todos os eventos registrados do Rapid Recovery Core, na barra de ícones, clique em (Eventos). Clique no menu suspenso do lado direito do título da página Tarefas e selecione **Diário**.

   Se você deseja visualizar um registro de todos os eventos de uma máquina protegida específica, navegue até a página **Resumo** da máquina especificada, clique no menu **Eventos** e clique **Registro**.

2. Como opção, para filtrar a lista de todos os eventos por data inicial, data final, descrição da mensagem de alerta ou qualquer combinação, faça o seguinte:
   a. Para filtrar por categoria de evento (erros, mensagens informativas ou avisos), clique no menu suspenso de status e selecione uma ou mais condições de status. As opções de filtro

de categoria de evento são erros, mensagens informativas e avisos, ou qualquer combinação das três.

b. Para filtrar por data e hora inicial, insira-as utilizando uma das seguintes opções:

- Na caixa de texto **De**, digite a data e hora no formato MM/DD/AAAA HH:MM AM/PM. Por exemplo, para pesquisar a partir do primeiro dia de janeiro de 2016 às 8h da manhã, insira 01/01/16 8:00 AM.
- Para selecionar a data e a hora atuais, clique no widget **Calendário** na caixa de texto **De** e, em seguida, clique na data atual. A hora atual é exibida automaticamente.
- Clique no widget **Calendário**, selecione a data e, em seguida, clique no widget Relógio e selecione o tempo desejado usando os controles. Clique fora do calendário para aceitar as alterações selecionadas.

c. Para filtrar por descrição da mensagem de alerta, insira a descrição na caixa de texto **Pesquisar mensagem**.

Por exemplo, para ver apenas alertas relacionados aos agentes, digite "agente;' para ver alertas relacionados às transferências, digite "transferência".

d. Para refinar ainda mais a lista de eventos exibida, você também pode definir uma data e hora final no mesmo formato.

A lista de eventos é filtrada imediatamente com base nos critérios selecionados.

Conceitos relacionados

See also: Sobre redução de repetição

Tarefas relacionadas

See also: Visualizar tarefas
See also: Suspender ou retomar tarefas agendadas
See also: Visualizar alertas
See also: Ver um diário de todos os eventos registrados
See also: Ver as tarefas em execução de qualquer página do Core Console
See also: Navegar entre tarefas, alertas e diário de eventos

Navegar entre tarefas, alertas e diário de eventos

Os eventos registrados nos logs do Core são visíveis no Core Console e podem ser divididos em três categorias: tarefas, alertas e um diário de todos os eventos registrados.

Independentemente de se estar vendo eventos do Core de uma máquina especificada, a exibição padrão para eventos é a página **Tarefas**. Clicando no menu suspenso à direita do título da página, você pode selecionar uma outra exibição de eventos.

Execute as etapas a seguir para ver eventos e navegar entre tarefas, alertas importantes e um diário de todos os eventos.

Você pode visualizar eventos que pertencem ao núcleo clicando em (Eventos) na barra de ícones.

Se você primeiro navegar para uma máquina protegida ou replicada e, em seguida, selecionar **Eventos** no menu na parte superior da página, você pode ver os eventos da máquina especificada.

Independentemente de se estar vendo eventos do Core de uma máquina especificada, a exibição padrão para eventos é a página **Tarefas**. Clicando no menu suspenso à direita do título da página, você pode selecionar uma outra exibição de eventos.

1. Se quiser ver todas as tarefas do Rapid Recovery Core, na barra de ícones, clique em (Eventos).

A exibição padrão mostra todas as tarefas do Core. Vá para a etapa 3.

2. Se desejar visualizar as tarefas de uma máquina protegida específica, acesse a página **Resumo** da máquina especificada e clique no menu **Eventos**.

   A exibição padrão mostra todas as tarefas da máquina selecionada. Vá para a etapa 3.

3. No canto superior esquerdo do painel **Tarefas**, clique em ▼ (a seta virada para baixo à direita do título Tarefas).

   Um menu suspenso é exibido.

4. Selecione uma das opções a seguir:

Opção	Descrição
Tarefa	Uma tarefa é um trabalho que o Rapid Recovery Core deve realizar, como transferir dados em uma cópia de segurança programada regular ou executar uma restauração a partir de um ponto de recuperação.
Alerta	Um alerta é uma notificação de prioridade relacionada a uma tarefa ou evento, como um erro, uma advertência ou uma mensagem informativa importante.
Registro	O diário mostra uma lista completa de todos os eventos registrados. Esta lista é mais abrangente do que o conjunto incluído nos alertas.

   A exibição selecionada de eventos é mostrada. Por exemplo, se você selecionou **Alertas**, a página Alertas é exibida

5. Para ver uma exibição diferente, volte para o menu suspenso à direita do painel Tarefas, Alertas ou Diário e selecione a opção para a exibição que você quer.

   A lista de eventos é filtrada para mostrar apenas o conjunto de eventos pertinente da exibição atual.

Tarefas relacionadas

See also: Visualizar tarefas
See also: Visualizar alertas
See also: Ver um diário de todos os eventos registrados
See also: Ver as tarefas em execução de qualquer página do Core Console

Noções básicas sobre as notificações de eventos no Rapid Recovery

O Rapid Recovery Core monitora muitos eventos e registra as informações para fins de diagnóstico e de operação.

Você pode configurar a notificação de eventos específicos. O Rapid Recovery permite que você escolha o método de notificação, assim como a duração de tempo para o qual o sistema deve reter um registro de tais eventos. Com o recurso de redução de repetição, você pode até ajustar a frequência para notificar você sobre o mesmo evento.

Por padrão, os trabalhos e os eventos monitorados no Core são salvos por 30 dias. Para alterar o período de retenção para eventos de monitoramento, consulte Configurar retenção de eventos

Você pode ser notificado de eventos por diferentes métodos. Os métodos de notificação suportados são apresentados na tabela a seguir:

Tabela 110. Métodos de notificação de evento suportados

Tipo de opção	Descrição	Definição padrão
E-mail	Notifica um usuário especificado por e-mail usando os parâmetros de configuração SMTP no Core e de acordo com o modelo de notificação por e-mail.	Desligar
Log de Eventos do Windows	Registra os eventos usando o API de Log de Eventos do Windows. Este log pode ser lido usando o Visualizador de Eventos do Windows ou aplicativos personalizados.	Em
syslogd	Registra os eventos destinados a serem lidos em um servidor de logs do Linux que também suporta o protocolo de mensagem syslog.	Desligar
Alerta de notificação do sistema	Quando este método de notificação é selecionado, as mensagens são mostradas por um breve período como uma janela pop-up no canto inferior direito do Rapid Recovery Core Console.	Em
Interceptação SNMP	Se você configurar o Rapid Recovery Core como um agente SNMP e este método de notificação for selecionado, os eventos são enviados para um servidor de logs usando o número de interceptação designado na caixa de diálogo Opções de notificação.	Em

Os grupos de notificação permitem que você especifique os tipos de eventos para os quais você quer ser notificado e defina o método de notificação.

O Rapid Recovery Core precisa de pelo menos um grupo de notificação e é fornecido com um grupo padrão que é automaticamente aplicado. Você pode usar as configurações padrão ou pode editá-las.

Opcionalmente, você pode adicionar e configurar grupos de notificação adicionais. Por exemplo, você pode usar o grupo padrão como está e configurar outro grupo que usa notificações por e-mail.

Como outro exemplo, você pode configurar um grupo de notificação personalizado para um único tipo de evento (por exemplo, Microsoft Exchange) e enviar todas as notificações relacionadas a um administrador do Exchange.

Para obter mais informações, consulte Configurar grupos de notificação.

Por padrão, as notificações por e-mail são desativadas. Para enviar notificações por e-mail, você precisa configurar um servidor de e-mail e editar ou adicionar um grupo de notificação com a opção **Notificar por e-mail** ativada. Esta configuração requer que você insira o endereço de e-mail para o qual as notificações serão enviadas. Para obter mais informações, consulte Configurar um servidor de e-mail.

Se estiver usando um servidor Exchange, você precisa configurar a transmissão no servidor. Caso contrário, apesar de os testes de e-mail serem bem-sucedidos, nenhuma notificação por e-mail será enviada. Para obter mais informações, consulte o administrador do Exchange Server.

O Core usa uma modelo de notificação por e-mail. O modelo inclui uma linha de assunto e conteúdo específico para o corpo da mensagem. Um modelo de notificação por e-mail padrão é incluído. O modelo identifica o Core e host do servidor, a data e a hora do evento, a natureza do evento e detalhes do erro, se relevante. Opcionalmente, você pode modificar o modelo padrão ou reverter qualquer personalização para restaurar a configuração padrão. Para obter mais informações, consulte Configurar um modelo de e-mail de notificação.

Você pode reduzir o número de eventos do mesmo tipo e escopo que são registrados e exibidos no Core Console usando o recurso de redução de repetição. Este recurso está habilitado por padrão. Você pode desabilitar esse recurso ou controlar o intervalo de tempo para o qual os eventos são combinados em uma única ocorrência no log de eventos. Para obter mais informações, consulte Sobre redução de repetição.

Conceitos relacionados

See also: Sobre redução de repetição

Tarefas relacionadas

See also: Configurar grupos de notificação

See also: Configurar retenção de eventos

Referências relacionadas

See also: Noções básicas sobre notificações por e-mail

Configurar grupos de notificação

NOTE: Deve-se primeiro configurar as definições do server SMTP se desejar enviar notificações como mensagens de e-mail, conforme descrito neste procedimento. Para obter mais informações sobre como definir as configurações do servidor de e-mail, consulte Configurar um servidor de e-mail.

Os grupos de notificação permitem definir conjuntos de eventos específicos sobre os quais os usuários são alertados e a maneira como essa notificação ocorre. Você pode configurar os seguintes métodos para o envio de alertas:

- Por e-mail
- No log de eventos do Windows
- Uso de syslogd
- Uso de alertas do sistema
- Usar alertas
- Usar trap de SNMP

O Rapid Recovery Core é fornecido com um grupo de notificação padrão para o Core. Você pode editar esse grupo para atender às suas necessidades. Opcionalmente, você pode configurar mais de um grupo de notificação com diferentes parâmetros de notificação.

Os grupos de notificação podem ser definidos no nível do Core ou para cada máquina protegida específica.

Execute as etapas deste procedimento para configurar os grupos de notificação para alertas.

1. Para definir as notificações no nível do Core, na barra de ícones, clique em (Mais) e, em seguida, selecione **Notificações**.

   A página **Notificações** é exibida. Pule para a Etapa 33.
2. Para definir as notificações para uma máquina protegida específica, faça o seguinte:
   a. No menu Máquinas protegidas, clique na máquina em relação à qual deseja especificar notificações.

   A página **Resumo** é mostrada.

   b. Na página **Resumo** da máquina protegida, no menu suspenso **Mais**, selecione **Notificações**.

   A página **Grupos de notificação personalizados** é exibida.
3. Se quiser adicionar um novo grupo de notificação, clique em **Adicionar Grupo**. Pule para a Etapa 5.

   A caixa de diálogo **Adicionar grupo de notificação** é exibida mostrando uma área de descrição geral e duas guias.
4. Se você quiser editar o grupo de notificação padrão ou um grupo de notificação existente, no painel Grupos de notificação, clique no menu suspenso (Mais) para o grupo de notificação adequado e selecione **Editar**.

A caixa de diálogo **Editar grupo de notificação** é exibida mostrando uma área de descrição geral e duas guias.

5. Na área de descrição geral, insira as informações básicas para o grupo de notificação, conforme descrito na tabela a seguir.

Opção	Descrição
Nome	Insira um nome para o grupo de notificação de eventos. Estas informações são obrigatórias. **CAUTION: O valor inserido para o nome do grupo de notificação não poderá ser alterado posteriormente.**
Descrição	Insira uma descrição que explique a finalidade do grupo de notificação de eventos. Estas informações são opcionais

6. Na guia **Ativar alertas**, configure o conjunto de eventos do sistema que resulta em alertas. Esses aparecem na página **Alertas** ao visualizar eventos no Core Console. Você pode selecionar conjuntos de eventos conforme descrito na tabela a seguir:

Opção	Descrição
Todos os alertas	Para criar alertas para todos os eventos, selecione
Erros	Para criar alertas para erros, no menu **Selecionar tipos**, clique em **Erro**. Isso é representado por um X vermelho.
Aviso	Para criar alertas para erros, no menu **Selecionar tipos**, clique em **Aviso**. Isso é representado por um ícone amarelo de ponto de exclamação.
Informações	Para criar alertas para mensagens informativas, no menu **Selecionar tipos**, clique em **Informações**. Isso é representado por um i azul.
Restaurar padrão	ou o grupo de notificação padrão do Core, para restaurar o conjunto de eventos que aparecem como alertas para o padrão, no menu **Selecionar tipos**, clique em **Restaurar para valores padrão**. **NOTE:** Esta opção está disponível ao editar o grupo de notificação padrão do Core apenas. Ela não está disponível para novos grupos de notificação do Core ou para a configuração de notificações de uma máquina protegida específica.

7. Para criar alertas para um tipo de evento específico (erro, aviso ou mensagem informativa), faça o seguinte:
    a. Se a opção **Todos os alertas** não exibir grupos de alerta, clique no símbolo de ângulo para a direita **>** que precede o rótulo Todos os alertas. O símbolo muda para uma seta voltada para baixo, e a visualização se expande para exibir os grupos.

b. Em seguida, clique no símbolo de ângulo para a direita **>** ao lado de qualquer grupo de alerta específico para exibir os eventos relacionados no grupo.

- Para definir alertas para todos os eventos em cada grupo, marque a caixa de seleção **Todos os alertas**.
- Para definir alertas para todos os eventos dentro de qualquer grupo de alerta, marque a caixa de seleção ao lado desse grupo.
- Para selecionar somente alguns tipos de alerta dentro de um grupo de alerta, expanda o grupo e selecione somente os eventos específicos em relação aos quais você desejar registrar, criar relatório e definir alertas.

8. Clique na guia **Opções de notificação**.
9. Na guia **Opções de notificação**, especifique como lidar com o processo de notificação.

Opção	Descrição
Notificar por e-mail	Designe os destinatários da notificação de e-mail. É possível optar por especificar vários endereços de e-mail separados, bem como cópias carbono e ocultas. **NOTE:** Se você estiver usando Exchange Server, a retransmissão SMTP deve ser configurada no servidor. Caso contrário, as notificações de eventos não serão enviadas ao endereço de e-mail designado. Para obter mais informações, consulte o administrador do Exchange Server.
Notificar pelo Log de eventos do Windows	Selecione essa opção se deseja que as notificações sejam comunicadas por meio do Log de Eventos do Windows.
Notificar por syslogd	Selecione essa opção se deseja que as notificações sejam comunicadas por meio de syslogd. Especifique os detalhes do syslogd nas seguintes caixas de texto: • Host: • Porta:
Notificar por alertas Toast	Selecione essa opção se deseja que as notificações sejam exibidas como mensagens pop-up no canto inferior direito da tela.
Notificar por interceptação SNMP	O Rapid Recovery Core funciona como um agente de SNMP, enviando interrupções (notificações sobre eventos específicos) para o gerenciador de SNMP. Isso permite que o Core transmita certas informações, como alertas, status do repositório e máquinas protegidas. Selecione essa opção se quiser que os eventos do Core sejam comunicados por trap de SNMP. Você precisa especificar também um número de interrupção, o qual é usado pelo gerenciador de SNMP.

10. Clique em **OK**.

Se estiver criando um novo grupo, você verá uma mensagem indicando que o nome do grupo de notificação definido não pode ser alterado após a criação do grupo. Outras propriedades dentro do grupo de notificação podem ser alteradas a qualquer momento.

- Se você estiver satisfeito com o nome do grupo, confirme essa mensagem e salve o seu trabalho.
- Se quiser alterar o nome do grupo, clique em **Não** para voltar à janela Criar grupo de notificação, atualize o nome do grupo e outras definições de grupo de notificação e salve seu trabalho.

O grupo de notificação é exibido na tabela de resumo. Você pode criar diferentes grupos de notificação usando qualquer conjunto de parâmetros.

Noções básicas sobre notificações por e-mail

Você pode configurar o Rapid Recovery Core para notificá-lo sobre eventos específicos pelo envio de uma mensagem de e-mail para um endereço de e-mail especificado por você. Os eventos que geram alertas e os métodos de notificação são definidos no grupo de notificação.

NOTE: É necessário estabelecer grupos de notificação mesmo que você não use e-mail como método de notificação. Para obter mais informações, consulte Configurar grupos de notificação.

O Rapid Recovery usa um modelo de notificação por e-mail que determina as informações enviadas em cada notificação. O modelo define a linha de assunto do e-mail relativo a cada alerta e o conteúdo no corpo da mensagem. O modelo possui definições padrão, que você pode usar como estão ou testar e modificar para atender às suas necessidades. A qualquer momento depois de personalizar o modelo de notificação, você pode escolher a opção Restaurar padrões para retornar usando o modelo padrão. Para obter informações sobre como visualizar e personalizar o modelo de e-mail, consulte Configurar um modelo de e-mail de notificação.

Se você escolher e-mail como uma das opções de notificação, precisará configurar primeiro um servidor de SMTP para e-mail. O Rapid Recovery Core utiliza o servidor definido para envio de alertas com base nos parâmetros do grupos de notificação.

Além disso, para receber notificações por e-mail, você precisa ativar a opção **Notificar por e-mail** dentro do grupo de notificação. Esta opção de notificação está desabilitada por padrão. A configuração **Notificar por e-mail** requer, no mínimo, um endereço "Para" definido. (Opcionalmente, você pode adicionar endereços de cópia e cópia oculta se desejado.)

Esta seção inclui os seguintes tópicos:

- Configurar um servidor de e-mail
- Configurar um modelo de e-mail de notificação

Configurar um servidor de e-mail

Execute as etapas deste procedimento para configurar um server de e-mail.

NOTE: Você também deve configurar as definições de grupo de notificação, incluindo a ativação da opção **Notificar por e-mail** antes que as mensagens de alertas de e-mail sejam enviadas pelo sistema. Para obter mais informações sobre especificação de eventos para recepção de alertas de e-mail, consulte Configurar grupos de notificação.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de configurações do Core no lado esquerdo da página Configurações, clique em **Servidor de SMTP**.
   - Role para baixo no lado direito da página Configurações até visualizar o cabeçalho **Servidor de SMTP**.
3. Clique na definição que você deseja alterar.

A definição selecionada se torna editável.

4. Insira as informações de configuração conforme descrito na tabela a seguir.

Opção	Descrição
Servidor SMTP	Digite o nome do server de e-mail a ser usado pelo modelo de notificação de e-mail. A convenção de nomenclatura inclui o nome do host, domínio e sufixo; por exemplo, smtp.gmail.com.
De	Insira o endereço de e-mail de devolução. Usado para especificar o endereço de e-mail de devolução para o modelo de notificação de e-mail; por exemplo, noreply@localhost.com.
Nome de usuário	Insira um nome de usuário do server de e-mail.
Senha	Insira a senha associada ao nome de usuário necessário para acessar o server de e-mail.
Porta	Insira um número de porta. Utilizado para identificar a porta do server de e-mail; por exemplo, porta 587 para o Gmail. O padrão é 25.
Tempo esgotado (segundos)	Insira um valor de número inteiro para especificar quanto tempo deve-se tentar se conectar ao server de e-mail. Utilizado para estabelecer o tempo em segundos antes de ocorrer o tempo limite. O padrão é 60 segundos.
TLS	Selecione essa opção se o server de e-mail usar uma conexão segura, como Transport Layer Security (TLS) ou Secure Sockets Layer (SSL).

5. Para cada definição, quando estiver satisfeito com suas alterações, clique na ✓ para salvar a alteração e sair do modo de edição, ou clique em ✕ para sair do modo de edição sem salvar.

   CAUTION: Se você não confirmar cada alteração, suas configurações não serão alteradas.

6. Clique em › **Enviar e-mail de teste** e faça o seguinte:
   a. Na caixa de diálogo **Enviar e-mail de teste**, insira um endereço de e-mail de destino para a mensagem de teste e clique em **Enviar**.
   b. Se a mensagem de teste falhar, saia da caixa de diálogo de erro e da caixa de diálogo **Enviar e-mail de teste** e revise suas configurações de servidor de e-mail. Em seguida, envie a mensagem de teste novamente.
   c. Quando a mensagem de teste for bem-sucedida, clique em **OK** para confirmar o êxito da operação.
   d. Verifique a conta de e-mail para a qual você enviou a mensagem com o e-mail de teste.

Configurar um modelo de e-mail de notificação

Quando você ativa as notificações de eventos do Rapid Recovery por e-mail, por padrão, um modelo padrão é criado para você. O servidor de e-mails SMTP definido para o Core usa esse modelo para enviar notificações sobre eventos do Rapid Recovery por e-mail.

Este tópico descreve o processo de configuração do modelo padrão de notificações de e-mail ou de personalização do conteúdo. Usando a opção Restaurar padrão, você pode restaurar as alterações do modelo padrão de notificação a qualquer momento.

CAUTION: Modifique o modelo por sua conta e risco. Você é responsável por testar quaisquer modificações no modelo. Somente o modelo padrão é suportado.

Execute as etapas deste procedimento para configurar um modelo de notificação de e-mail.

NOTE: Você também deve configurar um servidor de e-mail e as definições de grupo de notificação, incluindo a ativação da opção **Notificar por e-mail**, antes de as mensagens de alerta por e-mail serem enviadas. Para obter mais informações sobre como configurar um servidor de e-mail para o envio de alertas, consulte Configurar um servidor de e-mail. Para obter mais informações sobre especificação de eventos para recepção de alertas de e-mail, consulte Configurar grupos de notificação.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Notificações**.

   A página **Notificações** é exibida.
3. No painel Definições de e-mail, clique em **Alterar**.

   A caixa de diálogo **Edit Email Notification Configuration** (Editar configuração de notificação por e-mail) é mostrada.
4. Selecione **Ativar notificações de e-mail**.

   O modelo de e-mail está ativada e é visível. Os valores de modelo padrão de e-mail são descritos na etapa a seguir.
5. Revise o conteúdo da caixa de diálogo Editar configuração de notificação de e-mail e determine se o conteúdo padrão é adequado às suas necessidades.

Opção	Descrição
Habilitar notificações de e-mail	Esta configuração ativa ou desativa o modelo de notificações de e-mail. • Para ativar as notificações de e-mail, selecione esta opção. • Para desativar as notificações de e-mail, desmarque a opção.
Assunto do e-mail	O conteúdo deste campo de texto controla a linha de assunto em mensagens de e-mail enviadas como notificações de eventos do sistema. A linha de assunto de e-mail padrão é a seguinte: `<hostName> <level>: <name> para <agentName>`
E-mail	O conteúdo desta área de texto controla o corpo em mensagens de e-mail enviadas como notificações de eventos do sistema. O corpo de e-mail padrão é o seguinte:

Opção	Descrição
	<shortCompanyName> <coreProductName> em <hostName> relatou o evento <level> "<name>" Data/Hora: <localTimestamp> <message> <if(details.errorDetails)> <details.ErrorDetails.Message> <details.ErrorDetails.Details> <endif> --- Sobre este evento: <description> <coreAdminUrl>
Enviar e-mail de teste	Clicar neste botão envia uma mensagem de e-mail de teste para o endereço de e-mail especificado na caixa de diálogo **Enviar e-mail de teste** resultante.
Restaurar padrão	Clicar neste botão remove quaisquer alterações personalizadas do modelo de email e restaura os campos de assunto do email e de e-mail com o conteúdo padrão descrito nesta tabela.
OK	Clicar neste botão confirma e salva as configurações na caixa de diálogo Editar configuração de notificação de e-mail.
Cancelar	Clicar neste botão cancela quaisquer alterações na caixa de diálogo Editar configuração de notificação de e-mail.

6. Se desejar personalizar o modelo de e-mail, faça as alterações no texto ou nas variáveis descritas na etapa anterior. As variáveis usadas no padrão são descritas na tabela a seguir.

Opção	Descrição
hostName	O nome do host do Core
details	Os detalhes relacionados ao evento específico.
agentName	O nome da máquina protegida associada a esse evento, se o evento tiver o escopo de uma única máquina protegida.
repositoryName	O nome do repositório associado a esse evento, se o evento tiver o escopo de repositório.
jobSummary	O nome do trabalho associado a esse evento, se o evento tiver o escopo de trabalho.
remoteSlaveCoreName	O nome do core de destino remoto associado a esse evento, se o evento tiver o escopo de core de destino.

Opção	Descrição
remoteMasterCoreName	O nome do core de origem remota associado a esse evento, se o evento tiver o escopo de core de origem.
productName	O nome do produto; por exemplo, “AppAssure Core” ou “Rapid Recovery Core”. Este nome do produto pode ser alterado para uma marca com o uso de etiquetas brancas.
companyName	O nome da empresa que está vendendo o produto.

7. Na caixa de texto **Assunto do e-mail**, insira um assunto para o modelo de e-mail.

   O Assunto do e-mail é usado para definir o assunto do modelo de notificação por e-mail, por exemplo, <nome do host> - <nível>: <nome>.

8. Na caixa de texto **E-mail**, insira as informações do corpo do modelo que descrevem o evento, quando ocorreu e a gravidade.
9. Clique em **Enviar e-mail de teste** e faça o seguinte:
   a. Na caixa de diálogo Enviar e-mail de teste, insira um endereço de e-mail de destino para a mensagem de teste e clique em **Enviar**.
   b. Se a mensagem de teste falhar, saia da caixa de diálogo de erro e da caixa de diálogo Enviar e-mail de teste, clique em **OK** e salve as configurações atuais de modelo de e-mail. Em seguida, modifique suas configurações de servidor de e-mail conforme descrito no procedimento Configurar um servidor de e-mail. Certifique-se de digitar a senha novamente para essa conta de e-mail. Salve essas definições e volte a esse procedimento.
   c. Quando a mensagem de teste for bem-sucedida, clique em **OK** para confirmar o êxito da operação.
   d. Verifique a conta de e-mail para a qual você enviou a mensagem com o e-mail de teste.

Quando estiver satisfeito com os resultados de seus testes, retorne à caixa de diálogo Editar configuração de notificação de e-mail e clique em **OK** para fechar a caixa de diálogo e salvar as definições.

Definir as configurações de evento

Você pode definir algumas configurações específicas para eventos.

Por exemplo, você pode definir as configurações de redução de repetição para reduzir a quantidade de notificações que você vê para eventos repetidos idênticos.

Você pode também definir o intervalo de tempo, em dias, que os registros de eventos são mantidos no banco de dados.

Veja os seguintes tópicos para saber mais sobre como definir as configurações de evento.

- Sobre redução de repetição
- Configurar retenção de eventos

Referências relacionadas

See also: Como exibir eventos usando tarefas, alertas e páginas de diário
See also: Noções básicas sobre as notificações de eventos no Rapid Recovery

Sobre redução de repetição

É essencial que os administradores recebam uma notificação sobre a ocorrência de certos eventos. No entanto, em certas circunstâncias, pode ser frustrante ou inconveniente receber notificações repetidas sobre um evento do qual você está ciente. Mesmo que uma notificação seja gerada devido a uma falha ambiental sobre a qual você deseja saber imediatamente, é possível que a mesma condição de erro gere centenas ou milhares de eventos no log de eventos. Para reduzir a repetição no log de eventos e reduzir a inconveniência de receber repetidos alertas de notificação do sistema ou notificações por e-mail para o mesmo evento no Console do Core, o Rapid Recovery inclui uma definição de redução de repetição, que é habilitada por padrão e configurada em 5 minutos. Essa definição pode ser ajustada entre 1 e 60 minutos. Também é possível desabilitá-la completamente.

Quando a redução de repetição está desabilitada, cada vez que ocorre um evento do mesmo tipo e escopo, ele é registrado no banco de dados. Independentemente do tempo decorrido desde a ocorrência anterior do evento, cada nova ocorrência é mostrada na seção Alertas da página Eventos.

Quando a redução de repetição está habilitada (por exemplo, com o tempo padrão de cinco minutos), o evento é registrado no banco de dados de eventos e mostrado no log Alertas quando ocorre pela primeira vez. Se subsequentemente um evento do mesmo tipo e escopo é novamente registrado dentro do limite de tempo estabelecido, a contagem do evento no banco de dados aumenta em 1 para cada ocorrência repetida dentro do limite. O log mostra na parte de Alertas da página Eventos. No entanto, ele mostra o evento apenas uma vez, com a data e a hora da ocorrência mais recente. O log de eventos não é atualizado com o mesmo evento até a expiração do limite de tempo a partir da primeira ocorrência. Por exemplo, se definido para 5 minutos e o evento ocorrer novamente 6 minutos mais tarde, ele será exibido no log e você receberá outra notificação.

Configurar redução de repetição

Execute as etapas deste procedimento para configurar a redução de repetição dos eventos.

1. Navegue até o Rapid Recovery Core Console. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Notifications** (Notificações).

   A página **Notificações** é exibida.
2. No painel Redução de repetição, veja as definições existentes.
3. Para ativar, desativar ou alterar o tempo limite de eventos armazenados, clique em **Change** (Alterar).

   A caixa de diálogo **Editar redução de repetição** é exibida
4. Execute um dos seguintes:
   - Para desativar a redução de repetição, desmarque a opção **Habilitar redução de repetição**.
   - Para ativar a redução de repetição, marque a opção **Habilitar redução de repetição**.
   - Para alterar o limite de tempo (em minutos) para os quais os eventos idênticos repetidos são ignorados, na caixa de texto **__ minuto(s)**, insira um número entre 1 e 60.

   NOTE: A opção **Habilitar redução de repetição** deve ser marcada para alterar esse valor.
5. Clique em **OK** para salvar as configurações e fechar a caixa de diálogo.

Configurar retenção de eventos

Eventos e trabalhos rastreados no Core são salvos por um período determinado de tempo. A definição padrão é 30 dias. Este número pode ser definido entre 0 dias e 3652 dias (aproximadamente 10 anos).

Execute as etapas deste procedimento para configurar a retenção de eventos.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página Definições, clique em **Conexão do banco de dados**.
   - Role a tela para baixo no lado direito do da página Definições até que você possa ver o cabeçalho **Conexão do banco de dados**.

   As definições de conexão do database serão exibidas.
3. Para alterar a quantidade de dias durante os quais as informações de evento serão salvas no banco de dados, clique no campo de texto **Período de retenção (dias)**, insira um valor entre 0 e 3652, e, em seguida, clique em para salvar a alteração.

   O período de retenção de eventos é ajustado conforme especificado.

Relatório

Esta seção fornece uma visão geral dos relatórios disponíveis no Rapid Recovery Core Console.

Sobre os relatórios do Rapid Recovery

Você pode gerar esses relatórios no Rapid Recovery Core Console. Espera-se que outros relatórios também estejam disponíveis no Portal de proteção de dados.

Os relatórios disponíveis no Core Console são descritos na tabela a seguir.

Tabela 111. Relatórios do Rapid Recovery

Tipo de relatório	Descrição
Relatório do trabalho	Fornece um relatório básico sobre o status dos trabalhos bem-sucedidos, trabalhos com falha e trabalhos com erros. Os trabalhos com falha podem ainda ser vistos com mais detalhes em um Relatório de falhas. • Por padrão, o intervalo de tempo do relatório é para os últimos 31 dias. Isso pode ser personalizado. • Quando executado a partir do Core, este relatório pode especificar os detalhes de um ou mais Cores.Por padrão, esse conjunto de informações contém os trabalhos de todas as máquinas — servidores de banco de dados, máquina protegidas, máquinas replicadas e máquinas de ponto de recuperação apenas — nos Cores especificados. Nos parâmetros do relatório, você pode personalizar o relatório. Use os filtros para selecionar ou excluir algumas máquinas. Você pode também selecionar ou excluir trabalhos que são independentes de máquina; nesse caso, o relatório mostrará apenas o status dos trabalhos do Core. Para obter mais informações sobre esse tipo de relatório, consulte Noções básicas sobre o relatório do trabalho.
Relatório de resumo do trabalho	Fornece um relatório mais detalhado sobre o status de trabalhos bem-sucedidos, trabalhos com falha e trabalhos com erros, mostrando uma linha separada no relatório para cada tipo de trabalho, o que permite um melhor diagnóstico dos possíveis problemas. • Por padrão, o intervalo de tempo do relatório é para os últimos 31 dias. Isso pode ser personalizado. • Diferente do relatório do trabalho, este relatório não oferece uma seleção de Cores como um parâmetro. • Por padrão, esse conjunto de informações contém os trabalhos de todas as máquinas — servidores de banco de dados, máquina protegidas, máquinas replicadas e máquinas de ponto de recuperação apenas — e os trabalhos que são dependentes de máquina, por tipo de trabalho. Você pode personalizar o relatório. Use os filtros

Tipo de relatório	Descrição
	para selecionar ou excluir algumas máquinas. Você pode também selecionar ou excluir trabalhos que são independentes de máquina. • Quando executado a partir da perspectiva de uma máquina protegida do Core Console, o relatório resultante exibe o status dos trabalhos dessa máquina protegida apenas. Para obter mais informações sobre esse tipo de relatório, consulte Noções básicas sobre o relatório de resumo dos trabalhos.
Relatório de falhas	Fornece informações sobre os trabalhos do Core com falha conforme os critérios especificados. Esse relatório pode incluir detalhes da máquina protegido ou excluí-los. Assim como o Relatório do trabalho, este relatório pode também ser executado apenas a partir de uma máquina protegida selecionada no Core. O relatório resultante mostra detalhes sobre trabalhos com falha somente para a máquina protegida selecionada. Para obter mais informações sobre esse tipo de relatório, consulte Noções básicas sobre o relatório de falhas.
Relatório resumido	Fornece informações de resumo.Por padrão, esse conjunto de informações contém os trabalhos de todas as máquinas, ou seja, todas as máquina protegidas, replicadas e de ponto de recuperação apenas, nos Cores especificados. Nos parâmetros do relatório, você pode personalizar o relatório. Use os filtros para selecionar ou excluir algumas máquinas. Você pode também selecionar ou excluir trabalhos que são independentes de máquina; nesse caso, o relatório mostrará apenas o status dos trabalhos do Core. Este relatório não está disponível da perspectiva de uma única máquina protegida. As categorias de informações deste relatório são Core, licença e repositório. As informações são apresentadas na forma de listas, gráficos e tabelas. Para obter mais informações sobre esse tipo de relatório, consulte Noções básicas sobre o relatório resumido.
Relatório do repositório	Este tipo de relatório fornece um relatório de todos os repositórios no Core ou Cores selecionados. Você pode também selecionar qualquer repositório único disponível para o Core. Esse relatório é apenas da perspectiva do Core. Para obter mais informações sobre esse tipo de relatório, consulte Noções básicas sobre o relatório do Repositório.
Relatório de resumo clássico	Este relatório apresenta uma exibição resumida do sucesso das estatísticas do trabalho, resumos de repositório por GB, sucesso de instantâneos, tendências de uso de repositório e um resumo das máquinas protegidas em seu Core. Os parâmetros do relatório incluem o intervalo de datas e o Core relevante.
Relatório programado	Você pode também programar um desses relatórios no Core Console. A programação de um relatório faz com que o relatório que você especificar seja gerado repetidamente conforme a programação definida. Como opção, você pode estabelecer notificações de e-mail cada vez que um relatório for gerado. Para obter mais informações sobre como programar, modificar, pausar ou apagar relatórios, consulte Gerenciar relatórios programados no Core Console.

Baseado no tipo de relatório e nos parâmetros selecionados, você pode gerar um relatório em um ou mais Rapid Recovery Cores ou para uma ou mais máquinas protegidas.

Gerar um relatório no Core Console

Você pode gerar relatórios sob demanda a partir do Core Console. As seguintes regras se aplicam:

- Todos os relatórios podem ser gerados a partir do ponto de vista do Core.
- Além disso, dois tipos de trabalho (o Relatório do trabalho e o Relatório de falhas) podem ser gerados do ponto de vista de uma máquina protegida. Para tais relatórios, os dados gerados são relativos apenas à máquina selecionada.
- Os Relatório de falhas conterão dados apenas se os trabalhos nos Cores selecionados (ou máquinas protegidas) falharam.

O método de geração de relatórios sob demanda é similar se o relatório for gerado a partir do foco do Core ou se ele for gerado do ponto de vista de uma máquina protegida. No entanto, a navegação é ligeiramente diferente.

Você pode também agendar relatórios para que eles sejam gerados regularmente. Para obter mais informações sobre como programar, modificar, pausar ou apagar relatórios, consulte Gerenciar relatórios programados no Core Console.

Gerar um relatório de Core sob demanda

Conforme descrito no tópico Sobre os relatórios do Rapid Recovery, é possível gerar a faixa completa de relatórios disponíveis do Core Console.

Execute as etapas do procedimento a seguir para gerar um relatório do ponto de vista do Rapid Recovery Core.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Relatórios**.

   A página **Relatório do trabalho** é mostrada. À direita do nome do relatório no título da página, uma seta voltada para baixo é mostrada, a partir da qual você pode selecionar outro tipo de relatório.

   Se você quiser gerar um relatório de trabalho, vá para a etapa 6 para começar a especificação dos seu critérios de relatório.
3. Para escolher outro tipo de relatório, clique na seta à direita do nome do relatório para ver um menu de relatórios disponíveis.
4. Para definir relatórios programados, consulte Programar um relatório.
5. Para gerar um relatório do repositório apenas, vá para a etapa 11.
6. Para um relatório de trabalho, de resumo do trabalho, de falha, resumido ou Core (clássico), selecione um intervalo de datas no menu suspenso **Intervalo de datas**.

   Se você não escolher um período, a opção padrão (Últimos 31 dias) será usada. Você pode escolher entre as opções da tabela a seguir.

Opção	Descrição
Últimas 24 horas	Relata a atividade do último dia, referente à hora em que você gera o relatório.
Últimos 7 dias	Relata a atividade da última semana, referente à hora em que você gera o relatório.
Últimos 31 dias	Reporta a atividade dos últimos 31 dias, relativo ao horário em que o relatório for gerado.

Opção	Descrição
Últimos 90 dias	Reporta a atividade dos últimos 90 dias, relativo ao horário em que o relatório for gerado.
Últimos 365 dias	Relata a atividade do último ano, referente à hora em que você gera o relatório.
A todo o momento	Esse período abrange a vida útil do Core.
Personalizado	Esse período requer que você especifique adicionalmente as datas inicial e final.
Mês até a data	Reporta a atividade do primeiro dia do mês atual até a data em que o relatório for gerado.
Ano até a data	Reporta a atividade do primeiro dia do ano atual até a data em que o relatório for gerado.

NOTE: Em todos os casos, não existem dados de relatório disponíveis anteriores a implantação do Core, ou de antes de as máquinas serem protegidas no Core.

7. Para um relatório de trabalho, de falhas ou Core (clássico), no menu suspenso **Cores de destino**, selecione um ou mais Cores para os quais você quer gerar um relatório.

   A seleção padrão contém todos os Cores disponíveis.

8. No menu suspenso **Máquinas protegidas**, selecione a máquina ou as máquinas para as quais você quer gerar o relatório.

   Por padrão, esse conjunto de informações contém os trabalhos de todas as máquinas, ou seja, todas as máquina protegidas, replicadas e de ponto de recuperação apenas, nos Cores especificados. Nos parâmetros do relatório, você pode personalizar o relatório. Use os filtros para selecionar ou excluir algumas máquinas. Você pode também selecionar ou excluir trabalhos que são independentes de máquina; nesse caso, o relatório mostrará apenas o status dos trabalhos do Core.

   Você pode selecionar dentre:

Opção	Descrição
Selecionar todos	Esta opção seleciona todas as máquinas protegidas neste Core. **NOTE:** Você pode selecionar todas as máquinas e, em seguida, apagar algumas seleções para especificar um subconjunto de todas as máquinas.
Independente de máquina	Selecione esta opção para gerar um relatório que contenha os trabalhos da perspectiva de um Core. Tipos de trabalho como criar ou apagar um repositório ou criar um CD de inicialização não estão associados a uma máquina específica. Se estiver implantando o software do agente em uma máquina ainda não protegida, esse tipo de trabalho também é considerado como independente de máquina. Esses trabalhos não mostram uma máquina protegida na coluna Máquina protegida do relatório resultante. Em contraste, se você implantar o software do agente em uma máquina já protegida no Core,

Opção	Descrição
	o nome da máquina protegida será incluída no relatório. Ela não é considerada independente de máquina.
Máquinas protegidas	Esta opção mostra as máquinas protegidas por este Core. Você pode selecionar todas ou um subconjunto de máquinas protegidas.
Apenas pontos de recuperação	Esta opção mostra as máquinas que já foram protegidas uma vez, mas que ainda têm pontos de recuperação salvos no repositório.
[Cores de origem]	Se o seu Core for um Core de destino e replica pontos de recuperação para quaisquer máquinas protegidas em um Core de origem, o nome do Core de origem é mostrado (com todas as letras maiúsculas). Esta opção mostra uma lista de todas as máquinas protegidas nesse Core de origem. Você pode selecionar todas as máquinas replicadas nesse Core de destino ou você pode selecionar um subconjunto.
[Grupos personalizados]	Se você tiver grupos personalizados criados nesse Core, o nome de cada grupo personalizado aparecerá como uma opção. Será exibido todos os objetos nesse grupo personalizado. Você pode selecionar todos os objetos no grupo ou um subconjunto deles.

9. Se for gerar um relatório resumido, vá para a etapa 12.
10. Para um relatório de falhas, de trabalho ou de resumo do trabalho, no menu suspenso **Tipos de trabalho**, selecione os tipos de trabalho adequados.

    Por padrão, esse conjunto de informações inclui todos os trabalhos para as máquinas protegidas selecionadas. Nos parâmetros do relatório, você pode personalizar o relatório. Use os filtros para selecionar ou excluir todos os trabalhos na categoria Principais trabalhos e todos os trabalhos na categoria Outros trabalhos. Ou você pode expandir cada uma dessas categorias ao definir parâmetros do trabalho e selecionar apenas os tipos de trabalho de cada categoria que você deseja que apareça no relatório. Clique na caixa de seleção de qualquer tipo de trabalho para marcá-lo ou desmarcá-lo. Você pode selecionar alguns ou todos os trabalhos de cada categoria.

    Você pode escolher um dos seguintes tipos de trabalho **outros**:
11. Para um relatório do repositório, no menu Repositórios, selecione o repositório ou os repositórios que você deseja incluir no relatório.

    A seleção padrão contém todos os repositórios disponíveis.
12. Clique em **Pré-visualizar** para gerar o relatório com os critérios especificados.

Se os critérios de relatório selecionados não forem encontrados, o relatório ainda assim será gerado, mas com uma linha vazia. Por exemplo, se não houver erros, o conteúdo da coluna Erro será null no relatório.

13. Execute um dos seguintes:
    - Visualize o relatório gerado on-line.
    - Atualize o relatório dinamicamente alterando um dos critérios e, em seguida, clique em **Pré-visualizar** novamente.
    - Use o **menu Relatórios** para selecionar um formato de exportação (incluindo o formato padrão, PDF) e clique em  para exportar o relatório. Para obter mais informações sobre o menu Relatórios, consulte Usar o menu de relatórios.
    - Use a **barra de ferramentas Relatórios** para visualizar, manipular ou imprimir o relatório. Para obter mais informações sobre a barra de ferramentas Relatórios, consulte Usar a barra de ferramentas Relatórios.

Gerar um relatório de máquina protegida sob demanda

Você pode gerar um Relatório do trabalho ou um Relatório de falhas para qualquer máquina protegida.

Execute as etapas do procedimento a seguir para gerar um relatório para uma máquina protegida.

1. Navegue até o Rapid Recovery Core Console.
2. No menu Máquinas protegidas, selecione a máquina protegida da qual você quer ver um relatório.

   A página **Resumo** da máquina selecionada é exibida.
3. Na parte superior da página, nas opções de menu ao lado do nome da máquina protegida, clique na seta virada para baixo próxima a Relatórios e selecione um tipo de relatório.
   - Se você quiser gerar um relatório de todos os trabalhos relacionados a essa máquina protegida, incluindo os trabalhos com falha, clique em **Relatório do trabalho** e comece a especificar os critérios do relatório.
   - Se você quiser gerar apenas uma lista de trabalhos com falhas relacionados a essa máquina protegida, clique em **Relatório de falhas** e comece a especificar os critérios do relatório.
4. Para um Relatório do trabalho ou de falhas, selecione um período no menu suspenso **Período**.

   Se você não escolher um período, a opção padrão (Últimos 31 dias) será usada. Você pode escolher entre as opções da tabela a seguir.

Opção	Descrição
Últimas 24 horas	Relata a atividade do último dia, referente à hora em que você gera o relatório.
Últimos 7 dias	Relata a atividade da última semana, referente à hora em que você gera o relatório.
Últimos 31 dias	Relata a atividade dos últimos 31 dias, referente à hora em que você gera o relatório.
Últimos 90 dias	Reporta a atividade dos últimos 90 dias, relativo ao horário em que o relatório for gerado.

Opção	Descrição
Últimos 365 dias	Relata a atividade do último ano, referente à hora em que você gera o relatório.
A todo o momento	Esse período abrange a vida útil do Core.
Personalizado	Esse período requer que você especifique adicionalmente as datas inicial e final.
Mês até a data	Reporta a atividade do primeiro dia do mês atual até a data em que o relatório for gerado.
Ano até a data	Reporta a atividade do primeiro dia do ano atual até a data em que o relatório for gerado.

NOTE: Em todos os casos, não existem dados de relatório disponíveis anteriores a implantação do Core, ou de antes de as máquinas serem protegidas no Core.

5. No menu suspenso **Tipos de trabalho**, selecione os tipos de trabalho adequados.

   Por padrão, esse conjunto de informações inclui todos os trabalhos para as máquinas protegidas selecionadas. Nos parâmetros do relatório, você pode personalizar o relatório. Use os filtros para selecionar ou excluir todos os trabalhos na categoria Principais trabalhos e todos os trabalhos na categoria Outros trabalhos. Ou você pode expandir cada uma dessas categorias ao definir parâmetros do trabalho e selecionar apenas os tipos de trabalho de cada categoria que você deseja que apareça no relatório. Clique na caixa de seleção de qualquer tipo de trabalho para marcá-lo ou desmarcá-lo. Você pode selecionar alguns ou todos os trabalhos de cada categoria.

6. Clique em **Pré-visualizar** para gerar o relatório com os critérios especificados.

   Se os critérios de relatório selecionados não forem encontrados, o relatório ainda assim será gerado, mas com uma linha vazia. Por exemplo, se não houver erros, o conteúdo da coluna Erro será null no relatório.

7. Execute um dos seguintes:
   - Visualize o relatório gerado on-line.
   - Atualize o relatório dinamicamente alterando um dos critérios e, em seguida, clique em **Pré-visualizar** novamente.
   - Use o menu **Relatórios** para selecionar um formato de exportação e exportar o relatório. Para obter mais informações sobre o menu Relatórios, consulte Usar o menu de relatórios.
   - Use a **barra de ferramentas Relatórios** para visualizar, manipular ou imprimir o relatório. Para obter mais informações sobre a barra de ferramentas Relatórios, consulte Usar a barra de ferramentas Relatórios.

Gerenciar relatórios programados no Core Console

Você pode programar qualquer um dos relatórios disponíveis a partir do Core Console. A programação de um relatório fará com que ele seja gerado repetidamente no futuro. A programação define se o relatório deve ser gerado diariamente, semanalmente ou mensalmente.

Como opção, o Rapid Recovery permite que você envie uma notificação de e-mail a um ou mais destinatários quando cada relatório for gerado. O e-mail especifica o tipo de relatório, o formato do relatório e o período, e inclui o relatório como um anexo.

NOTE: Antes de enviar os relatórios por e-mail, você precisa configurar um servidor SMTP para o Core. Para obter mais informações, consulte Configurar um servidor de e-mail.

Independentemente de optar pelo envio de notificações de e-mail, você pode salvar os relatórios gerados localmente ou em um local de rede acessível ao servidor Core.

Você precisa especificar uma notificação de e-mail e entrega, ou que você precisa especificar um local onde os relatórios serão salvos. Você pode também escolher as duas opções.

Esta seção inclui os seguintes tópicos:

- Programar um relatório
- Modificar a programação de um relatório
- Interromper, retomar ou excluir um relatório programado

Conceitos relacionados

See also: Interromper, retomar ou excluir um relatório programado

Tarefas relacionadas

See also: Programar um relatório
See also: Modificar a programação de um relatório

Programar um relatório

Você pode programar um relatório disponível a partir do Core Console. Em seguida, o relatório é gerado de acordo com a programação definida até que você pause ou apague o relatório.

Você precisa especificar uma notificação de e-mail e entrega, ou que você precisa especificar um local onde os relatórios serão salvos. Você pode também escolher as duas opções.

Execute as etapas deste procedimento para programar um relatório.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Reports** (Relatórios).

   A página **Relatório do trabalho** é mostrada. Um seta virada para baixo aparece à direita do atual nome do relatório.
3. Clique na seta à direita do nome do relatório e selecione **Relatórios programados** no menu suspenso.

   A página **Relatórios programados** é exibida.
4. Para programar um relatório a ser gerado regularmente, clique em **Add** (Adicionar).

   O **Assistente de definição do programa de relatório** é exibido.
5. Na página **Configuração** do assistente, digite os detalhes para o relatório que você deseja programar e, em seguida, clique em **Avançar**. As opções de configuração são descritas na tabela a seguir.

Tabela 112. Opções de configuração de relatório programado

Máquina	Relatórios disponíveis
Nome	Digite o nome de exibição que você quer atribuir a essa programação específica. O nome padrão é Agendar relatório 1. Limite o nome em 64 caracteres ou menos. Não use ou .

Máquina	Relatórios disponíveis
Formato do relatório	Selecione um formato de saída para o relatório. Se você não selecionar um valor, o formato padrão (pdf) será usado.
Tipo de relatório	Selecione o tipo de relatório que você quer gerar de forma regular.
Rótulos do patch	Selecione os rótulos que você quer que apareça no seu relatório programado. É preciso selecionar pelo menos um rótulo. O recurso Grupos personalizados permite que você agrupe objetos do Core em um contêiner lógico, para o qual você define um rótulo. Ao usar o parâmetro Rótulos no Assistente de definição do programa de relatório, você pode selecionar um grupo personalizado para o qual relatórios programados serão executados. Se não houver nenhum rótulo personalizado, as opções disponíveis no menu suspenso Rótulos são Selecionar todos e Máquinas protegidas. Se forem mostrados grupos personalizados, cada grupo aparece como uma opção. Você pode selecionar ou desmarcar qualquer uma das opções para incluir ou excluir esses objetos no relatório programado.
Máquina protegida	Selecione uma ou mais máquinas protegidas a serem incluídas no relatório. Esta opção não está disponível para o relatório do repositório.
Tipos de trabalho	Selecione os tipos de trabalho que você quer que apareça no relatório. Por padrão, esse conjunto de informações contém os trabalhos de todas as máquinas, ou seja, todas as máquina protegidas, replicadas e de ponto de recuperação apenas, nos Cores especificados. Nos parâmetros do relatório, você pode personalizar o relatório. Use os filtros para selecionar ou excluir algumas máquinas. Você pode também selecionar ou excluir trabalhos que são independentes de máquina; nesse caso, o relatório mostrará apenas o status dos trabalhos do Core. O parâmetro Tipos de trabalho não está disponível para os tipos de relatórios programados Resumo do Core e Repositório.

6. Na página **Destino** do assistente, selecione um destino para os relatórios que você deseja programar. Você precisa escolher uma ou ambas as opções a seguir. Quando estiver satisfeito, clique em **Avançar**.
   - No campo **Enviar para endereços de e-mail**, digite um ou mais endereços de e-mail válidos para notificar os usuários por mensagem de e-mail quando um relatório programado for gerado.

     NOTE: Se você não especificar as notificações de e-mail e a entrega, você precisará especificar um local de armazenamento.
   - Selecione **Salvar como arquivo** para salvar os arquivos do relatório gerado em um local que você especificar, e no menu suspenso **Tipo de local**, selecione uma opção de local, rede ou armazenamento na nuvem. Em seguida, no campo **Local**, especifique as informações adicionais de local conforme descrito na tabela a seguir.

Tabela 113. Opções de Local para relatórios programados

Tipo de local	Descrição do tipo de local	Local
Local	Selecione o tipo de local Local para salvar os relatórios gerados em um caminho local que o Core pode acessar.	Especifique o caminho no campo Local. Digite um local acessível ao Core localmente.

Tipo de local	Descrição do tipo de local	Local
		Por exemplo, para armazenar relatórios na pasta Relatórios da unidade D, digite `D:\Relatórios\`.
Rede	Selecione o tipo de local Rede para salvar os relatórios gerados em um caminho que o Core pode acessar na rede. Especifique o caminho no campo Local.	Especifique o caminho no campo Local. Digite um local acessível ao Core na rede. Use o formato \\servername\sharename. Por exemplo, para armazenar relatórios sobre o servidor de dados na pasta compartilhada chamada Relatórios, digite `\\Data\Relatórios\`. Especifique as credenciais de rede nos campos Nome de usuário e Senha.
Nuvem	Selecione o tipo de local Nuvem para salvar os relatórios gerados em uma conta de armazenamento na nuvem configurada no Core. A conta de armazenamento já deve estar definida antes de executar esta etapa. Para obter informações sobre como configurar uma conta de armazenamento na nuvem para funcionar com o Core, consulte Contas de nuvem.	No campo Conta, selecione a conta de armazenamento na nuvem para usá-la para armazenar os relatórios gerados. No campo Contêiner, especifique um contêiner adequado na conta de armazenamento. No campo Nome da pasta, especifique a pasta onde os relatórios gerados futuros devem ser armazenados.

7. Quando estiver satisfeito com as opções de destino, clique em **Avançar**.
8. Na página **Programa** do assistente, no menu **Enviar dados**, selecione uma opção para determinar com que frequência o relatório especificado deve ser gerado. Você pode gerar relatórios diariamente, semanalmente ou mensalmente. Cada opção tem seus próprios parâmetros, conforme descrito na tabela a seguir.

Tabela 114. Opções de frequência para a geração dos relatórios programados

Frequência	Detalhes de frequência	Parâmetros de frequência
Diariamente	Gera e salva ou envia o relatório especificado uma vez por dia no horário definido. O horário padrão para esta ação é 12:00 (com base na hora do servidor do Core).	Para alterar o horário padrão que o relatório é gerado, no campo de texto de hora, digite um novo valor ou use os controles para alterar a hora, os minutos e AM ou PM.
Semanalmente	Gera e salva ou envia o relatório especificado uma vez por semana no horário e dia definidos. O horário padrão para esta ação é domingo às 12:00 (com base na hora do servidor do Core).	Para alterar o dia padrão que o relatório é gerado, no menu do dia da semana, selecione um dia da semana. Para alterar o horário padrão que o relatório é gerado, no campo de texto de hora, digite um novo valor ou use os controles para alterar a hora, os minutos e AM ou PM.
Mensalmente	Gera e salva ou envia o relatório especificado uma vez por mês na data e horário definidos.	Para alterar a data padrão que o relatório é gerado, no menu do dia do mês, selecione uma data.

Frequência	Detalhes de frequência	Parâmetros de frequência
	A data padrão para esta ação é o primeiro dia de cada mês às 12:00 (com base na hora do servidor do Core).	Para alterar o horário padrão que o relatório é gerado, no campo de texto de hora, digite um novo valor ou use os controles para alterar a hora, os minutos e AM ou PM.

9. Opcionalmente, na página **Programa** do assistente, se você quiser impedir que o relatório programado seja gerado até que você retome os relatórios pausados, selecione **Pausar geração de relatórios inicialmente**.

   Se você quiser que este relatório seja gerado conforme programado, desmarque essa opção.

10. Quando estiver satisfeito com o programa, clique em **Concluir** para sair do assistente e salve o trabalho.

    O novo programa de relatório é mostrado na tabela de resumo Relatórios resumidos.

Modificar a programação de um relatório

Depois que um relatório está programado, você pode modificar qualquer um de seus parâmetros ou detalhes. Você pode editar as informações de configuração do relatório (nome do relatório, formato de saída, tipo de relatório, repositórios incluídos. Você pode também alterar as opções de notificação por e-mail e o destino em que o relatório gerado será salvo. Por fim, você pode também alterar a programação do relatório.

Execute este procedimento para modificar os parâmetros de um relatório programado.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione **Reports** (Relatórios).

   A página **Relatório do trabalho** é mostrada. Um seta virada para baixo aparece à direita do atual nome do relatório.

3. Clique na seta à direita do nome do relatório e selecione **Relatórios programados** no menu suspenso.

   A página **Relatórios programados** é exibida.

4. Na tabela de resumo Relatórios programados, na linha do relatório que você quer modificar, clique no ícone (Mais opções) e selecione **Edit** (Editar).

   O **Assistente de definição do programa de relatório** é exibido.

5. Navegue pelas páginas desse assistente, alterando todos os parâmetros necessários. Para obter informações sobre algum parâmetro deste assistente, consulte o tópico Programar um relatório.
6. Na página **Programa** do assistente, clique em **Concluir** para fechar o assistente e salvar as alterações.

   O assistente irá fechar e a programação do relatório estará modificado.

Interromper, retomar ou excluir um relatório programado

Depois de programar um relatório, ele será gerado conforme a programação definida. Se você quiser interromper temporariamente a geração de um relatório programado, você pode pausar a programação.

Se um relatório programado estiver pausado e você desejar retomar a geração do relatório, você pode retomar o relatório conforme descrito neste procedimento.

Se um relatório programado estiver sendo gerado e você já não precisa dele, você pode apagá-lo.

Para determinar se um relatório programado está pausado, verifique a coluna status da tabela de resumo de relatórios programados. Uma esfera verde indica um relatório programado ativo; uma esfera amarela indica uma programação pausada; e uma esfera vermelha indica um erro.

Execute as etapas deste procedimento para pausar, retomar ou excluir uma programação de um relatório.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Mais) e, em seguida, selecione (Mais) **Reports** (Relatórios).

   A página **Relatório do trabalho** é mostrada. Um seta virada para baixo aparece à direita do atual nome do relatório.
3. Clique na seta à direita do nome do relatório e selecione **Relatórios programados** no menu suspenso.

   A página **Relatórios programados** é exibida.
4. Na tabela de resumo Relatórios programados, veja o status de todos os relatórios programados por meio dos indicadores coloridos.
5. Para cada relatório que você quiser pausar ou retomar, selecione a caixa de verificação na primeira coluna.
6. A partir das opções dos Relatórios programados acima da tabela de resumo, você pode fazer o seguinte:
   - Para pausar a geração dos relatórios selecionados, clique em **Pausar**.
   - Para retomar a geração de relatórios programados anteriormente pausados, clique em **Retomar**.
   - Para apagar as programações selecionadas de relatórios programados existentes, clique em **Excluir**.

     Apagar um relatório programado apenas impede a geração de futuros relatórios. Relatórios programados salvos anteriormente não são removidos.

Usar o menu de relatórios

O menu Relatórios aparece na parte superior da página ao exibir os relatórios. Este menu inclui o título do relatório, o qual também é um menu suspenso que permite que você veja quais tipos de relatório estão disponíveis. Abaixo deste menu há um ou mais filtros que ajudam você a definir seus critérios de relatório.

Os filtros específicos disponíveis dependem do tipo de relatório. Para obter informações sobre os parâmetros que se aplicam a cada tipo de relatório, consulte o respectivo tópico para entender esse tipo de relatório.

No lado direito do menu de relatórios, são exibidos alguns controles. Estes controles, descritos na tabela a seguir, ajudam você a gerar e exportar o relatório.

Tabela 115. Controles do menu de relatórios

Elemento de UI	Descrição
Botão de pré-visualização	Clique no botão de pré-visualização para gerar um relatório com base no tipo de relatório selecionado e nos parâmetros de relatório especificados nos filtros.
Menu suspenso para o formato de exportação	O menu suspenso Exportar permite que você selecione um formato de saída para o relatório. Se você não selecionar um valor, o formato padrão (pdf) será usado.
Botão/ícone de download	O botão de download exporta o relatório gerado no tipo de formato selecionado no menu Exportar.

Os relatórios incluem as unidades de medida, o que torna mais fácil determinar se uma coluna é representada em GB, TB ou segundos.

Se você não estiver satisfeito com a aparência de um relatório gerado ou exportado, você pode alterar a fonte usada nos relatórios. Para obter mais informações, consulte Gerenciamento de definições de relatórios.

Depois que um relatório é gerado, você pode usar a barra de ferramentas dos relatórios.

See also: Noções básicas sobre o relatório do trabalho
See also: Noções básicas sobre o relatório de falhas
See also: Noções básicas sobre o relatório resumido

Usar a barra de ferramentas Relatórios

Depois de gerá-lo a partir do menu Relatórios, o relatório é mostrado abaixo da barra de ferramentas Relatórios. A barra de ferramentas pode ajudar a manipular a saída do relatório, incluindo salvar e imprimir os relatórios.

No lado esquerdo da barra de ferramentas, há uma opção de barra lateral Alternar. Essa ferramenta expande ou encolhe a barra lateral, dando acesso a mais algumas opções de vídeo. À direita da barra de ferramentas, a opção Ferramentas expande um menu suspenso fornecendo os controles de navegação do relatório. Os elementos da barra de ferramentas Relatórios são descritos na tabela a seguir.

Tabela 116. Ícones da barra de ferramentas de relatórios

Ícone	Descrição
	**Barra lateral Alternar**. Todas as páginas do relatório são exibidas como miniaturas. Outras opções na barra lateral não são suportadas.
	**Barra lateral: Mostrar miniaturas**. Esta é a exibição padrão para todas as páginas de um relatório gerado.
	**Barra lateral: Mostrar estrutura de tópicos do documento**. Esse recurso não é suportado.
	**Barra lateral: Mostrar anexos**. Não há anexos para relatórios. Esse recurso não é suportado.
	**Procurar**. Permite que você pesquise um texto dentro do relatório gerado. Inclui opções para destacar todos os textos que correspondem aos critérios inseridos, e também coincidir ou não maiúsculas e minúsculas.
	**Página anterior**. Move a visualização do relatório para a página anterior.
	**Próxima página**. Segue para a próxima página na visualização do relatório.
	**Inserir o número da página**. Clique no campo de texto do número da página, digite um número de página válido e, em seguida, pressione Enter para ir até essa página na visualização do relatório.
	**Diminuir o zoom**. Permite que você diminua o zoom da visualização do relatório gerado. Cada clique sucessivo afasta ainda mais o zoom, até um mínimo de 25%.
	**Aumentar o zoom**. Permite que você aumente o zoom da visualização do relatório gerado. Cada clique sucessivo aproxima ainda mais o zoom, até um máximo de 1000%.

Ícone	Descrição
	**Zoom automático**. Permite que você controle a exibição do zoom do relatório gerado, incluindo visualizar no tamanho real, ajustar à página, largura total ou por porcentagem, incluindo 50%, 75%, 100%, 125%, 150%, 200%, 300% ou 400%.
	**Abrir arquivo**. Permite que você navegue no sistema de arquivos para localizar e abrir um relatório salvo.
	**Imprimir**. Permite imprimir o relatório gerado.
	**Ferramentas**. O menu suspenso Ferramentas expande ou retrai ao clicar neste ícone. As opções de Ferramentas estão descritas abaixo.
	**Ferramentas: Ir para a primeira página**. Leva você para a primeira página do relatório gerado.
	**Ferramentas: Ir para a última página**. Leva você para a última página do relatório gerado.
	**Ferramentas: Girar no sentido horário**. Esta opção gira a tela do relatório gerado no sentido horário.
	**Ferramentas: Girar no sentido anti-horário**. Esta opção gira a tela do relatório gerado no sentido anti-horário.
	**Ferramentas: Ferramenta de mão**. Ao selecionar esta ferramenta, permite que você mova o relatório ao clicar e arrastar ele pela tela.
	**Ferramentas: Propriedades do documento**. Fornece informações sobre as propriedades do documento do relatório gerado. Clique em **Fechar** para fechar esta janela.

Para obter informações sobre como gerar um relatório, consulte Gerar um relatório no Core Console.

Noções básicas sobre o relatório do trabalho

O Relatório do trabalho está disponível para o Rapid Recovery Core e para as máquinas protegidas no Core. Ele fornece uma maneira de visualizar o status dos trabalhos realizados por um Core ou uma máquina protegida selecionado. Linhas ou colunas de dados no relatório sem dados indicam que o parâmetro testado estava null. Por exemplo, se uma coluna (por exemplo, Erros) aparece sem qualquer informação, então não ocorreram erros para o registro selecionado. Se o relatório gera uma linha em branco, o trabalho para o registro selecionado reflete a atividade independente da máquina.

Para obter informações sobre como gerar um relatório do trabalho a partir do Core, consulte Gerar um relatório de Core sob demanda. Para obter informações sobre como gerar um relatório do trabalho para uma máquina protegida, consulte Gerar um relatório de máquina protegida sob demanda.

Ao gerar um relatório do trabalho, os detalhes do relatório são os seguintes:

- Critérios de seleção do relatório
- Uma tabela de resumo que mostra uma linha para cada trabalho no período especificado. Além de apresentar o Core, a máquina protegida e o tipo de trabalho adequados, cada linha contém:
  - Um resumo do trabalho
  - O status do trabalho
  - Todos os erros relacionados com o trabalho
  - As datas de início e término do trabalho
  - A duração do trabalho em segundos
  - O trabalho total em MB

Se as informações não forem relevantes para uma determinada categoria, essa célula será mostrada no relatório sem informações. Por exemplo, se o Core de uma determinada máquina protegida não contiver erros, a coluna Erro ficará em branco para essa linha do relatório.

Noções básicas sobre o relatório de resumo dos trabalhos

O relatório de resumo dos trabalhos está disponível ao reportar da perspectiva do Core apenas; este relatório não está disponível a partir dos relatórios de uma máquina protegida. Este relatório tem um resumo único, mostrando informações resumidas sobre todos os trabalhos executados no Core, incluindo uma contagem de trabalhos com falha, concluídos e cancelados. Ele mostra mais detalhes do que o relatório do trabalho, pois especifica cada trabalho como uma linha separada no relatório.

Para obter informações sobre como gerar um relatório de resumo dos trabalhos, consulte Gerar um relatório no Core Console.

Os parâmetros do relatório para esse tipo de relatório são:

- Período
- Máquinas protegidas
- Tipos de trabalho

Ao gerar um relatório de resumo dos trabalhos, os detalhes do relatório contêm os critérios de seleção para o relatório, bem como informações sobre máquinas protegidas, volumes e tipos de trabalho.

Informações do Core

A parte do Relatório resumido referente ao Core contém dados em relação ao Rapid Recovery Core que está sendo reportado. Essas informações incluem:

- O número de máquinas protegidas no Rapid Recovery Core
- O número de máquinas com trabalhos com falha

Resumo das máquinas protegidas

A parte do Relatório resumido referente às máquinas protegidas contém dados de todas as máquinas protegidas pelos Rapid Recovery Core selecionados e os volumes nessas máquinas.

A tabela mostra uma linha para cada tipo de trabalho de cada máquina, e contém a proporção de trabalhos bem-sucedidos (de qualquer tipo), o número de trabalhos concluídos, o número de trabalhos com falha e o número de trabalhos cancelados. (Os trabalhos cancelados não são considerados nessas estatísticas.)

Noções básicas sobre o relatório de falhas

O Relatório de falhas é um subconjunto do Relatório do trabalho e está disponível para o Rapid Recovery Core e para as máquinas protegidas no Core. O Relatório de falhas contém apenas os trabalhos cancelados e com falha relacionados no Relatório do trabalho e os compila em um único relatório que pode ser impresso e exportado. Se o relatório for gerado com uma linha em branco, não houve erros no período especificado nos critérios de relatório.

NOTE: Os resultados para os parâmetros de máquinas protegidas e Cores de destino aparecem apenas no relatório do nível do Core.

Para obter informações sobre como gerar um relatório do trabalho a partir do Core, consulte Gerar um relatório de Core sob demanda. Para obter informações sobre como gerar um relatório do trabalho para uma máquina protegida, consulte Gerar um relatório de máquina protegida sob demanda.

Ao gerar um Relatório de falhas, uma tabela de resumo que mostra uma linha para cada trabalho no período especificado. Além de apresentar o Core, a máquina protegida e o tipo de trabalho adequados, cada linha contém:

- Um resumo do trabalho
- O status do trabalho
- Todos os erros relacionados com o trabalho
- As datas de início e término do trabalho
- A duração do trabalho em segundos
- O trabalho total em MB

Noções básicas sobre o relatório resumido

O Relatório resumido está disponível para um ou mais Cores. Este relatório não está disponível entre relatórios de uma máquina protegida. O relatório resumido inclui informações sobre os repositórios no Rapid Recovery Core selecionado e as máquinas protegidas por esse Core. As informações aparecem como dois resumos dentro de um relatório.

Para obter informações sobre como gerar um Relatório resumido, consulte Gerar um relatório no Core Console.

Os parâmetros do relatório para esse tipo de relatório são:

- Período
- Máquinas protegidas

Ao gerar um Relatório resumido, os detalhes do relatório contêm os critérios de seleção para o relatório, bem como informações sobre repositórios e máquinas protegidas.

Informações do Core

A parte do Relatório resumido referente ao Core contém dados em relação ao Rapid Recovery Core que está sendo reportado. Essas informações incluem:

- A chave de licença (identificador)
- A versão atual do software Rapid Recovery Core

Resumo de repositórios

A parte do Relatório resumido referente aos Repositórios contém dados dos repositórios localizados no Rapid Recovery Core selecionado. Essas informações incluem:

- O número de repositórios no Rapid Recovery Core
- Um resumo dos repositórios no Core.

Resumo das máquinas protegidas

A parte do Relatório resumido referente às máquinas protegidas contém dados de todas as máquinas protegidas pelo(s) Rapid Recovery Core(s) selecionados. Inclui um gráfico e uma tabela de resumo.

A tabela mostra as máquinas protegidas na proporção de trabalhos bem-sucedidos (de qualquer tipo), em comparação aos trabalhos com falha. (Os trabalhos cancelados não são considerados nessas estatísticas.)

O X ou eixo horizontal mostra o número de máquinas protegidas. O Y ou eixo vertical mostra as camadas de sucesso. Especificamente, o eixo Y mostra, por máquina protegida, as quantidades:

- Não foram realizados trabalhos
- Menos de 50% bem-sucedidos
- 50% ou mais bem-sucedidos
- 100% bem-sucedidos

Abaixo do gráfico, são mostradas informações sobre as máquinas protegidas. Essas informações incluem:

- A quantidade de máquinas protegidas
- O número de máquinas protegidas com trabalhos com falha
- Uma tabela de resumo por máquina protegida, que mostra:
  - Nome da máquina protegida
  - Os volumes protegidos pela máquina
  - Espaço protegido, em GB (total e atual)
  - Taxa de alteração diária (média e mediana)
  - Estatísticas do trabalho (bem-sucedidos, concluídos, com falha, cancelados)
  - Se a criptografia foi aplicada
- A versão do Core

Noções básicas sobre o relatório do Repositório

O relatório do Repositório inclui informações sobre os repositórios no Rapid Recovery Core selecionado e as máquinas protegidas por esse Core. As informações aparecem como dois resumos dentro de um relatório.

Para obter informações sobre como gerar um relatório do Repositório do Core, consulte Gerar um relatório de Core sob demanda.

Os parâmetros para esse tipo de relatório incluem somente repositórios.

Ao gerar um relatório de repositório, os detalhes do relatório para cada repositório contêm uma lista de resumo dos repositórios no Core.

Noções básicas sobre o relatório de resumo clássico

O relatório de resumo clássico fornece um resumo sobre o período selecionado para uma variedade de métricas úteis para o seu Core.

A parte superior inclui três gráficos de pizza. O primeiro mostra as estatísticas do trabalho (trabalhos bem-sucedidos, cancelados e com falha). O segundo gráfico de pizza mostra o espaço por repositório em GB. O terceiro gráfico de pizza exibe estatísticas de instantâneo (trabalhos bem-sucedidos, cancelados e com falha).

Em seguida, há um gráfico de tendência que mostra o uso do repositório.

Por fim, o relatório inclui um resumo das máquinas protegidas.

Os parâmetros de relatório para este tipo de relatório contêm um intervalo de datas e o Core relevante.

Para obter informações sobre como gerar esse relatório a partir do Core, consulte Gerar um relatório de Core sob demanda.

Exportação da VM

Esta seção explica como exportar um ponto de recuperação para criar uma máquina virtual.

Exportação para máquinas virtuais usando o Rapid Recovery

A partir do Rapid Recovery Core, é possível exportar um ponto de recuperação de um computador com Windows ou Linux para uma máquina virtual (VM) em um dos vários formatos suportados. Se a máquina original protegida no Core falhar, você pode inicializar a máquina virtual para substitui-la temporariamente de forma rápida, dando a você tempo para recuperar a máquina protegida original sem tempo de inatividade substancial. Esse processo de exportação virtual resulta em uma VM com todas as informações de backup de um ponto de recuperação, bem como o sistema operacional e as definições da máquina protegida. A VM se torna um clone inicializável da máquina protegida.

NOTE: O ponto de recuperação utilizado deve fazer parte de uma cadeia completa de pontos de recuperação. Para obter mais informações sobre cadeias de pontos de recuperação, consulte o tópico Cadeias de pontos de recuperação e órfãos.

Você pode realizar uma exportação virtual a partir da página **Standby virtual** do Core Console; a partir de um ponto de recuperação específico exibido no Core; ou selecionando **Exportação do VM** no menu suspenso **Restaurar** da barra de botões.

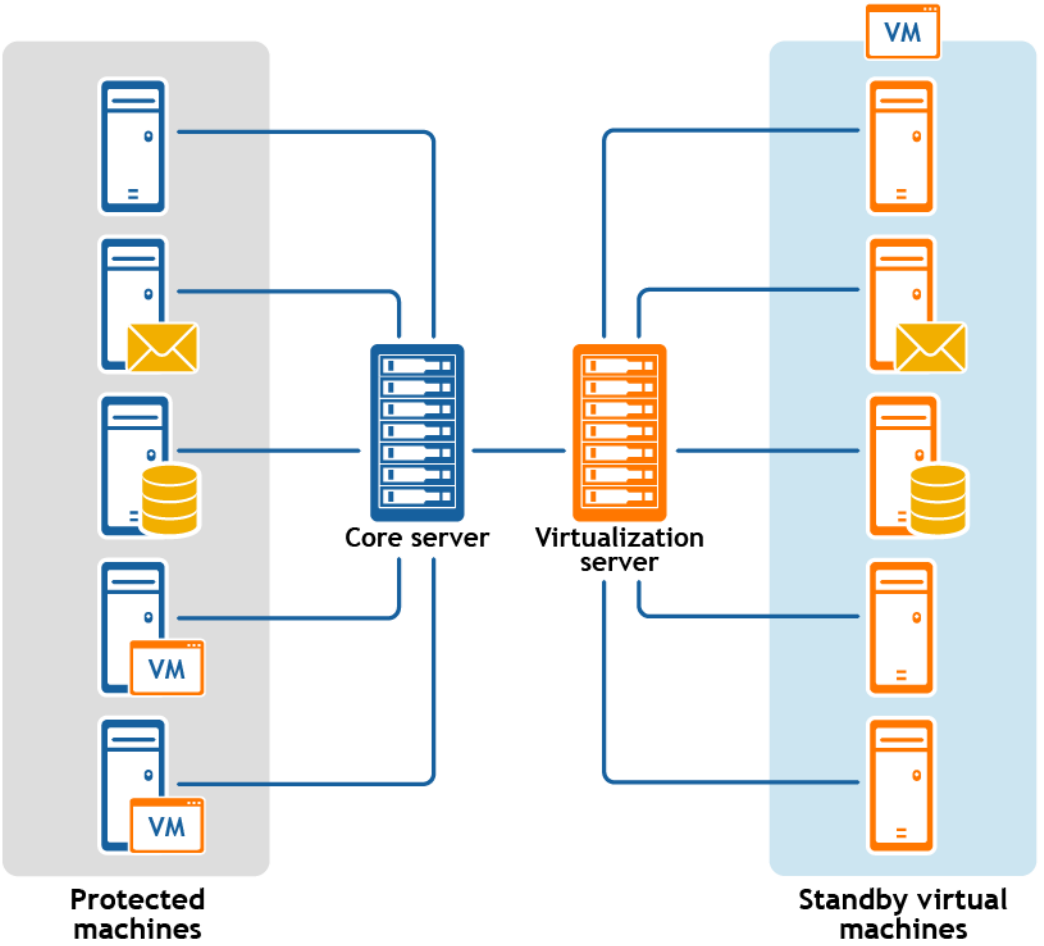
Ao realizar uma exportação virtual no Rapid Recovery Core, você tem duas opções:

- Você pode realizar uma **exportação virtual única**, que cria uma VM inicializável que representa um único snapshot das informações do ponto de recuperação selecionado. O trabalho de exportação é imediatamente colocado na fila e, ao ser concluído, a VM clonada é exportada para o local especificado. As informações de configuração usadas para uma exportação única não são salvas.
- Você pode configurar uma **exportação contínua**. Este processo cria uma VM inicializável do ponto de recuperação original especificado, salvando a VM em um local que você especificar. As informações de configuração para a execução dessa exportação virtual são salvas na página **Standby virtual** do Core Console. De modo subsequente, sempre que for capturado um novo instantâneo da máquina protegida, o Core enfileira um novo trabalho de exportação virtual e a VM inicializável é atualizada com as informações atualizadas. Como isso cria um recurso de alta disponibilidade para recuperação de dados, este recurso é chamado também de **Standby virtual**.

Entre o momento em que um trabalho de exportação virtual é enfileirado e é concluído, o trabalho fica listado no painel Fila de exportação da página Standby virtual no Core Console.

O diagrama a seguir mostra uma implementação típica de exportação de dados para uma máquina virtual.

Figura 5. Implementação de standby virtual



NOTE: Em uma configuração que envolve replicação, o Core mostrado representa o Core de destino. Se a replicação estiver definida entre dois Cores (origem e destino), será possível exportar dados do Core de destino apenas após a replicação inicial estar concluída.

Os hipervisores de VM compatíveis são vCenter/ESXi, VMware Workstation, Hyper-V, VirtualBox e Azure. Para obter informações sobre as versões aceitas desses hipervisores, consulte o tópico "Requisitos do hipervisor" no *Guia de requisitos do sistema do Rapid Recovery*.

Para ESXi, VMware Workstation ou Hyper-V, a versão da máquina virtual deve ser uma versão licenciada dessas máquinas virtuais, não as versões gratuitas ou de teste. A exportação para o Azure exige que você tenha uma conta no Azure, com outros pré-requisitos.

NOTE: Para o Azure, a exportação e a eventual implantação criam uma VM usando o gerenciamento de VM clássico e não o modelo de gerenciador de recursos mais recente. O trabalho com o Azure envolve aspectos únicos a esse provedor de serviços de nuvem. Para obter mais informações, consulte Antes da exportação virtual para o Azure.

Conceitos relacionados

See also: Exportar dados para uma máquina virtual ESXi
See also: Exportar dados para uma máquina virtual VMWare Workstation
See also: Exportar dados para uma máquina virtual VirtualBox
See also: Exportar dados para uma máquina virtual Azure

Tarefas relacionadas

See also: Gerenciar exportações

Referências relacionadas

See also: Exportar dados para uma máquina virtual Hyper-V

Exportar dados para uma máquina virtual ESXi

No Rapid Recovery, você pode exportar dados para ESXi realizando uma exportação única ou estabelecendo uma exportação contínua (para standby virtual). Execute as etapas dos procedimentos a seguir do tipo apropriado de exportação.

Realizar uma exportação única para ESXi

Execute as etapas deste procedimento para realizar uma exportação única para o ESXi.

1. No Rapid Recovery Core Console, na barra de botões, clique no menu suspenso **Restaurar** e em **Exportação do VM**.
2. No Assistente de exportação de máquina virtual, selecione **Exportação única**.
3. Clique em **Avançar**.
4. Na página Máquinas, selecione a máquina protegida que você deseja exportar.
5. Clique em **Avançar**.
6. Na página Pontos de recuperação, selecione o ponto de recuperação que você deseja usar na exportação.
7. Clique em **Avançar**.
8. Na página **Destino** do Assistente de exportação, no menu suspenso Exportar para uma máquina virtual, selecione **ESX(i)**.
9. Insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir e clique em **Avançar**.

Tabela 117. Parâmetros da máquina virtual

Opções	Descrição
Nome do host	Insira um nome para a máquina de host.
Porta	Insira a porta para a máquina de host. O padrão é 443.
Nome de usuário	Insira o nome de usuário de login na máquina de host.
Senha	Digite a senha de login na máquina de host.

10. Na página Opções de máquina virtual, insira as informações conforme descrito na tabela a seguir.

Tabela 118. Opções da máquina virtual

Opção	Descrição
Conjunto de recursos	Selecione um conjunto de recursos na lista suspensa.

Opção	Descrição
Local da configuração de VM	Selecione um armazenamento de dados na lista suspensa.
Nome da máquina virtual	Digite um nome para a máquina virtual.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • Usar a mesma quantidade de RAM da máquina de origem • Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.
Número de processadores	O número de processadores (CPUs) que você quer para a máquina virtual exportada. O valor mínimo é 1.
Cores por processador	O número de cores que você quer ter para cada processador. O valor mínimo é 1.
Aprovisionamento de disco	Selecione o tipo de aprovisionamento de disco das seguintes opções: • Thin (Dinâmico). O aprovisionamento dinâmico cria um disco virtual do tamanho do espaço usado nos volumes originais, em vez de todo o tamanho do volume. Por exemplo, se o volume original é de 1 TB, mas contém somente 2 GB de espaço usado, o Rapid Recovery cria um disco virtual de 2 GB. • Tradicional. O aprovisionamento tradicional cria um novo disco ou volume com o mesmo tamanho do volume original do servidor protegido, mesmo que somente uma parte do volume original esteja em uso. Por exemplo, caso o volume seja 1 TB, mas contém apenas 2 GB de espaço usado, o Rapid Recovery cria um disco virtual de 1 TB.
Mapeamento de disco	Especifique o tipo de mapeamento de disco nas seguintes opções: • Automático • Manual • Com VM
Versão	Selecione a versão do ESXi usado para criar a máquina virtual na lista suspensa.

11. Clique em **Avançar**.
12. Na página **Volumes**, selecione os volumes que deseja exportar e clique em **Avançar**.
13. Na página **Resumo**, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTE: Você pode monitorar o status e o progresso da exportação visualizando as páginas **Standby virtual** e **Eventos**.

Configurar a exportação contínua para ESXi

Conclua as etapas nesse procedimento para configurar uma exportação contínua para uma máquina virtual (VM) ESXi usando o Rapid Recovery. Também conhecida como configuração de standby virtual.

1. No Rapid Recovery Core Console, realize um dos procedimentos a seguir:

   - Na barra de botões do Core Console, clique no menu suspenso the **Restore** (Restaurar) e, em seguida, selecione **VM Export** (Exportação de VM).

     1. No Assistente de exportação de máquina virtual, selecione **Contínuo (Standby Virtual)**.
     2. Clique em **Avançar.**

   - Na barra de ícones do Core Console, clique em (Standby virtual).

     - Na página **Standby virtual**, clique em **Adicionar** para iniciar o Assistente de exportação de máquina virtual.

2. Na página **Máquinas** do Assistente de exportação de máquina virtual, selecione a máquina protegida que você deseja exportar.
3. Clique em **Avançar**.
4. Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar para a exportação.
5. Clique em **Avançar**.
6. Na página **Destino** do Assistente de exportação, no menu suspenso Recuperar para uma máquina virtual, selecione **ESXi**.
7. Insira as informações para acessar a máquina virtual, conforme descrito na tabela a seguir, e clique em **Avançar**.

Tabela 119. Credenciais de ESXi

Opção	Descrição
Nome do host	Insira um nome para a máquina de host.
Porta	Insira a porta para a máquina de host. O padrão é 443.
Nome de usuário	Insira as credenciais de login para a máquina de host.
Senha	Insira as credenciais de login para a máquina de host.

8. Na página **Opções de máquina virtual**, insira as informações conforme descrito na tabela a seguir.

Tabela 120. Opções da máquina virtual

Opção	Descrição
Conjunto de recursos	Selecione um conjunto de recursos na lista suspensa.
Armazenamento de dados	Selecione um armazenamento de dados na lista suspensa.
Nome da máquina virtual	Insira um nome para a máquina virtual.

Opção	Descrição
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • Usar a mesma quantidade de RAM da máquina de origem • Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.
Número de processadores	O número de processadores (CPUs) que você quer para a máquina virtual exportada. O valor mínimo é 1.
Cores por processador	O número de cores que você quer ter para cada processador. O valor mínimo é 1.
Aprovisionamento de disco	Selecione o tipo de aprovisionamento de disco das seguintes opções: • Thin (Dinâmico). O aprovisionamento dinâmico cria um disco virtual do tamanho do espaço usado nos volumes originais, em vez de todo o tamanho do volume. Por exemplo, se o volume original é de 1 TB, mas contém somente 2 GB de espaço usado, o Rapid Recovery cria um disco virtual de 2 GB. • Tradicional. O aprovisionamento tradicional cria um novo disco ou volume com o mesmo tamanho do volume original do servidor protegido, mesmo que somente uma parte do volume original esteja em uso. Por exemplo, se o volume original é de 1 TB, mas contém 2 GB de espaço usado, o Rapid Recovery cria um disco virtual de 1 TB.
Mapeamento de disco	Especifique o tipo de mapeamento de disco conforme adequado (Automático, Manual ou com VM).
Versão	Selecione a versão da máquina virtual.
Realizar a exportação única inicial	Selecione para realizar a exportação virtual imediatamente em vez de após o próximo snapshot programado (opcional)

9. Clique em **Avançar**.
10. Na página **Volumes**, selecione os volumes que deseja exportar e clique em **Avançar**.
11. Na página **Resumo**, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTE: Você pode monitorar o status e o progresso da exportação visualizando as páginas Standby virtual e Eventos.

Exportar dados para uma máquina virtual VMWare Workstation

No Rapid Recovery, é possível exportar dados para o VMWare Workstation realizando uma exportação única ou estabelecendo uma exportação contínua (para Standby virtual). Execute as etapas dos procedimentos a seguir do tipo apropriado de exportação.

Realizar uma exportação única para VMware Workstation

Execute as etapas deste procedimento para realizar uma exportação única para VMware Workstation.

1. No Console do Rapid Recovery Core, na barra de botões, clique no menu suspenso **Restaurar**, clique em **Exportação do VM**.
2. No Assistente de exportação de máquina virtual, selecione **Exportação única**.
3. Clique em **Avançar**.
4. Na página **Máquinas**, selecione a máquina protegida que você deseja exportar.
5. Clique em **Avançar**.
6. Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar para a exportação.
7. Clique em **Avançar**.
8. Na página **Destino** do Assistente de exportação, no menu suspenso Exportar para uma máquina virtual, selecione **VMware Workstation** e clique em **Avançar**.
9. Na página **Opções de máquina virtual**, insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Tabela 121. Parâmetros da máquina virtual

Opção	Descrição
Local da máquina de VM	Especifique o caminho da pasta local ou compartilhamento de rede no qual você deseja criar a máquina virtual. **NOTE:** Se você especificou um caminho de compartilhamento de rede, será preciso inserir credenciais de login válidas para uma conta que está registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.
Nome de usuário	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir um nome de usuário válido para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, um nome de usuário não é necessário.
Senha	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir uma senha válida para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, uma senha não é necessária.
Nome de VM	Insira um nome para a máquina virtual sendo criada, por exemplo, VM-0A1B2C3D4. **NOTE:** O nome padrão é o nome da máquina de origem.

Opção	Descrição
Versão	Especifique a versão do VMware Workstation da máquina virtual. Você pode selecionar dentre: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0 • VMware Workstation 11.0 • VMware Workstation 12.0
Quantidade de RAM (MB)	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • Usar a mesma quantidade de RAM da máquina de origem • Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.
Número de processadores	O número de processadores (CPUs) que você quer para a máquina virtual exportada. O valor mínimo é 1.
Cores por processador	O número de cores que você quer ter para cada processador. O valor mínimo é 1.

10. Clique em **Avançar**.
11. Na página **Volumes**, selecione os volumes para exportar, por exemplo, C:\ e D:\, e clique em **Avançar**.
12. Na página **Resumo**, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTE: Você pode monitorar o status e o progresso da exportação visualizando as páginas **Standby virtual** e **Eventos**.

Configurar a exportação contínua para VMware Workstation

Conclua as etapas nesse procedimento para configurar uma exportação contínua para uma máquina virtual (VM) VMware Workstation usando o Rapid Recovery. Também conhecida como configuração de standby virtual.

1. No Rapid Recovery Core Console, realize um dos procedimentos a seguir:
   - Na barra de botões do Core Console, clique no menu suspenso the **Restore** (Restaurar) e, em seguida, selecione **VM Export** (Exportação de VM).
     1. No Assistente de exportação de máquina virtual, selecione **Contínuo (Standby Virtual)**.

2. Clique em **Avançar.**

- Na barra de ícones do Core Console, clique em (Standby virtual).
  - Na página **Standby virtual**, clique em **Adicionar** para iniciar o Assistente de exportação de máquina virtual.

2. Na página **Máquinas** do Assistente de exportação de máquina virtual, selecione a máquina protegida que você deseja exportar.
3. Clique em **Avançar**.
4. Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar para a exportação.
5. Clique em **Avançar**.
6. Na página **Destino** do Assistente de exportação de máquina virtual, no menu suspenso Recuperar para uma máquina virtual, selecione **Área de trabalho do VMWare** e clique em **Avançar**.
7. Na página **Opções de máquina virtual**, insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Tabela 122. Parâmetros da máquina virtual

Opção	Descrição
Caminho de destino	Especifique o caminho da pasta local ou compartilhamento de rede no qual você deseja criar a máquina virtual. **NOTE:** Se você especificou um caminho de compartilhamento de rede, será preciso inserir credenciais de login válidas para uma conta que está registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.
Nome de usuário	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir um nome de usuário válido para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, um nome de usuário não é necessário.
Senha	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir uma senha válida para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, uma senha não é necessária.
Máquina virtual	Insira um nome para a máquina virtual sendo criada, por exemplo, VM-0A1B2C3D4. **NOTE:** O nome padrão é o nome da máquina de origem.

Opção	Descrição
Versão	Especifique a versão do VMware Workstation da máquina virtual. Você pode selecionar dentre: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0 • VMware Workstation 11.0 • VMware Workstation 12.0
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • Usar a mesma quantidade de RAM da máquina de origem • Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.
Número de processadores	O número de processadores (CPUs) que você quer para a máquina virtual exportada. O valor mínimo é 1.
Cores por processador	O número de cores que você quer ter para cada processador. O valor mínimo é 1.

8. Selecione **Realizar exportação única inicial** para realizar a exportação virtual imediatamente e não após o próximo snapshot programado.
9. Clique em **Avançar**.
10. Na página **Volumes**, selecione os volumes para exportar, por exemplo, C:\ e D:\, e clique em **Avançar**.
11. Na página **Summary** (Resumo), clique em **Finish** (Concluir) para concluir o assistente e iniciar a exportação.

NOTE: Você pode monitorar o status e o progresso da exportação visualizando as páginas Standby virtual e Eventos.

Exportar dados para uma máquina virtual Hyper-V

No Rapid Recovery, é possível exportar dados para a Exportação para Hyper-V realizando uma exportação única ou estabelecendo uma exportação contínua (para Standby virtual).

Para obter informações sobre os sistemas operacionais de host suportados para exportações de Hyper-V de primeira e segunda geração, consulte o tópico "Requisitos do hypervisor" no *Guia de requisitos do sistema do Rapid Recovery*.

Execute as etapas dos procedimentos a seguir do tipo apropriado de exportação.

Realizar uma exportação única de Hyper-V

Execute as etapas deste procedimento para realizar uma exportação única para o Hyper-V.

1. No Console do Rapid Recovery Core, na barra de botões, clique no menu suspenso **Restaurar**, clique em **Exportação do VM**.
2. No Assistente de exportação de máquina virtual, selecione **Exportação única**.
3. Clique em **Avançar**.
4. Na página **Máquinas**, selecione a máquina protegida que você deseja exportar.
5. Clique em **Avançar**.
6. Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar para a exportação.
7. Clique em **Avançar**.
8. Na página **Destino**, no menu suspenso Exportar para máquina virtual, selecione **Hyper-V**.
9. Para exportar para uma máquina local com a função Hyper-V atribuída, clique em **Usar a máquina local**.
10. Para indicar que o servidor Hyper-V está localizado em uma máquina remota, clique em **Host remoto** e insira as informações do host remoto conforme descrito na tabela a seguir.

Tabela 123. Informações do host remoto

Caixa de texto	Descrição
Nome do host	Insira um endereço IP ou nome de host para o server Hyper-V. Ele representa o endereço IP ou nome de host do server Hyper-V remoto.
Porta	Insira um número de porta para a máquina. Ele representa a porta através da qual o Core se comunica com esta máquina.
Nome de usuário	Insira o nome de usuário para o usuário com privilégios administrativos para a estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.
Senha	Insira a senha da conta de usuário com privilégios administrativos na estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.

11. Clique em **Avançar**.
12. Na página **Opções de máquinas virtuais**, na caixa de texto **Local da máquina de VM**, insira o caminho da máquina virtual; por exemplo, `D:\export`. Isso é usado para identificar o local da máquina virtual.

    NOTE: Você precisa especificar o local da máquina virtual para os servers Hyper-V local e remoto. O caminho precisa ser um caminho de local válido para o server Hyper-V. Diretórios não existentes são automaticamente criados. Você não deve tentar criá-los manualmente. A exportação para pastas compartilhadas (por exemplo, para `\\data\share`) não é permitida.

13. Na caixa de texto **Nome da máquina virtual**, insira o nome da máquina virtual.

    O nome inserido será exibido na lista de máquinas virtuais no console do Hyper-V Manager.

14. Para especificar o uso da memória, clique em um dos seguintes:

    - **Usar a mesma quantidade de RAM da máquina de origem**. Selecione essa opção para identificar se o uso da RAM é idêntico entre as máquinas virtuais e de origem.
    - **Usar uma quantidade específica de RAM.** Selecione essa opção caso você queira especificar a quantidade de RAM em MB.

A quantidade mínima é 1.024 MB e o máximo permitido pelo aplicativo é 65.536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

15. Para especificar o formato do disco, próximo a Formato do disco, clique em um dos seguintes:
    - VHDX
    - VHD

    NOTE: A exportação do Hyper-V suporta formatos de disco VHDX se a máquina de destino estiver executando o Windows 8 (Windows Server 2012) ou mais recente. Se o formato VHDX não for suportado por seu ambiente, a opção será desativada.

    NOTE: Se desejar exportar para a geração Hyper-V 2, somente o formato de disco VHDX é suportado.
16. Para especificar a geração do Hyper-V a fim de utilizar para exportação, clique em um dos seguintes:
    - Geração 1
    - Geração 2

    NOTE: Somente a geração 2 oferece suporte à opção de inicialização segura.
17. Especifique o adaptador de rede adequado para a VM exportada.
18. Na página **Volumes**, selecione os volumes a serem exportados; por exemplo, C:\.

    NOTE: Se os volumes selecionados forem maiores do que as alocações máximas adequadas suportadas pelo aplicativo conforme indicado abaixo, ou exceder a quantidade de espaço disponível, será exibido um erro.
    - Para o formato de disco VHDX, seus volumes selecionados não devem ser maiores do que 64 TB.
    - Para o formato de disco VHD, seus volumes selecionados não devem ser maiores do que 2040 GB.
19. Na página **Volumes**, clique em **Concluir** para concluir e iniciar a exportação.

    NOTE: Você pode monitorar o status e o progresso da exportação visualizando as páginas **Standby virtual** e **Eventos**.

Configurar a exportação contínua para Hyper-V

Conclua as etapas nesse procedimento para configurar uma exportação contínua para uma máquina virtual (VM) Hyper-V usando o Rapid Recovery. Também conhecida como configuração de standby virtual.

1. No Rapid Recovery Core Console, realize um dos procedimentos a seguir:
    - Na barra de botões do Core Console, clique no menu suspenso the **Restaurar** e, em seguida, selecione **Exportação de VM**.
        1. No Assistente de exportação de máquina virtual, selecione **Contínuo (Standby Virtual)**.

2. Clique em **Avançar.**

- Na barra de ícones do Core Console, clique em (Standby virtual).
  - Na página **Standby virtual**, clique em **Adicionar** para iniciar o Assistente de exportação de máquina virtual.

2. Na página **Máquinas** do Assistente de exportação de máquina virtual, selecione a máquina protegida que você deseja exportar.
3. Clique em **Avançar**.
4. Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar para a exportação.
5. Clique em **Avançar**.
6. Na página **Destino**, no menu suspenso Exportar para uma máquina virtual, selecione **Hyper-V** e realize um dos seguintes procedimentos:
   - Para exportar para uma máquina local com a função Hyper-V atribuída, clique em **Usar a máquina local**.
   - Para indicar que o servidor Hyper-V está localizado em uma máquina remota, clique em **Host remoto** e insira os parâmetros do host remoto conforme descrito na tabela a seguir.

Tabela 124. Informações do host remoto

Caixa de texto	Descrição
Nome do host	Insira um endereço IP ou nome de host para o server Hyper-V. Ele representa o endereço IP ou nome de host do server Hyper-V remoto.
Porta	Insira um número de porta para a máquina. Ele representa a porta através da qual o Core se comunica com esta máquina.
Nome de usuário	Insira o nome de usuário para o usuário com privilégios administrativos para a estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.
Senha	Insira a senha da conta de usuário com privilégios administrativos na estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.

7. Clique em **Avançar**.
8. Na página **Opções de máquinas virtuais**, na caixa de texto **Local da máquina de VM**, insira o caminho da máquina virtual; por exemplo, `D:\export`. Isso é usado para identificar o local da máquina virtual.

   NOTE: Você precisa especificar o local da máquina virtual para os servers Hyper-V local e remoto. O caminho precisa ser um caminho de local válido para o server Hyper-V. Diretórios não existentes são automaticamente criados. Você não deve tentar criá-los manualmente. A exportação para pastas compartilhadas (por exemplo, para `\\data\share`) não é permitida.
9. Na caixa de texto **Nome da máquina virtual**, insira o nome da máquina virtual.

   O nome inserido será exibido na lista de máquinas virtuais no console do Hyper-V Manager.
10. Para especificar o uso da memória, clique em um dos seguintes:
    - **Usar a mesma quantidade de RAM da máquina de origem**. Selecione essa opção para identificar se o uso da RAM é idêntico entre as máquinas virtuais e de origem.
    - **Usar uma quantidade específica de RAM.** Selecione essa opção caso você queira especificar a quantidade de RAM em MB.

A quantidade mínima é 1.024 MB e o máximo permitido pelo aplicativo é 65.536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

11. Para especificar o formato do disco, próximo a Formato do disco, clique em um dos seguintes:
    - VHDX
    - VHD

    NOTE: A exportação do Hyper-V suporta formatos de disco VHDX se a máquina de destino estiver executando o Windows 8 (Windows Server 2012) ou mais recente. Se o formato VHDX não for suportado por seu ambiente, a opção será desativada.

    NOTE: Se desejar exportar para a geração Hyper-V 2, somente o formato de disco VHDX é suportado.
12. Para especificar a geração do Hyper-V a fim de utilizar para exportação, clique em um dos seguintes:
    - Geração 1
    - Geração 2

    NOTE: Somente a geração 2 oferece suporte à opção de inicialização segura.
13. Especifique o adaptador de rede adequado para a VM exportada.
14. Na página **Volumes**, selecione os volumes a serem exportados; por exemplo, C:\.

    NOTE: Se os volumes selecionados forem maiores do que as alocações máximas adequadas suportadas pelo aplicativo conforme indicado abaixo, ou exceder a quantidade de espaço disponível, será exibido um erro.
    - Para o formato de disco VHDX, seus volumes selecionados não devem ser maiores do que 64 TB.
    - Para o formato de disco VHD, seus volumes selecionados não devem ser maiores do que 2040 GB.
15. Selecione **Realizar exportação única inicial** para realizar a exportação virtual imediatamente e não após o próximo snapshot programado.
16. Na página **Volumes**, clique em **Concluir** para concluir e iniciar a exportação.

    NOTE: Você pode monitorar o status e o progresso da exportação visualizando as páginas **Standby virtual** e **Eventos**.

Exportar dados para uma máquina virtual VirtualBox

No Rapid Recovery, você pode exportar dados para o VirtualBox realizando uma exportação única ou estabelecendo uma exportação contínua (para standby virtual).

Execute as etapas dos procedimentos a seguir do tipo apropriado de exportação.

NOTE: Para realizar esse tipo de exportação para uma VM do VirtualBox em um host Windows, é preciso ter o VirtualBox instalado na máquina do Core. As VMs hospedadas em Linux não compartilham esse requisito.

Realizar uma exportação única de VirtualBox

Para exportar para uma VM do VirtualBox em um host Windows remoto, é preciso ter o VirtualBox instalado na máquina do Core. Esse requisito não se aplica a VMs hospedadas no Linux.

Execute as etapas deste procedimento para realizar uma exportação única para o VirtualBox.

1. No Console do Rapid Recovery Core, na barra de botões, clique no menu suspenso **Restaurar**, clique em **Exportação do VM**.
2. No Assistente de exportação de máquina virtual, selecione **Exportação única**.
3. Clique em **Avançar**.
4. Na página **Máquinas**, selecione a máquina protegida que você deseja exportar.
5. Clique em **Avançar**.
6. Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar para a exportação.
7. Clique em **Avançar**.
8. Na página **Destino** do Assistente de exportação, no menu suspenso Exportar para uma máquina virtual, selecione **VirtualBox** e clique em **Avançar**.
9. Na página **Opções de máquina virtual**, selecione **Usar a máquina do Windows**.
10. Insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Tabela 125. Parâmetros da máquina virtual

Opção	Descrição
Nome da máquina virtual	Insira um nome para a máquina virtual sendo criada. **NOTE:** O nome padrão é o nome da máquina de origem.
Caminho de destino	Especifique um caminho de destino local ou remoto para criar a máquina virtual. **NOTE:** O caminho de destino não deve ser um diretório raiz. Se você especificou um caminho de compartilhamento de rede, será preciso inserir credenciais de login válidas (nome de usuário e senha) para uma conta que está registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • Usar a mesma quantidade de RAM da máquina de origem • Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

11. Para especificar uma conta de usuário para a máquina virtual, selecione **Especifique a conta de usuário para a máquina virtual exportada** e insira as seguintes informações. Isso se refere a uma conta de usuário específica para a qual a máquina virtual será registrada caso existam múltiplas contas de usuários na máquina virtual. Quando essa conta de usuário estiver conectada, somente esse usuário verá essa

máquina virtual no gerenciador do VirtualBox. Se uma conta não for especificada, a máquina virtual será registrada para todos os usuários existentes na máquina com Windows e VirtualBox.

- Nome de usuário - insira o nome de usuário com o qual a máquina virtual é registrada.
- Senha - insira a senha dessa conta de usuário.

12. Clique em **Avançar**.
13. Na página **Volumes**, selecione os volumes para exportar, por exemplo, C:\ e D:\, e clique em **Avançar**.
14. Na página **Summary** (Resumo), clique em **Finish** (Concluir) para concluir o assistente e iniciar a exportação.

NOTE: Você pode monitorar o status e o progresso da exportação visualizando as páginas **Standby virtual** e **Eventos**.

Configurar a exportação contínua para VirtualBox

Para exportar para uma VM do VirtualBox em um host Windows remoto, é preciso ter o VirtualBox instalado na máquina do Core. Esse requisito não se aplica a VMs hospedadas no Linux.

Conclua as etapas nesse procedimento para realizar uma exportação contínua para uma máquina virtual (VM) VirtualBox usando Rapid Recovery.

1. No Rapid Recovery Core Console, escolha uma das opções a seguir:

   - Na barra de botões do Core Console, clique no menu suspenso the **Restaurar** e, em seguida, selecione **Exportação de VM**.

     1. No Assistente de exportação de máquina virtual, selecione **Contínuo (Standby Virtual)**.
     2. Clique em **Avançar.**

   - Na barra de ícones do Core Console, clique em (Standby virtual).
     - Na página **Standby virtual**, clique em **Adicionar** para iniciar o Assistente de exportação de máquina virtual.

2. Na página **Máquinas** do Assistente de exportação de máquina virtual, selecione a máquina protegida que você deseja exportar.
3. Clique em **Avançar**.
4. Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar para a exportação.
5. Clique em **Avançar**.
6. Na página **Destino** do Assistente de exportação, no menu suspenso **Recuperar para uma máquina virtual**, selecione **VirtualBox**.
7. Na página **Virtual Machine Options** (Opções de máquina virtual), selecione **Remote Linux Machine** (Máquina Linux remota).
8. Insira as informações sobre a máquina virtual conforme descrito na tabela a seguir.

Tabela 126. Definições da máquina Linux remota

Opção	Descrição
Nome de host do VirtualBox	Insira um endereço IP ou nome de host para o server VirtualBox. Este campo representa o endereço IP ou nome de host do server VirtualBox remoto.
Porta	Insira um número de porta para a máquina. Este número representa a porta através da qual o Core se comunica com esta máquina.

Opção	Descrição
Nome da máquina virtual	Insira um nome para a máquina virtual sendo criada. **NOTE:** O nome padrão é o nome da máquina de origem.
Caminho de destino	Especifique um caminho de destino para criar a máquina virtual. **NOTE:** Recomenda-se criar uma pasta raiz a partir da raiz para que a máquina virtual seja executa a partir da raiz. Se você não usar a raiz, será preciso criar uma pasta de destino manualmente na máquina de destino antes de configurar a exportação. Também será preciso conectar ou carregar manualmente a máquina virtual após a exportação.
Nome de usuário	Nome de usuário da conta na máquina de destino, por exemplo, raiz.
Senha	Senha para a conta de usuário na máquina de destino.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • Usar a mesma quantidade de RAM da máquina de origem • Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

9. Selecione **Realizar exportação única inicial** para realizar a exportação virtual imediatamente e não após o próximo snapshot programado.
10. Clique em **Avançar**.
11. Na página **Volumes**, selecione os volumes de dados a serem exportados e clique em **Avançar**.
12. Na página **Summary** (Resumo), clique em **Finish** (Concluir) para concluir o assistente e iniciar a exportação.

NOTE: Você pode monitorar o status e o progresso da exportação visualizando as páginas Standby virtual e Eventos.

Exportar dados para uma máquina virtual Azure

No Rapid Recovery, você pode exportar dados para o Azure realizando uma exportação única ou estabelecendo uma exportação contínua (para standby virtual). A exportação única para a plataforma Azure inclui a implantação no fluxo de trabalho. Se você estiver usando uma exportação contínua, você pode também, posteriormente, implantar os arquivos exportados para uma VM inicializável.

Para obter mais informações sobre como trabalhar com o Azure, consulte

Para obter os pré-requisitos referentes à exportação virtual para o Azure, consulte Antes da exportação virtual para o Azure.

Para obter uma descrição detalhada dos aspectos exclusivos da exportação virtual para o Azure, consulte Exportar e implantar VMs para Azure.

Para obter mais informações sobre as configurações e preços do Azure, consulte a página preço de máquinas virtuais no site do Azure.

Para links para outras referências úteis no sotes da Microsoft, consulte .

Para obter informações sobre os procedimentos relacionados à exportação ou à implantação de VMs no Azure, consulte os seguintes links relacionados.

Conceitos relacionados

See also: Exportar dados para uma máquina virtual VirtualBox

Tarefas relacionadas

See also: Configurar a exportação contínua para Azure
See also: Implantar uma máquina virtual no Azure
See also: Realizar uma exportação única para o Azure

Trabalhar com o Microsoft Azure

O Microsoft Azure é uma plataforma de computação em nuvem baseada em assinatura. As informações a seguir são fornecidas aos clientes do Rapid Recovery para facilitar o uso do Azure com nosso produto.

- Aviso de isenção de responsabilidade da interface do Azure
- Criar um contêiner na conta de armazenamento do Azure
- Exportar e implantar VMs para Azure
- Documentação do Microsoft Azure

Aviso de isenção de responsabilidade da interface do Azure

A interface do Microsoft Azure está sujeita a alterações.

As informações fornecidas neste documento relacionadas às etapas necessárias no Azure estavam atualizadas na data da publicação. Essas informações são fornecidas como um serviço a nossos clientes para ajudá-los com os pré-requisitos do Azure.

No entanto, ao trabalhar com o Azure, saiba que etapas específicas, URLs ou até mesmo a interface do Azure podem mudar a qualquer momento, o que está fora do nosso controle.

Caso você esteja enfrentando dificuldades em executar quaisquer etapas relacionadas à sua conta do Azure, busque ajuda de um representante do Microsoft Azure.

Criar um contêiner na conta de armazenamento do Azure

- Você precisa ter acesso administrativo a uma conta no Azure.
- Você precisa ter uma conta de armazenamento definida na sua conta do Azure.

Quando você faz uma exportação virtual, as informações são armazenadas em um contêiner dentro da conta de armazenamento do Azure. Você pode definir o contêiner da sua conta no Azure antes de executar a exportação virtual, usando o procedimento abaixo. Ou você pode definir o contêiner como parte do processo de exportação da página **Destino** do assistente.

Execute as etapas descritas neste procedimento para criar um contêiner na conta de armazenamento do Azure.

1. Abra o painel do Microsoft Azure.
2. Na área de navegação à esquerda, clique em **Todos os recursos**.
3. No painel **Todos os recursos**, clique no nome da conta de armazenamento no qual você quer armazenar dados das exportações virtuais do Rapid Recovery.
4. No painel **Configurações**, clique em **Blobs**.
5. Na parte superior do painel **serviço Blob**, no cabeçalho, clique em **+ Contêiner**.
6. No painel **Novo contêiner**, no campo **Nome**, digite o nome do novo contêiner.

   NOTE: Digite um nome entre 3 e 63 caracteres, usando apenas letras minúsculas, números e hífens.

7. No painel **Novo contêiner**, no menu suspenso **Tipo de acesso**, selecione o tipo de contêiner adequado que definirá se o contêiner poderá ser acessado publicamente. Use o seguinte como orientação.

Opção	Descrição
Privado	Esta opção restringe o contêiner ao proprietário da conta.
Blob	Esta opção permite acesso de leitura público para Objetos Binários Grandes (Blobs).
Contêiner	Esta opção permite acesso de leitura e lista público a todo o contêiner.

   Por exemplo, selecione **Contêiner**.

8. Clique em **Criar**.

   Se os alertas de notificação do sistema estiverem ativos, você verá uma mensagem indicando que o contêiner foi criado com sucesso.

   A página **serviço Blob** é atualizada com o novo nome do contêiner exibido na lista.

Documentação do Microsoft Azure

A Microsoft tem farta documentação sobre o uso do Azure disponível em seu centro de documentação.

Para mais informações sobre como criar uma conta Azure, configurar uma máquina virtual para uso conjunto com um núcleo Rapid Recovery ou AppAssure, adicionar uma conta de armazenamento e mais, consulte a documentação da Microsoft em https://azure.microsoft.com/en-us/documentation.

Por exemplo, para obter informações sobre como gerenciar as máquinas virtuais do, consulte https://azure.microsoft.com/en-us/documentation/services/virtual-machines/windows/.

Para assistir vídeos on-line sobre como usar o Azure, consulte http://azure.microsoft.com/en-us/get-started/.

NOTE: O site do Azure usa códigos de idioma e país para seus endereços da web, o que afeta a exibição do conteúdo. Por exemplo, `https://azure.microsoft.com/[country-code]/[destination]/`.

NOTE: Os URLs do Azure utilizados neste documento incluem o código de país para inglês dos Estados Unidos. Para outros idiomas, com base nas configurações do seu computador e conteúdo que a Microsoft oferece, as URLs podem variar de acordo com esses códigos.

Links relevantes da Microsoft

Seguem alguns artigos relevantes em sites da Microsoft:

- Página de login do Azure (EUA)
- Página inicial do Microsoft Azure
- Centro de documentação da Microsoft
- Documentação de máquinas virtuais do Windows
- Vídeos: Comece a usar o Azure
- Preços de máquinas virtuais Azure
- Serviços Azure por região
- Sobre contas de armazenamento do Azure
- Como criar uma conta de armazenamento no Azure
- Como conectar um disco de dados a uma máquina virtual do Windows no portal do Azure
- Utilize o serviço de importação/exportação do Microsoft Azure para transferir dados para o armazenamento Blob
- Preços de exportação/importação
- Armazenamento: importar/exportar as unidades de disco rígido para o Windows Azure (publicação de blog)

Antes da exportação virtual para o Azure

O Rapid Recovery permite que você execute a exportação virtual (única ou standby virtual) para o Microsoft Azure.

Antes de executar uma exportação virtual de qualquer máquina protegida no Rapid Recovery, você precisa primeiro associar a sua conta de nuvem do Azure ao Core, conforme descrito no tópico Adicionar uma conta de nuvem.

Você precisa ter uma conta de armazenamento adequada no Azure. Para obter mais informações sobre como criar uma conta de armazenamento no Azure, consulte as informações de suporte do Azure citadas no tópico .

Na sua conta de armazenamento, você pode criar dinamicamente um contêiner para armazenar exportações ou usar um contêiner existente. Para obter mais informações sobre como criar um contêiner de armazenamento, consulte Criar um contêiner na conta de armazenamento do Azure.

Ao contrário de outras formas de exportação virtual usando o Rapid Recovery, a exportação de VM para o Azure inclui dois processos, descritos em detalhes no tópico Exportar e implantar VMs para Azure.

Exportar e implantar VMs para Azure

Diferente da exportação virtual para outras plataformas, a exportação virtual para o Azure é composta por dois processos: exportação e implantação.

Esteja ciente de que os clientes do Microsoft Azure são responsáveis por suas próprias taxas. Alguns aspectos da nossa integração com o Azure são projetados com essa estrutura de taxas em mente. Por exemplo, a Microsoft cobra taxas quando você implanta uma máquina virtual no Azure e quando dados são transmitidos do Azure para outra fonte.

NOTE: Visto que a Microsoft pode alterar pré-requisitos, exigências, custos, e assim por diante, sempre verifique essas informações com o Azure. Para obter mais informações, consulte o site do Azure ou entre em contato com um representante Azure.

Para evitar que incorram custos desnecessários, a exportação virtual para o Azure consiste em dois processos separados para cobrir os custos que podem não ser necessários.

O processo de **exportação** extrai o conjunto necessário de arquivos do Rapid Recovery, valida-os e carrega-os no contêiner especificado no Azure. Esses arquivos são:

- Um arquivo de disco rígido virtual (VHD) para cada volume no ponto de recuperação.
- Um arquivo XML, que contém informações de metadados sobre cada disco (uma lista de arquivos presentes em cada disco e um sinalizador indicando se um volume é um disco do sistema).
- Um arquivo VHD contendo o instantâneo de backup.

Com exceção dos custos para o armazenamento necessário, a exportação por si só não resultará em quaisquer taxas do Azure.

O processo de **implantação** combina esses arquivos em uma máquina virtual inicializável. A implantação usa diretamente as APIs REST de nuvem do Azure. O conjunto original de arquivos colocados no Azure durante o processo de exportação é somente leitura no Azure, e consome espaço, mas, de outra maneira, não resultará em custos do Azure. Quando você implanta esses arquivos, uma cópia duplicada deles é criada, armazenada em um contêiner separado definido por você e combinados em uma máquina virtual em funcionamento. De uma perspectiva da conta Azure, após a implantação, taxas serão cobradas de você referentes à VM em seus servidores. Como a VM implantada é uma cópia dos arquivos exportados, o processo de implantação também duplica a quantidade de espaço de armazenamento usado no Azure para essa exportação virtual.

Para uma exportação virtual única, não há nenhum mecanismo para a implantação como um processo separado. Assim, para a exportação ser útil, você deve implantar para o Azure ao criar a máquina virtual sob demanda. Como resultado, as exportações únicas para o Azure têm um custo imediato associado ao VM que você implantar.

Ao estabelecer o standby virtual para uma máquina protegida no Azure, a fim de evitar o uso de espaço de armazenamento adicional e os custos de VM, você pode simplesmente definir o processo de exportação. O resultado é uma exportação virtual inicial para o Azure atualizada continuamente. Cada vez que um instantâneo é capturado no Core, os arquivos exportados são atualizados na sua conta do Azure com informações atualizadas. Antes de usar a exportação virtual como uma VM inicializável, você precisa implantá-la, o que aciona os custos de VM no Azure. Se você não precisa converter os arquivos exportados para uma máquina protegida para uma VM inicializável, nenhum custo de VM será incorrido na sua conta do Azure.

Para obter informações sobre como realizar uma exportação única para o Azure, incluindo a implantação, consulte o tópico Realizar uma exportação única para o Azure.

Para obter informações sobre como configurar uma exportação contínua para o Azure, excluindo a implantação, consulte o tópico Configurar a exportação contínua para Azure.

Para obter informações sobre como implantar os últimos arquivos exportados para criar uma VM em standby virtual inicializável no Azure, consulte o tópico Implantar uma máquina virtual no Azure.

Realizar uma exportação única para o Azure

Antes de você executar uma exportação única para o Azure, você precisará do seguinte:

- Você precisa ter uma máquina protegida com pelo menos um ponto de recuperação em um Rapid Recovery Core que você quer exportar para o Azure.
- O acesso remoto deve estar ativado na máquina protegida para a VM implantada inicializar com sucesso.
- Você precisa ter acesso administrativo a uma conta no Azure.
- Opcionalmente, antes de exportar, você pode criar um contêiner adequado na conta de armazenamento do Azure dentro do qual os dados exportados serão armazenados. Para obter mais informações, consulte o tópico Criar um contêiner na conta de armazenamento do Azure.

Conforme descrito no tópico Exportar e implantar VMs para Azure, a exportação virtual para o Azure consiste em dois processos: exportação e implantação.

O processo de **exportação** extrai o conjunto necessário de arquivos do Rapid Recovery, valida-os e carrega-os no contêiner especificado no Azure. Esses arquivos são:

- Um arquivo de disco rígido virtual (VHD) para cada volume no ponto de recuperação
- Um arquivo XML, que contém informações de metadados sobre cada disco (uma lista de arquivos presentes em cada disco e um sinalizador indicando se um volume é um disco do sistema)
- Um arquivo VHD contendo o instantâneo de backup

O processo de **implantação** combina esses arquivos em uma máquina virtual inicializável. A implantação usa diretamente as APIs REST de nuvem do Azure. O conjunto original de arquivos colocados no Azure durante o processo de exportação é somente leitura no Azure, e consome espaço, mas não resulta em custos adicionais do Azure. Quando você implanta esses arquivos, uma cópia duplicada deles é criada, armazenada em um contêiner separado definido por você e combinados em uma máquina virtual em funcionamento. De uma perspectiva da conta Azure, após a implantação, taxas serão cobradas de você com respeito à VM em seus servidores. O processo de implantação também duplica a quantidade de espaço de armazenamento usado no Azure para essa exportação virtual.

Para uma exportação virtual única, não há nenhum mecanismo para a implantação como um processo separado; portanto, para a exportação ser útil, você deve implantar ao criar a máquina virtual sob demanda.

Ao estabelecer o standby virtual para uma máquina protegida no Azure, a fim de evitar o uso de espaço de armazenamento adicional e os custos de VM, você pode exportar e continuamente atualizar o ponto de recuperação automaticamente, sem a necessidade de implantar. Em seguida, você pode implantar no Azure apenas quando e se você precisar usar a máquina virtual. Para obter mais informações sobre a implantação de um standby virtual no Azure para uma máquina virtual em funcionamento, consulte o tópico Implantar os dados de standby virtual para uma máquina virtual no Azure.

Execute as etapas deste procedimento para realizar uma exportação única para o Azure sob demanda, incluindo a implantação para uma VM.

1. No Rapid Recovery Core Console, clique no menu suspenso **Restaurar** e selecione **Exportação de VM**.

   O assistente de exportação de máquina virtual é exibido.
2. Na página **Selecionar tipo de exportação de VM** do assistente, selecione **Exportação única** e, em seguida, clique em **Avançar**.

   A página **Máquinas** do assistente é exibida.
3. Na página **Máquinas**, selecione a máquina protegida que deseja exportar e clique em **Avançar**.
4. Na página **Pontos de recuperação**, percorra a lista de pontos de recuperação, se necessário, e selecione o ponto de recuperação que você quer usar na exportação. Depois, clique em **Avançar**.
5. Na página **Destino**, no menu suspenso Exportar para uma máquina virtual, selecione **Azure**.
6. Insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir e clique em **Avançar**.

Tabela 127. Credenciais do Azure

Opções	Descrição
Arquivo de configurações de publicação	O arquivo de configurações de publicação é um documento XML gerado no Azure que contém os certificados de gerenciamento das informações de assinatura do Azure. **NOTE:** As configurações de publicação só precisam ser definidas uma vez por conta do Azure a partir da UI do Core. Depois disso, elas são armazenadas em cache. Quando este arquivo for solicitado, faça login na sua conta do Azure e baixe-o da sua VM em https://manage.windowsazure.com/publishsettings/index?client=powershell. O arquivo define a API AzureServiceManagement e as informações sobre a sua assinatura do Azure, incluindo as credenciais seguras. Este arquivo deve ser definido no Rapid Recovery Core antes de você conectar-se à sua conta e realizar uma exportação virtual.

Opções	Descrição
	Para fins de segurança, armazene o arquivo em um local seguro e apague-o depois de usá-lo neste procedimento.
Assinatura	Se você acabou de adicionar arquivos de configurações de publicação, essa informação é inserida automaticamente com as informações do arquivo de configurações de publicação. **NOTE:** As configurações de publicação só precisam ser definidas uma vez por conta do Azure a partir da UI do Core. Depois disso, elas são armazenadas em cache. Se você quiser usar um arquivo de configurações de publicação adicionado anteriormente, use a lista suspensa para selecionar um arquivo. Se você quiser adicionar um arquivo de configurações de publicação, use o botão + para abrir a janela **Carregar certificado** e acessar o arquivo. Quando este arquivo for solicitado, faça login na sua conta do Azure e baixe-o da sua VM em https://manage.windowsazure.com/publishsettings/index?client=powershell. Para fins de segurança, armazene o arquivo em um local seguro e apague-o depois de usá-lo neste procedimento.
Conta	Inserida automaticamente a partir do arquivo de assinatura; é a conta de nuvem do Azure associada ao Core. **NOTE:** Você precisa primeiro associar a conta de nuvem do Azure ao Core, conforme descrito no tópico Adicionar uma conta de nuvem.
Nome do contêiner	No menu suspenso, selecione o nome do contêiner adequado associado à conta de nuvem do Azure se ele já existe. Ou, digite um nome para um novo contêiner. **NOTE:** Digite um nome entre 3 e 63 caracteres, usando apenas letras minúsculas, números e hífens.
Nome da pasta	Especifique um nome para a pasta dentro do contêiner para armazenar a máquina virtual exportada. **NOTE:** Uma pasta do Azure não pode conter nenhum dos seguintes caracteres: / \ : * ? " < > |

7. Na página **Implantação**, digite um destino para a VM implantada, conforme descrito na tabela a seguir, e clique em **Avançar**.

Tabela 128. Implantar seguindo as opções do Azure

Opção	Descrição
Nome do serviço de nuvem	O serviço de nuvem do Azure é um contêiner para máquinas virtuais que usa o modelo de gerenciamento clássico. Se você já tem um serviço de nuvem, no menu suspenso **Nome do serviço de nuvem**, selecione o nome do serviço de nuvem adequado. Ou, no campo **Nome do serviço de nuvem**, digite um nome significativo único para o serviço de nuvem. **NOTE:** As assinaturas do Microsoft Azure têm limites padrão no número de serviços de nuvem (normalmente 25). Certifique-se de não exceder os limites de assinatura.

Opção	Descrição
Nome da implantação	Se você tiver selecionado um serviço de nuvem com máquinas virtuais existentes, este campo é preenchido automaticamente. Se você tiver selecionado um serviço de nuvem sem máquinas virtuais, digite um nome para esta nova implantação. **NOTE:** Digite um nome entre 3 e 63 caracteres, usando apenas letras minúsculas, números e hífens.
Contêiner de destino	Digite um nome para o contêiner que irá armazenará sua VM. **NOTE:** Digite um nome entre 3 e 63 caracteres, usando apenas letras minúsculas, números e hífens.

8. Na página **Opções de máquina virtual**, insira as informações conforme descrito na tabela a seguir.

Tabela 129. Opções da máquina virtual

Opção	Descrição
Nome da máquina virtual	Digite um nome para a máquina virtual. **NOTE:** Digite um nome entre 3 e 15 caracteres, usando apenas letras minúsculas, números e hífens.
Tamanho da máquina virtual	No menu suspenso, selecione um tamanho adequado para a VM. **NOTE:** Para obter mais informações sobre as configurações e preços do Azure, consulte a página preço de máquinas virtuais no site do Azure. Para links para outras referências úteis no sotes da Microsoft, consulte .
Ponto de extremidade (definições de acesso remoto)	A seguir, veja as opções da VM para as definições de acesso remoto.
Nome	Selecione **Desktop remoto** ou **SSH**.
Protocolo	Selecione **TCP** ou **UDP**
Portas	Portas públicas e privadas; por padrão, use a 3389. Altere se necessário.
Portas do servidor de dados de transferência	Portas públicas e privadas; por padrão, use a 8009. Altere se necessário.
Portas do agente	Portas públicas e privadas; por padrão, use a 8006. Altere se necessário.

9. Clique em **Avançar**.
10. Na página **Volumes**, selecione os volumes que você quer exportar e, em seguida, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTE: Você pode monitorar o status e o progresso da exportação vendo a fila de exportação na página **Standby virtual** ou na página **Eventos**.

Configurar a exportação contínua para Azure

Antes de executar uma exportação virtual contínua para o Azure, você precisará:

- Você precisa ter uma máquina protegida com pelo menos um ponto de recuperação em um Rapid Recovery Core que você quer exportar para o Azure.
- O acesso remoto deve estar ativado na máquina protegida para a VM implantada inicializar com sucesso.
- Você precisa ter acesso administrativo a uma conta no Azure.
- Para associar sua conta do Azure ao Core, você precisa primeiro baixar um arquivo de configurações de publicação do Azure. Para obter mais informações, consulte Obter o arquivo de configurações de publicação para sua conta do Azure.
- Opcionalmente, antes de exportar, você pode criar um contêiner adequado na conta de armazenamento do Azure dentro do qual os dados exportados serão armazenados. Lembre-se de que os requisitos de armazenamento crescem à medida que sua máquina protegida protege mais dados. Na sua conta do Azure, o contêiner que você especifica deve estar associado a um local de armazenamento com espaço suficiente para acomodar a máquina virtual. Para obter mais informações, consulte o tópico Criar um contêiner na conta de armazenamento do Azure.

Execute as etapas descritas neste procedimento para executar a exportação virtual contínua da máquina selecionada para um contêiner especificado em uma conta de nuvem do Azure usando o Rapid Recovery.

NOTE: Este processo não inclui a implantação dos arquivos exportados para criar uma VM inicializável. Para obter o procedimento para a implantação, consulte Implantar uma máquina virtual no Azure.

1. No Rapid Recovery Core Console, escolha uma das opções a seguir:
   - Na barra de botões do Core Console, clique no menu suspenso the **Restore** (Restaurar) e, em seguida, selecione **VM Export** (Exportação de VM).
     1. No Assistente de exportação de máquina virtual, selecione **Contínuo (Standby Virtual)**.
     2. Clique em **Avançar.**
   - Na barra de ícones do Core Console, clique em (Standby virtual).
     - Na página **Standby virtual**, clique em **+Adicionar** para abrir o Assistente de exportação de máquina virtual.
2. Na página **Máquinas** do Assistente de exportação de máquina virtual, selecione a máquina protegida que você deseja exportar.
3. Clique em **Avançar**.
4. Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar para a exportação.
5. Clique em **Avançar**.
6. Na página **Destino**, no menu suspenso Exportar para uma máquina virtual, selecione **Azure**. .
7. Insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir e clique em **Avançar**.

Tabela 130. Credenciais do Azure

Opções	Descrição
Arquivo de configurações de publicação	Essa opção aparece somente se você ainda não tiver associado a assinatura do Azure ao Core. Se você vir essa opção, baixe o arquivo conforme descrito no tópico Obter o arquivo de configurações de publicação para sua conta do Azure e associe sua assinatura ao Core. Essa associação deve ser concluída para que você possa se conectar à sua conta do Azure a partir do Core e executar uma exportação virtual.

Opções	Descrição
	NOTE: As configurações de publicação só precisam ser definidas uma vez por conta do Azure a partir da UI do Core. Depois disso, elas são armazenadas em cache. Para fins de segurança, armazene o arquivo em um local seguro e apague-o depois de usá-lo neste procedimento.
Assinatura	Se você acabou de adicionar arquivos de configurações de publicação, essa informação é inserida automaticamente com as informações do arquivo de configurações de publicação. **NOTE:** As configurações de publicação só precisam ser definidas uma vez por conta do Azure a partir da UI do Core. Depois disso, elas são armazenadas em cache. Se você quiser usar um arquivo de configurações de publicação adicionado anteriormente, use a lista suspensa para selecionar um arquivo. Se você quiser adicionar um arquivo de configurações de publicação, use o botão + para abrir a janela **Carregar certificado** e acessar o arquivo.
Conta	Inserida automaticamente a partir do arquivo de assinatura; é a conta de nuvem do Azure associada ao Core. **NOTE:** Você precisa primeiro associar a conta de nuvem do Azure ao Core, conforme descrito no tópico Adicionar uma conta de nuvem
Nome do contêiner	No menu suspenso, selecione o nome do contêiner adequado associado à conta de nuvem do Azure se ele já existe. Ou, digite um nome para um novo contêiner. **NOTE:** Digite um nome entre 3 e 63 caracteres, usando apenas letras minúsculas, números e hífens.
Nome da pasta	Especifique um nome para a pasta dentro do contêiner para armazenar a máquina virtual exportada. **NOTE:** Uma pasta do Azure não pode conter nenhum dos seguintes caracteres: / \ : * ? " < > |
Realizar a exportação única inicial	Ao definir o standby virtual, selecione esta opção para colocar a tarefa de exportação na fila imediatamente. Desmarque a opção se você quiser que o Core aguarde até a próxima reinicialização forçada ou instantâneo de backup programado.

8. Clique em **Avançar**.
9. Na página **Volumes**, selecione os volumes que deseja exportar e clique em **Avançar**.
10. Na página **Resumo**, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTE: Você pode monitorar o status e o progresso da exportação visualizando as páginas Standby virtual e Eventos.

Os parâmetros de standby virtual que você definir neste procedimento resultam na exportação dos arquivos necessários para criar uma VM em sua conta do Azure. Depois de cada instantâneo (forçado ou programado), esses arquivos são atualizados no Azure com todas as novas informações de backup. Antes de poder iniciar esses arquivos como uma VM, você precisa implantar a VM no Azure. Para obter o procedimento para a implantação, consulte Implantar uma máquina virtual no Azure.

Implantar uma máquina virtual no Azure

Antes de você implantar uma VM no Azure, você precisa ter uma máquina protegida em um Rapid Recovery Core com pelo menos um ponto de recuperação, e você precisa configurar uma exportação contínua (standby virtual) do Core Console. Para obter mais informações sobre como configurar a exportação contínua, consulte Configurar a exportação contínua para Azure. Este processo também requer que você tenha uma conta do Azure com armazenamento suficiente associado ao Core.

Ao configurar o standby virtual para uma máquina protegida no Azure, as últimas informações de backup são continuamente exportadas do Core para a sua conta do Azure após cada instantâneo de backup. Esse processo substitui o conjunto anterior de arquivos de exportação por informações de backup atualizadas. Antes de poder iniciar a exportação virtual como uma máquina virtual (por exemplo, se a máquina protegida original falhou), você precisa primeiro implantar a partir do Core Console. Este processo gera uma VM inicializável em um novo contêiner

Execute as etapas descritas neste procedimento para implantar os arquivos de exportação de standby virtual mais recentes para uma VM inicializável no Azure.

1. Na barra de ícones do Rapid Recovery Core Console, clique em (Standby virtual).
2. No painel **Standby virtual**, identifique a máquina no seu Rapid Recovery Core que está configurada para exportação contínua para o Azure.
3. Na linha que representa a máquina de standby virtual que você deseja implantar, clique em (Mais opções) e selecione **Implantar máquina virtual**.

   O **Assistente de implantação para o Azure** será exibido.
4. Na página **Destino**, no menu suspenso **Nome do serviço de nuvem**, selecione o nome do serviço de nuvem adequado entre as opções disponíveis na sua conta do Azure.
5. Clique em **Avançar**.
6. Na página Pontos de recuperação, selecione o ponto de recuperação que você deseja usar na exportação.
7. Clique em **Avançar**.
8. Na página **Destino** do Assistente de exportação, no menu suspenso Exportar para uma máquina virtual, selecione **ESX(i)**.
9. Insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir e clique em **Avançar**.

Tabela 131. Parâmetros da máquina virtual

Opções	Descrição
Nome do serviço de nuvem	Se você já tem um serviço de nuvem, no menu suspenso **Nome do serviço de nuvem**, selecione o nome do serviço de nuvem adequado. Ou, no campo **Nome do serviço de nuvem**, digite um nome significativo único para o serviço de nuvem. O nome do serviço de nuvem está associado ao grupo de recursos da conta do Azure. Se no Azure você tiver privilégios administrativos, consulte a documentação do Azure para criar a conta apropriada. Se você não ver uma conta de serviço de nuvem adequada, peça ajuda ao seu administrador do Azure. **NOTE:** As assinaturas do Microsoft Azure têm limites padrão no número de serviços de nuvem (normalmente 25). Certifique-se de não exceder os limites de assinatura.
Nome da implantação	Se você tiver selecionado um serviço de nuvem com máquinas virtuais existentes, este campo é preenchido automaticamente. Se você tiver selecionado um serviço de nuvem sem máquinas virtuais, digite um nome para esta nova implantação. **NOTE:** Digite um nome entre 3 e 63 caracteres, usando apenas letras minúsculas, números e hífens.

Opções	Descrição
Contêiner de destino	Digite um nome para o contêiner que irá armazenará sua VM. **NOTE:** Digite um nome entre 3 e 63 caracteres, usando apenas letras minúsculas, números e hífens.

10. Na página Opções de máquina virtual, insira as informações conforme descrito na tabela a seguir e, em seguida, clique em **Avançar**.

Tabela 132. Opções da máquina virtual

Opção	Descrição
Nome da máquina virtual	Digite um nome para a máquina virtual. **NOTE:** Digite um nome entre 3 e 15 caracteres, usando apenas letras minúsculas, números e hífens.
Tamanho da máquina virtual	No menu suspenso, selecione um tamanho adequado para a VM. **NOTE:** Para obter mais informações sobre as configurações e preços do Azure, consulte a página preço de máquinas virtuais no site do Azure. Para links para outras referências úteis no sotes da Microsoft, consulte .
Ponto de extremidade (definições de acesso remoto)	
Nome	Selecione **Desktop remoto** ou **SSH**.
Protocolo	Selecione **TCP** ou **UDP**
Portas	Portas públicas e privadas; por padrão, use a 3389. Altere se necessário.
Portas do servidor de dados de transferência	Portas públicas e privadas; por padrão, use a 8009. Altere se necessário.
Portas do agente	Portas públicas e privadas; por padrão, use a 8006. Altere se necessário.

11. Na página **Discos**, selecione os volumes que você quer exportar e, em seguida, clique em **Concluir** para fechar o assistente e iniciar a implantação.

NOTE: Você pode monitorar o andamento da implantação visualizando as tarefas na página **Eventos**.

Ao concluir a implantação, na conta do Azure, você pode ver a nova VM na exibição **Ver máquinas (clássico)** do Azure. Uma vez que a VM está disponível, você também pagará taxas. Para não ter custos contínuos, exclua as VM implantadas quando não forem necessárias. Você pode sempre implantar uma VM a partir do conjunto mais recente de arquivos de exportação virtual repetindo este procedimento.

Gerenciar exportações

Caso o Core tenha uma configuração de exportação contínua, os parâmetros de configuração de cada exportação virtual são exibidos como uma linha na página **Standby virtual**. Aqui você pode ver o status das exportações contínuas estabelecidas e gerenciar as máquinas de standby virtual. Você pode adicionar um standby virtual, forçar uma exportação, pausar ou retomar um standby virtual, ou remover os requisitos de exportação contínua do Core Console.

Quando uma exportação única acontece, o trabalho é listado na fila de exportação da página **Standby virtual**. Durante esse tempo, você pode pausar, retomar ou cancelar a operação de exportação única.

NOTE: O Rapid Recovery suporta exportação do Hyper-V para Window 8, Window 8.1, Windows 10, Windows Server 2012, Windows Server 2012 R2 e Windows Server 2016.

A exportação virtual para uma VM com standby virtual não ocorre caso a VM esteja ligada.

Conclua as etapas nesse procedimento para gerenciar exportações virtuais.

1. A partir do Core Console, na barra de ícones, clique em (Standby virtual).

   A página **Standby virtual** é exibida. Aqui você pode ver duas tabelas de definições de exportação salvas. Elas incluem as informações descritas na tabela a seguir.

Tabela 133. Informações de standby virtual

Coluna	Descrição
Selecione um item	Para cada fila na tabela de resumo, você pode marcar a caixa de seleção para realizar ações na lista de opções do menu anterior à tabela.
Indicador de status	As esferas coloridas na coluna Status mostram o status de standby virtual. Quando você passa o cursor sobre o círculo colorido, a condição de status é exibida. • **Verde**. O standby virtual foi configurado com êxito, está ativo e não foi pausado. A próxima exportação é realizada logo depois da conclusão do próximo snapshot. • **Amarelo**. Standby virtual pausa, mas os parâmetros ainda estão definidos e salvos no Core. No entanto, depois de uma nova transferência, o trabalho de exportação não iniciará automaticamente e não haverá exportações novas para essa máquina protegida até o status mudar.
Nome da máquina	O nome da máquina de origem.
Tipo de exportação	Clique em para ver o tipo de exportação. Mostra o tipo de plataforma de máquina virtual para a exportação, como ESXi, VMware Workstation, Hyper-V, VirtualBox ou Azure.
Última exportação	Clique em para ver o tipo de exportação. Mostra a data e a hora da última exportação. Caso uma exportação tenha sido recém-adicionada, mas não tenha sido concluída, uma mensagem é exibida informando que a exportação ainda não foi realizada. Caso uma exportação tenha falhado ou tenha sido cancelada, uma mensagem correspondente também é exibida.

Coluna	Descrição
Destino	A máquina virtual e o caminho para o qual os dados estão sendo exportados.
Definições	O menu suspenso (Mais opções) permite realizar as seguintes funções: • **Editar**. Permite editar as definições de standby virtual. • **Forçar**. Força uma exportação virtual. • **Pausar**. Pausa a exportação virtual. Disponível apenas quando o status está ativo. • **Retomar**. Retoma a exportação virtual. Disponível apenas quando o status está pausado. • **Remover**. Remove o requisito para exportação contínua. Não remove a VM exportada atualizada mais recentemente. • **Implantar máquina virtual**. Para a exportação contínua do Azure apenas, converte os arquivos exportados na sua conta do Azure para uma VM inicializável.

Tabela 134. Informações da fila de exportação

Coluna	Descrição
Selecione um item	Para cada fila na tabela de resumo, você pode marcar a caixa de seleção para realizar ações na lista de opções do menu anterior à tabela. Essas opções incluem: • **Cancelar**. Cancela a exportação virtual única atual. • **Definições**. Permite que você atualize a configuração de exportações simultâneas máxima.
Indicador de status	Mostra o status da exportação atual como uma porcentagem. Quando não houver exportações únicas na fila, essa coluna não tem valor.
Nome da máquina	O nome da máquina de origem.
Tipo de exportação	Clique em para ver o tipo de exportação. Mostra o tipo de plataforma de máquina virtual para a exportação, como ESXi, VMware, Hyper-V, VirtualBox ou Azure.
Tipo de programa	Clique em para ver o tipo de programação. Mostra o tipo de exportação (Única ou Contínua).
Destino	A máquina virtual e o caminho para o qual os dados estão sendo exportados.

2. Para gerenciar as definições de exportação salvas, selecione uma exportação e clique em um dos seguintes:
   - **Editar**. Abre o **Assistente de exportação de máquina virtual** para a página **Opções de VM**. Aqui você pode alterar o local da VM exportada, alterar a versão do tipo de VM ou especificar RAM

ou processadores para a exportação. Para iniciar imediatamente a exportação do VM, selecione **Realizar a exportação única inicial**.

- **Forçar**. Força uma nova exportação. Essa opção pode ser útil quando o standby virtual está em pausa e é retomado, o que significa que o trabalho de exportação será reiniciado somente após uma nova transferência. Se não quiser esperar a nova transferência, poderá forçar uma exportação.
- **Pausar**. Pausa uma exportação ativa.
- **Retomar**. Retoma o requisito de continuar a exportação no próximo snapshot programado ou forçado.

3. Para remover uma exportação do sistema, selecione a exportação e clique em **Remover**.

   A configuração da exportação é removida permanentemente do sistema. A remoção da configuração de standby virtual não remove qualquer máquina virtual exportada como resultado da configuração.
4. Para implantar uma VM para o Azure, selecione **Implantar máquina virtual** e preencha os detalhes no assistente de implantação para o Azure.

   Os dados da exportação virtual mais recente salva na sua conta do Azure são implantados na sua conta Azure associada a uma máquina virtual inicializável.
5. Para gerenciar o número de exportações executadas simultaneamente, faça o seguinte:
   - Em Fila de exportação, clique em **Configurações**.
   - Na caixa de diálogo **Máximo de exportações simultâneas**, insira o número de exportações que você deseja executar simultaneamente. O número padrão é 5.
   - Clique em **Salvar**.
6. Para cancelar uma exportação única ou contínua listada no momento na Fila de exportação, selecione a exportações e clique em **Cancelar**.
7. Para adicionar uma nova exportação de standby virtual, é possível clicar em **Adicionar** para iniciar o Assistente de exportação. Concluir o assistente resulta em uma exportação contínua para a máquina protegida selecionada. Para obter mais informações sobre a definição de standby virtual para uma máquina virtual específica, consulte um dos seguintes tópicos:
   - Configurar a exportação contínua para ESXi
   - Configurar a exportação contínua para VMware Workstation
   - Configurar a exportação contínua para Hyper-V
   - Configurar a exportação contínua para VirtualBox
   - Configurar a exportação contínua para Azure

Restaurar dados

Esta seção descreve como restaurar dados armazenados em cópias de segurança.

Sobre como restaurar dados com o Rapid Recovery

O Rapid Recovery Core pode restaurar instantaneamente dados ou recuperar máquinas para máquinas físicas ou virtuais a partir dos pontos de recuperação. Os pontos de recuperação contêm snapshots de volume de agentes capturados no nível do bloco. Esses snapshots reconhecem o aplicativo, ou seja, todas as transações abertas e os registros de transações contínuas são concluídos e os caches são descarregados em disco antes da criação do snapshot. O uso de snapshots que reconhecem aplicativos em conjunto com o Verified Recovery permite que o Core realize vários tipos de recuperações, incluindo:

- Recuperação de arquivos e pastas
- Recuperação de volumes de dados usando Live Recovery
- Recuperação de volumes de dados para Microsoft Exchange Server e Microsoft SQL Server, usando Live Recovery
- Bare metal restore, usando o Universal Recovery
- Bare metal restore para hardware diferente, usando o Universal Recovery
- Exportação única, por demanda e contínua para máquinas virtuais

NOTE: Ao restaurar dados ou ao executar uma exportação virtual, o ponto de recuperação utilizado deve ser parte de uma cadeia completa de pontos de recuperação. Para obter mais informações sobre cadeias de pontos de recuperação, consulte o tópico Cadeias de pontos de recuperação e órfãos.

Noções básicas sobre Live Recovery

Live Recovery é um recurso de restauração de dados no Rapid Recovery Core. Se a máquina protegida apresentar uma falha de dados de um volume do Windows sem sistema, você poderá restaurar dados a partir de um ponto de recuperação no Rapid Recovery Core. A seleção do Live Recovery no Restore Wizard permite que os usuários continuem imediatamente operações de negócios com inatividade quase zero. O Live Recovery durante a restauração dá acesso imediato aos dados, mesmo enquanto o Rapid Recovery continua restaurando dados em segundo plano. Esse recurso permite tempo de recuperação quase zero, mesmo que a restauração envolva terabytes de dados.

Rapid Recovery Core usa tecnologia de backup e recuperação com base em bloco exclusiva que permite acesso total ao usuário para servidores de destino durante o processo de recuperação. Os blocos solicitados são recuperados sob demanda para recuperação total.

O Live Recovery se aplica a máquinas físicas e virtuais protegidas pelo Rapid Recovery Core, com as seguintes exclusões:

- O Live Recovery é acessível a volumes Windows sem sistema. A unidade C:/ e a partição reservada para o sistema não podem ser restauradas usando-se o Live Recovery.
- O Live Recovery é acessível a volumes com base no Windows usando-se o Rapid Recovery Agent. Os volumes sem agente ou os volumes Linux não podem usufruir o Live Recovery.

O Live Recovery permite restaurar de maneira instantânea ou servidores virtuais diretamente do arquivo de backup. Quando um volume sem sistema está sendo restaurado, o Rapid Recovery apresenta os metadados de volume para o Sistema operacional de maneira instantânea, o que torna esses dados disponíveis sob demanda. Por exemplo, se volume do banco de dados do Microsoft Exchange estiver corrompido, o Live Recovery poderá restaurar o volume, o banco de dados e os serviços do Exchange em questão de minutos.

Esse recurso fornece o método mais rápido de recuperar grandes quantidades de dados com o mínimo de inatividade. Os usuários podem continuar imediatamente operações de negócios.

Assim que o Live Recovery começa, o volume restaurado e o conteúdo se tornam disponíveis instantaneamente. Rapid RecoveryCore continua restaurando os dados em segundo plano, mesmo que o volume, os dados, os aplicativos e os serviços já estejam novamente em produção. Se dados específicos forem solicitados, o processo em segundo plano priorizará a restauração desses dados imediatamente. Essa funcionalidade eficiente permite que até mesmo o contrato de serviço mais rígido seja atendido.

Depois que você iniciar o Live Recovery, metadados (estrutura de diretório, descritores de segurança, atributos de arquivo NTFS, mapa de espaço livre etc.) do volume de destino serão restaurados rapidamente na máquina protegida. Assim, o volume e o conteúdo se tornam disponíveis para o sistema. O Agente do Rapid Recovery começa a restaurar blocos de dados do servidor Core do Rapid Recovery, gravando os blocos no volume de destino.

Solicitações de dados que ainda não tiverem sido restauradas serão atendidas imediatamente, com o programa solicitante ou o sistema que desconhece que os blocos acabaram de ser restaurados.

Restaurar dados de pontos de recuperação

O Rapid Recovery protege seus dados em máquinas Windows e Linux. Os backups das máquinas protegidas são salvos no repositório associado ao Rapid Recovery Core como pontos de recuperação. Nesses pontos de recuperação, você pode restaurar seus dados usando um dos métodos a seguir.

- No Rapid Recovery Core Console, você pode restaurar volumes inteiros a partir de um ponto de recuperação de um volume que não seja de sistema, substituindo os volumes na máquina de destino. Para obter mais informações, consulte Sobre restauração de volumes a partir de um ponto de recuperação.
- Você também pode restaurar volumes inteiros em máquinas Linux de pontos de recuperação usando a linha de comando do agente Linux. Para obter mais informações sobre como usar o utilitário de linha de comando local_mount, consulte Restaurar volumes em uma máquina Linux usando a linha de comando.

Não é possível restaurar um volume que contenha o sistema operacional diretamente de um ponto de recuperação, porque a máquina para a qual você está restaurando está usando o sistema operacional e os drivers que estão incluídos no processo de restauração. Se você deseja restaurar a partir de um ponto de recuperação em agente um volume do sistema (por exemplo, a unidade C da máquina protegida), realize uma bare metal restore (BMR). Isso envolve a criação de uma imagem inicializável a partir do ponto de recuperação, o que inclui o sistema operacional e os arquivos de configuração, bem como os dados. Em seguida, você inicia o computador de destino a partir dessa imagem inicializável para concluir a restauração. A imagem inicializável é diferente se a máquina que você deseja restaurar usa um sistema operacional Windows ou Linux. Se você deseja restaurar a partir de um ponto de recuperação em um volume do sistema em uma máquina com Windows, consulte Realizar uma restauração sem sistema operacional para máquinas Windows. Se você deseja restaurar

a partir de um ponto de recuperação em um volume do sistema em uma máquina com Linux, consulteRealizar uma restauração sem sistema operacional para máquinas Windows.

Se você tiver um RAID de software em uma máquina Linux protegida pelo Rapid Recovery Agent versão 6.2, você pode restaurar o RAID de software a partir de um ponto de recuperação.

NOTE: Como esse recurso foi introduzido no versão 6.2, ele não é compatível com os instantâneos obtidos em versões mais recentes do Agent. Se você atualizar o Rapid Recovery Agent para o versão 6.2 ou posterior e, em seguida, capturar instantâneos em seu Rapid Recovery Core, será possível restaurar o RAID de software de novos instantâneos.

Finalmente, em contraste com a restauração de volumes inteiros, é possível montar um ponto de recuperação a partir de uma máquina com Windows e navegar pelas pastas e arquivos individuais para recuperar apenas um conjunto específico de arquivos. Para obter mais informações, consulte Restaurar um diretório ou arquivo usando o Windows Explorer. Se for preciso fazer isso e preservar as permissões de arquivos originais (por exemplo, ao restaurar uma pasta de usuário em um server de arquivos), consulte Restaurar um diretório ou arquivo e preservar as permissões usando o Windows Explorer.

Os tópicos desta seção descrevem informações sobre como restaurar dados em máquinas físicas. Para obter mais informações sobre a exportação de dados protegidos de um ponto de recuperação para uma máquina virtual, consulte Exportação da VM.

NOTE: Ao recuperar dados em máquinas com Windows, se o volume que você está restaurando está com a deduplicação de dados do Windows ativada, será preciso ter certeza que a deduplicação também está ativada no server do Core. O Rapid Recovery suporta o Windows 8, Windows 8.1, Windows 10, Windows Server 2012, Windows Server 2012 R2 e Windows Server 2016 para transferências normais (de base e incrementais), bem como para restauração de dados, bare metal restore e exportações virtuais. Para obter mais informações sobre os tipos de volumes suportados e não suportados para backup e recuperação, consulte o tópico "Limitações de suporte para volumes dinâmicos e básicos", no *Guia de requisitos do sistema do Rapid Recovery*.

Sobre o recurso de pesquisa e restauração de arquivo

O recurso de pesquisa e restauração de arquivo do Rapid Recovery permite que você encontre um ou mais arquivos nos pontos de recuperação de uma máquina protegida. Em seguida, você pode restaurar um ou mais dos resultados para um disco local.

Como pesquisar diretrizes

Na página **Pesquisa de arquivo** do Core Console, você pode procurar por um arquivo a partir de um conjunto de pontos de recuperação da máquina que você selecionar. Os critérios de pesquisa são divididos em dois grupos: básico e avançado.

O grupo básico contém os seguintes parâmetros:

- A máquina protegida cujos pontos de recuperação você quer pesquisar.
- Um intervalo de tempo que limita a pesquisa a apenas pontos de recuperação criados entre o horário de início e o horário de término.
- O nome ou a máscara do arquivo que você deseja encontrar. Você pode usar o curinga "?" para substituir qualquer caractere e o "*" para substituir nenhum ou múltiplos caracteres; no entanto, nomes de arquivos mais específicos produzem resultados mais específicos.
- Uma lista de caminhos para os diretórios nos quais pesquisar.

NOTE: Todos os critérios básicos são obrigatórios. Se nenhum diretório for fornecido, o Rapid Recovery pesquisa todos os volumes da máquina protegida especificada.

O botão **Mais opções** revela o grupo avançado, que contém os seguintes parâmetros:

- A opção para pesquisar recursivamente nos subdiretórios do local de pesquisa ou somente no local especificado.
- A capacidade de executar um algoritmo que aumenta a velocidade das pesquisas em volumes NTFS.
- A capacidade de limitar o número de resultados da pesquisa a uma soma mais gerenciável.

NOTE: Critérios de pesquisa específicos produzem resultados de pesquisa mais rápidos e precisos. A inclusão dos subdiretórios (por exemplo, `C:\work\documents\accounting` em vez de `C:`) reduz o tempo total para concluir a pesquisa, pois fornece máscaras de arquivo restritivas (por exemplo, `invoice*.pdf` em vez de `in*.*`).

Como o recurso continua pesquisando através dos pontos de recuperação e dos locais mesmo após o arquivo solicitado ser encontrado, você pode pausar ou parar uma pesquisa antes dela terminar. Você pode executar várias pesquisas simultaneamente, mas você não pode começá-las ao mesmo tempo. Por exemplo, para encontrar outro arquivo, você pode começar uma segunda pesquisa enquanto a primeira pesquisa ainda está em andamento. No entanto, você só pode pesquisar uma máquina protegida de cada vez.

NOTE: No exemplo anterior, pausar a primeira pesquisa libera mais memória para a segunda pesquisa, o que ajuda a concluir a segunda pesquisa mais rapidamente. Executar várias pesquisas de uma só vez consome muita memória e aumenta o tempo que leva para concluir uma pesquisa.

Cada pesquisa aparece como uma guia na página. Ao terminar a pesquisa, você pode fechar as guias individualmente ou todas de uma vez.

Diretrizes de restauração

Depois de encontrar o arquivo, você pode restaurá-lo diretamente da página **Pesquisa de arquivo**.

O recurso de pesquisa e restauração de arquivo limita as capacidades de restauração a apenas locais no Core. Você não pode restaurar um arquivo para uma máquina protegida.

Tarefas relacionadas

See also: Localizar e restaurar um arquivo

Localizar e restaurar um arquivo

Quando você quiser restaurar um arquivo em vez de um volume, você pode usar o Rapid Recovery para encontrar esse arquivo entre os pontos de recuperação da sua máquina protegida. Pesquisar critérios, como, por exemplo, o intervalo de datas e o diretório, permite que você refine a pesquisa a um pequeno grupo de pontos de recuperação relevantes.

NOTE: Pesquisar critérios específicos produz resultados de pesquisa mais rápidos e precisos, e consome menos memória. A inclusão dos subdiretórios (por exemplo, `C:\work\documents\accounting` em vez de `C:`) reduz o tempo total para concluir a pesquisa, pois fornece máscaras de arquivo restritivas (por exemplo, `invoice*.pdf` em vez de `in*.*`).

Depois de encontrar o arquivo, você pode, então, restaurá-lo diretamente da lista de resultados da pesquisa.

1. Na barra de ícones do Rapid Recovery Core Console, clique no menu suspenso **Mais** e selecione **Pesquisa de arquivo**.

   A página **Pesquisa de arquivos** é aberta.
2. Na página **Pesquisa de arquivos**, para procurar um arquivo dentro dos pontos de recuperação de uma máquina protegida específica, preencha as informações descritas na tabela a seguir.

Tabela 135. Critérios de pesquisa de arquivos

Pesquisar critérios para encontrar um arquivo de dentro dos pontos de recuperação de uma máquina protegida.

Caixa de texto	Descrição
Máquina	Selecione a máquina protegida que você quer pesquisar na lista suspensa. **NOTE:** Você pode pesquisar nos pontos de recuperação de apenas uma máquina protegida de cada vez.
Intervalo de datas de pontos de recuperação	Especifique a data e a hora do ponto de recuperação mais antigo e do ponto de recuperação mais recente que você deseja pesquisar. Apenas os pontos de recuperação criados dentro deste intervalo serão consultados. **NOTE:** O intervalo de tempo padrão é o mês anterior. Por exemplo, se fizer a pesquisa em terça-feira, 22 de agosto de 2017, às 14:04, o intervalo de datas padrão é das 14:04 do dia 22/07/2017 até 14:04 do dia 22/08/2017.
Nome do arquivo (pode usar os caracteres curingas * e ?)	Digite o nome do arquivo ou uma máscara de arquivo para o arquivo que você deseja localizar e restaurar. Caracteres curingas podem ser usados como substitutos de caracteres desconhecidos. **NOTE:** Você pode usar o curinga "?" para substituir qualquer caractere e o curinga "*" para substituir nenhum ou múltiplos caracteres.
Diretórios a pesquisar	Lista um ou mais diretórios na máquina protegida para limitar a pesquisa a apenas esses locais. **NOTE:** Se nenhum diretório for fornecido, o Rapid Recovery pesquisa todos os volumes da máquina protegida especificada.

3. Como opção, clique em **Mais opções** e, em seguida, preencha as informações descritas na tabela a seguir.

Tabela 136. Mais opções de pesquisa de arquivo

Mais critérios de pesquisa para encontrar um arquivo de dentro dos pontos de recuperação de uma máquina protegida.

Caixa de texto	Descrição
Incluir os subdiretórios	Pesquisa em todos os subdiretórios dos diretórios relacionados na Etapa 3. Ativado por padrão.
Usar o algoritmo de pesquisa rápida para volumes NTFS	Pesquisa volumes NTFS sem montá-los, analisando as estruturas de dados do sistema de arquivos, o que é mais rápido e consome menos memória durante a pesquisa. Ativado por padrão. **NOTE:** Se você obteve um falha durante uma pesquisa em um volume NTFS, tente executar a pesquisa novamente sem essa opção selecionada.
Limitar os resultados da pesquisa para	Digite o número máximo de resultados que você deseja que apareça nos resultados. O padrão é 1000.

4. Clique em **Iniciar pesquisa**

Começa a pesquisa. Cada pesquisa aparece como uma guia em **Resultados da pesquisa**. Você pode usar os botões de cada guia para pausar ou parar uma pesquisa, ou você pode clicar no **X** na guia para excluir a pesquisa. Várias pesquisas podem ser executadas simultaneamente.

5. Nos resultados da pesquisa, selecione o arquivo que você quer restaurar.
6. Clique em **Restaurar**.

   A caixa de diálogo **Restaurar arquivos** é aberta.
7. Em **Local**, digite um caminho de destino para o arquivo restaurado na máquina na qual o Core está instalado e em execução.
8. Clique em **Restaurar**.

   O arquivo selecionado é restaurado para o caminho do destino especificado com a árvore de diretório original na qual o arquivo foi mostrado na máquina protegida.

Conceitos relacionados

See also: Sobre o recurso de pesquisa e restauração de arquivo

Sobre restauração de volumes a partir de um ponto de recuperação

É possível restaurar volumes em uma máquina protegida a partir dos pontos de recuperação armazenados no Rapid Recovery Core usando o assistente de Restauração de máquinas.

NOTE: Em versões anteriores, esse processo era conhecido como realizar uma reversão.

NOTE: O Rapid Recovery suporta a proteção e recuperação de máquinas configuradas com partições EISA. O suporte também foi estendido para máquinas Windows 8, Windows 8.1, Windows Server 2012, Windows Server 2012 R2 e Windows Server 2016 que usam o Windows Recovery Environment (Windows RE).

É possível iniciar uma restauração a partir de qualquer local no Rapid Recovery clicando no ícone **Restaurar** na barra de botões do Rapid Recovery Core Console. Ao iniciar uma restauração dessa maneira, é preciso especificar qual das máquinas protegidas no Core você deseja restaurar e, depois, explorar até o volume que deseja restaurar.

Ou você pode ir até a página **Pontos de recuperação** para uma máquina específica, clicar no menu suspenso para um ponto de recuperação específico e, em seguida, selecionar **Restaurar**. Se uma restauração for iniciada dessa maneira, siga começando com a Etapa 5 no tópico Restaurar volumes a partir de um ponto de recuperação.

Você também pode restaurar a partir de um ponto de recuperação em uma máquina Linux na linha de comando. Para obter mais informações, consulte o tópico Restaurar volumes em uma máquina Linux usando a linha de comando.

Se você deseja restaurar a partir de um ponto de recuperação em um volume do sistema, ou restaurar a partir de um ponto de recuperação utilizando um CD de inicialização, você deve realizar uma Bare Metal Restore (BMR). Para obter informações sobre a BMR, consulte Restauração sem sistema operacional para máquinas Windows, e para obter informações de pré-requisitos para sistemas operacionais Windows ou Linux, consulte Pré-requisitos para realizar uma restauração sem sistema operacional para uma máquina Windows e Pré-requisitos para realizar uma bare metal restore em máquinas Linux, respectivamente. É possível acessar as funções da BMR a partir do Core Console conforme descrito no roteiro para cada sistema operacional. Também é possível realizar uma BMR a partir do assistente de Restauração de máquinas. Esse procedimento irá direcioná-lo ao ponto adequado no assistente para o procedimento Realizar um bare metal restore usando o Assistente de restauração de máquina.

Restaurar volumes a partir de um ponto de recuperação

Para restaurar volumes a partir de um ponto de recuperação, seu computador deve estar protegido no Core no nível de volume, e o Core deve conter os pontos de recuperação a partir dos quais você executará a operação de restauração.

Execute o procedimento a seguir para restaurar volumes em um ponto de recuperação.

1. Para restaurar um volume em uma máquina protegida, navegue até o Core Console e clique em **Restaurar** na barra de botões do Rapid Recovery.

   O Assistente de restauração de máquinas é exibido.

2. Na página **Máquinas protegidas**, selecione a máquina protegida da qual deseja restaurar os dados e clique em **Avançar**.

   Aparece a página **Pontos de recuperação**.

3. Na lista de pontos de recuperação, procure o snapshot que deseja restaurar da máquina protegida.

   - Se necessário, use os botões na parte inferior da página para exibir páginas adicionais dos pontos de recuperação.
   - Como opção, para limitar o número de pontos de recuperação que aparecem na página **Pontos de recuperação** do assistente, você pode filtrar por volumes (se definidos) ou por data de criação do ponto de recuperação.

4. Clique em qualquer ponto de recuperação para selecioná-lo e em **Avançar**.

   Aparece a página **Destino**.

5. Na página **Destino**, escolha a máquina para a qual deseja restaurar os dados da seguinte forma:

   - Para restaurar os dados a partir do ponto de recuperação selecionado para a mesma máquina, e se os volumes que deseja restaurar não incluem o volume do sistema, selecione **Recuperar em uma máquina protegida (apenas volumes que não são do sistema)**, confirme se a máquina de destino está selecionada e clique em **Avançar**.

     A página **Mapeamento de volume** é exibida. Vá para a Etapa 9.

   - Para restaurar os dados a partir do ponto de recuperação selecionado em uma máquina protegida diferente (por exemplo, substituir o conteúdo da Machine2 pelos dados da Machine1), selecione **Recuperar em uma máquina protegida (apenas volumes que não são do sistema)**, selecione a máquina de destino na lista e clique em **Avançar**.

     A página **Mapeamento de volume** é exibida. Vá para a Etapa 9.

   - Se você deseja restaurar a partir do ponto de recuperação selecionado na mesma máquina ou em uma máquina diferente usando um CD de inicialização, esse processo é considerado uma bare metal restore (BMR). Para obter informações sobre a BMR, consulte Bare metal restore.

NOTE: A realização de uma BMR tem requisitos específicos, com base no sistema operacional da máquina que você deseja restaurar. Para entender esses pré-requisitos, consulte Pré-requisitos para realizar uma restauração sem sistema operacional para uma máquina Windows e Pré-requisitos para realizar uma bare metal restore em máquinas Linux, respectivamente.

NOTE: Se os volumes que deseja restaurar incluem o volume do sistema, selecione **Recuperar em qualquer máquina de destino usando um CD de inicialização**. Esta opção irá notificá-lo a criar um CD de inicialização.

- Para continuar e criar o CD de inicialização com as informações do ponto de recuperação selecionado utilizando o assistente de Restauração de máquinas, clique em **Avançar** e vá para a Realizar uma restauração sem sistema operacional para máquinas Windows.
- Se você já criou o CD de inicialização e a máquina de destino foi iniciada utilizando-o, vá para a Etapa 8 do tópico Realizar uma restauração sem sistema operacional para máquinas Windows.

- Se você deseja restaurar a partir de um ponto de recuperação em um volume do sistema (por exemplo, a unidade C da máquina agente chamada Machine1), esse processo também é considerado uma BMR. Selecione **Recuperar em qualquer máquina de destino usando um CD de inicialização**. Esta opção irá notificá-lo a criar um CD de inicialização.
  - Para continuar e criar o CD de inicialização com as informações do ponto de recuperação selecionado utilizando o assistente de Restauração de máquinas, clique em **Avançar** e vá para a Realizar uma restauração sem sistema operacional para máquinas Windows.
  - Se você já criou o CD de inicialização, vá para a Etapa 6.

6. Inicie a máquina que você deseja restaurar utilizando o CD de inicialização. Para obter mais informações para BMR em uma máquina com Windows, consulte Como carregar o CD de inicialização e iniciar o computador de destino, e para BMR em uma máquina com Linux, consulte Carregar o Live DVD e iniciar o computador de destino.
7. No server do Core, na página **Destino** do assistente de Restauração de máquinas, selecione **Já possuo um CD de inicialização executando na máquina de destino** e insira as informações sobre a máquina à qual deseja se conectar, conforme descrito na tabela a seguir.

Tabela 137. Informações da máquina

Caixa de texto	Descrição
Endereço IP	O endereço IP da máquina na qual deseja restaurar. É idêntico ao endereço IP exibido no URC.
Chave de autenticação	A senha específica para se conectar ao server selecionado. É idêntico à chave de autenticação exibida no URC.

8. Clique em **Avançar**.

   Se as informações de conexão inseridas correspondem ao URC, e se o Core e o server de destino podem identificar um ao outro corretamente na rede, os volumes do ponto de recuperação selecionado são carregados. A página **Mapeamento de disco** é exibida.

   Para concluir sua BMR a partir do assistente de Restauração de máquinas, vá para a Etapa 9 do tópico Realizar uma restauração sem sistema operacional para máquinas Windows.

NOTE: O Rapid Recovery suporta partições FAT32 e ReFS. Apenas restauração completa e BRM são suportados, pois há uma limitação de driver com ReFS. A restauração é implementada no modo de usuário, exportação de VM e assim por diante. Se um Core está protegendo pelo menos um volume agente que contém o sistema de arquivos ReFS, ele deve ser instalado em máquinas com Windows 8,1, Windows 10 (Enterprise ou Pro apenas), Windows 2012, Windows Server 2012 ou Windows Server 2012 R2, quem fornece suporte nativo ao formato ReFS. Caso contrário, a funcionalidade ficará limitada, e operações que envolvem tarefas, como a montagem de uma imagem de volume, não funcionarão. O Rapid Recovery Core Console apresentará as mensagens de erro aplicáveis a essas ocorrências. A bare metal restore da configuração de discos de espaços de armazenamento também não é suportada nesta versão. Para obter mais detalhes, consulte o *Guia de instalação e atualização do Rapid Recovery*.

9. Na página **Mapeamento de volume**, para cada volume no ponto de recuperação que você deseja restaurar, selecione o volume de destino apropriado. Se você não deseja restaurar um volume, na coluna Volumes de destino, selecione **Não restaurar**.
10. Selecione **Exibir opções avançadas** e faça o seguinte:

    - Para restaurar em máquinas com Windows, se quiser usar o Live Recovery, selecione **Live Recovery**.

      Usando a tecnologia de recuperação instantânea Live Recovery no Rapid Recovery, é possível recuperar ou restaurar instantaneamente os dados em suas máquinas físicas ou virtuais a partir de pontos de recuperação armazenados de máquinas Windows, incluindo Espaços de Armazenamento do Microsoft Windows. O Live Recovery não está disponível para máquinas Linux ou MVs que usam proteção sem agente.

    - Se você deseja forçar a desmontagem dos volumes selecionados antes de iniciar a restauração, selecione **Forçar desmontagem**.

      CAUTION: Se você não forçar uma desmontagem antes de restaurar os dados, a restauração pode falhar com um erro indicando que o volume está em uso.

11. Clique em **Avançar.**
12. Na página **Desmontar bancos de dados**, se os volumes que você quer restaurar contêm bancos de dados Oracle, SQL ou Microsoft Exchange, você será solicitado a desmontá-los. Se você quiser remontar automaticamente esses bancos de dados após a restauração ser concluída, selecione **Remontar automaticamente todos os bancos de dados após o ponto de recuperação ser restaurado**. Caso contrário, desmarque essa opção.

    NOTE: O gravador VSS apropriado captura instantâneos do banco de dados no modo de backup. Se você optar por não remontar todos os bancos automaticamente (a opção padrão), depois de restaurar, inicie manualmente os bancos de dados.

13. Clique em **Avançar.**

A página Aviso pode ser exibida e solicitar que você feche todos os programas nos volumes que você quer restaurar. Se houver algum, clique em Avançar novamente.

14. Na página **Resumo**, selecione a opção **IMPORTANTE! Eu sei que esta operação sobrescreverá os volumes selecionados com os dados do ponto de recuperação selecionado** para confirmar que você entende as consequências de uma restauração de volume.

    WARNING: Esta opção enfatiza a consequência que todos os dados salvos no volume selecionado após a data e a hora do ponto de recuperação selecionado serão perdidos devido à restauração.

15. Clique em **Concluir**.

Restaurar um diretório ou arquivo usando o Windows Explorer

Você pode utilizar o Windows Explorer para copiar e colar diretórios e arquivos de um ponto de recuperação montado em qualquer máquina Windows. Isso pode ser útil quando você quer distribuir apenas uma parte de um ponto de recuperação para os usuários.

Quando você copia diretórios e arquivos, as permissões de acesso do usuário que está executando a operação de cópia são usadas e aplicadas aos diretórios e arquivos colados. Se você quiser restaurar diretórios e arquivos para seus usuários e preservar as permissões de arquivos originais (por exemplo, ao restaurar uma pasta de usuário em um server de arquivos), consulte Restaurar um diretório ou arquivo e preservar as permissões usando o Windows Explorer.

1. Monte o ponto de recuperação que contém os dados que você deseja restaurar. Para obter detalhes, consulte Montar um ponto de recuperação.
2. No Windows Explorer, navegue até o ponto de recuperação montado e selecione os diretórios e arquivos que você deseja restaurar. Clique com o botão direito e selecione **Copiar**.
3. No Windows Explorer, navegue até o local da máquina onde você deseja restaurar os dados. Clique com o botão direito e selecione **Colar**.

Restaurar um diretório ou arquivo e preservar as permissões usando o Windows Explorer

Você pode utilizar o Windows Explorer para copiar e colar diretórios e arquivos de um ponto de recuperação montado em qualquer máquina Windows e, ao mesmo tempo, preservar as permissões de acesso aos arquivos.

Por exemplo, se você precisar restaurar um pasta acessada somente por usuários específicos em um servidor de arquivos, pode usar os comandos Copiar e Colar com Permissões para garantir que os arquivos restaurados mantenham as permissões que restringem o acesso. Dessa forma, você pode evitar a necessidade de aplicar manualmente as permissões aos diretórios e arquivos restaurados.

Alguns arquivos têm restrições de acesso que exigem privilégios administrativos. Especialmente para o Windows Server 2012 e sistemas operacionais posteriores, o usuário que tentar a restauração deve ter as permissões NTFS corretas para que a restauração com permissões seja bem-sucedida. Por exemplo, para copiar todas as permissões NTFS de um ponto de montagem, o usuário deve ter privilégios administrativos (com todas as permissões NTFS).

NOTE: O comando Colar com Permissões é instalado com os softwares Rapid Recovery Core e Agent. Ele não está disponível no Local Mount Utility.

1. Monte o ponto de recuperação que contém os dados que você deseja restaurar. Para obter detalhes, consulte Montar um ponto de recuperação.
2. No Windows Explorer, navegue até o ponto de recuperação montado e selecione os diretórios e arquivos que você deseja restaurar. Clique com o botão direito e selecione **Copiar**.
3. No Windows Explorer, navegue até o local da máquina onde você deseja restaurar os dados. Clique com o botão direito e selecione **Colar com Permissões**.

   NOTE: Nesta etapa, se o comando Colar com Permissões estiver desativado no menu acionado com o botão direito, o Windows Explorer não está reconhecendo os arquivos que você quer copiar. Repita a Etapa 2 para habilitar o comando Colar com permissões no menu acessado com o botão direito do mouse.

Restaurar clusters e nós de cluster

A restauração é o processo de restaurar os volumes em uma máquina a partir de pontos de recuperação. Para um cluster de servers, realize a restauração no nível de nó ou da máquina. Esta seção fornece orientações sobre como realizar uma restauração em volumes de cluster.

Realizar uma restauração de clusters CCR e DAG (Exchange)

Execute as etapas deste procedimento para realizar uma restauração de clusters CCR e DAG (Exchange).

1. Desative todos os nós, com exceção de um.
2. Realize uma restauração usando o procedimento Rapid Recovery padrão da máquina conforme descrito em Sobre restauração de volumes a partir de um ponto de recuperação e Restaurar volumes em uma máquina Linux usando a linha de comando.
3. Quando a restauração for concluída, monte todos os bancos de dados para os volumes de cluster.
4. Ative todos os outros nós.
5. Para o Exchange, navegue até o Console de gerenciamento do Exchange e, para cada banco de dados, execute a operação Atualizar cópia de banco de dados.

Realizar uma restauração de clusters SCC (Exchange, SQL)

Execute as etapas deste procedimento para realizar uma restauração em clusters de SCC (Exchange, SQL).

1. Desative todos os nós, com exceção de um.
2. Realize uma restauração usando o procedimento Rapid Recovery padrão da máquina conforme descrito em Sobre restauração de volumes a partir de um ponto de recuperação e Restaurar volumes em uma máquina Linux usando a linha de comando.
3. Depois que a restauração for concluída, monte todos os bancos de dados a partir dos volumes de cluster.
4. Ative todos os outros nós, um por um.

> **NOTE:** Não é preciso executar nenhuma reversão no disco de quórum. Ele pode ser regenerado automaticamente ou usando a funcionalidade do serviço de cluster.

Restauração a partir de um arquivo anexado

Existem duas maneiras como você pode restaurar dados de um arquivo: você pode usar um arquivo como uma origem para uma bare metal restore (BMR); ou você pode anexar um arquivo, montar um ponto de recuperação do arquivo e restaurar os dados arquivados.

Quando você anexa um arquivo, ele é exibido em Arquivos anexados na página Arquivos do Console do Core, e o conteúdo do arquivo se torna acessível na área de navegação à esquerda. O conteúdo é exibido sob o nome do arquivo. Máquinas que foram arquivadas são exibidas como máquinas "apenas pontos de recuperação", de maneira que você possa acessar os pontos de recuperação da mesma forma como faria para uma máquina protegida no momento: montando um ponto de recuperação, localizando o item que você deseja recuperar e usando o Windows Explorer para copiar e colar o item no destino.

Há vantagens em restaurar a partir de um arquivo anexado, em vez de importar um arquivo para um repositório.

- A restauração a partir de um arquivo anexado economiza o tempo que você pode gastar importando um arquivo inteiro para um repositório.
- Além disso, quando você importa um arquivo, os pontos de recuperação arquivados são adicionados ao repositório.

  Como esses pontos de recuperação arquivados devem ser os itens mais antigos no repositório, eles podem ser acumulados de acordo com a política de retenção durante o próximo trabalho noturno. (Embora essa ação não os exclua do arquivo, você pode reimportá-los no dia seguinte.)
- Por fim, o Core lembra a associação do anexo com arquivos, mesmo depois de destacar um arquivo, o que deixa mais rápido e fácil anexar o arquivo novamente mais tarde.

  Você pode remover a associação excluindo o anexo.

Para restaurar dados de um arquivo anexado, conclua as seguintes etapas usando os links relacionados:

NOTE: O procedimento de restauração a partir de um arquivo anexado presume que você já tenha um arquivo de pontos de recuperação acumulados.

1. Anexe o arquivo.
2. Monte o ponto de recuperação que contém os dados que você deseja recuperar.
3. Restaure dados usando qualquer um dos seguintes métodos:
   - Restaure dados, como arquivo ou pasta, a partir do ponto de recuperação.
   - Restaure todo o ponto de recuperação.
   - Exporte o ponto de recuperação para uma máquina virtual.

See also: Noções básicas sobre arquivos
See also: Anexar um arquivo
See also: Importação de um arquivo
See also: Montar um ponto de recuperação
See also: Restaurar um diretório ou arquivo usando o Windows Explorer
See also: Restaurar volumes a partir de um ponto de recuperação
See also: Exportação para máquinas virtuais usando o Rapid Recovery
See also: Como realizar uma BMR com base em um arquivo

Restauração de e-mail no Rapid Recovery

O recurso de restauração de e-mail no Rapid Recovery permite que você restaure uma caixa de correio, uma pasta ou um item – como uma mensagem, evento do calendário ou contato – do armazenamento de dados de uma máquina protegida do Exchange Server. É possível restaurar a seleção para uma pasta de recuperação, para fonte original ou para um ou mais arquivos PST.

Você pode acessar a página de restauração de e-mail pelo menu **Mais (**...) do Rapid Recovery Core Console. Nela, você poderá executar as seguintes ações:

- Abrir um banco de dados do Exchange
- Restaurar um item do banco de dados aberto
- Fechar o banco de dados
- Procurar um item no banco de dados aberto

Para obter mais informações, consulteAbrir um banco de dados do Exchange no Rapid Recovery e Restaurar um item de e-mail no Rapid Recovery.

Pré-requisitos de restauração de e-mail

Antes de restaurar itens de e-mail, você deve atender aos seguintes pré-requisitos:

- Ter o Outlook 2007 ou posterior instalado na máquina do Core.
- Ter pelo menos um perfil configurado no Microsoft Outlook.
- O perfil do Outlook deve ter permissões de controle total, incluindo permissões Enviar como e Receber como.Para obter mais informações, consulte.
- A opção Modo Cache do Exchange, no perfil do Outlook associado ao Rapid Recovery deve estar desabilitada.
- A máquina do Core deve estar no mesmo domínio do banco de dados do Exchange.
- O banco de dados do Exchange necessário deve estar aberto, e você deve estar na página **Restauração de email** do Rapid Recovery Core Console.Para obter mais informações, consulteAbrir um banco de dados do Exchange no Rapid Recovery.

Sem as permissões apropriadas e uma instância do Outlook instalada na máquina do Core, não é possível realizar a recuperação de itens do Exchange, mesmo que o servidor Exchange esteja protegido por um Rapid Recovery Core.

Abrir um banco de dados do Exchange no Rapid Recovery

Antes de iniciar esta tarefa, é preciso cumprir os pré-requisitos a seguir:

- Ter o Outlook 2007 ou posterior instalado na máquina do Core.
- A máquina do Core deve estar no mesmo domínio do banco de dados do Exchange.
- As permissões adequadas devem estar definidas no Exchange. Para obter mais informações, consulte .

O Rapid Recovery permite que você restaure itens de email sem sair da interface. Os itens de e-mail residem no banco de dados do Exchange no ponto de recuperação da máquina protegida do Exchange Server, que você pode abrir usando o Assistente para abrir bancos de dados do Exchange.

1. No Rapid Recovery Core Console, clique no menu Mais (**...**) e depois clique em **Restauração de email**.
2. Na página **Restauração de email**, para acessar o banco de dados do Exchange onde o item de email está armazenado, clique em **Abrir banco de dados**.

O Assistente para abrir bancos de dados do Exchange será aberto.

3. Na página **Local** do assistente, você pode abrir um banco de dados a partir de uma máquina protegida ou de um caminho local, como sua máquina atual ou um compartilhamento de arquivos:
   - **Abrir a partir da máquina protegida**: Clique em **Avançar** e passe para a próxima etapa desta tarefa.
   - **Abrir a partir do caminho local**: Digite as informações a seguir do local e clique em **Concluir**:
     - Caminho do arquivo de banco de dados
     - Caminho dos logs
     - Caminho do sistema
4. Na página **Máquinas**, selecione a máquina protegida que armazena o banco de dados do Exchange e clique em **Avançar**.
5. Na página **Pontos de recuperação**, selecione o ponto de recuperação referente ao período do qual você quer abrir o banco de dados e clique em **Avançar**.
6. Na página **Bancos de dados**, selecione o banco de dados do Exchange que você quer abrir e clique em **Avançar**.

   O Rapid Recovery abre o banco de dados selecionado e o exibe na página **Restauração de email**, com a caixas de correio e pastas listadas à esquerda em uma árvore de navegação expansível. Os itens nas pastas são exibidos à direita.

   NOTE: O tempo que leva para o Rapid Recovery abrir o banco de dados do Exchange depende do tamanho do banco de dados.

Para restaurar um item do banco de dados aberto, consulte Restaurar um item de e-mail no Rapid Recovery.

Restaurar um item de e-mail no Rapid Recovery

Antes de iniciar esta tarefa, certifique-se de que tenha cumprido os pré-requisitos para a realização de uma restauração de e-mail.Para obter mais informações, consultePré-requisitos de restauração de e-mail.

O recurso de restauração de e-mail no Rapid Recovery permite que você restaure uma caixa de correio, uma pasta ou um item – como uma mensagem, evento do calendário ou contato – do armazenamento de dados de uma máquina protegida do Exchange Server. É possível restaurar a seleção para uma pasta de recuperação, para fonte original ou para um ou mais arquivos PST. Para restaurar um item de e-mail noRapid Recovery Core Console, conclua as etapas a seguir.

1. No banco de dados do Exchange aberto na página **Restauração de e-mail**, selecione o item que deseja recuperar e, na barra de ações de **Restauração de e-mail**, clique em **Restaurar**.

O **Assistente de restauração de e-mail** será aberto.

2. Na página **Sessão de restauração**, escolha uma das opções a seguir e clique em **Avançar**.
   - Se estiver restaurando itens de e-mail pela primeira vez, digite um nome de exibição e suas credenciais do Outlook para a sessão de restauração. Em seguida, você pode selecionar essa sessão para uma futura restauração.
   - Se você tiver sessões de restauração criadas anteriormente, selecione uma das opções a seguir:
     - Selecione **Usar uma sessão de restauração existente** e selecione uma sessão na lista suspensa.
     - Selecione **Criar uma nova sessão de restauração** e digite um nome de exibição e suas credenciais do Outlook para a sessão de restauração.
3. Na página **Destino**, selecione o local de destino do item restaurado nas opções a seguir e clique em **Avançar**:

Tabela 138. Destinos de restauração de e-mail

Opção	Descrição
Restaurar na pasta de recuperação	Recupera os itens selecionados (inclusive a hierarquia de pastas) em uma pasta de recuperação em uma caixa de correio online que você escolhe. Vá para a Etapa 4.
Restaurar no local original	Direciona o item selecionado (incluindo a hierarquia de pastas) para a caixa de e-mail no armazenamento de dados online no qual ele residia originalmente. Vá para a Etapa 5.
Restaurar no arquivo PST	Salva os itens selecionados (incluindo a hierarquia de pastas) criando um arquivo PST ou gravando em um arquivo PST existente. Vá para a Etapa 6.
Restaurar no(s) arquivo(s) PST (arquivo separado para cada caixa de correio)	Salva cada caixa de correio como um arquivo PST. Vá para a Etapa 6.

4. Se você tiver selecionado **Restaurar na pasta de recuperação**, na página **Configuração**, selecione um **perfil** na lista suspensa, procure e selecione o catálogo de endereços do Outlook e, em seguida, vá para a Etapa 7.

   Opcionalmente, selecione **Mostrar opções avançadas** para personalizar ainda mais a restauração com as seguintes opções:

Tabela 139. Opções avançadas de restauração de e-mail

Opção	Descrição
Operação de manutenção com erro	Determina a maneira como resolver e gerenciar eventuais erros que possam ocorrer durante o processo de restauração. Selecione uma das opções a seguir: • **Efetuar log e continuar**. Coleta mensagens de erro em um log e continua o processo de restauração. • **Notificar usuário**. Pausa a restauração e exibe uma mensagem na caixa de diálogo Monitorar Tarefa Ativa ao encontrar um erro, e oferece a opção de continuar ou cancelar a restauração. • **Abortar restauração**. Encerra o processo de restauração quando ocorre um erro.

Opção	Descrição
Restaurar objetos excluídos	Para o banco de dados Exchange 2010, 2013 e 2016, restaura os itens que foram excluídos permanentemente. Para o banco de dados Exchange 2007, restaura itens tachados da pasta atual.
Restaurar regras de e-mail	Restaura todas as regras que o usuário tinha no momento em que houve o backup dos dados.

5. Se você tiver selecionado **Restaurar no local original**, na página **Configuração**, selecione o **perfil** de destino do Outlook, selecione um **tipo de restauração** nas opções a seguir e vá para a Etapa 7:
   - **Restaurar apenas diferenças**. Identifica se o item que está sendo restaurado já está presente na pasta de destino e só conclui a restauração se não há duplicação do item. Também chamado de restauração diferencial.
   - **Criar entradas duplicadas**. Restaura todos os itens selecionados sem sobrescrever os existentes, causando a duplicação dos itens que já existiam.
   - **Substituir caso seja mais recente**. Restaura itens mais novos que não estão presentes no armazenamento de dados online. Restaura também itens que estão presentes no armazenamento de dados online, mas que são mais antigos que os itens na cópia do banco de dados Exchange.

   Opcionalmente, selecione **Mostrar opções avançadas** para personalizar ainda mais a restauração com as seguintes opções:

Tabela 140. Opções avançadas de restauração de e-mail

Opção	Descrição
Operação de manutenção com erro	Determina a maneira como resolver e gerenciar eventuais erros que possam ocorrer durante o processo de restauração. Selecione uma das opções a seguir: • **Efetuar log e continuar**. Coleta mensagens de erro em um log e continua o processo de restauração. • **Notificar usuário**. Pausa a restauração e exibe uma mensagem na caixa de diálogo Monitorar Tarefa Ativa ao encontrar um erro, e oferece a opção de continuar ou cancelar a restauração. • **Abortar restauração**. Encerra o processo de restauração quando ocorre um erro.
Restaurar objetos excluídos	Para o banco de dados Exchange 2010, 2013 e 2016, restaura os itens que foram excluídos permanentemente. Para o banco de dados Exchange 2007, restaura itens tachados da pasta atual.
Restaurar regras de e-mail	Restaura todas as regras que o usuário tinha no momento em que houve o backup dos dados.
Restaurar permissões do usuário	Restaura as permissões personalizadas configuradas para uma pasta pública. **NOTE:** Essa opção só está disponível quando você restaura uma pasta pública para o local original. Se você não selecionar a opção de restaurar permissões, as permissões da pasta padrão serão restauradas com o conteúdo.

6. Se você tiver selecionado **Restaurar no arquivo PST** ou **Restaurar no(s) arquivo(s) PST (arquivo separado para cada caixa de correio)**, na página **Configuração**, conclua as seguintes seleções e vá para a Etapa 7:
   a. **Perfil**. Selecione um perfil do Outlook na lista suspensa.

b. **Armazenamento de PST primário**. Para localizar e selecionar a pasta de destino inicial para o arquivo PST, digite o caminho ou selecione um arquivo existente.

c. **Armazenamento de PST de overflow (opcional)**. Se o destino principal tiver espaço insuficiente para o arquivo PST, selecione um destino secundário para o arquivo PST.

NOTE: Não atribua o local de overflow ao mesmo disco do local principal.

Opcionalmente, selecione **Mostrar opções avançadas** para personalizar ainda mais a restauração com as seguintes opções:

Tabela 141. Opções avançadas de restauração de e-mail

Opção	Descrição
Operação de manutenção com erro	Determina a maneira como resolver e gerenciar eventuais erros que possam ocorrer durante o processo de restauração. Selecione uma das opções a seguir: • **Efetuar log e continuar**. Coleta mensagens de erro em um log e continua o processo de restauração. • **Notificar usuário**. Pausa a restauração e exibe uma mensagem na caixa de diálogo Monitorar Tarefa Ativa ao encontrar um erro, e oferece a opção de continuar ou cancelar a restauração. • **Abortar restauração**. Encerra o processo de restauração quando ocorre um erro.
Restaurar objetos excluídos	Para o banco de dados Exchange 2010, 2013 e 2016, restaura os itens que foram excluídos permanentemente. Para o banco de dados Exchange 2007, restaura itens tachados da pasta atual.

7. Clique em **Concluir**.

Os itens serão restaurados no destino selecionado. Você pode monitorar o andamento do trabalho na página Eventos.

Bare metal restore

Esta seção descreve como restaurar completamente uma máquina protegida Windows a partir de hardware semelhante ou diferente.

Restauração sem sistema operacional para máquinas Windows

Os servidores, quando funcionando conforme o esperado, executam as tarefas conforme estão configurados. É apenas quando falham que as coisas mudam. Quando ocorre um evento catastrófico, deixando um server inoperante, medidas imediatas são necessárias para restaurar a funcionalidade total da máquina.

O Rapid Recovery fornece a capacidade de realizar uma bare metal restore (BMR) em suas máquinas Windows ou Linux. A BMR é um processo que restaura a configuração completa do software de um sistema específico. A operação de restauração recupera não só os dados do server, mas também reformata o disco rígido e reinstala o sistema operacional e todos os aplicativos de software. Para realizar uma BMR, especifique um ponto de recuperação de uma máquina protegida e reverta (realize uma restauração) para a máquina física ou virtual designada. Se estiver realizando uma restauração em um volume do sistema, isso é considerado uma BMR. Se estiver realizando uma restauração e for necessário um CD de inicialização, isso também é considerado uma BMR. Outras circunstâncias em que você pode decidir realizar uma bare metal restore incluem atualização de hardware ou substituição do server. Em ambos esses casos, você realiza uma restauração a partir de um ponto de recuperação para o hardware atualizado ou substituído.

O Rapid Recovery oferece suporte aos sistemas operacionais Windows 8, 8.1 e Windows Server 2012, 2012 R2 inicializados a partir de partições FAT32 EFI disponíveis para proteção ou recuperação, bem como volumes ReFS (Resilient File System).

NOTE: A bare metal restore da configuração de discos de espaços de armazenamento (um recurso do Windows 8.1) também não é suportada nesta versão. Atualmente, apenas a restauração completa e a BMR são suportadas, visto que existe uma limitação do driver com ReFS, de modo que a restauração é implementada em modo de usuário, exportação da VM, e assim por diante. Se um Core está protegendo pelo menos um volume agente que contém o sistema de arquivos ReFS, ele deve ser instalado em um Windows 8, Windows 8.1, Windows Server 2012 ou uma máquina com Windows Server 2012 R2, desde que esses sistemas operacionais ofereçam suporte nativo ao formato ReFS. Caso contrário, a funcionalidade será limitada, e operações que envolvem tarefas, como a montagem de uma imagem de volume, não funcionarão. ORapid Recovery Core Console apresentará as mensagens de erro aplicáveis a essas ocorrências.

Apenas os sistemas operacionais Linux suportados estão disponíveis para proteção ou recuperação. Inclui Ubuntu, Red Hat Enterprise Linux, CentOS e SUSE Linux Enterprise Server (SLES). Para obter mais detalhes, consulte o *Guia de instalação e atualização do Rapid Recovery*.

É possível realizar uma BMR em máquinas físicas ou virtuais. Um benefício adicional é que o Rapid Recovery permite realizar uma BMR seja o hardware semelhante ou diferente. Realizar uma BMR no Rapid Recovery separa o sistema operacional de uma plataforma específica, proporcionando portabilidade.

Exemplos de realização de uma BMR para hardwares semelhantes incluem a substituição do disco rígido do sistema existente ou troca de server com falha por uma máquina idêntica.

Exemplos de realização de uma BMR para hardwares diferentes incluem a restauração de um sistema com falha com um server produzido por um fabricante diferente ou com configuração diferente. Esse processo envolve a criação de uma imagem de CD de inicialização, gravação da imagem em disco, inicialização do server de destino

a partir da imagem de inicialização, conexão com a instância do console de recuperação, mapeamento dos volumes, início da recuperação e monitoramento do processo. Depois que a bare metal restore for concluída, você poderá continuar com a tarefa de carregar o sistema operacional e os aplicativos de software no server restaurado, seguida pelo estabelecimento de definições exclusivas necessárias para sua configuração.

A bare metal restore é usada não apenas em cenários de recuperação após desastres, mas também para migração de dados ao atualizar ou substituir servers.

Como restaurar máquinas virtuais

Embora a bare metal restore (BMR) seja suportada para máquinas virtuais, também é interessante notar que é mais fácil realizar uma exportação virtual para uma VM do que realizar uma BMR em uma máquina física. Para obter mais informações sobre como realizar uma exportação de VM para máquinas virtuais, consulte Exportação para máquinas virtuais usando o Rapid Recovery.

Para realizar uma BMR em uma máquina Windows, consulte o tópico específico para Windows, incluindo os pré-requisitos. Para obter mais informações, consulte Realizar uma restauração sem sistema operacional para máquinas Windows.

Também é possível realizar uma BMR a partir do Assistente de restauração de máquinas. Para fazer isso, comece pelo procedimento Sobre restauração de volumes a partir de um ponto de recuperação e, quando for direcionado nesse procedimento, vá até Realizar uma restauração sem sistema operacional para máquinas Windows.

Para realizar uma BMR em uma máquina Linux, consulte Realizar uma bare metal restore em máquinas Linux. Além de realizar uma BMR usando o utilitário de linha de comando local_mount, agora ela pode ser realizada de dentro da UI do Core Console. O roteiro leva as duas abordagens em conta.

Realizar uma restauração sem sistema operacional para máquinas Windows

Para realizar uma bare metal restore em máquinas com Windows, realize as tarefas a seguir.

- Criar uma imagem de inicialização do Windows. Essa imagem ISO do CD de inicialização será usada para iniciar a unidade de destino, a partir da qual é possível acessar o Universal Recovery Console para se comunicar com as cópias de segurança no Core. Consulte Entender a criação do CD de inicialização para máquinas Windows.
    - Se você precisar de mídia física para iniciar a máquina de destino, precisará transferir a imagem ISO do CD de inicialização para a mídia. Consulte Como transferir a imagem ISO do CD de inicialização para a mídia.
    - Em todos os casos, é preciso carregar a imagem de inicialização no server de destino e iniciar o server da imagem de inicialização. Consulte Como carregar o CD de inicialização e iniciar o computador de destino.

NOTE: Esse processo descreve como gerenciar uma imagem do CD de inicialização da caixa de diálogo Criar CD de inicialização. Também é possível realizar essas etapas a partir de um assistente de Restauração de máquinas, começando da página CD de Inicialização do assistente. Acesse isso quando especificar Recuperar em qualquer máquina de destino usando um CD de inicialização a partir da página Destino do assistente.

- Iniciar uma bare metal restore para Windows. Depois que a máquina de destino é iniciada a partir do CD de inicialização, é possível iniciar a BMR. Consulte Como usar o Universal Recovery Console para uma BMR. Ele envolve as seguintes tarefas:
  - Iniciar uma restauração a partir de um ponto de recuperação do Core. Consulte Como selecionar um ponto de recuperação e iniciar uma BMR.
  - Mapeie os volumes. Consulte Sobre como mapear volumes para uma restauração sem sistema operacional.
  - Se a restauração for em hardware diferente e o armazenamento e drivers de rede necessário não estiverem presentes no CD de inicialização, talvez seja necessário carregar os drivers a partir de um dispositivo de mídia portátil. Para obter mais informações, consulte Carregar drivers usando o Universal Recovery Console.
- Realização de uma BMR a partir do assistente de Restauração de máquinas. De forma opcional, os processos para gerenciamento de uma imagem de inicialização do Windows e para iniciar a BMR, incluindo todas as subtarefas, podem ser realizados a partir do assistente de Restauração de máquinas. Para obter informações sobre como abrir o assistente, consulte as etapas 1 à 5 do Sobre restauração de volumes a partir de um ponto de recuperação.
- Confirmação de um bare metal restore. Após iniciar o procedimento de bare metal restore, você pode confirmar e monitorar o progresso. Consulte Confirmar uma bare metal restore.
  - É possível monitorar o progresso de sua restauração. Consulte Visualizar o progresso da recuperação.
  - Depois de concluída, você pode iniciar o server restaurado. Consulte Iniciar um servidor de destino restaurado
  - Solucionar problemas do processo de BMR. ConsulteComo solucionar problemas de conexão com o Universal Recovery Console e Como reparar problemas de inicialização.

Pré-requisitos para realizar uma restauração sem sistema operacional para uma máquina Windows

Antes de iniciar o processo de realização de uma bare metal restore de uma máquina com Windows, é preciso garantir que as seguintes condições e critérios estejam presentes:

- Uma CPU (unidade de processamento central) de 64 bits. O CD de inicialização do Rapid Recovery contém o sistema operacional Win 5.1 PE. Os BMRs do Rapid Recovery não são compatíveis com CPUs x86. Você só pode executar um BMR em uma CPU de 64 bits.

NOTE: Esse requisito é novo a partir da versão 6.0.

- Cópias de segurança da máquina que você deseja restaurar. É preciso ter um Rapid Recovery Core funcional que contenha pontos de recuperação do server protegido que você deseja restaurar
- Hardware para restaurar (novo ou antigo, similar ou não). A máquina de destino deve atender aos requisitos de instalação de um agente; para obter mais detalhes, consulte o Guia de instalação e atualização do Rapid Recovery.
- Software e mídia de imagem. É preciso ter um CD ou DVD virgem e um software de gravação de disco ou de criação de imagem ISO. Se gerenciar máquinas remotamente usando software de computação de rede virtual, como o UltraVNC, você precisará ter também o VNC Viewer.
- Drivers do adaptador de rede e de armazenamento compatíveis. Se a restauração for para hardware diferente, é preciso ter drivers de armazenamento compatíveis e drivers do adaptador de rede para a máquina de destino, incluindo drivers de RAID, AHCI e chipset, conforme o caso.
- Partições e espaço de armazenamento, conforme apropriado. Certifique-se que há espaço suficiente no disco rígido para criar partições de destino na máquina de destino que conterá os volumes de origem. Todas as partições de destino devem ser pelo menos do mesmo tamanho da partição de origem original.
- Partições compatíveis. Sistemas operacionais Windows 8, Windows 8.1, Windows 10, Windows Server 2012 e Windows Server 2012 R2 inicializados a partir de partições FAT32 EFI disponíveis para proteção ou recuperação, bem como volumes ReFS (Resilient File System). As partições UEFI são tratadas como simples volumes FAT32. Transferências incrementais são totalmente suportadas e protegidas. O Rapid Recovery fornece suporte de sistemas UEFI para BMR, incluindo discos GPT de particionamento automático.

Realizar um bare metal restore usando o Assistente de restauração de máquina

Você pode usar o Assistente de restauração para criar um CD de inicialização, bem como executar um bare metal restore (BMR).

Antes de realizar uma BMR, consulte Pré-requisitos para realizar uma restauração sem sistema operacional para uma máquina Windows ou Pré-requisitos para realizar uma bare metal restore em máquinas Linux, conforme adequado. Se for iniciar uma BMR para uma máquina com Windows a partir do Core Console, consulte Realizar uma restauração sem sistema operacional para máquinas Windows.

A máquina protegida deve ter o software Agent instalado e deve ter pontos de recuperação a partir dos quais você realizará a operação de restauração.

Gerenciar uma imagem de inicialização do Windows através do assistente inclui as seguintes ações:

- Iniciar o criação do CD de inicialização.
- Definir o caminho para a imagem na máquina Core.
- Selecionar o ambiente de recuperação adequado para o hardware que você quer restaurar.
- Opcionalmente, definir os parâmetros de conexão para o agente restaurado com o objetivo de usar a rede ou o UltraVNC.
- Opcionalmente, injetar drivers para o hardware que você quer restaurar.
- Opcionalmente, transferir a imagem de inicialização para uma mídia física.
- Inicializar a máquina com os dados que você deseja restaurar a partir do CD.
- Conectar-se ao Universal Recovery Console.
- Mapear volumes.
- Iniciar o bare metal restore do ponto de recuperação selecionado no Core.

> **NOTE:** Esse processo descreve como gerenciar uma imagem do CD de inicialização do assistente de Restauração de máquinas como parte do processo para realizar uma BMR utilizando esse assistente. Também é possível gerenciar uma imagem de inicialização da caixa de diálogo Criar CD de inicialização. Para obter informações sobre o gerenciamento de uma imagem do CD de inicialização fora do assistente de Restauração de máquinas, consulte Entender a criação do CD de inicialização para máquinas Windows.

1. Para restaurar um volume em uma máquina protegida, navegue até o Core Console e clique em **Restore** (Restaurar) na barra de botões do Rapid Recovery.

   O Assistente de restauração de máquinas é exibido.
2. Na página Máquinas, selecione a máquina protegida que deseja restaurar e clique em **Avançar**.

   Aparece a página Pontos de recuperação.
3. Selecione o ponto de recuperação que você quer usar para restaurar a máquina.
   - Como opção, se quiser limitar a quantidade de pontos de recuperação exibidos, você pode filtrar por volumes (se definidos) ou por data de criação do ponto de recuperação. Você pode também procurar por um determinado ponto de recuperação.
4. Clique em **Avançar**.
5. Na página Destino, selecione **Recuperar em qualquer máquina de destino usando um CD de inicialização**.
   - Se você ainda não tiver sido carregado um CD de inicialização na máquina que você quer restaurar, clique em **Avançar** e, em seguida, continue na Etapa 6.
   - Se você já tiver carregado um CD de inicialização na máquina de destino BMR, selecione **Eu já tenho um CD de inicialização em execução na máquina de destino**, clique em **Avançar** e, em seguida, vá para a Etapa 16.
6. Na página CD de inicialização, no campo de texto Caminho de saída, digite o caminho onde a imagem ISO do CD de inicialização deve ser armazenada.

   > **NOTE:** Se a unidade compartilhada na qual você deseja armazenar a imagem estiver com pouco espaço em disco, você pode criar um disco conforme necessário no caminho; por exemplo, F:\filename.iso.

NOTE: A extensão do arquivo deve ser .iso. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen, barra invertida (apenas como delimitador de caminho) e ponto (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

7. Como opção, para definir os parâmetros de rede para o computador de destino ou para adicionar recursos do UltraVNC, selecione **Exibir opções avançadas** e execute o seguinte procedimento:
   - Para estabelecer uma conexão de rede com o destino BMR, selecione **Use o seguinte endereço IP** e digite as informações conforme descrito na tabela a seguir.

Tabela 142. Opções de conexão de rede

Opção	Descrição
Endereço IP	O endereço IP da máquina restaurada.
Máscara de sub-rede	A máscara de sub-rede da máquina restaurada.
Gateway padrão	Especifique o gateway padrão da máquina restaurada.
Servidor DNS	Especifique o server de nome de domínio da máquina restaurada.

   - Se você já tiver uma conta do UltraVNC e gostaria de usá-la para concluir a BMR, selecione **Adicionar UltraVNC** e, em seguida, digite as informações descritas na tabela a seguir.

Tabela 143. Credenciais de conexão com o UltraVNC

Opção	Descrição
Senha	A senha da sua conta UltraVNC.
Porta	A porta que você quer usar para se conectar ao destino BMR. A porta padrão é 5900.

8. Clique em **Avançar**.
9.
   - Para estabelecer uma conexão de rede para a máquina restaurada, selecione **Use o seguinte endereço IP**, como descrito na tabela a seguir.
   - Para definir as informações de UltraVNC, selecione **Adicionar UltraVNC**, conforme descrito na tabela a seguir.

     Use essa opção se você precisar de acesso remoto ao console de recuperação. Não é possível efetuar login usando Microsoft Terminal Services enquanto o CD de inicialização é utilizado.

Tabela 144. Conexão UltraVNC

Opção	Descrição
Senha	Especifique uma senha para essa conexão UltraVNC.
Porta	Especifique uma porta para essa conexão UltraVNC. A porta padrão é 5900.

10. Quando estiver satisfeito com suas seleções na página CD de inicialização, clique em **Avançar**.
11. Como opção, na página Injeção de drivers, se você pretende restaurar hardware diferente, injete o controlador de armazenamento adequado e outros drivers para o sistema de destino seguindo as etapas:

a. Baixe os drivers no website do fabricante do servidor e descompacte-os.
b. Compacte cada driver em um arquivo .zip, usando um utilitário de compressão adequado (por exemplo, WinZip).
c. Na página Injeção de drivers do Assistente de restauração de máquina, clique em **Adicionar um arquivo de drivers**.
d. Navegue pelo sistema de arquivamento para localizar o arquivo do driver compactado, selecione-o e clique em **Abrir**.
e. Repita a Etapa c e a Etapa d, conforme o caso, até injetar todos os drivers necessários.

Para obter mais informações sobre a injeção de drivers, consulte Entender a injeção de drivers em um CD de inicialização.

NOTE: Nem todas as versões do Windows são compatíveis com a injeção automática de drivers. Se o seu sistema operacional não for compatível, salve manualmente os drivers em `C:\Program Files\AppRecovery\Core\BootCdKit\Drivers\`.

O Rapid Recovery cria a imagem ISO do CD de inicialização.

12. Clique em **Avançar**.
13. Inicie a máquina de destino BMR e, em seguida, siga uma das opções:
    - Se você pode inicializar a máquina de destino da imagem ISO do CD de inicialização, faça-o agora.
    - Caso não seja possível, copie a imagem ISO para uma mídia física (um CD ou um DVD), carregue o disco na máquina de destino, configure a máquina para carregar a partir do CD de inicialização e reinicie a partir do CD de inicialização.

      NOTE: Talvez seja necessário alterar as definições de BIOS da máquina de destino para garantir que o volume carregado primeiro seja o CD de inicialização.

      A máquina de destino, quando iniciada a partir do CD de inicialização, exibe a interface do Universal Recovery Console (URC). Esse ambiente é usado para restaurar a unidade do sistema ou volumes selecionados diretamente do Rapid Recovery Core. Observe o endereço IP e as credenciais da chave de autenticação no URC, que são atualizados cada vez que é feita uma inicialização a partir do CD de inicialização.
14. Na página Conexão do Assistente de restauração de máquina no Core Console, digite as informações de autenticação da instância URC da máquina que você deseja restaurar da seguinte maneira:

Tabela 145. Opções de autenticação

Opção	Descrição
Endereço IP	O endereço IP fornecido no URC na máquina de destino.
Chave de autenticação	A chave de autenticação fornecida no URC na máquina de destino.

15. Clique em **Avançar**.
16. Na página Mapeamento de disco, se você quiser mapear os volumes manualmente, vá para a Etapa 10. Caso queira mapear os volumes automaticamente, execute as etapas a seguir:
    a. No menu suspenso Mapeamento de volume, selecione **Automático**.
    b. Na lista de volumes, certifique-se de que os volumes que você quer restaurar estão selecionados. Todos os dispositivos estão selecionados por padrão.

    Se você não quiser restaurar um volume relacionado, desmarque a opção.

    NOTE: Pelo menos um volume deve ser selecionado para realizar a restauração.

    c. No lado direito, selecione o disco de destino para a restauração.
    d. Clique em **Avançar**.

e. Na página Visualização de mapeamento de disco, revise os parâmetros das ações de restauração selecionadas.

f. Vá para a Etapa 18.

17. Para mapear volumes manualmente, na página Mapeamento de disco, execute as seguintes etapas:

    a. No menu suspenso Mapeamento de volume, selecione **Manual**.

    b. Na coluna Destino, selecione um volume de destino que você quer restaurar. Como opção, se você não deseja restaurar um volume relacionado, desmarque a opção.

    NOTE: Pelo menos um volume deve ser selecionado para realizar a restauração.

18. Clique em **Concluir**.

    CAUTION: Todas as partições e dados atuais na unidade de destino serão removidos permanentemente e substituídos pelo conteúdo do ponto de recuperação selecionado, incluindo o sistema operacional e todos os dados.

19. Se os volumes que deseja restaurar contiverem bancos de dados do Oracle, SQL Server ou Microsoft Exchange, e se você estiver realizando uma Live Restore, na página Desmontar bancos de dados, será solicitado que você os desmonte. Como opção, se você quiser remontar esses bancos de dados após a restauração ser concluída, selecione **Remontar automaticamente todos os bancos de dados após o ponto de recuperação ser restaurado**.

20. Clique em **Restaurar**.

21. Na mensagem de status, clique em **OK** para confirmar que o processo de restauração foi iniciado.

    A restauração será iniciada. É possível monitorar o progresso na página Eventos. Para obter mais informações, consulte Como exibir eventos usando tarefas, alertas e páginas de diário.

Entender a criação do CD de inicialização para máquinas Windows

Uma bare metal restore para Windows exige uma imagem de inicialização chamada de CD de inicialização, criada pela definição de parâmetros no Rapid Recovery Core. Essa imagem é adaptada às suas necessidades específicas. Use a imagem para iniciar a máquina de destino do Windows. Com base nas particularidades do seu ambiente, pode ser preciso transferir esta imagem para uma mídia física como um CD ou DVD. Você deve, então, carregar virtual ou fisicamente a imagem de inicialização e iniciar o server Windows a partir da imagem de inicialização.

A primeira etapa ao realizar uma bare metal restore (BMR) de uma máquina com Windows é criar o arquivo do CD de inicialização no Rapid Recovery Core Console. Trata-se de uma imagem ISO inicializável que contém a interface do Universal Recovery Console (URC) do Rapid Recovery, um ambiente usado para restaurar a unidade do sistema ou o server inteiro diretamente do Rapid Recovery Core.

A imagem ISO do CD de inicialização criada é adaptada à máquina que está sendo restaurada e, portanto, deve conter os drivers corretos de rede e de armazenamento em massa. Se for prevista a restauração em hardware diferente da máquina em que o ponto de recuperação se originou, inclua o controlador de armazenamento e outros drivers no CD de inicialização. Para obter informações sobre como injetar esses drivers no CD de inicialização, consulte Entender a injeção de drivers em um CD de inicialização.

Entender a injeção de drivers em um CD de inicialização

A imagem de CD de inicialização exige que os drivers de armazenamento reconheçam as unidades de server e os drivers do adaptador de rede a fim de se comunicarem com o Rapid Recovery Core pela rede.

Um conjunto genérico de drivers do controlador de armazenamento e de adaptador de rede do Windows 8.1 x64 é incluído automaticamente ao gerar um CD de inicialização para Windows. Isso atende aos requisitos de sistemas mais recentes. Sistemas de outros fabricantes ou sistemas mais antigos podem exigir uma injeção de drivers de controlador de armazenamento e de adaptador de rede ao criar o CD de inicialização. Se você descobrir que o CD de inicialização criado não contém os drivers necessários para executar a restauração, também poderá carregá-los na máquina de destino usando o URC. Para obter mais informações, consulte Carregar drivers usando o Universal Recovery Console.

Ao criar o CD de inicialização, a injeção de drivers é usada para facilitar a interoperabilidade entre o console de recuperação, o adaptador de rede e o armazenamento no server de destino.

Os dados restaurados a partir do ponto de recuperação incluem drivers para o hardware usado anteriormente. Se for feita uma bare metal restore para um hardware diferente, será preciso injetar também drivers do controlador de armazenamento no sistema operacional que está sendo restaurado usando o URC após os dados terem sido restaurados para a unidade. Isso permite que o sistema operacional restaurado seja inicializado usando o novo conjunto de hardware. Depois que o OS é inicializado após a restauração, é possível baixar e instalar os drivers adicionais necessários para que o OS possa interagir com seu novo hardware.

Criar uma imagem ISO do CD de inicialização

Um CD de inicialização é o termo que o Rapid Recovery usa para se referir ao local de armazenamento portátil da imagem ISO reservada para fazer uma bare metal restore (BMR). A imagem contém o Universal Recovery Console (URC) do Rapid Recovery.

Para executar uma BMR em uma máquina, você precisa iniciar a máquina do CD de inicialização, o qual iniciará o URC. O URC é o que torna possível conectar o destino da BMR ao local do ponto de recuperação que você quer usar para executar a restauração.

1. No Rapid Recovery Core Console em que o servidor que você precisa restaurar é protegido, na barra de ícones, clique no menu (Mais) e, em seguida, clique em **Boot CDs** (CDs de inicialização).
2. Na página CDs de inicialização, clique em **Criar CD de inicialização**.

   A caixa de diálogo Criar CD de inicialização é exibida.
3. Na caixa de diálogo Criar CD de inicialização, na caixa de texto **Caminho de saída**, insira o caminho onde deseja armazenar a imagem ISO do CD de inicialização.

   NOTE: A extensão do arquivo deve ser .iso. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen, barra invertida (apenas como delimitador de caminho) e ponto (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
4. Em Opções de conexão, realize um dos procedimentos a seguir:
   - Para obter o endereço IP dinamicamente usando o protocolo DHCP (Dynamic Host Configuration Protocol), selecione **Obter o endereço IP automaticamente**.
   - Para especificar um endereço IP estático para o URC, selecione **Usar o seguinte endereço IP** e, em seguida, digite as seguintes informações:
     - Endereço IP
     - Máscara de sub-rede
     - Gateway padrão
     - Servidor DNS

   NOTE: É preciso especificar todos esses quatro campos.
5. Se você necessita de acesso remoto para o console de recuperação e você tiver o UltraVNC instalado, nas Opções de UltraVNC, execute as seguintes etapas:

NOTE: O UltraVNC permite que você gerencie o URC remotamente enquanto ele está em uso. Não é possível efetuar login usando Microsoft Terminal Services enquanto o CD de inicialização é utilizado.

a. Selecione **Adicionar UltraVNC**.
b. Digite sua **Senha de UltraVNC**.
c. Digite a **Porta de UltraVNC**. A porta padrão é 5900.

NOTE: As Opções de UltraVNC só estão disponíveis se você já tiver o UltraVNC instalado. Para tornar essas opções disponíveis, vá para http://www.uvnc.com/downloads/ultravnc/ para fazer o download do UltraVNC versão 1.0.9.1 ou posterior para a arquitetura x64. Instale-o e salve o arquivo winvnc.exe em C:\Program Files\AppRecovery\Core\BootCdKit\UltraVnc_x64\.

6. Se você pretende restaurar hardware diferente, injete o controlador de armazenamento adequado e outros drivers para o sistema de destino seguindo as etapas:

NOTE: Nem todas as versões do Windows são compatíveis com a injeção automática de drivers. Se o seu sistema operacional não for compatível, salve manualmente os drivers em C:\Program Files \AppRecovery\Core\BootCdKit\Drivers\.

a. Baixe os drivers no website do fabricante do servidor e descompacte-os.
b. Compacte cada driver em um arquivo .zip, usando um utilitário de compressão adequado (por exemplo, WinZip).
c. Na caixa de diálogo Criar CD de inicialização, no painel Drivers, clique em **Adicionar um arquivo de drivers**.
d. Navegue pelo sistema de arquivamento para localizar o arquivo do driver compactado, selecione-o e clique em **Abrir**.

O arquivo do driver é exibido no painel Drivers da caixa de diálogo Criar CD de inicialização.

e. Repita a Etapa c e a Etapa d, conforme o caso, até adicionar todos os drivers necessários.
f. No painel Drivers, selecione os drivers que você quer injetar.

Para obter mais informações sobre a injeção de drivers, consulte Entender a injeção de drivers em um CD de inicialização.

7. Clique em **Criar CD de inicialização**.

O Rapid Recovery cria e salva o CD de inicialização com o nome do arquivo fornecido.

8. Para monitorar o andamento dessa tarefa, vá até a barra de ícones e clique no ícone Eventos.

Para obter mais informações sobre o monitoramento de eventos do Rapid Recovery, consulte Como exibir eventos usando tarefas, alertas e páginas de diário.

Ao concluir a criação da imagem ISO, um registro da imagem aparece na página Cds de inicialização, a qual você pode acessar do menu Mais na barra de ícones.

Para acessar a imagem ISO, navegue até o caminho de saída especificado ou clique no link da página CDs de inicialização para salvar a imagem em um local do qual seja possível carregá-la para o novo sistema; por exemplo, uma unidade de rede.

Como transferir a imagem ISO do CD de inicialização para a mídia

Ao criar o arquivo do CD de inicialização, ele é armazenado como uma imagem ISO no caminho especificado. Você deve ser capaz de montar a imagem como uma unidade no servidor em que você está executando a bare metal restore.

Você pode gravar imagem ISO do CD de inicialização em CD ou em DVD acessível na inicialização do sistema.

Quando você inicia a máquina a partir do CD de inicialização, o Universal Recovery Console é iniciado automaticamente.

Se for executar uma BMR em uma máquina virtual, esta etapa não será necessária. Basta carregar a imagem ISO em uma unidade e editar as configurações dessa VM para iniciar essa unidade.

Como carregar o CD de inicialização e iniciar o computador de destino

Depois de criar a imagem do CD de inicialização, é necessário inicializar o servidor de destino com o CD de inicialização recém-criado.

Para se conectar ao Rapid Recovery Core Console ou usar o Chromium para baixar drivers adicionais, você deve primeiro carregar um controlador e um adaptador de rede Ethernet. Para obter mais informações, consulte Carregar drivers usando o Universal Recovery Console.

NOTE: Se você tiver criado o CD de inicialização usando o DHCP, deverá capturar o endereço IP e a senha.

1. No novo servidor, carregue a imagem do CD de inicialização do local apropriado e reinicie o servidor pela imagem do CD de inicialização para carregar o software Rapid Recovery Agent e o Win PE 5.1.

   A máquina de destino mostra uma tela azul da Quest com o ícone de três botões na parte superior da tela.
2. Para abrir a interface do usuário do Universal Recovery Console (URC) do Rapid Recovery, clique no ícone da Quest na parte superior da tela.

   O endereço IP e a senha da máquina são exibidos em Autenticação.

   NOTE: Uma nova senha temporária é gerada cada vez que a máquina é iniciada com o CD de inicialização. Anote o endereço IP exibido no painel de Configurações dos adaptadores de rede e a senha de autenticação exibida no painel de Autenticação. Você precisará dessas informações mais tarde durante o processo de recuperação de dados para fazer logon novamente no console.

   NOTE: Se não houver endereço IP fornecido, carregue o controlador e o adaptador de rede Ethernet.
3. Se desejar alterar o endereço IP, selecione-o e clique em **Change** (Alterar).

   NOTE: Se você tiver especificado um endereço IP na caixa de diálogo Criar CD de inicialização, o Universal Recovery Console o usará e exibirá na tela Definições de adaptadores de rede.

A máquina está pronta para você se conectar ao Core, selecione um ponto de recuperação e continue o processo sem sistema operacional.

Como usar o Universal Recovery Console para uma BMR

Antes de iniciar uma bare metal restore (BMR) em uma máquina com Windows, as seguintes condições devem ser satisfeitas:

- Para restaurar um ponto de recuperação salvo no Core, é necessário ter o hardware apropriado disponível. Para obter mais informações, consulte Pré-requisitos para realizar uma restauração sem sistema operacional para uma máquina Windows.
- A máquina com Windows de destino da BMR deve ser iniciada usando a imagem do CD de inicialização. Para obter mais informações, consulte Entender a criação do CD de inicialização para máquinas Windows.

Uma BMR inicia uma máquina usando um ponto de recuperação selecionado por você. O ponto de recuperação inclui drivers do hardware anterior. Se for feita uma restauração para um hardware diferente, será preciso injetar drivers do controlador de armazenamento no sistema operacional que está sendo restaurado usando o URC

após os dados terem sido restaurados na unidade. Isso permite que o sistema operacional restaurado seja inicializado usando o novo conjunto de hardware. Depois de iniciar o SO, é possível baixar e instalar os drivers adicionais necessários que o SO precisa para interagir com seu novo hardware.

Para iniciar uma BMR no Rapid Recovery Core Console, realize as tarefas a seguir.

- Como selecionar um ponto de recuperação e iniciar uma BMR
- Sobre como mapear volumes para uma restauração sem sistema operacional
- Carregar drivers usando o Universal Recovery Console

Esse processo é uma etapa do Realizar uma restauração sem sistema operacional para máquinas Windows.

Sobre as ferramentas do Universal Recovery Console

O Universal Recovery Console (URC) inclui acesso a ferramentas que possam auxiliar na conclusão de uma bare metal restore (BMR).

Você pode encontrar as seguintes ferramentas clicando no ícone central na parte superior da tela inicial da Quest em um destino BMR de inicialização no URC:

- **Far Manager.** Essa ferramenta é semelhante ao Windows Explorer. Ela oferece uma maneira de procurar arquivos no servidor até concluir a BMR e instalar um sistema operacional com a própria função de navegação, como Windows Explorer.
- **Chromium.** Esse navegador de fonte aberta permite acessar à Internet em um servidor com um controlador de rede carregado por meio do URC.
- **PuTTY.** Essa ferramenta é um emulador de terminal de fonte aberta. No contexto de uma BMR Rapid Recovery, isso permite se conectar a um dispositivo de armazenamento NAS que não inclui uma interface de usuário. Esse recurso poderá ser necessário se você quiser restaurar de um arquivo e o arquivo estiver em um NAS.
- **Bloco de Notas.** Como em um sistema operacional Windows, essa ferramenta permite digitar notas não formatadas e exibir arquivos de log.
- **Gerenciador de Tarefas.** Como em um sistema operacional Windows, essa ferramenta permite gerenciar processos e monitorar o desempenho do servidor enquanto a restauração estiver em progresso.
- **Editor do Registro.** Como em um sistema operacional Windows, essa ferramenta permite alterar o Registro do sistema do destino BMR.
- **Prompt de comando.** Essa ferramenta permite executar comandos no destino BMR fora do URC até você instalar uma interface de usuário.

Carregar drivers usando o Universal Recovery Console

Esse recurso permite adicionar os drivers que não foram incluídos na imagem ISO, mas são necessários para uma bare metal restore bem-sucedida.

Essa tarefa é uma das etapas do Realizar uma restauração sem sistema operacional para máquinas Windows. Faz parte do processo de Como usar o Universal Recovery Console para uma BMR.

Ao criar um CD de inicialização, você pode adicionar drivers necessários à imagem ISO. Depois de inicializar a máquina de destino, você também pode carregar drivers de armazenamento ou de rede de dentro do Universal Recovery Console (URC).

Se você estiver restaurando em um hardware diferente, precisará injetar os drivers de controlador de armazenamento, RAID, AHCI, chipset e outros drivers se eles não estiverem no CD de inicialização. Esses drivers permitem que o sistema operacional opere com sucesso todos os dispositivos em seu server de destino depois que o sistema for reiniciado após o processo de restauração.

Execute as etapas de um dos procedimentos a seguir para carregar drivers usando o URC:

- Carregar drivers no Universal Recovery Console usando mídia portátil
- Como carregar um driver no URC usando o Chromium

Carregar drivers no Universal Recovery Console usando mídia portátil

As seguintes tarefas são pré-requisitos para este procedimento.

- Criar uma imagem ISO do CD de inicialização
- Como transferir a imagem ISO do CD de inicialização para a mídia
- Como carregar o CD de inicialização e iniciar o computador de destino

Execute o procedimento a seguir para usar um dispositivo de mídia portátil para carregar drivers no Universal Recovery Console (URC).

1. Em uma máquina conectada à Internet, baixe os drivers do site do fabricante para o servidor e descompacte-os.
2. Compacte cada driver em um arquivo .zip, usando um utilitário de compressão adequado (por exemplo, WinZip).
3. Copie e salve o arquivo .zip dos drivers em um dispositivo de mídia portátil, como, por exemplo, uma unidade USB.
4. Remova a mídia da máquina conectada e insira-a no server de destino de inicialização.
5. No servidor de destino, carregue o CD de inicialização e inicie a máquina.

   A tela inicial da Quest é exibida.
6. Para iniciar o URC, clique no **ícone da Quest**.

   O URC é aberto na guia do Gerenciador de driver do CD de inicialização.
7. Expanda a lista **Outros dispositivos**.

   Essa lista mostra os drivers que são necessários para o hardware, mas que não estão incluídos no CD de inicialização.
8. Clique com o botão direito em um dispositivo da lista e, em seguida, clique em **Carregar driver**.
9. Na janela Selecionar modo de carregamento do driver, selecione uma das opções a seguir:
   - Carregar pacote de driver único (o driver será carregado sem verificação de suporte do dispositivo
   - Verificar pasta dos pacotes de driver (os drivers do dispositivo selecionado serão pesquisados na pasta selecionada)
10. Expanda a unidade do dispositivo de mídia portátil, selecione o driver (com a extensão de arquivo .inf) e clique em **OK**.

    O driver é carregado no sistema operacional atual.
11. Na janela Informações, clique em **OK** para confirmar que o driver foi carregado com êxito.
12. Repita este procedimento conforme necessário para cada driver que você deseja carregar.

Como carregar um driver no URC usando o Chromium

As seguintes tarefas são pré-requisitos para este procedimento.

- Criar uma imagem ISO do CD de inicialização
- Como transferir a imagem ISO do CD de inicialização para a mídia
- Como carregar o CD de inicialização e iniciar o computador de destino

Conclua o procedimento a seguir para usar o navegador Chromium que vem instalado no CD de inicialização para carregar drivers enquanto estiver no URC.

1. No servidor de destino, carregue o CD de inicialização e inicie a máquina.

   A tela inicial da Quest é exibida.
2. Para iniciar o URC, clique no **ícone da Quest**.

   O URC é aberto na guia do Gerenciador de driver do CD de inicialização.
3. No destino BMR, clique nas ferramentas (ícone central) na parte superior da tela e em **Chromium**.
4. No navegador Chromium, navegue até um site onde você possa baixar o driver necessário.
5. Baixe o driver ou os drivers no local escolhido, como uma pasta local ou um compartilhamento de arquivos em rede.
6. Expanda a lista **Outros dispositivos**.

   Essa lista mostra os drivers que são necessários para o hardware, mas que não estão incluídos no CD de inicialização.
7. Clique com o botão direito em um dispositivo da lista e, em seguida, clique em **Carregar driver**.
8. Na janela Selecionar modo de carregamento do driver, selecione uma das opções a seguir:
   - Carregar pacote de driver único (o driver será carregado sem verificação de suporte do dispositivo)
   - Examinar pasta em busca de pacotes de driver (os drivers do dispositivo selecionado são pesquisados na pasta selecionada)
9. Navegue até o local onde você salvou o driver, selecione o driver e clique em **OK**.

   O driver é carregado no sistema operacional atual.
10. Na janela Informações, clique em **OK** para confirmar que o driver foi carregado com êxito.
11. Repita este procedimento conforme necessário para cada driver que você deseja carregar.

Como selecionar um ponto de recuperação e iniciar uma BMR

Depois que o Universal Recovery Console (URC) estiver acessível no computador de destino da bare metal restore (BMR), você deverá selecionar o ponto de recuperação que você deseja restaurar.

Navegue até o Core Console para selecionar o ponto de recuperação que você deseja carregar e designar o console de recuperação como o destino dos dados restaurados.

NOTE: Essa etapa é necessária para executar a BMR em todas as máquinas Windows e opcional para executar a BMR em máquinas Linux.

Essa tarefa é uma das etapas do Realizar uma restauração sem sistema operacional para máquinas Windows. Faz parte do processo de Como usar o Universal Recovery Console para uma BMR.

Em caso de realização de uma BMR para uma máquina Linux no Core Console, essa tarefa também é uma etapa em Realizar uma bare metal restore em máquinas Linux Faz parte do processo de Realizar uma bare metal restore em uma máquina Linux usando a linha de comando.

1. No Rapid Recovery Core Console, na lista de máquinas protegidas, clique no nome da máquina protegida que você deseja restaurar.

   A página Resumo da máquina selecionada é exibida.
2. Clique em **Pontos de recuperação**.
3. Próximo do ponto de recuperação que você deseja usar na BMR, clique no menu suspenso e em **Restaurar**.

   O Assistente de restauração de máquinas é exibido.
4. Selecione **Recuperar em qualquer máquina de destino usando um CD de inicialização**.
5. Selecione **Eu já tenho um CD de inicialização em execução na máquina de destino**.

   As caixas de texto de autenticação são exibidas.
6. Insira as informações sobre a máquina que você deseja restaurar conforme descrito na tabela a seguir.

Tabela 146. Informações da máquina de destino

Caixa de texto	Descrição
Endereço IP	O endereço IP da máquina na qual deseja restaurar. É idêntico ao endereço IP exibido no URC.
Chave de autenticação	A senha específica para se conectar ao server selecionado. É idêntico à chave de autenticação exibida no URC.

7. Clique em **Avançar**.

   Se as informações de conexão inseridas correspondem ao URC, e se o Core e o server de destino podem identificar um ao outro corretamente na rede, os volumes do ponto de recuperação selecionado são carregados, e a página Mapeamento de disco é exibida. Nesse caso, a próxima etapa é mapear volumes.
8. Vá até Sobre como mapear volumes para uma restauração sem sistema operacional para saber mais sobre as opções de mapeamento de disco.

Sobre como mapear volumes para uma restauração sem sistema operacional

Depois de se conectar ao Universal Recovery Console, você precisa mapear volumes entre aqueles relacionados no ponto de recuperação e os volumes existentes no hardware de destino.

O Rapid Recovery tenta mapear os volumes automaticamente. Se você aceitar o mapeamento padrão, o disco na máquina de destino será limpo e reparticionado e quaisquer dados anteriores serão excluídos. O alinhamento é realizado na ordem em que os volumes estão relacionados no ponto de recuperação e os volumes são alocados aos discos de forma adequada de acordo com o tamanho, e assim por diante. Supondo que haja espaço suficiente na unidade de destino, nenhum particionamento será necessário ao utilizar o alinhamento automático do disco. Um disco pode ser usado em diversos volumes. Se você mapear manualmente as unidades, observe que não poderá usar o mesmo disco duas vezes.

Para o mapeamento manual, é preciso ter a nova máquina corretamente formatada antes de restaurá-la. A máquina de destino deve ter uma partição separada para cada volume no ponto de recuperação, incluindo o volume reservado do sistema. Para obter mais informações, consulte Como usar o Universal Recovery Console para uma BMR.

Execute o procedimento para uma das seguintes opções de mapeamento de disco:

- Como mapear manualmente discos para uma BMR
- Mapear manualmente discos para obter uma BMR

CAUTION: Embora o Rapid Recovery suporte as partições FAT32 e ReFS, atualmente, apenas a restauração completa e a BMR são suportadas, visto que existe uma limitação do driver com ReFS, de modo que a restauração é implementada em modo de usuário, exportação da VM, e assim por diante. Se um Core está protegendo pelo menos um volume agente que contém o sistema de arquivos ReFS, ele deve ser instalado em máquinas com Windows 8,1, Windows 10 (Enterprise ou Pro somente), Windows Server 2012, Windows Server 2012 R2 ou Windows Server 2016, quem fornece suporte nativo ao formato ReFS. Caso contrário, a funcionalidade ficará limitada, e operações que envolvem tarefas, como a montagem de uma imagem de volume, não funcionarão. O Rapid Recovery **Core Console apresentará as mensagens de erro aplicáveis a essas ocorrências.**

CAUTION: A bare metal restore da configuração de discos de espaços de armazenamento não é suportada. Para obter mais detalhes, consulte o *Guia de instalação e atualização do Rapid Recovery*

Essa tarefa é uma das etapas do Realizar uma restauração sem sistema operacional para máquinas Windows. Faz parte do processo de Como usar o Universal Recovery Console para uma BMR.

Se for feita uma BMR em uma máquina com Linux no Core Console, essa tarefa também será uma etapa do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Iniciar uma restauração sem sistema operacional para Linux.

Como mapear manualmente discos para uma BMR

Esse procedimento permite mapear automaticamente discos durante uma bare metal restore (BMR) usando o Assistente de restauração de máquina.

Conclua as etapas no procedimento a seguir para selecionar automaticamente os volumes que você deseja recuperar e o local de restauração.

1. Na página Mapeamento de disco do Assistente de restauração de máquina, ao lado do mapeamento de volume, selecione **Automático** no menu suspenso.
2. Na tabela esquerda, verifique se os volumes apropriados estão listados e selecionados.

   NOTE: Em geral, em uma BMR, deve-se restaurar, no mínimo, o volume reservado do sistema e o volume do sistema (em geral, mas nem sempre, o volume C:\). Você precisa selecionar pelo menos um volume para realizar uma BMR.
3. Na tabela direita, selecione o disco ou os discos para os quais você deseja mapear volumes no computador de destino.
4. Clique em **Avançar**.
5. Na página Visualização de mapeamento de disco, revise o mapeamento dos volumes do ponto de recuperação e o volume de destino da restauração.
6. Para começar a restauração, clique em **Concluir**.

   CAUTION: Se você selecionar Iniciar restauração, todas as partições e os dados existentes na unidade de destino serão removidos permanentemente e substituídos pelo conteúdo do ponto de recuperação selecionado, inclusive o sistema operacional e todos os dados.

Mapear manualmente discos para obter uma BMR

Este procedimento descreve como designar que discos devem ser armazenados e em que locais na máquina restaurada.

Para mapear os discos manualmente, você precisa primeiro usar o DiskPart na linha de comando do computador de destino de BMR para criar e formatar volumes de destino. Para obter mais informações, consulte DiskPart Command-Line Options (Standard 7 SP1) na área de trabalho do desenvolvedor da Microsoft.

Execute as etapas do procedimento a seguir para selecionar manualmente os volumes que deseja restaurar e o local de restauração.

1. Na página de mapeamento disco do assistente de restauração de máquina, ao lado do mapeamento de volume, selecione **Manual** no menu suspenso.

   NOTE: Se não existirem volumes na unidade da máquina para os quais você esteja realizando uma restauração sem sistema operacional (BMR), não será possível ver essa opção ou mapear os volumes manualmente.

2. Na área Mapeamento de volume, em Volume de origem, confirme se o volume de origem está selecionado e se os volumes adequados estão relacionados abaixo dele e estão selecionados.
3. Em Destino, no menu suspenso, selecione o destino correto que é o volume de destino para realizar a restauração do ponto de recuperação sem sistema operacional e depois clique em **Restaurar**.
4. Na caixa de diálogo de confirmação, revise o mapeamento da origem do ponto de recuperação e do volume de destino da restauração.
5. Para iniciar a restauração, clique em **Iniciar restauração**.

   CAUTION: Se você selecionar Começar a restauração, todas as partições e dados existentes na unidade de destino serão removidos permanentemente e substituídos por conteúdo do ponto de recuperação selecionado, incluindo o sistema operacional e todos os dados.

Como realizar uma BMR com base em um arquivo

O Rapid Recovery permite restaurar uma máquina sem sistema operacional usando um ponto de recuperação arquivado.

As seguintes tarefas são pré-requisitos para este procedimento.

- Criar uma imagem ISO do CD de inicialização
- Como carregar o CD de inicialização e iniciar o computador de destino

No Universal Recovery Console (URC), você pode acessar o Rapid Recovery Core e recuperar um ponto de recuperação para uma restauração. Você também pode optar por restaurar a máquina sem sistema operacional em um ponto de recuperação armazenado em um arquivo. O URC permite atingir esse arquivo, independentemente de estar em uma unidade local, um compartilhamento de rede ou uma conta de nuvem.

1. No URC, clique na guia **Restaurar do arquivo**.
2. Na lista suspensa **Tipo de local**, selecione o local do arquivo. Você pode escolher dentre as opções a seguir.
   - Local
   - Rede
   - Nuvem
3. Insira as credenciais descritas na tabela a seguir de acordo com a seleção do tipo de local.

Tabela 147. Opções de credenciais do tipo de local

Tipo de local	Opção	Descrição
Local	Caminho local	O local atual do arquivo.

Tipo de local	Opção	Descrição
Rede	Caminho de rede	O local atual do arquivo.
	Usuário	O nome de usuário para acesso do compartilhamento de rede.
	Senha	A senha para acesso do compartilhamento de rede.
Nuvem	Tipo de nuvem	O fornecedor do local de armazenamento da nuvem. Selecione uma das seguintes opções: • Microsoft Azure • Amazon S3 • Fornecido pelo OpenStack • Arquivos do Rackspace Cloud • Google Cloud

4. Se você tiver selecionado um tipo de nuvem, complete as credenciais pertencentes ao fornecedor de nuvem.
   - Para o Microsoft Azure, conclua as seguintes etapas:
     1. Insira as seguintes credenciais:
        - Nome da conta de armazenamento
        - Chave de acesso
     2. Para o nome Contêiner, na lista suspensa, selecione um contêiner.
     3. Para o caminho da nuvem, na lista suspensa, selecione o caminho do arquivo.
   - Para o Amazon S3, conclua as etapas a seguir
     1. Insira as seguintes credenciais:
        - Chave de acesso
        - Chave secreta
     2. Para o nome Contêiner, na lista suspensa, selecione um contêiner.
     3. Para o caminho da nuvem, na lista suspensa, selecione o caminho do arquivo.
   - Para contas Desenvolvido com o OpenStack ou Arquivos do Rackspace Cloud, conclua as seguintes etapas:
     1. Especifique as seguintes informações:
        - Região
        - Usuário
     2. Selecione uma das opções a seguir:
        - Senha
        - Chave de API
     3. Na caixa de texto, insira as informações com base na seleção na Etapa c.
     4. Especifique as seguintes informações:
        - ID do locatário
        - URL de autenticação

- Nome do contêiner
- Caminho da nuvem

◦ Para contas do Google Cloud, execute as seguintes etapas:

1. Insira as seguintes credenciais:
   - Arquivo de certificado
   - Chave privada
2. Especifique as seguintes informações:
   - ID do projeto
   - E-mail da conta de serviço
3. No campo Nome do Contêiner, na lista suspensa, selecione o contêiner adequado.
   Para o caminho da nuvem, na lista suspensa, selecione o caminho do arquivo

5. Clique em **Avançar**.
6. Na página **Máquinas**, selecione a máquina que deseja restaurar e clique em **Avançar**.
7. Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar para restaurar a máquina e clique em **Avançar**.
8. Na página **Mapeamento**, selecione uma das seguintes opções e conclua as etapas correspondentes:

- Na lista suspensa **Mapeamento de volume**, selecione **Automático**.

1. Na tabela esquerda, verifique se os volumes apropriados estão listados e selecionados.

   NOTE: Em geral, em uma BMR, deve-se restaurar, no mínimo, o volume reservado do sistema e o volume do sistema (em geral, mas nem sempre, o volume `C:\`). Você precisa selecionar pelo menos um volume para realizar uma BMR.

2. Na tabela direita, selecione o disco ou os discos para os quais você deseja mapear volumes no computador de destino.

- No menu suspenso **Mapeamento de volume**, selecione **Manual**.

NOTE: Para mapear os discos manualmente, você precisa primeiro usar o DiskPart na linha de comando para criar e formatar volumes de destino. Para obter mais informações, consulte DiskPart Command-Line Options (Standard 7 SP1) na área de trabalho do desenvolvedor da Microsoft.

NOTE: Se não existirem volumes na unidade da máquina para os quais você esteja realizando uma restauração sem sistema operacional (BMR), não será possível ver essa opção ou mapear os volumes manualmente.

  - Em **Volumes de destino**, no menu suspenso, selecione o volume de destino adequado para cada volume no ponto de recuperação.

9. Na caixa de texto **Caminho de mapas de montagem**, digite um destino para o armazenamento temporário de mapeamento arquivos.

   O local padrão é `X:\ProgramData\AppRecovery\IndexEntriesMaps`.

   NOTE: Para garantir que o destino tenha espaço livre suficiente, divida a capacidade de volume total da montagem por 1.024. Por exemplo, usando-se a fórmula `(Mount volume total capacity) / 1024 = Free space` e, em seguida, `1 TB / 1024 = 1 GB`.

10. Clique em **Restaurar**.

    O URC mapeia os volumes para os novos discos.

11. Clique em **Restaurar**.

O URC restaura os dados para o computador de destino. Você pode visualizar o progresso na guia **Progresso da restauração**.

12. Depois que a restauração estiver concluída, remova o CD de inicialização.
13. Para inicializar o computador de destino BMR no Windows, reinicie a máquina.

Carregar os drivers no sistema operacional

Este procedimento descreve como carregar drivers no sistema operacional em um destino bare metal restore (BMR).

Para injetar drivers no sistema operacional, as seguintes tarefas já precisam ter sido realizadas:

- Criado um CD de inicialização usando o Boot CD Builder do Rapid Recovery Core Console. Para obter mais informações, consulte Criar uma imagem ISO do CD de inicialização.
- Carregado o CD de inicialização no destino BMR. Para obter mais informações, consulte Como carregar o CD de inicialização e iniciar o computador de destino.
- Carregado todos os drivers ou controladores necessários para armazenamento e rede. Para obter mais informações, consulte Carregar drivers usando o Universal Recovery Console.
- Realizado uma restauração usando o Assistente de restauração de máquina no Rapid Recovery Core Console ou um arquivamento a partir do Universal Recovery Console. Para obter mais informações, consulte Realizar um bare metal restore usando o Assistente de restauração de máquina e Como realizar uma BMR com base em um arquivo.

Depois de executar uma restauração, o processo não estará completo até que você injete os drivers para o sistema operacional no destino bare metal restore (BMR). Essa tarefa é adicional ao carregamento dos drivers no URC.

1. Depois de clicar em Restauração no procedimento BMR de sua escolha (veja os pré-requisitos), clique na guia **Gerenciamento de driver do Windows existente**.
2. Na lista suspensa, selecione um sistema operacional.

   O URC procura os drivers disponíveis.
3. Para carregar drivers adicionais, clique em **Forçar carregamento**.
4. Navegue pelo sistema de arquivamento para localizar o arquivo do driver compactado e selecione-o.
5. Clique em **OK**.

   O URC carrega o driver no sistema operacional que você selecionou.
6. Repita a Etapa 3 até a Etapa 5 para cada driver adicional que você precisar carregar.
7. Reinicie o computador de destino BMR.

   A BMR terminou. Se você tiver qualquer problema ao reinicializar, consulte Como reparar problemas de inicialização.

Realizar uma bare metal restore em máquinas Linux

No Rapid Recovery, você pode realizar uma bare metal restore (BMR) em uma máquina Linux, inclusive uma restauração do volume do sistema. A funcionalidade BMR tem suporte usando utilitário `local_mount` da linha de comando e na UI do Core Console.

CAUTION: O Rapid Recovery **suporta tipos de partição ext2 somente se o kernel for 3.10 e superior. Se estiver usando um kernel anterior, converta as partições ext2 em ext3, ext4 ou XFS antes de começar a proteção e fazer backup da máquina.**

CAUTION: Quando você inicializa uma máquina Linux restaurada pela primeira vez após uma BMR, o Rapid Recovery **gera uma imagem de base da máquina restaurada. Dependendo da quantidade de dados na máquina, esse processo leva mais tempo do que a captura de um instantâneo incremental. Para obter mais informações sobre imagens de base e snapshots incrementais, consulte Noções básicas sobre programações de proteção.**

Para realizar uma bare metal restore em máquinas Linux, execute as tarefas a seguir.

- Gerenciar uma imagem de inicialização do Linux Essa imagem ISO de inicialização do Live DVD será usada para iniciar a unidade de destino, a partir da qual é possível acessar o Universal Recovery Console para se comunicar com as cópias de segurança no Core. Consulte Gerenciar uma imagem de inicialização do Linux.
  - Para obter a imagem de inicialização para a BMR, certifique-se de que a versão do LiveDVD corresponda à versão do Core. Para obter mais informações, consulte Sobre a imagem ISO de inicialização para Linux e depois Baixar uma imagem ISO de inicialização para Linux.
  - Se você precisar de mídia física para iniciar a máquina de destino Linux, precisará transferir a imagem ISO para a mídia. Consulte Salvar a imagem ISO do Live DVD em mídia.
  - Em todos os casos, será preciso carregar a imagem de inicialização no server de destino e iniciar o server da imagem de inicialização. Consulte Carregar o Live DVD e iniciar o computador de destino.
  - Depois de carregar a mídia, você deverá conectar a máquina Linux ao Rapid Recovery Core. Consulte Conectar-se ao destino BMR a partir do Rapid Recovery Core.
- Gerenciar partições. Talvez seja necessário criar ou montar partições antes de executar uma BMR em uma máquina Linux. Consulte Como gerenciar partições do Linux.
  - O sistema Linux em que você está executando uma BMR deve ter as mesmas partições dos volumes de origem no ponto de recuperação. Talvez seja necessário criar partições adicionais no sistema de destino. Consulte Criar partições na unidade de destino.
  - Se você estiver realizando uma BMR manual, deverá montar as partições primeiro. Consulte Montar partições a partir da linha de comando. As etapas para montar as partições estão incluídas no processo para executar uma BMR a partir da linha de comando. Consulte Realizar uma bare metal restore em uma máquina Linux usando a linha de comando.

    Se estiver usando o autoparticionamento para BMR no Core Console, você não precisará montar as partições. O Rapid Recovery restaurará as mesmas partições incluídas nos pontos de recuperação que estão sendo restaurados.
- Iniciar uma bare metal restore para Linux. Depois que a máquina de destino é iniciada a partir da imagem de inicialização do Live DVD, é possível iniciar a BMR. As tarefas obrigatórias dependem da realização disso na interface do usuário do Rapid Recovery ou na linha de comando usando o utilitário local_mount. Consulte Iniciar uma restauração sem sistema operacional para Linux.
  - Se você estiver usando o Core Console, deverá iniciar uma restauração a partir de um ponto de recuperação do Core. Consulte Como selecionar um ponto de recuperação e iniciar uma BMR.
  - Se você estiver usando o Core Console, precisará mapear os volumes na interface do usuário. Consulte Sobre como mapear volumes para uma restauração sem sistema operacional.
  - Como opção, ao restaurar da linha de comando, você poderá usar o utilitário de tela para melhorar sua capacidade de rolar e ver os comandos no console do terminal. Esse utilitário é aberto por

padrão. Se fechá-lo, você poderá iniciá-lo novamente. Para obter mais informações, consulte Iniciar o utilitário Screen.

- Se você estiver usando local_mount, todas as tarefas serão realizadas na linha de comando. Para obter mais informações, consulte Realizar uma bare metal restore em uma máquina Linux usando a linha de comando.

- Confirmação de um bare metal restore. Após iniciar o procedimento de bare metal restore, você pode confirmar e monitorar o progresso. Consulte Confirmar a restauração sem sistema operacional na linha de comando.
  - É possível monitorar o progresso de sua restauração. Consulte Visualizar o progresso da recuperação.
  - Depois de concluída, você pode iniciar o server restaurado. Consulte Iniciar um servidor de destino restaurado.
  - Solucionar problemas do processo de BMR. ConsulteComo solucionar problemas de conexão com o Universal Recovery Console e Como reparar problemas de inicialização.

Pré-requisitos para realizar uma bare metal restore em máquinas Linux

Antes de iniciar o processo de realização de uma bare metal restore em uma máquina com Linux, é preciso garantir que as seguintes condições e critérios estejam presentes:

- Cópias de segurança da máquina que você deseja restaurar. É preciso ter um Rapid Recovery Core funcional que contenha pontos de recuperação do server protegido que você deseja restaurar.
- Hardware para restaurar (novo ou antigo, similar ou não). A máquina de destino deve atender aos requisitos de instalação de um agente; para obter mais detalhes, consulte o *Guia de instalação e atualização do Rapid Recovery*.
- Imagem de inicialização do Live DVD. Obtenha a imagem ISO do Linux Live DVD, que inclui uma versão inicializável do Linux. Baixe-a do Portal de licenças do Rapid Recovery em https://licenseportal.com. Se houver problemas para baixar o Live DVD, entre em contato com o Suporte de proteção de dados da Quest.
- Software e mídia de imagem. Se usar mídia física, é preciso ter um CD ou DVD virgem e um software de gravação de disco ou de criação de imagem ISO.
- Drivers do adaptador de rede e de armazenamento compatíveis. Se a restauração for para hardware diferente, é preciso ter drivers de armazenamento compatíveis e drivers do adaptador de rede para a máquina de destino, incluindo drivers de RAID, AHCI e chipset para o sistema operacional de destino, conforme o caso.
- Partições e espaço de armazenamento, conforme apropriado. Certifique-se que há espaço suficiente no disco rígido para criar partições de destino na máquina de destino que conterá os volumes de origem. Todas as partições de destino devem ser pelo menos do mesmo tamanho da partição de origem original.
- Restaurar caminho. Identifique o caminho da restauração, que é o caminho do descritor de arquivo de dispositivo. Para identificar o caminho do descritor de arquivo de dispositivo, use o comando `fdisk` em uma janela de terminal.

Gerenciar uma imagem de inicialização do Linux

Uma bare metal restore para Linux exige uma imagem de inicialização do Live DVD, que pode ser baixada do Portal de licenças do Rapid Recovery. Use essa imagem para iniciar a máquina Linux de destino. Com base nas

particularidades do seu ambiente, pode ser preciso transferir esta imagem para uma mídia física como um CD ou DVD. Você deve, então, carregar virtual ou fisicamente a imagem de inicialização e iniciar o servidor Linux a partir da imagem de inicialização.

NOTE: O Live DVD era conhecido anteriormente como Live CD.

O gerenciamento de uma imagem de inicialização do Linux é uma etapa em Realizar uma bare metal restore em máquinas Linux.

Você pode realizar as seguintes tarefas:

- Sobre a imagem ISO de inicialização para Linux
- Salvar a imagem ISO do Live DVD em mídia
- Carregar o Live DVD e iniciar o computador de destino
- Conectar-se ao destino BMR a partir do Rapid Recovery Core

Sobre a imagem ISO de inicialização para Linux

A primeira etapa ao realizar uma bare metal restore (BMR) em uma máquina com Linux é baixar a imagem ISO do Linux Live DVD do Portal de licenças do Rapid Recovery. O Live DVD funciona com todos os sistemas de arquivo Linux suportados pelo Rapid Recovery, e inclui uma versão inicializável do Linux, um utilitário de tela e a interface do Universal Recovery Console (URC) do Rapid Recovery. O Universal Recovery Console do Rapid Recovery é um ambiente usado para restaurar a unidade do sistema ou o server inteiro diretamente do Rapid Recovery Core.

NOTE: A Organização Internacional de Padronização (ISO) é um órgão internacional de representantes de diversas organizações nacionais que define padrões para sistemas de arquivos. ISO 9660 é uma norma de sistema de arquivos usada em mídia de disco óptico para troca de dados, e ela suporta vários sistemas operacionais. Uma imagem ISO é a imagem de disco ou arquivo, que contém dados para todos os setores do disco, bem como o sistema de arquivos do disco.

Baixar uma imagem ISO de inicialização para Linux

Para concluir uma bare metal restore para uma máquina Linux, você precisa de uma imagem ISO do Live DVD que corresponda à sua versão do Rapid Recovery. A versão atual do Live DVD está disponível no Portal de licenças do Rapid Recovery em https://licenseportal.com. Se você precisar de uma versão diferente, entre em contato com o Suporte de proteção de dados da Quest.

NOTE: Para obter mais informações sobre o Portal de licenças do Rapid Recovery, consulte o *Guia do usuário do portal de licenças do Rapid Recovery*.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Gerenciar uma imagem de inicialização do Linux.

Para baixar a imagem ISO do Live DVD, siga as etapas deste procedimento.

1. Faça login no Portal de licenças do Rapid Recovery em https://licenseportal.com.
2. No menu de navegação esquerdo, clique em **Downloads**.

   A página **Downloads** será exibida.
3. Role a tela para baixo até os aplicativos baseados em Linux, na seção Linux Live DVD, clique em **Download**.
4. Salve a imagem ISO do Live DVD.

NOTE: Ao restaurar uma máquina virtual, salve a imagem em um local de rede e configure a VM para iniciar a partir de uma unidade de CD ou DVD associada à imagem.

5. Se estiver restaurando a partir de uma máquina física, grave a imagem ISO do CD de inicialização em um CD ou DVD a partir do qual a máquina de destino possa ser iniciada. Para obter mais informações, consulte Salvar a imagem ISO do Live DVD em mídia.

Salvar a imagem ISO do Live DVD em mídia

Quando você baixar o arquivo Linux Live DVD, ele será armazenado como uma imagem ISO no caminho que você especificou. Você deve poder inicializar a máquina Linux de destino a partir da imagem do Live DVD.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Gerenciar uma imagem de inicialização do Linux.

1. Grave a imagem ISO do CD de inicialização em mídia de CD ou DVD.

   Se for executar uma BMR em uma máquina virtual, esta etapa não será necessária. Basta carregar a imagem ISO em uma unidade e editar as definições de máquina dessa VM para iniciar essa unidade. Você também pode usar a exportação virtual para restaurar uma VM Linux. Para obter mais informações, consulte Exportação da VM.

Carregar o Live DVD e iniciar o computador de destino

Depois de obter a imagem ISO do Live DVD, você precisa iniciar a máquina Linux a partir do Live DVD recém-criado.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Gerenciar uma imagem de inicialização do Linux.

1. Navegue até o novo servidor e carregue a imagem do Live DVD do local apropriado. Especifique que o servidor será iniciado a partir da imagem do Live DVD.
2. Inicie a máquina.

   É exibida uma tela de abertura do Rapid Recovery e uma janela de terminal se abre, exibindo o endereço IP e a senha de autenticação da máquina.

   NOTE: Uma nova senha temporária é gerada cada vez que a máquina é iniciada com a imagem do Live DVD.
3. Anote o endereço IP e a senha de autenticação exibidos na tela de introdução. Você precisará dessas informações mais tarde durante o processo de recuperação de dados para fazer logon novamente no console.

Conectar-se ao destino BMR a partir do Rapid Recovery Core

Depois de iniciar a máquina Linux de destino com o Live DVD, essa máquina ficará pronta para o usuário se conectar a ela a partir do Core e iniciar o processo de bare metal restore. É possível realizar esse processo usando um de dois métodos:

- Iniciar uma restauração no Rapid Recovery Core Console. Para obter mais informações, consulte Iniciar uma restauração sem sistema operacional para Linux.
- Iniciar de uma restauração a partir da Linha de comando usando o utilitário local_mount. Para obter mais informações, consulte Realizar uma bare metal restore em uma máquina Linux usando a linha de comando.

Como gerenciar partições do Linux

Ao executar uma BMR, a unidade de destino na qual os dados serão restaurados deve ter as mesmas partições do ponto de recuperação que você está restaurando. Pode ser necessário criar partições para atender a esse requisito.

Você pode iniciar a restauração na linha de comando usando o utilitário local_mount ou no Rapid Recovery Core Console. Se for restaurar usando a interface do usuário, você deverá montar as partições primeiro.

O gerenciamento de partições no Linux é uma das etapas do Realizar uma bare metal restore em máquinas Linux.

Você pode realizar as seguintes tarefas:

Tarefas relacionadas

See also: Criar partições na unidade de destino
See also: Formatar partições na unidade de destino
See also: Montar partições a partir da linha de comando

Criar partições na unidade de destino

Geralmente, ao executar uma BMR, a unidade de destino é um novo volume que pode consistir em uma única partição. A unidade na máquina de destino deve ter a mesma tabela de partições do ponto de recuperação, incluindo o tamanho dos volumes. Se a unidade de destino não contiver as mesmas partições, você deverá criá-las antes de executar a bare metal restore. Use o utilitário fdisk para criar partições na unidade de destino iguais às partições na unidade de origem.

CAUTION: O procedimento abaixo é apenas um exemplo. Ambientes de clientes são diferentes. Você deve alterar os comandos que usa de acordo com os aspectos específicos do ambiente.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Como gerenciar partições do Linux.

1. Como opção, você pode usar o utilitário Screen. Esse utilitário é iniciado por padrão e permanece ativo até você reinicializar a máquina.

   NOTE: Se você fechá-lo explicitamente e quiser reabri-lo, consulte Iniciar o utilitário Screen.

2. Na linha de comando, digite o seguinte comando e pressione **Enter** para alterar os privilégios para executar como administrador e depois liste as partições de disco existentes:

   ```
   sudo fdisk -l
   ```

   Uma lista de todos os volumes será exibida.

   Este exemplo pressupõe que o volume que você quer particionar seja /dev/sda. Se o volume for diferente (por exemplo, para unidades mais antigas, você poderá ver /dev/hda), altere os comandos de acordo.

3. Para criar uma nova partição de inicialização, digite o seguinte comando e pressione **Enter**:

   ```
   sudo fdisk /dev/sda
   ```

4. Para criar uma nova partição de inicialização, digite o seguinte comando e pressione **Enter**:

   ```
   n
   ```

5. Para criar uma nova partição primária, digite o seguinte comando e pressione **Enter**:

   ```
   p
   ```

6. Para especificar um número de partição, digite o número da partição e pressione **Enter**. Por exemplo, para especificar a partição 1, digite 1 e pressione **Enter**.
7. Para usar o primeiro setor, 2048, pressione **Enter**.
8. Aloque uma quantidade apropriada à partição de inicialização digitando o sinal de adição e a quantidade alocada e pressione **Enter**.

Por exemplo, para alocar 500 M para a partição de inicialização, digite o seguinte e pressione **Enter**:

```
+512000K
```

9. Para ativar/desativar um sinalizador inicializável para a partição de inicialização (para tornar a partição inicializável), digite o seguinte comando e pressione **Enter**:

   ```
   a
   ```

10. Para atribuir um sinalizador inicializável à partição apropriada, digite o número da partição e pressione **Enter**. Por exemplo, para atribuir um sinalizador inicializável para a partição 1, digite 1 e pressione **Enter**.
11. Continue particionando o disco conforme necessário.
12. Para salvar todas as alterações no utilitário fdisk, digite o seguinte comando e pressione **Enter**:

    w

Formatar partições na unidade de destino

Depois de criar partições em um novo volume na unidade de destino para realizar a restauração sem sistema operacional, se não estiver usando a partição automática, você deverá formatar as partições para elas serem montadas. Se essa situação se aplica a você, siga este procedimento para formatar partições em formatos ext3, ext4 ou XFS.

Para todos os outros cenários, você não precisa formatar partições conforme descrito neste tópico.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Como gerenciar partições do Linux.

1. Como opção, você pode usar o utilitário Screen. Esse utilitário é iniciado por padrão e permanece ativo até você reinicializar a máquina.

   NOTE: Se você fechá-lo explicitamente e quiser reabri-lo, consulte Iniciar o utilitário Screen.

2. Na linha de comando, digite o seguinte comando e pressione **Enter** para alterar os privilégios para executar como administrador e depois liste as partições de disco existentes:

   ```
   sudo fdisk -l
   ```

   Uma lista de todos os volumes será exibida.

   Este exemplo pressupõe que a partição que você quer formatar seja /dev/sda1. Se o volume for diferente (por exemplo, para unidades mais antigas, você poderá ver /dev/hda), altere os comandos de acordo.

3. Selecione um dos comandos a seguir com base no formato que você quer usar para a partição de destino:

   - Para formatar uma partição no formato ext3, digite o seguinte comando e pressione **Enter**:

     ```
     sudo mkfs.ext3 /dev/sda1
     ```

   - Para formatar uma partição no formato ext4, digite o seguinte comando e pressione **Enter**:

     ```
     sudo mkfs.ext4 /dev/sda1
     ```

   - Para formatar uma partição no formato XFS, insira o seguinte comando e pressione **Enter**:

     ```
     sudo mkfs.xfs /dev/sda1
     ```

     A partição selecionada é formatada de acordo.

4. Opcionalmente, se você precisar formatar outras partições, repita este procedimento.

Montar partições a partir da linha de comando

Se estiver realizando uma BMR usando o Rapid Recovery Core Console, você deverá primeiro montar as partições apropriadas na máquina de destino. Faça isso a partir da linha de comando no Universal Recovery Console.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Como gerenciar partições do Linux.

Conclua as etapas deste procedimento para montar partições na máquina Linux antes de executar uma restauração.

1. Na linha de comando, digite o seguinte comando e pressione **Enter** para alterar os privilégios para executar como administrador e depois liste as partições de disco existentes:

   ```
   sudo fdisk -l
   ```

   Uma lista de todos os volumes será exibida.

2. Formate todas as partições de que você precisará para realizar uma BMR no diretório de montagem. Eles devem corresponder aos volumes que estão no ponto de recuperação. Por exemplo, se o volume que deseja montar chama-se sda1 e o diretório de montagem é mnt, digite o seguinte comando e pressione **Enter**:
3. Monte todas as partições de que você precisará para realizar a BMR no diretório de montagem. Eles devem corresponder aos volumes que estão no ponto de recuperação. Por exemplo, se o volume que deseja montar chama-se sda1 e o diretório de montagem é mnt, digite o seguinte comando e pressione **Enter**:

   ```
   mount /dev/sda1 /mnt
   ```

4. Repita a Etapa 3 conforme necessário até você ter montado todos os volumes obrigatórios.

   Depois de montar os volumes, você poderá realizar uma restauração na máquina Linux de destino no Rapid Recovery Core Console. Consulte Iniciar uma restauração sem sistema operacional para Linux.

Iniciar uma restauração sem sistema operacional para Linux

Antes de iniciar uma bare metal restore (BMR) para uma máquina com Linux, as seguintes condições devem ser satisfeitas:

- Para restaurar um ponto de recuperação salvo no Core, é necessário ter o hardware apropriado disponível. Para obter mais informações, consulte Pré-requisitos para realizar uma bare metal restore em máquinas Linux.
- A máquina com Linux de destino da BMR deve ser iniciada usando a imagem de inicialização do Live DVD. Para obter mais informações, consulte Gerenciar uma imagem de inicialização do Linux.
- O número de volumes na máquina com Linux a ser restaurada deve corresponder ao número de volumes no ponto de recuperação. Também é preciso decidir se deseja restaurar a partir do Rapid Recovery Core Console ou da linha de comando usando local_mount. Para obter mais informações, consulte Como gerenciar partições do Linux.
- Se a restauração for feita a partir da UI do Core Console, a primeira etapa para iniciar a BMR é selecionar o ponto de recuperação apropriado, depois iniciar a restauração no hardware especificando o endereço IP e uma senha temporária obtida a partir do Universal Recovery Console. A seguir, você precisa mapear as unidades e iniciar a restauração.

Esse processo é uma etapa do Realizar uma bare metal restore em máquinas Linux.

Para iniciar uma BMR no Rapid Recovery Core Console, realize as tarefas a seguir.

- Como selecionar um ponto de recuperação e iniciar uma BMR
- Sobre como mapear volumes para uma restauração sem sistema operacional

Se a restauração for feita da linha de comando usando o utilitário local_mount, primeiro será preciso definir os privilégios apropriados, montar volumes, executar o local_mount, obter informações sobre o Core na lista de máquinas, conectar-se ao núcleo, obter uma lista de pontos de recuperação, selecionar o ponto de recuperação do qual deseja reverter em bare metal restore e iniciar a restauração.

Como opção, você pode iniciar o utilitário Screen.

Para iniciar uma BMR na linha de comando, realize as tarefas a seguir.

- Iniciar o utilitário Screen
- Realizar uma bare metal restore em uma máquina Linux usando a linha de comando

Iniciar o utilitário Screen

Incluído no Live DVD, o Screen é um utilitário que está disponível quando você inicia a partir do Live DVD no Universal Recovery Console. O Screen permite que os usuários gerenciem vários shells simultaneamente por uma única sessão do SSH (Secure Shell) ou janela do console. Isso permite realizar uma tarefa em uma janela de terminal (como confirmar volumes montados) e, enquanto isso é executado, abrir ou alternar para outra instância de shell e realizar outra tarefa (como executar o utilitário local_mount).

O utilitário Screen também tem o próprio buffer de rolagem, que permite rolar a tela para ver quantidades maiores de dados, como uma lista de pontos de recuperação.

NOTE: Esse utilitário é fornecido para sua conveniência; o uso do utilitário Screen é opcional.

O utilitário Screen inicia na máquina inicializada com o Live DVD por padrão. No entanto, se você tiver fechado este aplicativo, deverá iniciar o utilitário Screen a partir do Live DVD usando o procedimento abaixo.

1. Se a máquina foi inicializada a partir do Live DVD, na janela do terminal, digite screen e pressione **Enter**.

   O utilitário Screen é iniciado.

Realizar uma bare metal restore em uma máquina Linux usando a linha de comando

Depois que a imagem ISO do Live DVD estiver acessível na máquina na qual você deseja realizar uma BMR e o número e tamanho dos volumes forem correspondentes entre a máquina de destino e o ponto de recuperação no qual deseja executar a bare metal restore, será possível iniciar essa restauração na linha de comando usando o utilitário local_mount.

NOTE: Esse componente era chamado de `aamount`.

Se você quiser realizar uma BMR usando a UI do Rapid Recovery Core Console, consulte Como selecionar um ponto de recuperação e iniciar uma BMR.

NOTE: Ao realizar este procedimento, não tente montar pontos de recuperação na pasta /tmp, que contém os arquivos rapidrecovery-vdisk (antigo aavdisk).

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Realizar uma bare metal restore em uma máquina Linux usando a linha de comando.

Conclua as etapas deste procedimento para selecionar um ponto de recuperação no Core para reverter para a máquina de destino BMR física ou virtual.

1. Para executar o utilitário local_mount Rapid Recovery como raiz, digite o seguinte comando e pressione **Enter**:

   ```
   sudo local_mount
   ```

2. Para listar as máquinas protegidas, digite o seguinte comando e pressione **Enter**:

   ```
   lm
   ```

3. Quando solicitado, especifique as informações de conexão do Rapid Recovery Core conforme descrito na seguinte tabela, pressionando **Enter** após cada comando obrigatório:

Tabela 148. Informações de conexão do Rapid Recovery Core

Caixa de texto	Descrição	Obrigatório
Endereço IP ou o nome de host do Rapid Recovery Core	O nome do host ou endereço IP do Rapid Recovery Core.	Sim
Domínio	O domínio do Rapid Recovery Core. Isso é opcional.	Não
Usuário	O nome de usuário de um usuário administrativo no Core.	Sim
Senha	A senha usada para conectar o usuário administrativo ao Core.	Sim

Uma lista é exibida mostrando as máquinas protegidas pelo Rapid Recovery Core. Ela lista as máquinas encontradas por número de item de linha, o nome de exibição ou endereço IP do host e um número de ID para a máquina.

4. Para listar os pontos de recuperação para a máquina que você deseja restaurar, digite o comando de listagem de pontos de recuperação usando a sintaxe a seguir e pressione **Enter**:

```
lr <machine_line_item_number>
```

NOTE: Você também pode inserir o número de ID da máquina neste comando em vez do número do item de linha.

Uma lista exibe os pontos de recuperação de base e incrementais dessa máquina. Essa lista inclui:

- Um número de item de linha
- Carimbo de data e hora
- Uma lista de letras de volumes dentro do ponto de recuperação
- Local do volume
- Tamanho do ponto de recuperação
- Um número de ID para o volume que inclui um número de sequência no final, que identifica o ponto de recuperação.

5. Para selecionar o ponto de recuperação para restauração, digite o comando a seguir e pressione **Enter**:

```
r <recovery_point_ID_number> <path>
```

CAUTION: Você deve garantir que o volume do sistema não esteja montado.

NOTE: Se você tiver iniciado a máquina a partir do Live DVD, o volume do sistema não está montado.

Esse comando reverte a imagem do volume especificada pelo ID do Core para o caminho especificado. O caminho da restauração é o do descritor de arquivo de dispositivo e não do diretório no qual está montado.

NOTE: Você também pode especificar um número de linha no comando em vez do número de ID do ponto de recuperação para identificar o ponto de recuperação. Nesse caso, use o número de linha de agente/máquina (do resultado de `lm`), seguido do número da linha do ponto de recuperação e da letra de volume (da lista de volumes com letras dentro do ponto de recuperação), seguidos pelo caminho. Por exemplo:

```
r <machine_line_item_number> <base_image_recovery_point_line_number>
<volume_letter> <path>
```

Por exemplo, digite: `r 1 24 a /dev/sda1`

Nesse comando, `<path>` é o descritor de arquivo do volume real.

6. Quando solicitado a continuar, digite y para Sim e pressione **Enter**.

   Depois que a restauração iniciar, uma série de mensagens serão exibidas para notificá-lo sobre o status da conclusão da restauração.

   NOTE: Se você receber uma mensagem de exceção, os detalhes sobre essa exceção poderão ser encontrados no arquivo local_mount.log. O arquivo local_mount.log está localizado em `/var/log/apprecovery`.

7. Depois de uma restauração bem-sucedida, saia de local_mount digitando `exit` e pressione **Enter**.
8. A próxima etapa é verificar a restauração. Para obter mais informações, consulte Confirmar a restauração sem sistema operacional na linha de comando.

Restaurar volumes em uma máquina Linux usando a linha de comando

Antes de restaurar dados de um ponto de recuperação usando a linha de comando, você deve desmontar o disco no qual fará a restauração de dados.

No Rapid Recovery, é possível restaurar volumes em suas máquinas Linux protegidas usando o utilitário de linha de comando `local_mount`.

NOTE: Esse processo antes era chamado de reversão. Ao realizar este procedimento, não tente montar pontos de recuperação na pasta /tmp, que contém os arquivos rapidrecovery-vdisk (antigo aavdisk).
A restauração de volumes também é suportada nas máquinas protegidas no Rapid Recovery Core Console. Para obter mais informações, consulte Sobre restauração de volumes a partir de um ponto de recuperação.

CAUTION: Para restaurar a partição de sistema ou raiz (/) ou todo o sistema operacional, consulte Realizar uma bare metal restore em máquinas Linux.

1. Execute o utilitário Rapid Recovery`local_mount` como raiz, por exemplo:

   ```
   sudo local_mount
   ```

2. No prompt de montagem do Rapid Recovery, digite o comando a seguir para listar as máquinas protegidas.

   ```
   lm
   ```

3. Quando solicitado, digite o endereço IP ou nome do host do servidor do Rapid Recovery Core Core.
4. Insira as credenciais de login desse server, ou seja, o nome de usuário e a senha.

   Aparece uma lista que mostra as máquinas protegidas por esse servidor do Rapid Recovery Core. Ela lista as máquinas protegidas encontradas por número de item de linha, nome do host/endereço IP e um número de ID para a máquina (por exemplo: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2).

5. Insira o seguinte comando para relacionar os pontos de recuperação atualmente montados para a máquina especificada:

```
lr <machine_line_item_number>
```

NOTE: Observe que você também pode inserir o número de ID da máquina neste comando em vez do número do item de linha.

Uma exibição em lista exibe os pontos de recuperação de base e incremental da máquina. Essa lista inclui um número de item de linha, data/carimbo de data e hora, localização do volume, tamanho de ponto de recuperação e número de ID do volume que inclui um número de sequência no fim (por exemplo,"293cc667-44b4-48ab-91d8-44bc74252a4f:2"), que identifica o ponto de recuperação.

6. Insira o seguinte comando para selecionar um ponto de recuperação a restaurar:

   ```
   r <volume_recovery_point_ID_number> <device path>
   ```

   Esse comando restaura a imagem do volume especificada pela ID do Core para o caminho especificado. O caminho da restauração é o do descritor de arquivo de dispositivo e não o diretório no qual está montado.

   - Você também pode especificar um número de linha no comando em vez do número de ID do ponto de recuperação para identificar o ponto de recuperação. Nesse caso, você usaria o número de linha da máquina protegida (da saída lm), seguido do número da linha do ponto de recuperação e letra de volume, seguido pelo caminho, como, r <machine_line_item_number> <recovery_point_line_number> <volume_letter> <caminho>. Nesse comando, <caminho> é o descritor de arquivo do volume real.

     Por exemplo, se o resultado de `lm` listar três máquinas protegidas e você digitar o comando `lr` para a máquina protegida número `2` para restaurar o volume `23` do ponto de recuperação `b` no volume que foi montado no diretório `/dev/sda5`, o comando deverá ser:

     ```
     r2 23 b /dev/sda5
     ```

     NOTE: É possível restaurar para / se necessário. Se estiver executando uma restauração sem sistema operacional usando um Live DVD, presume-se que você quer restaurar para uma máquina diferente. Para obter mais informações, consulte Iniciar uma restauração sem sistema operacional para Linux.

7. Quando solicitado para continuar, digite `y` para Sim.

   Depois que a restauração continuar, uma série de mensagens será exibida para notificá-lo sobre o status.

8. Após uma restauração bem-sucedida, o utilitário `local_mount` montará e reconectará automaticamente o módulo do kernel no volume restaurado se o destino antes estava protegido e montado. Caso contrário, será necessário montar o volume restaurado no disco local e, em seguida, confirmar se os arquivos estão restaurados (por exemplo, é possível usar o comando `sudo mount` e depois o comando `ls`.)

Confirmar uma bare metal restore

Depois de realizar uma bare metal restore (BMR), você poderá confirmar o progresso da restauração. Quando a ação for concluída com sucesso, você poderá iniciar o server restaurado. Algumas etapas de resolução de problemas são incluídas se houver dificuldades para se conectar ao Universal Recovery Console a fim de concluir a restauração e, se necessário, reparar problemas de inicialização com a máquina restaurada.

Você pode realizar as seguintes tarefas:

- Visualizar o progresso da recuperação
- Iniciar um servidor de destino restaurado
- Como solucionar problemas de conexão com o Universal Recovery Console
- Como reparar problemas de inicialização

Visualizar o progresso da recuperação

Execute as etapas deste procedimento para visualizar o progresso da restauração de dados de um ponto de recuperação (incluindo a bare metal restore) iniciado no Rapid Recovery Core Console.

1. Depois de iniciar o processo de restauração de dados de um ponto de recuperação, enquanto a tarefa estiver em andamento, você pode visualizar seu progresso no menu suspenso  **Tarefas em execução** no Core Console.
2. É possível visualizar informações detalhadas na página **Eventos**. Para obter mais informações sobre o monitoramento de eventos do Rapid Recovery, consulte Como exibir eventos usando tarefas, alertas e páginas de diário.

Iniciar um servidor de destino restaurado

Execute as etapas deste procedimento para iniciar o server de destino restaurado.

NOTE: Antes de iniciar o server de destino restaurado, confirme se a recuperação foi bem-sucedida. Para obter mais informações, consulte Visualizar o progresso da recuperação.

Essa tarefa é uma das etapas do Realizar uma restauração sem sistema operacional para máquinas Windows. Faz parte do processo de Confirmar uma bare metal restore

1. No servidor de destino, verifique se o Universal Recovery Console do Rapid Recovery está ativo.
2. Ejete o CD de inicialização (ou desconecte a mídia física com a imagem do CD de inicialização) do server restaurado.
3. No Universal Recovery Console, clique no ícone de menu de Energia na parte superior da tela e, em seguida, clique em **Reinicialização**.
4. Especifique para iniciar o sistema operacional normalmente.
5. Efetue login na máquina. O sistema deve ser restaurado para o estado capturado no ponto de recuperação.

Como solucionar problemas de conexão com o Universal Recovery Console

Encontramos a seguir as etapas da solução de problemas de conexão com a imagem do CD de inicialização como parte do processo de Como selecionar um ponto de recuperação e iniciar uma BMR.

Se um erro for exibido indicando que o Core não pôde se conectar ao servidor remoto, qualquer uma das várias causas possíveis a seguir são prováveis.

- Confirme se o endereço IP e a senha atual exibidos no URC são idênticos às informações inseridas na caixa de diálogo Instância do console de recuperação.
- Para acessar o servidor no qual deseja restaurar os dados, o Core deve ser capaz de identificar o servidor na rede. Para determinar se a identificação do servidor, você poderá abrir um prompt de comando no Core e fazer um ping do endereço IP do server de BMR de destino. Também é possível abrir um prompt de comando no server de destino e fazer um ping para o endereço IP do Rapid Recovery Core.
- Verifique se as configurações do adaptador de rede são compatíveis entre o Core e o servidor BMR de destino.

Como reparar problemas de inicialização

As seguintes tarefas são pré-requisitos para este procedimento.

- Criar uma imagem ISO do CD de inicialização
- Como carregar o CD de inicialização e iniciar o computador de destino
- Carregar drivers usando o Universal Recovery Console

Conclua as etapas deste procedimento para reparar problemas de inicialização. Lembre-se de que se você restaurou em um hardware diferente, precisará ter controlador de armazenamento injetado, RAID, AHCI, chipset e outros drivers se eles ainda não estiverem no CD de inicialização. Esses drivers permitem que o sistema operacional utilize todos os dispositivos no servidor de destino com êxito. Para obter mais informações, consulte Carregar drivers usando o Universal Recovery Console. Conclua o procedimento a seguir para reparar problemas de inicialização no servidor de destino.

1. No Universal Recovery Console, clique na guia **Gerenciador de driver do Windows existente**.
2. Clique em **Reparar problemas de inicialização**.

   Os parâmetros de inicialização no registro de inicialização do servidor de destino são reparados automaticamente.

Confirmar a restauração sem sistema operacional na linha de comando

A Quest recomenda realizar as seguintes etapas para confirmar se uma bare metal restore foi concluída na linha de comando.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux.

- Realizar uma verificação do sistema de arquivos no volume restaurado
- Como usar a linha de comando para tornar uma máquina Linux restaurada inicializável

Realizar uma verificação do sistema de arquivos no volume restaurado

Uma vez executada uma bare metal restore a partir da linha de comando, você deve executar a verificação do sistema de arquivos no volume restaurado para garantir que os dados restaurados do ponto de recuperação não estejam corrompidos.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Confirmar a restauração sem sistema operacional na linha de comando.

Execute a tarefa abaixo para executar uma verificação do sistema de arquivos no volume restaurado.

1. Na linha de comando do Universal Recovery Console da máquina Linux restaurada, para verificar se as partições apropriadas estão montadas, digite o seguinte comando e pressione **Enter**:

   ```
   df
   ```
2. Se o volume restaurado não estiver montado, vá para Etapa 3. Se o volume restaurado estiver montado, desmonte-o digitando o seguinte comando e pressionando **Enter**:

   ```
   umount <ponto de montagem>
   ```
3. Execute uma verificação do sistema de arquivos nos volumes restaurados digitando o seguinte comando e pressione **Enter**:

   ```
   fsck -f <volume>
   ```

Se o fsck retornar limpo, o sistema de arquivos foi verificado.

4. Monte os volumes adequados novamente digitando o seguinte comando no formato `mount <volume> <pasta>` e pressione **Enter**.

   Por exemplo, se o caminho do volume for prod/sda1 e a pasta na qual se deseja montar for mnt, digite o seguinte e pressione **Enter**:

   ```
   mount /dev/sda1 /mnt
   ```

Como usar a linha de comando para tornar uma máquina Linux restaurada inicializável

Ao concluir uma verificação limpa do sistema de arquivos no volume restaurado, você deve criar partições inicializáveis.

O GRUB (GNU Grand Unified Bootloader) é um carregador de inicialização que permite que os administradores configurem qual configuração de sistema operacional ou kernel específica é usada para iniciar o sistema. Após uma BMR, o arquivo de configuração do GRUB deve ser modificado para que a máquina use o UUID (identificador universal exclusivo) apropriado para o volume raiz. Antes desta etapa, você deve montar os volumes de inicialização e raiz e verificar os UUIDs de cada um. Isso garante que você possa inicializar a partir de partição.

NOTE: Este procedimento aplica-se a máquinas Linux que usam o GRUB1 ou GRUB2. Quando você usar este procedimento, certifique-se de que a partição de inicialização esteja íntegra e segura.

GRUB ou GRUB2 costuma ser instalado com sistemas operacionais Linux. Você pode realizar esse procedimento usando a versão que acompanha a distribuição Linux. Se uma versão do GRUB não estiver instalada, você terá que reinstalar a versão padrão apropriada à sua distribuição Linux.

CAUTION: Quando você inicializa uma máquina Linux restaurada pela primeira vez após uma BMR, o Rapid Recovery **gera uma imagem de base da máquina restaurada. Dependendo da quantidade de dados na máquina, esse processo leva mais tempo do que a captura de um instantâneo incremental. Para obter mais informações sobre imagens de base e snapshots incrementais, consulte Noções básicas sobre programações de proteção.**

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Confirmar a restauração sem sistema operacional na linha de comando.

Execute a tarefa abaixo para criar partições inicializáveis usando a linha de comando.

1. Você deve montar o volume raiz primeiro e, em seguida, o volume de inicialização. Monte cada volume restaurado usando os seguintes comandos:
   a. Para montar o volume raiz, digite o seguinte comando e pressione **Enter**:

      ```
      mount /<restored volume[root]> /mnt
      ```

      Por exemplo, se /dev/sda2 for o volume raiz, digite mount /dev/sda2 /mnt and e pressione **Enter**.

   b. Para montar o volume de inicialização, digite o seguinte comando e pressione **Enter**:

      ```
      mount /<restored volume[boot]> /mnt/boot
      ```

      Por exemplo, se /dev/sda1 for o volume de inicialização, digite mount /dev/sda1 /mnt/boot e pressione **Enter**.

   NOTE: Algumas configurações do sistema podem incluir o diretório de inicialização como parte do volume raiz.

2. Se o tamanho do volume estiver aumentando, isto é, se o volume de destino na nova máquina Linux for maior que o volume que estava no ponto de recuperação, exclua qualquer arquivo de dados de bitmap existente.
3. Obtenha o identificador universal exclusivo (UUID) dos novos volumes usando o comando `blkid`. Digite o seguinte e pressione **Enter**:

   ```
   blkid [volume]
   ```

NOTE: Você também pode usar o comando `ls -l /dev/disk/by-uuid`.

4. Se estiver fazendo uma BMR em um novo disco na máquina de destino, comente a partição de memória virtual em fstab no volume raiz.
5. A modificação dos caminhos fstab e mtab deve ocorrer no volume restaurado, e não no Live DVD. Não há necessidade de modificar os caminhos no Live DVD. Prepare-se para a instalação do GRUB digitando os comandos a seguir. Após cada comando, pressione **Enter**:

   ```
   mount --bind /dev /mnt/dev
   mount --bind /proc /mnt/proc
   mount --bind /sys /mnt/sys
   ```
6. Altere o diretório raiz digitando o seguinte comando e pressione **Enter**:

   ```
   chroot /mnt /bin/bash
   ```
7. Obtenha o UUID antigo da partição ou partições no arquivo `/etc/fstab` dos pontos de recuperação montados e compare-o aos UUIDs das partições raiz (para Ubuntu e CentOS), de inicialização (para CentOS e RHEL) ou de dados digitando o seguinte comando e pressionando **Enter**:

   ```
   less /mnt/etc/fstab
   ```
8. Obtenha o UUID antigo das partições no arquivo `/etc/mtab` dos pontos de recuperação montados e compare-o aos UUIDs das partições raiz (para Ubuntu e CentOS), de inicialização (para CentOS e RHEL) ou de dados digitando o seguinte comando e pressionando **Enter**:

   ```
   less /mnt/etc/mtab
   ```
9. Se estiver usando o SLES 11, instale o GRUB digitando os seguintes comandos, pressionando **Enter** depois de cada um:

   ```
   grub-install --recheck /dev/sda
   grub-install /dev/sda
   ```
10. Se você estiver usando Ubuntu, CentOS 6.x, RHEL 6.x ou Oracle Linux 6.x, instale GRUB digitando o seguinte comando e pressione **Enter**:

    ```
    grub-install /dev/sda
    ```
11. Se você estiver usando SLES 12, CentOS 7, RHEL 7 ou Oracle 7, instale GRUB2 digitando o seguinte comando e pressione **Enter**:

    ```
    grub2-install /dev/sda
    ```
12. Após concluir a instalação, execute uma das seguintes atualizações:
    - Para SLES:

      ```
      grub-install.unsupported --recheck /dev/sda
      grub-install.unsupported /dev/sda
      update-grub
      ```

      NOTE: Se o comando `update-grub` não existir na sua distribuição Linux, ignore essa opção.
    - Para outras distribuições:

      ```
      grub-install /dev/sda
      update-grub
      ```

      NOTE: Se o comando `update-grub` não existir na sua distribuição Linux, ignore essa opção.
13. Remova o disco do Live DVD da unidade de CD-ROM ou DVD e reinicie a máquina Linux.

Como gerenciar dados de classificação por vencimento

Esta seção descreve como gerenciar dados de instantâneo de classificação por vencimento salvos em seu repositório. Contém informações sobre como reter pontos de recuperação em seu repositório, políticas de retenção e o processo resultante de rollup de pontos de recuperação para economizar espaço. Descreve a capacidade de relocar pontos de recuperação do seu repositório para uma solução de backup e deduplicação DR da Quest.

Esta seção descreve também como gerenciar políticas de retenção que controlam o rollup e como forçar o rollup sob demanda.

Retenção de dados, enfileiramento para armazenamento secundário e arquivamento

Cada vez que o seu Core captura um snaphot, os dados são salvos como um ponto de recuperação em seu repositório. Os pontos de recuperação naturalmente se acumulam com o passar do tempo. O Core usa uma política de retenção para determinar quanto tempo os dados de snapshot ficarão retidos no repositório. Ao executar trabalhos noturnos (especificamente, durante o processo de rollup), o Core impõe a política de retenção para reduzir a quantidade consumida de espaço de armazenamento. A data de cada ponto de recuperação é comparada com a data do ponto de recuperação mais recente. O Core então acumula (combina) pontos de recuperação mais antigos. Com o passar do tempo, pontos de recuperação mais antigos no repositório são continuamente substituídos por outros mais recentes à medida que os pontos de recuperação mais antigos, eventualmente, alcançam a idade mais antiga definida no período de retenção.

A partir do Questversão 6.1.1, você pode também relocar pontos de recuperação do seu repositório DVM para um repositório de camadas em uma solução de backup e deduplicação DR da Rapid Recovery. Isso libera armazenamento no seu repositório principal.

Para definir os pontos de recuperação em camadas no armazenamento secundário usando esse método, você precisa primeiro adicionar a solução DR como um repositório no seu Rapid Recovery Core. Para obter mais informações sobre a criação de um novo repositório de camadas secundário em um DR, consulte Criar um repositório de camadas.Em seguida, no nível da máquina protegida, especifique na política de retenção a idade em que deseja que os pontos de recuperação sejam realocados do repositório principal para o secundário. Para obter mais informações, consulte Personalizar as definições de política de retenção de uma máquina protegida (especialmente as etapas 7 e 10).

NOTE: Independentemente de onde os pontos de recuperação estão localizados (um repositório DVM local primário, ou um repositório de camadas secundário em uma solução de backup DR), eles ainda estão sujeitos à política de retenção, e ainda serão acumulados. Se você precisar manter pontos de recuperação mais antigos, um método consiste em arquivar. A outra abordagem é desativar o rollup ou ampliar o período de retenção das máquinas protegidas relevantes.

Para manter pontos de recuperação que, de outra forma seriam combinados e, finalmente excluídos, você pode criar um arquivo a partir do Console do Core. Um arquivo contém uma cópia do conjunto completo de pontos de recuperação para as máquinas protegidas no seu Core, no momento em que foram criados. Posteriormente,

você pode acessar informações arquivadas do Core Console. Em contraste com os pontos de recuperação no repositório, os pontos de recuperação em um arquivo não são acumulados.

Os arquivos são úteis para manter os dados em conformidade, fazer o backup do Core, propagar os dados de replicação para uma réplica remota do Core e economizar espaço no Core para reter as transações recentes fundamentais para a empresa enquanto mantém os backups por um período de tempo mais longo.

Para obter mais informações sobre arquivos, consulte Arquivamento.

Gerenciar políticas de retenção

Uma política de retenção é um conjunto de regras que determina o período de tempo para o Core manter pontos de recuperação antes de começar o processo de rollup. As políticas de retenção podem ser definidas para combinações com base em horas, dias, semanas, meses e anos. Você pode definir até seis regras (a política padrão define cinco regras).

Considerando que você pode fazer backup de 5 em 5 minutos (com a frequência mínima de uma vez por hora para o DL1000), a primeira regra na política de retenção normalmente define quanto tempo será a retenção de todos os pontos de recuperação. Por exemplo, se você fizer o backup de uma máquina a cada quinze minutos, 96 pontos de recuperação serão salvos no repositório para aquela máquina por dia, até que o rollup seja iniciado. Sem o gerenciamento de sua política de retenção, essa quantidade de dados pode rapidamente preencher um repositório.

NOTE: Os administradores devem observar que backups frequentes podem causar impacto no tráfego de rede. Outros fatores que afetam o tráfego de rede incluem outras transferências (como replicação), a taxa de alteração de seus dados, o hardware de sua rede, cabos e comutadores.

O Core vem predefinido com uma política padrão de retenção. A política padrão mantém:

- Todos os pontos de recuperação por 3 dias
- Um ponto de recuperação por hora por dois dias
- Um ponto de recuperação por dia para quatro dias
- Um ponto de recuperação por semana por três semanas
- Um ponto de recuperação por mês por dois meses
- Um ponto de recuperação por ano para X anos (desativado na política padrão).

Seguindo esta política padrão, o ponto de recuperação mais antigo normalmente tem 92 dias. Os dados depois da data de originação serão apagados para uma política padrão.

A definição da política de retenção em nível de Core aplica-se automaticamente a todas as máquinas que o Core protege. Você pode alterar a política padrão para atender às suas necessidades.

Para qualquer máquina, você também pode criar uma política de retenção personalizada. A definição da política em nível de máquina permite que você especifique uma política de retenção diferente da política padrão do Core. Para obter mais informações sobre a configuração de políticas de retenção, consulte Configurar as definições da política de retenção padrão do Core e Personalizar as definições de política de retenção de uma máquina protegida.

Configurar as definições da política de retenção padrão do Core

A política de retenção do Core especifica por quanto tempo os pontos de recuperação de uma máquina protegida são armazenados no repositório.

A política de retenção do Core é imposta pelo processo de rollup, que é executado como um dos componentes da execução de trabalhos noturnos. Nesse momento, os pontos de recuperação além da idade especificada na política de retenção são submetidos a um "rollup" (combinados) em menos pontos de recuperação, que abrangem um período de tempo menos granular. Aplicar a política de retenção todas as noites resulta no rollup contínuo de cópias de segurança antigas. Com o tempo, os pontos de recuperação mais antigos são excluídos, com base nos requisitos especificados nessa política de retenção.

Diferentes definições de retenção podem ser configuradas para Cores de origem e de destino.

NOTE: Esse tópico é específico para personalizar as definições de política de retenção no Rapid Recovery Core. Ao salvar definições de política de retenção personalizadas no Core, você estabelece as definições de política de retenção padrão que podem ser aplicadas a todas as máquinas protegidas por esse Core. Para obter mais informações sobre a personalização das definições da política de retenção para máquinas protegidas individuais, consulte Personalizar as definições de política de retenção de uma máquina protegida.

1. Navegue até o Rapid Recovery Core Console.
2. Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
   - Na lista de definições do Core no lado esquerdo da página Definições, clique em **Trabalhos noturnos**.
   - Role a tela para baixo no lado direito do da página Definições até que você possa ver o cabeçalho **Trabalhos noturnos**.

   As definições do core de Trabalhos noturnos serão exibidas.
3. Em **Trabalhos noturnos**, clique em **Alterar**.

   A caixa de diálogo **Trabalhos noturnos** é exibida.
4. Para especificar os intervalos de tempo para retenção de dados de cópia de segurança, conforme necessário, no painel de Trabalhos noturnos, selecione a opção **Rollup** e clique em **Definições**.

   A caixa de diálogo **Configuração** para a política de retenção padrão do Core será exibida.
5. Para restaurar as definições da política de retenção do Core para os valores padrão a qualquer momento, na parte inferior da caixa de diálogo Configuração, clique em **Restaurar padrão** e, em seguida, clique em **Sim** para confirmar.

   Todas as definições serão restauradas para os valores padrão descritos na tabela na Etapa 6.
6. Insira a programação padrão para reter pontos de recuperação, conforme descrito na tabela a seguir. A primeira configuração especifica o período de retenção principal para todos os pontos de recuperação salvos no repositório. Cada configuração adicional, quando ativada, fornece um nível de retenção mais granular, especificando os intervalos entre os quais pontos de recuperação devem passar por rollup. Essas configurações definem por quanto os pontos de recuperação são mantidos.

   As opções da política de retenção são descritas na tabela a seguir.

Tabela 149. Opções do Programa para política padrão de retenção

Caixa de texto	Descrição
Manter todos os pontos de recuperação por n [período de retenção]...	Especifica o período de retenção principal para todos os pontos de recuperação salvos no repositório. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é 3 dias. Você pode selecionar dentre: Dias, Semanas, Meses e Anos
…e depois manter um ponto de recuperação	Se selecionada, essa configuração mantém um ponto de recuperação por hora pelo período que você especificar. O padrão é 2 dias. Você pode escolher entre dias, semanas, meses ou anos.

Caixa de texto	Descrição
por hora por n [período de retenção]	Se você não quiser salvar pelo menos um ponto de recuperação por hora, desmarque essa opção.
…e depois manter um ponto de recuperação por dia por n [período de retenção]	Se selecionada, essa configuração mantém um ponto de recuperação por dia pelo período que você especificar. O padrão é 4 dias. Você pode escolher entre dias, semanas, meses ou anos. Se você não quiser salvar pelo menos um ponto de recuperação diariamente, desmarque essa opção.
…e depois manter um ponto de recuperação por semana por n [período de retenção]	Se selecionada, essa configuração mantém um ponto de recuperação por semana pelo período que você especificar. O padrão é 3 semanas. Você pode escolher entre semanas, meses e anos. Se você não quiser salvar pelo menos um ponto de recuperação semanalmente, desmarque essa opção.
…e depois manter um ponto de recuperação por mês por n [período de retenção]	Se selecionada, essa configuração mantém um ponto de recuperação por mês pelo período que você especificar. O padrão é 2 meses. Você pode escolher entre meses e anos. Se você não quiser salvar pelo menos um ponto de recuperação mensalmente, desmarque essa opção.
…e depois manter um ponto de recuperação por ano por n [período de retenção]	Se selecionada, essa configuração mantém um ponto de recuperação por ano pelo número de anos que você especificar. O padrão (1 ano) é desativado por padrão. Se você quiser salvar pelo menos um ponto de recuperação anualmente, selecione essa opção e especifique um número de anos. Se você não quiser salvar pelo menos um ponto de recuperação anualmente, desmarque essa opção.

O ponto de recuperação mais antigo é determinado pelas definições da política de retenção.

O seguinte é um exemplo de como o período de retenção é calculado.

Manter todos os pontos de recuperação por três dias.

... e, em seguida, manter um ponto de recuperação por hora por três dias

... e, em seguida, manter um ponto de recuperação por hora por quatro dias

... e, em seguida, manter um ponto de recuperação por semana por três semanas

... e, em seguida, manter um ponto de recuperação por mês por dois meses

... e, em seguida, manter um ponto de recuperação por mês por um ano

Neste exemplo, o ponto de recuperação mais antigo teria um ano e três meses.

7. Quando estiver satisfeito com suas definições da política de retenção, clique em **Salvar**.

   A caixa de diálogo **Configuração** será fechada.

8. Na caixa de diálogo **Trabalhos noturnos**, clique em **OK**.

   A caixa de diálogo **Trabalhos noturnos** será exibida. A política de retenção definida será aplicada durante o rollup noturno.

   Também será possível aplicar essas definições ao especificar a política de retenção para qualquer máquina protegida individual. Para obter mais informações sobre a definição de políticas de retenção para uma máquina protegida, consulte Personalizar as definições de política de retenção de uma máquina protegida.

Personalizar as definições de política de retenção de uma máquina protegida

Se você quiser relocar pontos de recuperação de uma máquina protegida específica de um repositório DVM primário para um repositório de camadas, o repositório de camadas já deverá existir. Para definir um repositório de camadas, consulte o tópico Criar um repositório de camadas.

A política de retenção de uma máquina protegida especifica por quanto tempo os pontos de recuperação são armazenados no repositório. Por padrão, cada máquina protegida usa a política de retenção estabelecida para o Core, a menos que você especifique uma política de retenção personalizada, conforme descrito neste procedimento.

A partir do Rapid Recovery versão 5.4.1, o AppAssure inclui a capacidade de definir políticas de retenção discrepantes entre uma máquina protegida no Core de origem e a máquina replicada correspondente no Core de destino.

Use este procedimento para definir uma política de retenção personalizada para uma máquina protegida, incluindo uma máquina replicada.

NOTE: O que se segue aplica-se a ambientes que fazem o upgrade a partir do Rapid Recovery Core versão 5.3.x até a versão 5.4.1 ou qualquer versão do AppAssure. Se você quiser personalizar uma política de retenção para qualquer máquina replicada, primeiro realize o upgrade dos Cores de origem e de destino para o AppAssure Core versão 5.4.1 e, em seguida, execute o trabalho de verificação de repositório em cada repositório no Core de destino. A conclusão deste trabalho tende a levar um bom tempo, com base no tamanho de seu repositório e no sistema de armazenamento subjacente. Para obter mais informações sobre este trabalho, consulte Sobre como verificar a integridade dos repositórios DVM. Para obter informações sobre como realizar este trabalho, consulte Executar uma verificação de integridade em um repositório DVM.

1. No menu Máquinas do Rapid Recovery Core Console, clique no nome da máquina que você quer modificar.

   A página **Resumo** da máquina selecionada será exibida.

2. Clique no menu **Definições**.

   A página **Definições** será exibida, mostrando os parâmetros de configuração da máquina selecionada.

3. Opcionalmente, clique no link **Trabalhos noturnos** para descer na página Definições e visualizar todas as definições de trabalhos noturnos.

4. Sob o título Trabalhos noturnos, clique em **Alterar**.

   A caixa de diálogo **Trabalhos noturnos** é exibida.

5. Para especificar os intervalos de tempo para retenção de dados de cópia de segurança, conforme necessário, selecione a opção **Rollup** e clique em **Definições**.

   A caixa de diálogo **Configuração** da política de retenção será exibida.

6. Se você estiver personalizando as definições de políticas de retenção para uma máquina replicada e receber uma notificação de cautela para realizar a Verificação de integridade em seu repositório, prossiga com esta etapa. Caso contrário, vá para a etapa 7.
   a. Se você está preparado para executar este trabalho, clique em **Verificar integridade**
   b. Clique em **Sim** para confirmar o trabalho de verificação de integridade.

> **NOTE:** A execução desse trabalho pode levar um bom tempo, com base no tamanho de seu repositório. Durante este tempo, você não poderá realizar nenhuma outra ação (Snapshots, replicação, exportação virtual e assim por diante) no repositório. Para obter mais informações sobre este trabalho, consulte Sobre como verificar a integridade dos repositórios DVM.

- Depois que o trabalho de verificação de repositório concluir todos os trabalhos filho com sucesso, retorne a este procedimento e siga para a próxima etapa.

7. Na caixa de diálogo **Configuração**, realize um dos procedimentos a seguir:
   - Para usar uma política de retenção padrão para esta máquina protegida, selecione **Usar a política de retenção padrão** e, em seguida, clique em **Salvar**. A política padrão será aplicada a essa máquina protegida.
   - Para definir uma política de retenção personalizada para este agente, selecione **Usar a política de retenção personalizada** e, em seguida, continue na próxima etapa.

   A caixa de diálogo **Configuração** expande-se para mostrar informações da política de retenção personalizada.
8. Insira a programação personalizada para reter pontos de recuperação, conforme descrito na tabela a seguir. A primeira configuração especifica o período de retenção principal para todos os pontos de recuperação salvos no repositório. Cada configuração adicional, quando ativada, fornece um nível de retenção mais granular, especificando os intervalos entre os quais pontos de recuperação devem passar por rollup. Essas configurações definem por quanto os pontos de recuperação são mantidos.

Tabela 150. Opções do Programa para política de retenção personalizada

Caixa de texto	Descrição
Manter todos os pontos de recuperação por n [período de retenção]...	Especifica o período de retenção principal para todos os pontos de recuperação salvos no repositório. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é 3 dias. Você pode selecionar dentre: Dias, Semanas, Meses e Anos
…e depois manter um ponto de recuperação por hora por n [período de retenção]	Se selecionada, essa configuração mantém um ponto de recuperação por hora pelo período que você especificar. O padrão é 2 dias. Você pode escolher entre dias, semanas, meses ou anos. Se você não quiser salvar pelo menos um ponto de recuperação por hora, desmarque essa opção.
…e depois manter um ponto de recuperação por dia por n [período de retenção]	Se selecionada, essa configuração mantém um ponto de recuperação por dia pelo período que você especificar. O padrão é 4 dias. Você pode escolher entre dias, semanas, meses ou anos. Se você não quiser salvar pelo menos um ponto de recuperação diariamente, desmarque essa opção.
…e depois manter um ponto de recuperação por semana por n [período de retenção]	Se selecionada, essa configuração mantém um ponto de recuperação por semana pelo período que você especificar. O padrão é 3 semanas. Você pode escolher entre semanas, meses e anos. Se você não quiser salvar pelo menos um ponto de recuperação semanalmente, desmarque essa opção.
…e depois manter um ponto de recuperação por mês por n [período de retenção]	Se selecionada, essa configuração mantém um ponto de recuperação por mês pelo período que você especificar. O padrão é 2 meses. Você pode escolher entre meses e anos.

Caixa de texto	Descrição
	Se você não quiser salvar pelo menos um ponto de recuperação mensalmente, desmarque essa opção.
…e depois manter um ponto de recuperação por ano por n [período de retenção]	Se selecionada, essa configuração mantém um ponto de recuperação por ano pelo número de anos que você especificar. O padrão (1 ano) é desativado por padrão. Se você quiser salvar pelo menos um ponto de recuperação anualmente, selecione essa opção e especifique um número de anos. Se você não quiser salvar pelo menos um ponto de recuperação anualmente, desmarque essa opção.

O seguinte é um exemplo de como o período de retenção é calculado.

Manter todos os pontos de recuperação por três dias.

... e, em seguida, manter um ponto de recuperação por hora por três dias

... e, em seguida, manter um ponto de recuperação por hora por quatro dias

... e, em seguida, manter um ponto de recuperação por semana por três semanas

... e, em seguida, manter um ponto de recuperação por mês por dois meses

... e, em seguida, manter um ponto de recuperação por mês por um ano

Neste exemplo, o ponto de recuperação mais antigo teria um ano e 3 meses.

9. Se vocêdeseja manter os pontos de recuperação no repositório DVM principal, ignore a etapa 11.
10. Se você quiser relocar pontos de recuperação do repositório DVM primário para um repositório de camadas secundárioarmazenado em uma solução de backup da série Quest DR, faça o seguinte:
    a. Selecione a opção **Relocate outdated recovery points to a tiering repository** (Relocar pontos de recuperação obsoletos para um repositório de camadas).
    b. Especifique a idade na qual você deseja relocar os pontos de recuperação do seu repositório principal para o repositório de camadas.

    Você pode especificar a idade em semanas, meses ou anos. O período mais curto que você pode definir é 1 semana.

    c. No menu suspenso **Select a repository** (Selecione um repositório), selecione o repositório de camadas para o qual você deseja relocar todos os pontos de recuperação da máquina especificada.

> **NOTE:** Independentemente de onde os pontos de recuperação estão localizados (um repositório DVM primário local ou um repositório de camadas secundário em uma solução de backup DR), eles ainda estão sujeitos à política de retenção, e ainda serão acumulados. Se você precisar manter pontos de recuperação mais antigos, um método consiste em arquivar. A outra abordagem é desativar o rollup ou ampliar o período de retenção das máquinas protegidas relevantes.

11. Clique em **Salvar**.

Forçar rollup para uma máquina protegida

Você pode ignorar a política de retenção programada, forçando o rollup dos pontos de recuperação no nível da máquina protegida.

1. No menu Máquinas protegidas do Rapid Recovery Core Console, clique no nome de uma máquina protegida específica.

A página **Resumo** da máquina de seleção é exibida.

2. Clique no menu suspenso **Mais** na parte superior da visualização da máquina protegida e selecione **Política de retenção**.

   A página **Política de retenção** referente à máquina especificada é exibida.

3. Clique em **Forçar rollup**.
4. Na caixa de diálogo, clique em **Sim** para confirmar.

   O Rapid Recovery inicia o rollup para esta máquina independentemente do programa da política de retenção.

Arquivamento

Esta seção fornece informações conceituais sobre arquivos do Rapid Recovery, incluindo casos de negócios para criá-los, opções de armazenamento e usos. Também descreve como criar arquivos de uso único ou um arquivos que são continuamente atualizados conforme uma programação. Os tópicos descrevem como pausar ou editar arquivos programados, como forçar ou verificar um arquivo e como conectar ou importar um arquivo.

Noções básicas sobre arquivos

O Rapid Recovery Core salva dados de instantâneo no repositório. Enquanto um repositório pode residir em diferentes tecnologias de armazenamento (como SAN, DAS ou NAS), o fator de desempenho mais crítico é a velocidade. Os repositórios usam mídias de curto período (rápidos e mais caros). Para impedir que um repositório seja enchido rapidamente, o Core impõe uma política de retenção, que com o passar do tempo acumula pontos de recuperação e, mais à frente, substitui-os por dados de backup mais recentes.

Se você precisa manter pontos de recuperação, se para significância histórica, conformidade legal, atender políticas de armazenamento de dados externo ou outros motivos, você pode criar um arquivo. Um arquivo é uma cópia de pontos de recuperação do seu repositório para as máquinas especificadas ao longo de um intervalo de datas que você designar. O arquivamento de um conjunto de pontos de recuperação não apaga os pontos de recuperação originais no seu repositório. Em vez disso, o arquivo congela a coleção de pontos de recuperação no momento em que o arquivo foi criado, como uma cópia separada em um local de armazenamento especificado. Diferentemente dos pontos de recuperação no seu repositório, os dados em um arquivo não estão sujeitos a rollup.

Você pode criar, importar e acrescentar arquivos a partir da opção  **Archive** (Arquivo) na barra de botões, ou na página **Archives** (Arquivos) acessível pelo ícone (Mais) no Core Console.

See also: Opções de criação e armazenamento de arquivo
See also: Opções de armazenamento e arquivamento da Amazon
See also: Opções de cadeia de pontos de recuperação para arquivos
See also: Métodos para acessar um arquivo
See also: Usos para arquivos
See also: Criar um arquivo

Opções de criação e armazenamento de arquivo

Você pode criar um arquivo único sob demanda a qualquer momento.

Você pode também definir os requisitos para arquivo agendado contínuo. Essa ação cria um arquivo de pontos de recuperação para as máquinas que você selecionar e no local que você designar. Pontos de recuperação adicionais para essas máquinas são então continuamente acrescentadas ao arquivo com uma programação (diariamente, semanalmente ou mensalmente) definida por você.

Ao criar um arquivo, você especifica onde quer salvá-lo. Você pode armazenar um arquivo em um sistema de arquivos (localmente ou em uma rede) ou em uma conta de armazenamento na nuvem.

NOTE: Antes de arquivar em uma conta na nuvem, você precisa adicionar primeiro as credenciais para a conta de armazenamento no seu Rapid Recovery Core. Para obter mais informações sobre como definir uma conta de nuvem no Core, consulte Adicionar uma conta de nuvem.

Se for armazenar o arquivo em uma conta de armazenamento na nuvem da Amazon, você deve definir a classe de armazenamento ao criar a conta. Para arquivar diretamente no Amazon Glacier, você pode especificar o armazenamento do Glacier quando definir o local no Assistente de arquivo. Para obter mais informações sobre as classes de armazenamento da Amazon, consulte Opções de armazenamento e arquivamento da Amazon.

- Os arquivos únicos são somente leitura. Ao criar um arquivo únicos, o local de destino que você especifica deve ficar vazio.
- Ao usar o arquivo programado, o Core acrescenta pontos de recuperação adicionais ao arquivo existente.
- Se a mídia de armazenamento que você selecionou ficar sem espaço, o Rapid Recovery pausa o trabalho de arquivo, permitindo que você especifique outro local. O seu arquivo é então dividido em segmentos, os quais podem residir em locais diferentes, conforme o espaço permitir.

See also: Adicionar uma conta de nuvem

Opções de armazenamento e arquivamento da Amazon

Ao arquivar dados em uma conta do Amazon Simple Storage Service (S3), você poderá escolher entre várias classes de armazenamento. Cada uma delas tem diferentes custos, benefícios e restrições de acesso associados. Os preços podem variar de acordo com a região. O Rapid Recoveryversão 6.2 estende o suporte das contas de armazenamento da Amazon para todas as classes de armazenamento. Isso é útil quando você planeja armazenar arquivos do Rapid Recovery na nuvem da Amazon.

Saber quais são as classes de armazenamento disponíveis e a diferença entre os prazos para acessar essas classes é fundamental para controlar os custos de armazenamento com eficiência e, ao mesmo tempo, poder acessar seus arquivos em períodos aceitáveis.

NOTE: O Quest fornece essas informações como cortesia para seus clientes do Rapid Recovery para chamar a atenção para os fatores de preços de armazenamento. Esses conceitos pode ajudá-lo a planejar e definir o orçamento de acordo. Você é responsável por todos os custos de armazenamento na Amazon ou por qualquer outro provedor de serviços na nuvem. Como a Amazon pode alterar pré-requisitos, requisitos, custos, definições da camada de armazenamento e assim por diante, use o site da Amazon como a fonte principal e autoritativa dessas informações.

Em geral, a Amazon atualmente oferece as classes de armazenamento a seguir.

Padrão. Essa classe de armazenamento é para os dados que você planeja acessar com frequência ou acessar rapidamente. Essa classe é a opção de armazenamento padrão de todos os assistentes, janelas e caixas de diálogo do Rapid Recovery. Não há taxa adicional para recuperar informações na classe de armazenamento padrão.

Acesso infrequente padrão (IA). Essa classe de armazenamento é mais econômica que a padrão, destinada a dados que você não pretende acessar frequentemente. Há uma taxa de recuperação associada ao acesso dos dados na classe de armazenamento. No entanto, a disponibilidade é imediata. A Amazon cobra taxas por objetos excluídos do armazenamento do acesso infrequente antes de 30 dias.

Glacier. Essa classe de armazenamento é para armazenamento de longo prazo de dados que não requerem acesso em tempo real. É mais econômica para armazenamento de longo prazo de dados que raramente são recuperados. Há uma taxa de recuperação associada ao acesso dos dados nessa classe de armazenamento. A Amazon cobra taxas por objetos excluídos do Glacier antes de 90 dias. A recuperação dos dados armazenados no Glacier não é imediata. Os tempos de recuperação padrão exigem de 3 a 5 horas; a recuperação em massa para grandes quantidades de dados pode demorar até 12 horas. As recuperações urgentes podem demorar até 5 minutos. Taxas são cobradas para cada opção de recuperação.

NOTE: Diferentemente das outras classes de armazenamento da Amazon, o Rapid Recovery não suporta a criação de uma conta de nuvem que seja específica da classe Glacier. Para arquivar dados na classe Glacier, escolha uma conta de nuvem da Amazon e selecione a opção **Use Glacier storage** (Usar armazenamento Glacier) na página **Location** (Local) do assistente de arquivamento.

Armazenamento de redundância reduzida (RRS). Essa categoria é uma classe de armazenamento de baixo custo projetada para dados reprodutíveis não críticos com menos redundância que a classe de armazenamento padrão. Há uma taxa de recuperação mínima associada ao acesso dos dados nessa classe de armazenamento. Espera-se que uma porcentagem fracionada (a Amazon cita em torno de 0,01%) dos objetos armazenados nessa classe seja irrecuperável.

Para obter as informações mais recentes, consulte sempre os materiais no site da Amazon.

Em geral, as seguintes diretrizes se aplicam:

- Se você espera restaurar dados regularmente de um arquivo do Rapid Recovery, a classe Padrão é provavelmente a melhor opção.
- De uma perspectiva de custo, se você pretende restaurar dados ocasionalmente, considere o Acesso infrequente padrão.
- A classe Glacier destina-se ao armazenamento a frio de pontos de recuperação arquivados dos quais você raramente espera restaurar dados. Um bom exemplo de quando usar o armazenamento Glacier é salvar os dados para conformidade com normas. O armazenamento Glacier está disponível como uma opção do assistente de arquivamento.
- Para armazenamento de dados reprodutíveis não críticos, considere a opção RRS.

Opções de cadeia de pontos de recuperação para arquivos

Antes de criar o seu arquivo, você deve decidir a abordagem adequada para cadeias de pontos de recuperação. Use as informações a seguir para determinar que opção selecionar na página **Opções** do Assistente de arquivo.

- **Criar cadeias completas de pontos de recuperação, incluindo imagens base referenciadas fora do intervalo de datas.** Se você selecionar a opção para criar cadeias completas de pontos de recuperação, você pode executar a gama completa de ações de restauração para qualquer ponto de recuperação no arquivo. Essa opção inclui a restauração no nível do arquivo, no nível do volume e bare metal restore. Quando você seleciona essa opção, as cadeiras inteiras de pontos de recuperação são salvas com o seu arquivo. Você pode restaurar dados mesmo se a imagem base correspondente ao ponto de recuperação selecionado for anterior ao intervalo de datas do seu arquivo. No entanto, o tamanho do arquivo deste arquivo é maior, para garantir que você tenha acesso aos dados na cadeia inteira de pontos de recuperação.
- **Incluir apenas os pontos de recuperação no intervalo de datas. Essa opção economiza espaço, mas você é o responsável pelo arquivamento de todas as imagens base necessárias.** Se você incluir apenas os pontos de recuperação no intervalo de datas especificado no seu arquivo, o tamanho do arquivo do arquivo é menor. Para os dados em que a imagem base está incluída no intervalo de datas especificado, você tem acesso à gama completa de opções de restauração. No entanto, se você quiser recuperar dados capturados em uma imagem base de uma data anterior ao intervalo de datas especificado, você pode ficar limitado à recuperação em nível de arquivo apenas. Dados fora do intervalo do arquivo morto são órfãos.

Para obter mais informações sobre cadeias de pontos de recuperação, consulte o tópico Cadeias de pontos de recuperação e órfãos.

Conceitos relacionados

See also: Cadeias de pontos de recuperação e órfãos

Tarefas relacionadas

See also: Criar um arquivo
See also: Editar um arquivo programado

Métodos para acessar um arquivo

Quando você precisa acessar os dados em um ponto de recuperação arquivado, você tem duas opções.

- Para os arquivos criados com o Rapid Recovery versão 6.0.1 e posteriores, você pode anexar o arquivo. O arquivo acrescentado é mostrado no menu de navegação à esquerda do Core Console. Você poderá procurar os pontos de recuperação no arquivo e tomar as mesmas ações sobre esses dados como com quaisquer outros pontos de recuperação atualmente no seu repositório, sem importar esses dados para o seu repositório.
- Você pode importar um arquivo, restaurando esses pontos de recuperação para o seu repositório. Em seguida, você pode realizar as mesmas ações sobre esses dados como com quaisquer outros pontos de recuperação atualmente em seu Core. O Rapid Recovery Core é compatível com versões anteriores, com suporte para importação de arquivos de todas as versões AppAssure e Rapid Recovery.

CAUTION: Como o Core reconhece as datas originais dos pontos de recuperação em um arquivo, os pontos de recuperação importados de um arquivo podem ser acumulados ou excluídos durante o próximo período de trabalho noturno, se sua idade exceder o período de retenção. Se quiser reter pontos de recuperação mais antigos importados de um arquivo, você pode desativar o rollup ou estender o período de retenção para as máquinas protegidas relevantes.

Quando precisar ter acesso aos dados em um ponto de recuperação arquivado, você poderá posteriormente anexar (para Rapid Recovery 6.x e posterior) ou importar o arquivo, restaurando esses pontos de recuperação em seu repositório.

Tarefas relacionadas

See also: Anexar um arquivo
See also: Importação de um arquivo

Usos para arquivos

Quando um arquivo é criado, ele pode ser usado das seguintes maneiras:

- Um arquivo pode ser usado para mover dados entre repositórios.
- Um arquivo pode ser anexado ao Core Console e montado como um sistema de arquivos para recuperação de arquivos simples ou pastas. Algumas restrições são cabíveis.
- Um arquivo pode ser importado para um repositório. Se quaisquer pontos de recuperação no arquivo já tiverem passado por rollup ou excluídos do repositório, essa ação os restaurará.
- Um arquivo pode ser usado como fonte para uma bare metal restore ou para exportar para uma máquina virtual.

Criar um arquivo

Você pode usar esse procedimento para criar um arquivo único ou um arquivamento programado.

Se você planeja criar um arquivo em um local da nuvem, adicione primeiro sua conta de nuvem ao Rapid Recovery Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.

Um arquivo único é um arquivo criado sob demanda para uma máquina específica. Um arquivo programado é um arquivo que reaparece automaticamente na data e na hora especificadas no assistente. Ao agendar um arquivamento recorrente, você atende à necessidade de arquivamento frequente de dados de máquinas protegidas sem a inconveniência de definir repetidamente de um arquivo único.

Ao criar o seu arquivo, você precisa decidir incluir uma cadeia inteira de pontos de recuperação no seu arquivo. Para obter mais informações, consulte Opções de cadeia de pontos de recuperação para arquivos.

1. Na barra de botões do Rapid Recovery Core Console, clique em **Arquivar**.

   O assistente de arquivo é aberto.
2. Na página **Tipo de arquivo** do assistente, selecione uma das opções a seguir:
   - Arquivo único
   - Arquivo contínuo (por programa)
3. Clique em **Avançar**.
4. Na página **Local**, selecione uma opção na lista suspensa **Tipo de local** e insira as informações conforme descritas na seguinte tabela.

Tabela 151. Opções de tipo de local de arquivo

Opção	Caixa de texto	Descrição
Local	Local	Insira o caminho do local onde você deseja que o arquivo resida, por exemplo, `d:\work\archive`.
Rede	Local	Insira o caminho do local onde você deseja que o arquivo resida, por exemplo, `\\servername\sharename`.
	Nome de usuário	Insira o nome de usuário referente ao usuário que tem acesso ao compartilhamento de rede.
	Senha	Insira a senha do usuário que tem acesso ao compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTE:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados serão salvos.
	Usar armazenamento Glacier	Para armazenar o arquivo no armazenamento Amazon Glacier, selecione esta opção. Esta opção destina-se ao armazenamento de longo prazo dos arquivos.

Opção	Caixa de texto	Descrição
		Para obter mais informações, consulte Opções de armazenamento e arquivamento da Amazon.

5. Clique em **Avançar**.
6. Na página **Máquinas** do assistente, selecione a(s) máquina(s) protegida(s) que você desejar arquivar e, em seguida, clique em **Avançar**.
7. Execute um dos seguintes:
   - Se você optar pela criação de um arquivo único, pule para a Etapa 14.
   - Se você optar pela criação de um arquivamento programado, pule para a Etapa 8
8. Na página **Programa**, selecione uma das seguintes opções na lista suspensa **Enviar dados**:
   - Diariamente
   - Semanalmente
   - Mensalmente
9. Insira as informações descritas na tabela a seguir dependendo de sua seleção da Etapa 8.

Tabela 152. Enviar as opções de dados

Opção	Caixa de texto	Descrição
Diariamente	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.
Semanalmente	No dia de semana	Selecione um dia da semana no qual deseja criar automaticamente o arquivo.
	Na hora	Selecione a hora do dia na qual você deseja criar um arquivo.
Mensalmente	No dia do mês	Selecione o dia do mês no qual deseja criar automaticamente o arquivo.
	Na hora	Selecione a hora do dia na qual você deseja criar um arquivo.

10. Opcionalmente, se você não quiser que o trabalho de arquivo seja iniciado na próxima hora programada depois de concluir o assistente, selecione **Pausar o arquivamento inicial**.

> **NOTE:** Talvez você deseje pausar o arquivo agendado se precisar de tempo para preparar o local de destino antes de arquivar os resumos. Se você não selecionar essa opção, o arquivamento começa no horário agendado.

11. Clique em **Avançar**.
12. Na página **Opções** de um arquivo contínuo, selecione uma das ações de reciclagem descritas na seguinte tabela.

Tabela 153. Opções de reciclagem de arquivo contínuo

Caixa de texto	Descrição
Substitua esse core	Substitui quaisquer dados arquivados preexistentes pertencentes a este Core, porém deixa os dados de outros Cores intactos.
Apagar completamente	Apaga todos os dados arquivados do diretório antes de gravar o novo arquivo.

Caixa de texto	Descrição
Incremental	Permite que você adicione pontos de recuperação a um arquivo existente. Compara pontos de recuperação para evitar duplicação de dados que existem no arquivo.

13. Na página **Opções** de um arquivo contínuo, determine se deseja incluir cadeias de pontos de recuperação inteiras no seu arquivo. Para obter mais informações sobre as opções de cadeias de pontos de recuperação, consulte Opções de cadeia de pontos de recuperação para arquivos. Execute um dos seguintes:
    - Selecione **Criar cadeias completas de pontos de recuperação, incluindo imagens base referenciadas fora do intervalo de datas** e, em seguida, vá para a Etapa 17.
    - **Selecione Incluir apenas os pontos de recuperação no intervalo de datas. Essa opção economiza espaço, mas você é o responsável por arquivar quaisquer imagens base necessárias** e, em seguida, vá para a Etapa 17.
14. Na página **Opções** de um arquivo único, insira as informações descritas na seguinte tabela.

Tabela 154. Opções de arquivo único

Caixa de texto	Descrição
Tamanho máximo	Grandes arquivos de dados podem ser divididos em vários segmentos. Selecione a quantidade máxima de espaço que você deseja reservar para criar o arquivo efetuando uma das seguintes ações: • Selecione **Destino inteiro** para reservar todo o espaço disponível no caminho fornecido para o destino fornecido na Etapa 4. (Por exemplo, se o local for `D:\work\archive`, todo o espaço disponível na unidade D: será reservado). • Selecione a caixa de texto, insira a quantidade de espaço e depois selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar. **NOTE:** Os arquivos na nuvem Amazon são automaticamente divididos em segmentos de 50 GB. Os arquivos da nuvem Microsoft Azure são automaticamente divididos em segmentos de 200 GB.
Reciclar ação	Selecione uma das seguintes opções de ação de reciclagem: • **Não reutilizar.** Não substitui ou apaga nenhum dado arquivado existente no local. Se o local não estiver vazio, o Rapid Recovery permitirá a seleção de um local diferente. • **Substituir este Core.** Substitui quaisquer dados arquivados preexistentes pertencentes a este Core, porém deixa os dados de outros Cores intactos. • **Apagar completamente.** Apaga todos os dados arquivados do diretório antes de gravar o novo arquivo. • **Incremental.** Permite que você adicione pontos de recuperação a um arquivo existente. Compara pontos de recuperação para evitar duplicação de dados que já existem no arquivo.
Comentários	Insira qualquer informação adicional necessária para o arquivo. O comentário é exibido se você importar o arquivo mais tarde.
Criar cadeias completas de pontos de recuperação, incluindo	Selecione essa opção para arquivar toda a cadeia de pontos de recuperação. Essa opção é selecionada por padrão.

Caixa de texto	Descrição
imagens base referenciadas fora do intervalo de datas.	
Incluir apenas os pontos de recuperação no intervalo de datas. Essa opção economiza espaço, mas você é o responsável pelo arquivamento de todas as imagens base necessárias.	Selecione esta opção para arquivar apenas os pontos de recuperação incrementais sem imagens base. **NOTE:** Esta opção resulta em um arquivo de pontos de recuperação órfãos. Você não conseguirá usá-los para recuperação até que você arquive também suas imagens base relacionadas. Para obter mais informações sobre as opções de cadeias de pontos de recuperação, consulte Opções de cadeia de pontos de recuperação para arquivos.

15. Se você tiver selecionado a opção para incluir somente pontos de recuperação no intervalo de datas, clique em **Avançar**. Caso contrário, clique em **Concluir**.
16. Na página **Período**, insira manualmente a data inicial e a data final dos pontos de recuperação a serem arquivados ou selecione a data/hora clicando no ícone de calendário e, depois, no ícone abaixo da janela do calendário.
17. Clique em **Concluir**.

    O assistente é fechado.

Arquivar na nuvem

Quando os dados atingirem o final de um período de retenção, você pode desejar ampliar essa retenção criando um arquivo dos dados antigos. Quando você arquiva dados, há sempre uma dúvida de onde armazená-los. O Rapid Recovery permite carregar o arquivo em uma variedade de provedores de nuvem diretamente do Core Console. As nuvens compatíveis incluem Microsoft Azure, Amazon S3, qualquer provedor baseado em OpenStack, Rackspace Cloud Files e Google Cloud.

Exportar um arquivo a uma nuvem utilizando o Rapid Recovery envolve os seguintes procedimentos:

- Adicionar sua conta de nuvem ao Rapid Recovery Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
- Arquive seus dados e exporte-os para sua conta em nuvem. Para obter mais informações, consulte Criar um arquivo.
- Recuperar dados arquivados anexando um arquivo ou importando-o do local da nuvem. Para obter mais informações, consulte Anexar um arquivo ou Importação de um arquivo, respectivamente.

Editar um arquivo programado

O Rapid Recovery permite que você altere os detalhes de um arquivo programado. Para editar um arquivo agendado, execute as etapas do procedimento a seguir.

1. No Rapid Recovery Core Console, clique no menu suspenso **Mais** na barra de ícones e, em seguida, selecione **Arquivos**.
2. Na página **Arquivos**, sob Arquivos programados, clique no menu suspenso ao lado do arquivo que você deseja alterar, e depois clique em **Editar**.

   O **assistente de arquivo** é aberto.
3. Na página **Local** do Assistente de arquivo, selecione uma das seguintes opções a partir na lista suspensa **Tipo de local**:
   - Local
   - Rede
   - Nuvem
4. Digite os detalhes para o arquivamento conforme descrito na tabela a seguir com base no tipo de local selecionado na Etapa 3.

Tabela 155. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Local	Local	Insira o caminho do local onde você deseja que o arquivo resida, por exemplo, `d:\work\archive`.
Rede	Local	Insira o caminho do local onde você deseja que o arquivo resida, por exemplo, `\\servername\sharename`.
	Nome de usuário	Insira o nome de usuário referente ao usuário que tem acesso ao compartilhamento de rede.
	Senha	Insira a senha do usuário que tem acesso ao compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTE:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados serão salvos.
	Usar armazenamento Glacier	Para armazenar o arquivo no armazenamento Amazon Glacier, selecione esta opção. Esta opção destina-se ao armazenamento de longo prazo dos arquivos.

Opção	Caixa de texto	Descrição
		Para obter mais informações, consulte Opções de armazenamento e arquivamento da Amazon.

5. Clique em **Avançar**.
6. Na página **Máquinas** do assistente, selecione quais máquinas protegidas ou máquinas que contêm os pontos de recuperação que você deseja arquivar. Limpar as máquinas que você não quer arquivar.
7. Clique em **Avançar**.
8. Na página **Programa**, selecione uma das seguintes opções na lista suspensa **Enviar dados**:
   - Diariamente
   - Semanalmente
   - Mensalmente
9. Insira as informações descritas na tabela a seguir dependendo de sua seleção da Etapa 8.

Tabela 156. Enviar as opções de dados

Opção	Caixa de texto	Descrição
Diariamente	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.
Semanalmente	No dia de semana	Selecione um dia da semana no qual deseja criar automaticamente o arquivo.
	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.
Mensalmente	No dia do mês	Selecione o dia do mês no qual deseja criar automaticamente o arquivo.
	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.

10. Opcionalmente, para adiar o arquivamento e retomar posteriormente, selecione **Pausar o arquivamento inicial**.

> **NOTE:** Talvez você deseje pausar o arquivo agendado se precisar de tempo para preparar o local de destino antes de arquivar os resumos. Se você não selecionar essa opção, o arquivamento começa no horário agendado.

11. Clique em **Avançar**.
12. Na página **Opções**, use a lista suspensa **Reciclar ação** para selecionar uma das opções descritas na tabela a seguir:

Tabela 157. Opções de reciclagem de arquivo

Caixa de texto	Descrição
Incremental	Permite que você adicione pontos de recuperação a um arquivo existente. Compara pontos de recuperação para evitar duplicação de dados que já existem no arquivo.
Substitua esse core	Substitui quaisquer dados arquivados preexistentes pertencentes a este core, porém deixa os dados de outros cores intactos.

Caixa de texto	Descrição
Apagar completamente	Apaga todos os dados arquivados do diretório antes de gravar o novo arquivo.

13. Na página **Opções** do assistente, determine se deseja incluir cadeias de pontos de recuperação inteiras no seu arquivo. Para obter mais informações sobre as opções de cadeias de pontos de recuperação, consulte Opções de cadeia de pontos de recuperação para arquivos. Execute um dos seguintes:
    - Selecione **Criar cadeias completas de pontos de recuperação, incluindo imagens base referenciadas fora do intervalo de datas**.
    - **Selecione Incluir apenas os pontos de recuperação no intervalo de datas. Essa opção economiza espaço, mas você é o responsável pelo arquivamento de todas as imagens base necessárias**.
14. Clique em **Concluir**.

    O Rapid Recovery aplica-se às suas alterações no arquivo.

Pausar ou retomar um arquivo programado

Se você já tiver um trabalho de arquivamento programado, você pode pausar ou retomar esta ação, conforme necessário.

Pode haver vezes que deseje pausar um trabalho de arquivamento programado, como quando precisar alterar o local do arquivo de destino. Se você optou anteriormente por pausar o arquivamento, ao executar o procedimento Criar um arquivo, você pode retomar o arquivamento programado mais tarde. Execute as etapas do procedimento a seguir para pausar ou retomar o arquivo agendado.

1. No Rapid Recovery Core Console, clique no menu **Mais** na barra de ícones e, em seguida, selecione **Arquivos**.
2. Na página **Arquivos**, sob Arquivos programados, realize um dos procedimentos a seguir:
    - Selecione o arquivo de preferência, e depois clique em uma das seguintes ações disponíveis:
        - Pausar
        - Retomar
    - Ao lado do arquivo de preferência, clique no menu suspenso e em uma das seguintes ações disponíveis, conforme adequado:
        - Pausar
        - Retomar

    O status do arquivo é exibido na coluna Programar.

Forçar um trabalho de arquivo

Usando esse procedimento, você pode forçar o Rapid Recovery a realizar um trabalho de arquivo programado a qualquer momento.

Para forçar um trabalho de arquivo, você precisa ter um arquivo programado no Core.

1. No Rapid Recovery Core Console, na barra de ícones, clique no menu **Mais** na barra de ícones e, em seguida, selecione **Arquivos**.
2. Na página Arquivos, em Arquivos programados, clique no menu suspenso ao lado do arquivo que deseja forçar e clique em **Forçar**.

   O Rapid Recovery arquiva os pontos de recuperação de acordo com as configurações que você escolher para o arquivo, independentemente da hora definida para o arquivo programado.

Verificar um arquivo

A verificação de um arquivo verifica se um arquivo e seu conteúdo estão suficientemente íntegros para recuperação.

Você pode examinar um arquivo quanto à integridade de sua estrutura, dos segmentos de dados e dos arquivos do índice pela realização de uma verificação de arquivo. A verificação de arquivo verifica a presença de todos os arquivos necessários dentro do arquivo e a integridade dos arquivos. Para realizar uma verificação do arquivo, execute as etapas do procedimento a seguir.

1. No Rapid Recovery Core Console, na barra de ícones, clique no menu **Mais** na barra de ícones e, em seguida, selecione **Arquivos**.
2. Na página **Arquivos**, clique em **Verificar**.

   A caixa de diálogo **Check Archive** (Verificar arquivamento) é exibida.
3. Para **Tipo de local**, selecione uma das seguintes opções a partir da lista suspensa:
   - Local
   - Rede
   - Nuvem
4. Com base no tipo de local selecionado na Etapa 3, insira os detalhes do arquivo, conforme descrito na seguinte tabela.

Tabela 158. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Local	Local	Insira o caminho local para o arquivo.
Rede	Local	Insira o caminho de rede para o arquivo.
	Nome de usuário	Insira o nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira a senha para o caminho da rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTE:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.

Opção	Caixa de texto	Descrição
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Selecione a pasta na qual os dados arquivos estão salvos; por exemplo, Rapid Recovery-7-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

5. Marque ou desmarque as verificações descritas na seguinte tabela. Por padrão, todas as opções são selecionadas.

   NOTE: Não desmarque todas as verificações. Você deve selecionar pelo menos uma opção.

Opção	Descrição
Offsets de mapeamento de arquivos de índice	Essa opção verifica se todos os dados na estrutura interna do arquivo estão no local correto.
Integridade da estrutura	Essa opção verifica a presença de determinados arquivos internos e a estrutura da pasta do arquivo. Se algum arquivo ou pasta estiver ausente, a verificação apresentará falha.
Integridade da soma de verificação	Essa opção verifica a integridade dos segmentos de dados no arquivo para garantir a integridade dos segmentos.

6. Clique em **Verificar arquivo**.

   O Rapid Recovery verifica o arquivo de acordo com suas seleções.

Anexar um arquivo

Anexar um arquivo permite ver os pontos de recuperação do arquivo.

Você deve ter um arquivo preexistente criado no Rapid Recovery Core 6.0.1 ou posterior para concluir esse procedimento. Para obter mais informações, consulte Criar um arquivo.

Quando você anexa um arquivo, o nome do arquivo fornecido aparece como um menu do arquivo no menu de navegação à esquerda do Core Console. Cada máquina protegida com pontos de recuperação do arquivo é listada separadamente abaixo do menu do arquivo. Você pode clicar em qualquer nome da máquina no arquivo e navegar em seus pontos de recuperação. Você pode também realizar as mesmas ações como quaisquer outros pontos de recuperação visíveis no seu Core.

Anexar o arquivo também armazena em cache as credenciais para acessar as informações. Até que você exclua a definição do arquivo anexado, pode facilmente reanexar e destacar o arquivo, tornando seus pontos de recuperação facilmente acessíveis.

Use esse procedimento para anexar um arquivo.

1. No Rapid Recovery Core Console Core Console, clique no menu **Archive** (Arquivo) e, em seguida, selecione **Attach Archive** (Anexar arquivo).

   A caixa de diálogo **Anexar arquivo** é exibida.

2. Na caixa de texto **Nome**, insira um nome para este arquivo anexado.

   O valor que você digita neste campo é mostrado no menu de navegação à esquerda como o nome do menu do arquivo.

Segundo as melhores práticas de nomes de exibição, o nome do arquivo deve conter entre 1 e 64 caracteres alfanuméricos, incluindo espaços. Não use caracteres proibidos ou frases proibidas.

3. Na lista suspensa **Tipo de local**, selecione o tipo de local do arquivo entre as seguintes opções:
   - Local
   - Rede
   - Nuvem
4. Digite os detalhes para o arquivamento conforme descrito na tabela a seguir com base no tipo de local selecionado na Etapa 3.

Tabela 159. Detalhes do tipo do local

Opção	Caixa de texto	Descrição
Local	Local	Digite o caminho para o arquivo; por exemplo, `D:\Work\Archive`.
Rede	Local	Digite o caminho para o arquivo; por exemplo, `\\servername\sharename`.
	Nome de usuário	Insira o nome de usuário para o login no compartilhamento de rede.
	Senha	Insira a senha para o login no compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTE:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
	Contêiner	Selecione o contêiner do arquivo associado à sua conta no menu suspenso.
	Nome da pasta	Insira o nome da pasta dos dados arquivados; por exemplo, Rapid-Recovery-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

5. Clique em **Anexar**.

   O arquivo é anexado a este Core e monta o conteúdo como um sistema de arquivos.

Importação de um arquivo

Você pode usar esse procedimento para importar um arquivo uma vez ou programar um arquivo para ser importado em uma base recorrente.

Quando desejar recuperar dados arquivados, você poderá importar o arquivo inteiro para um local especificado.

CAUTION: Execute essa etapa somente após consideração cuidadosa. A importação de um arquivo preenche novamente o repositório com o conteúdo do arquivo, substituindo quaisquer dados novos no repositório desde a captura do arquivo.

Para importar um arquivo, execute as etapas do procedimento a seguir.

1. Na barra do menu do Rapid Recovery Core Console, clique no menu suspenso **Arquivar** e selecione **Importar arquivo**.

O **Assistente de importação de arquivo** é aberto.

2. Na página **Tipo de importação** do assiste selecione uma das opções a seguir:
   - Importação única
   - Importação contínua (por programa)
3. Clique em **Avançar**.
4. Na página **Local**, selecione o local do arquivo que deseja importar na lista suspensa e insira as informações conforme descritas na seguinte tabela:

Tabela 160. Opções de tipo de local de arquivo importado

Opção	Caixa de texto	Descrição
Local	Local	Insira o caminho do local onde você deseja que o arquivo resida, por exemplo, `d:\work\archive`.
Rede	Local	Insira o caminho de rede onde você deseja que o arquivo resida, por exemplo, `\\servername\sharename`.
	Nome de usuário	Insira o nome de usuário referente ao usuário que tem acesso ao compartilhamento de rede.
	Senha	Insira a senha do usuário que tem acesso ao compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTE:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados serão salvos.

5. Clique em **Avançar**.
6. Na página **Informações do arquivo**, se desejar importar cada máquina incluída no arquivo, selecione **Importar todas as máquinas**.
7. Siga uma das opções a seguir com base na sua seleção:
   - Se você tiver selecionado **Importação única** na etapa 2, selecionado **Importar todas as máquinas** na etapa 6 e todas as máquinas estiverem presentes no Core—como máquinas somente protegidas, replicadas ou de pontos de recuperação— vá para a etapa 12.
   - Se você tiver selecionado **Importação contínua (por programa)** na etapa 2, selecionado **Importar todas as máquinas** na etapa 6 e pelo menos uma máquina não estiver presente no Core—como máquinas somente protegidas, replicadas ou de pontos de recuperação—clique em **Avançar** e vá para a etapa 9.
   - Se você não tiver importado todas as máquinas na etapa 6, clique em **Avançar** e avance para a etapa 8.
8. Na página **Máquinas**, selecione as máquinas que deseja importar do arquivo.
   - Se você tiver selecionado **Importação única** na etapa 2 e pelo menos uma máquina não estiver presente no Core—como máquinas somente protegidas, replicadas ou de pontos de recuperação—

utilize as listas suspensas para selecionar um repositório para cada máquina que deseja importar e vá para a etapa 12.

- Se todas as máquinas já estiverem presentes no Core—como máquinas somente protegidas, replicadas ou de pontos de recuperação—vá para a etapa 12.

9. Clique em **Avançar**.
10. Na página **Repositório**, siga uma das seguintes opções:
    - Se um repositório estiver associado ao Core, selecione uma das opções na seguinte tabela.

Tabela 161. Opções de repositório

Opção	Descrição
Utilize um repositório existente	Selecione um repositório atualmente associado a esse Core na lista suspensa.
Criar um repositório	Na caixa de texto do servidor, insira o nome do servidor no qual deseja salvar o novo repositório—por exemplo, servername ou localhost—e consulte Criar um repositório de DVM.

    - Se nenhum repositório estiver associado ao Core, insira o nome do servidor no qual deseja salvar o novo repositório—por exemplo, servername ou localhost—e consulte Criar um repositório de DVM.

11. Se você tiver optado por **Importação contínua (por programa)** na etapa 2, na página **Programa**, selecione as opções descritas na seguinte tabela.

Tabela 162. Opções de programação de importação

Opção	Descrição
Diariamente	Clique no ícone de relógio e utilize as setas para cima e para baixo para selecionar a hora de início do trabalho de arquivo. Se estiver utilizando um sistema de 12 horas, clique no botão AM ou PM para especificar o período do dia.
Semanalmente	Selecione o dia da semana e a hora de início do trabalho de arquivo. Se estiver utilizando um sistema de 12 horas, clique no botão AM ou PM para especificar o período do dia.
Mensalmente	Selecione o dia do mês e a hora de início do trabalho de arquivo. Se estiver utilizando um sistema de 12 horas, clique no botão AM ou PM para especificar o período do dia.
Pausar a importação inicial	Selecione essa opção se não desejar que o trabalho de importação seja iniciado na próxima hora programada depois de concluir o assistente. **NOTE:** Você pode desejar pausar a importação programada se precisar de tempo para preparar o local de destino antes de importar os resumos. Se você não selecionar essa opção, a importação será iniciada na hora programada.

12. Clique em **Concluir**.

Contas de nuvem

O Rapid Recovery Core permite definir conexões entre os provedores de serviços de nuvem e armazenamento em nuvem e o Rapid Recovery. Os serviços de nuvem compatíveis incluem Microsoft Azure, Amazon Web Services (AWS), qualquer provedor baseado em OpenStack (incluindo o Rackspace) e Google Cloud. As plataformas específicas do governo dos EUA incluem AWS GovCloud (US) e Azure Government. Você pode adicionar qualquer número da contas de nuvem ao Core Console, incluindo diversas contas do mesmo provedor.

A finalidade da adição de contas de nuvem ao Core Console é trabalhar com elas como descrito no tópico Sobre contas de nuvem.

Depois de adicionadas, você pode gerenciar a conexão entre o Core e as contas de nuvem. Especificamente, você pode editar o nome de exibição ou as informações de credenciais, configurar as opções de conexão da conta ou remover a conta do Rapid Recovery. Quando você editar ou remover contas de nuvem no Core Console, não altere as contas de nuvem em si, apenas a vinculação entre essas contas e sua capacidade de acessá-las no Core Console.

Esta seção descreve como definir links entre contas existentes de provedores de armazenamento na nuvem ou de provedores de serviços de nuvem e o Rapid Recovery Core Console. Também descreve como gerenciar essas contas de nuvem no Rapid Recovery.

Os tópicos são:

- Sobre contas de nuvem
- Considerando opções de armazenamento na nuvem
- Adicionar uma conta de nuvem
- Editar uma conta de nuvem
- Remover uma conta de nuvem

Sobre contas de nuvem

O Rapid Recovery funciona com contas de nuvem destas formas:

- **Arquivo**. Você pode armazenar um arquivo único ou um arquivo agendado contínuo na nuvem. Esse recurso é suportado por todos os tipos de conta de nuvem com suporte. Quando você arquivar na nuvem, poderá acessar posteriormente as informações nos pontos de recuperação arquivados, anexando o arquivo (para arquivos criados na versão 6.0.1 ou posterior). Para todos os arquivos, também é possível importar o arquivo. Você também pode executar uma bare metal restore de um arquivo.
- **Exportação virtual.** Você pode executar uma exportação virtual para uma conta de nuvem do Azure. Isso inclui uma exportação única de uma máquina virtual ou uma exportação contínua para uma VM de standby virtual.

Para obter informações conceituais sobre as várias contas de nuvem, consulte Considerando opções de armazenamento na nuvem.

Para obter informações sobre como configurar as definições de tempo limite entre o Core e as contas de nuvem, consulte Configurar as definições de conexão da conta de nuvem.

Para obter informações sobre como executar uma exportação virtual para a nuvem do Azure, consulte Exportar dados para uma máquina virtual Azure.

Considerando opções de armazenamento na nuvem

Este tópico aborda o suporte para contas de armazenamento na nuvem do Governo dos EUA. Também fala sobre as vantagens e desvantagens entre o custo e outros fatores na escolha de contas de nuvem para arquivamento.

Contas de nuvem seguras para o Governo dos EUA

Os órgãos governamentais federais, estaduais e locais dos Estados Unidos e seus parceiros têm acesso a mais opções de conta de nuvem. O Rapid Recovery suporta as seguintes ofertas para o Governo e contas de nuvem relacionadas:

- **AWS GovCloud (US).**O Amazon Web Services oferece um serviço chamado AWS GovCloud (US). Essa é uma região isolada do AWS projetada para atender aos requisitos específicos de conformidade e normas. Usar esse serviço permite que agências governamentais e clientes dos Estados Unidos juntem-se às empresas privadas que estão aproveitando as vantagens das contas de nuvem. o Rapid Recovery suporta o arquivamento em contas de armazenamento do Amazon S3 no AWS GovCloud.
- **Azure Government.** Azure Government é plataforma de nuvem exclusivamente para as agências governamentais federais, estaduais, locais e tribais dos Estados Unidos e seus parceiros. O Rapid Recovery suporta o Azure Government da mesma forma que oferecemos suporte padrão do Azure. Por exemplo:
  - O Rapid Recovery suporta o arquivamento em contas de armazenamento do Azure Government e do Azure padrão.
  - O Rapid Recovery suporta a exportação virtual para uma máquina virtual Azure (uma única vez ou standby virtual) em plataformas públicas e do Azure Government.
  - O Rapid Recovery suporta a replicação em Cores locais para um destino de replicação na plataforma de nuvem pública ou do Azure Government. Para qualquer uma das plataformas, quando estiver conectado ao Azure Marketplace, você poderá selecionar o “Destino de replicação do Rapid Recovery” no marketplace do Azure Government. Usando essa VM, os serviços de computação do Azure e o armazenamento que você adiciona à VM para seu repositório, os usuários podem definir de forma rápida e fácil um Core de destino que replica seus dados de backup locais na nuvem do Azure Government.

Equilíbrio entre tempo de acesso, custo e conveniência do arquivamento em contas de nuvem

Para oferecer aos nossos usuários opções econômicas de arquivamento na nuvem e exportação virtual, o Rapid Recovery continua a expandir o suporte dos provedores de armazenamento na nuvem (e as classes de armazenamento para os provedores líderes que as oferecem). Os usuários instruídos podem aproveitar as políticas para equilibrar a conveniência, o tempo de acesso aos dados e o custo do arquivo de dados.

Ao considerar as estratégias para arquivar ou exportar para a nuvem, os usuários do Rapid Recovery são incentivados a entender o equilíbrio entre o custo inicial para armazenar os dados, a frequência com que os dados serão usados, a necessidade de acessar os dados em um período previsto e os custos associados à recuperação dos dados.

Alguns provedores (como o Amazon S3) oferecem diferentes classes de armazenamento. Escolher a classe de armazenamento correta pode economizar seu dinheiro se suas pressuposições sobre esses fatores forem precisas. A Quest recomenda que os usuários do Rapid Recovery consultem as políticas de armazenamento de dados pelo menos uma vez por ano para garantir que estejam usando os recursos de forma eficaz. Da mesma forma, os administradores analisar com cautela os dados que serão arquivados ou exportados para contas de nuvem, para que você possa atualizar o planeamento e migrar os dados de acordo.

O custo do armazenamento de dados, para alguns fornecedores, é extremamente baixo ou, em alguns casos, de graça. No entanto, os provedores de serviços de nuvem geralmente cobram encargos em sua conta quando você

acessa ou recupera esses dados. Geralmente, são taxas diferentes com base na urgência com que você precisa acessar os dados. Em alguns casos, usar armazenamento mais caro (como o Amazon S3 padrão) é mais eficaz em termos de custo se você planeja restaurar dados de pontos de recuperação do que se você armazenar dados no Glacier e precisar restaurá-los.

A Amazon permite definir políticas de ciclo de vida de dados que movimentam os dados entre as classes de armazenamento do Amazon S3 ao longo do tempo. Por exemplo, você pode armazenar dados recém-carregados usando a classe de armazenamento Padrão, movê-los para o Acesso infrequente padrão 30 dias depois e, em seguida, para o Armazenamento de redundância reduzida após decorrido mais um período de 60 dias. Você também pode arquivar dados explicitamente para qualquer tipo de conta de nuvem do Amazon S3 no Glacier, usando o Assistente de arquivamento. Isso é recomendável quando se espera que a recuperação de dados seja muito infrequente. Antes de selecionar essa opção, familiarize-se com as taxas relacionadas ao acesso, tempo de armazenamento e assim por diante. Consulte o tópico Opções de armazenamento e arquivamento da Amazon.

Alguns recursos do Rapid Recovery foram projetados especificamente para a nuvem. Se for realizar uma exportação virtual para a nuvem com o Azure, considere o standby virtual. Esse processo permite criar uma máquina virtual totalmente inicializável na nuvem do Azure. Os arquivos de VM são continuamente atualizados com os pontos de recuperação recém-capturados. Ao contrário do standby virtual realizado no local, os arquivos de VM não são implantados em uma VM inicializável até que ou a menos que você precise deles. O custo inicial do standby virtual no Azure envolve apenas armazenamento. Os custos de computação (que no Azure podem ser consideráveis no longo prazo) são cobrados somente se a VM for implantada, o que é necessário para configurar uma VM e executar uma restauração.

Também é possível replicar um Core local na nuvem do Azure usando o destino de replicação do Rapid Recovery. Você pode configurar rápida e facilmente um Core de destino selecionando “Destino de replicação do Rapid Recovery” no Azure Marketplace. O Core de destino incorre custos de computação. Você também precisa se planejar para armazenamento do repositório no Azure. A novidade no versão 6.2 é que agora você pode usar o destino de replicação alvo na nuvem do Azure Government. Para obter informações sobre replicação no Azure, consulte o *Guia de configuração do destino de replicação do Rapid Recovery para o Microsoft Azure*.

Os usuários do Rapid Recovery que usam essas opções de armazenamento na nuvem devem entender as compensações entre custo inicial para armazenar dados, a necessidade de acessar esses dados em determinado período e os custos associados à recuperação dos dados.

Por exemplo, o custo do armazenamento de dados, para alguns fornecedores, é extremamente baixo ou, em alguns casos, de graça. No entanto, os provedores de serviços de nuvem geralmente cobram encargos em sua conta quando você acessa ou recupera esses dados. Geralmente, são taxas diferentes com base na urgência com que você precisa acessar os dados. Em alguns casos, usar armazenamento mais caro (como o Amazon S3 padrão) é mais eficaz em termos de custo se você planeja restaurar dados de pontos de recuperação do que se você armazenar dados no Glacier e precisar restaurá-los.

A Amazon permite definir políticas de ciclo de vida de dados que movimentam os dados entre as classes de armazenamento do Amazon S3 ao longo do tempo. Por exemplo, você pode armazenar dados recém-carregados usando a classe de armazenamento Padrão, movê-los para a classe IA padrão 30 dias depois e, em seguida, para o Amazon Glacier após decorrido mais um período de 60 dias.

Adicionar uma conta de nuvem

Antes que você possa mover os dados em qualquer direção entre uma conta de nuvem e o seu Core, você precisa adicionar os dados da conta do provedor da nuvem ao Rapid Recovery Core Console. Essas informações identificam a conta de nuvem no Core Console enquanto armazena em cache, seguramente, as informações da conexão. Esse processo então permite que o Rapid Recovery Core se conecte à conta de nuvem para executar as operações que você especificar.

Para adicionar uma conta em nuvem, execute as etapas do procedimento a seguir.

1. Na barra de ícones do Rapid Recovery Core Console, clique no ícone **Mais** e, em seguida, selecione **Contas de nuvem**.

A página **Contas de nuvem** é exibida.

2. Na página **Contas de nuvem**, clique em **Adicionar nova conta**.

   A caixa de diálogo **Add New Account** (Adicionar nova conta) é mostrada.

3. Selecione um provedor de nuvem compatível na lista suspensa de tipo de nuvem.
4. Digite os detalhes conforme descrito na tabela a seguir com base no tipo de nuvem selecionado na Etapa 3.

Tabela 163. Detalhes da conta de nuvem

Tipo de nuvem	Caixa de texto	Descrição
Microsoft Azure	Nome de exibição	Digite um nome de exibição para essa conta de nuvem para exibir no Rapid Recovery Core Console; por exemplo, Conta de Nuvem 1 do Azure.
	Nome da conta de armazenamento	Insira o nome de sua conta de armazenamento do Microsoft Azure. **NOTE:** O nome deve corresponder precisamente ao nome da conta de armazenamento no Azure. Deve conter apenas letras minúsculas e números, e ter entre 3 e 24 caracteres.
	Chave de acesso	Insira a chave de acesso para sua conta. **NOTE:** Você pode digitar a chave principal ou secundária. Para obter a chave de acesso da conta do Azure, verifique **Chaves** em **Configurações**.
	Usar o protocolo HTTPS	Selecione esta opção para usar o protocolo https seguro em vez do protocolo http padrão.
Amazon S3	Nome de exibição	Digite um nome de exibição para essa conta de nuvem para exibir no Rapid Recovery Core Console; por exemplo, Conta de Nuvem 1 do Amazon S3.
	Chave de acesso	Digite a chave de acesso para sua conta de nuvem da Amazon.
	Chave secreta	Insira a chave secreta para esta conta.
	Ponto de extremidade de serviço	Opcionalmente, se estiver usando uma conta de armazenamento compatível com o S3 diferente de uma conta de armazenamento padrão do Amazon S3, digite o URL http ou https totalmente qualificado dessa conta de armazenamento.
	Classe de armazenamento	Selecione uma classe de armazenamento para a conta do S3. Você pode selecionar dentre: • Padrão • Padrão - Acesso infrequente • Armazenamento de redundância reduzido Se quiser arquivar no Glacier, você pode definir sua contas de nuvem da Amazon usando qualquer classe de armazenamento listada. A

Tipo de nuvem	Caixa de texto	Descrição
		opção de selecionar o armazenamento Glacier está acessível no Assistente de arquivamento. **NOTE:** Para obter mais informações sobre as classes de armazenamento, consulte o tópico Considerando opções de armazenamento na nuvem.
Fornecido pelo OpenStack	Nome de exibição	Digite um nome de exibição para essa conta de nuvem para exibir no Rapid Recovery Core Console; por exemplo, Conta de Nuvem 1 do OpenStack.
	Região	Digite a região para sua conta de nuvem.
	Nome de usuário	Insira o nome de usuário para sua conta de nuvem baseada no OpenStack.
	Senha ou chave de API	Selecione se deseja usar uma senha ou uma chave de API e digite sua seleção para esta conta.
	ID do locatário	Insira seu ID do locatário para esta conta.
	URL de autenticação	Insira a URL de autenticação para esta conta. Este é o URL base para a instância da nuvem. Se não for fornecido, o Rapid Recovery Core usa o URL padrão, https://identity.api.rackspacecloud.com.
Arquivos do Rackspace Cloud	Nome de exibição	Digite um nome de exibição para essa conta de nuvem para exibir no Rapid Recovery Core Console; por exemplo, Conta de Nuvem 1 do Rackspace.
	Região	Use a lista suspensa para selecionar a região para a sua conta.
	Nome de usuário	Insira o nome de usuário para sua conta em nuvem do Rackspace.
	Senha ou chave de API	Selecione se deseja usar uma senha ou uma chave de API e digite sua seleção para esta conta.
	ID do locatário	Insira seu ID do locatário para esta conta.
	URL de autenticação	Insira a URL de autenticação para esta conta. Este é o URL base para a instância da nuvem. Se não for fornecido, o Rapid Recovery Core usa o URL padrão, https://identity.api.rackspacecloud.com.
Google Cloud	Nome de exibição	Digite um nome de exibição para essa conta de nuvem para exibir no Rapid Recovery Core Console; por exemplo, Conta de Nuvem 1 do Google.
	Arquivo de certificado	Procure e selecione o arquivo de certificado do Google para autenticar essa conta de nuvem.
	Chave privada	Insira a chave privada para essa conta.

Tipo de nuvem	Caixa de texto	Descrição
	ID do projeto	Insira a ID do projeto associada a essa conta.
	E-mail da conta de serviço	Insira o endereço de e-mail registrado no Google Cloud como o proprietário dessa conta de serviço de nuvem.

5. Clique em **Salvar**.

   A caixa de diálogo fecha e sua conta aparece na página **Contas de nuvem** do Core Console.

Editar uma conta de nuvem

Caso precise alterar as informações para se conectar à conta de nuvem, por exemplo, para atualizar a senha ou editar o nome de exibição, você pode fazer isso na página **Contas de nuvem** do Rapid Recovery Core Console. Execute as etapas do procedimento a seguir para editar uma conta em nuvem.

1. Na barra de ícones do Rapid Recovery Core Console, clique no ícone **Mais** e, em seguida, selecione **Contas de nuvem**.

   A página **Contas de nuvem** é exibida.

2. Ao lado da conta em nuvem que desejar editar, clique no menu suspenso , e depois clique em **Editar**.

   A janela **Editar conta** é aberta.

3. Edite os detalhes conforme necessário e, em seguida, digite novamente a senha (ou uma chave de API, uma chave secreta, uma chave privada, e assim por diante) necessária para se conectar à conta da nuvem. Em seguida, clique em **Salvar**.

   NOTE: Não é possível editar o tipo de nuvem.

Remover uma conta de nuvem

Se você interromper seu serviço em nuvem, ou decidir parar de usá-lo em um Core específico, você pode desejar remover sua conta em nuvem do Core Console. Execute as etapas do procedimento a seguir para remover uma conta em nuvem.

1. Na barra de ícones do Rapid Recovery Core Console, clique no ícone **Mais** e, em seguida, selecione **Cloud Accounts** (Contas de nuvem).

   A página **Contas de nuvem** é exibida.

2. Ao lado da conta em nuvem que desejar editar, clique no menu suspenso , e depois clique em **Remove** (Remover).
3. Na caixa de diálogo **Apagar conta**, clique em **Sim** para confirmar que quer remover a conta.
4. Se a conta de nuvem estiver atualmente em uso, uma segunda caixa de diálogo solicita que você confirme se você ainda deseja removê-la. Clique em **Sim** para confirmar.

   NOTE: Remover uma conta atualmente em uso faz com que todos os trabalhos de arquivamento para esta conta falhem.

   A caixa de diálogo é fechada e as credenciais para acessar a conta de nuvem especificada são removidas do Core.

O Local Mount Utility

Esta seção descreve como fazer download, instalar e usar o Utilitário de montagem local (LMU) do Rapid Recovery baseado no Windows para montar pontos de recuperação e explorar o conteúdo de um nível de arquivo usando uma máquina que não hospeda o Rapid Recovery Core.

Sobre o Local Mount Utility

O Local Mount Utility (LMU) é um aplicativo baseado em Windows que pode ser obtido por download e que permite montar um ponto de recuperação do Rapid Recovery em um dos três modos disponíveis em qualquer computador Windows compatível. O utilitário simples pode ser instalado nos mesmos sistemas operacionais Windows de 32 e 64 bits do software Rapid Recovery Agent, mas não precisa ser instalado no mesmo computador que o Agent. O LMU inclui os drivers rapidrecovery-vdisk (antigo aavdisk) e aavstor, mas não é executado como serviço. Quando o utilitário é instalado, por padrão, ele é instalado no diretório `C:\Program Files\AppRecovery\Local Mount Utility`, e um atalho aparece na área de trabalho da máquina.

Embora o utilitário tenha sido projetado para acesso remoto a uma máquina Rapid Recovery Core, também é possível instalar o LMU na mesma máquina de um Rapid Recovery Core. Quando executado em um Core, o aplicativo reconhece e exibe todas as montagens desse Core, incluindo montagens realizadas por meio do Rapid Recovery Core Console. Da mesma forma, as montagens realizadas no LMU também aparecem no Core Console.

Quando o LMU é instalado na mesma máquina, como um Mailbox Restore, o LMU inicia automaticamente o Mailbox Restore quando você o usa para abrir um banco de dados do Exchange. O Mailbox Restore é o aplicativo Quest Rapid Recovery usado para restaurar itens e armazenamento de dados do Microsoft Exchange. Você pode instalá-lo no momento da instalação do LMU ou do Rapid Recovery Core. Para obter mais informações sobre o Mailbox Restore, consulte o *Guia do usuário do Mailbox Restore for Exchange.*

NOTE: As máquinas Linux usam um utilitário de linha de comando, local_mount, para consultar o Core de máquinas protegidas e seus respectivos pontos de recuperação. Da mesma forma, essa ferramenta permite que os usuários montem remotamente um volume de ponto de recuperação; permite que os usuários explorem o conteúdo do volume no nível de arquivo; e permite que os usuários restaurem arquivos individuais ou um volume inteiro a partir do ponto de recuperação, incluindo BMR do volume do sistema. Para obter mais informações, consulte o *Guia do usuário do Rapid Recovery.*

Trabalhar com máquinas Rapid Recovery Core no Utilitário de montagem local

O Utilitário de montagem local (LMU) permite que você trabalhe com um número ilimitado de máquinas Core local ou remotamente. Se você instalar o LMU em um servidor Rapid Recovery Core, essa máquina será mostrada automaticamente no LMU como o localhost. Todos os Cores remotos adicionais aparecem como seus nomes de máquinas ou endereços IP, dependendo das informações que foram inseridas ao serem adicionadas.

Com o LMU, você pode adicionar, editar e remover máquinas Core. Para obter mais informações, consulte os procedimentos a seguir:

- Adicionar uma máquina Core ao Local Mount Utility
- Alterar as opções do Local Mount Utility
- Como editar definições de conexão do Core no Local Mount Utility
- Reconectar a um Core
- Como remover uma máquina Rapid Recovery Core do Local Mount Utility

Tarefas relacionadas

See also: Adicionar uma máquina Core ao Local Mount Utility
See also: Alterar as opções do Local Mount Utility
See also: Como editar definições de conexão do Core no Local Mount Utility
See also: Reconectar a um Core
See also: Como remover uma máquina Rapid Recovery Core do Local Mount Utility

Adicionar uma máquina Core ao Local Mount Utility

Para montar um ponto de recuperação, você deve adicionar uma máquina do Core ao LMU. Não há limite para a quantidade de Cores que podem ser adicionados.

Conclua o procedimento a seguir para configurar o LMU adicionando um Core.

1. Na máquina na qual o LMU está instalado, inicie o LMU clicando duas vezes no ícone na área de trabalho.
2. Execute um dos seguintes:
   - No menu Local Mount Utility, no canto superior esquerdo, clique em **Adicionar Core**.
   - Clique com o botão direito do mouse no espaço em branco do painel esquerdo e clique em **Adicionar Core**.

   A caixa de diálogo **Adicionar Core** é exibida.
3. Na caixa de diálogo **Adicionar Core**, insira as credenciais solicitadas, descritas na tabela a seguir.

Tabela 164. Credenciais do Rapid Recovery **Core**

Opção	Descrição
Nome do host	O nome ou o endereço IP do Core a partir do qual você deseja montar pontos de recuperação. **NOTE:** Se você estiver instalando o LMU em uma máquina do Rapid Recovery Core, o LMU adicionará automaticamente a máquina localhost.
Porta	O número da porta utilizada para comunicar-se com o Core. O número de porta padrão é 8006.
Usar minhas credenciais de usuário do Windows	Selecione esta opção se as credenciais que você usa para acessar o Core são as mesmas que suas credenciais do Windows.
Usar credenciais específicas	Selecione esta opção se as credenciais que você usa para acessar o Core são diferentes das suas credenciais do Windows.

Opção	Descrição
Nome de usuário	O nome de usuário usado para acessar a máquina do Core. **NOTE:** Essa opção só permanecerá disponível se você escolher usar credenciais específicas.
Senha	A senha usada para acessar a máquina do Core. **NOTE:** Essa opção só permanecerá disponível se você escolher usar credenciais específicas.

4. Clique em **Conectar.**
5. Se você estiver adicionando vários Cores, repita todas as etapas conforme necessário.

Alterar as opções do Local Mount Utility

Conclua o procedimento a seguir para alterar as opções de todos os Rapid Recovery Cores conectados ao LMU.

1. Na interface do usuário do Local Mount Utility, clique em **Opções**.
2. Na caixa de diálogo **Opções**, você pode alterar a definição descrita na tabela a seguir.

Tabela 165. Definições do Core

Opção	Descrição
Local	Use o botão **Procurar** ou insira um caminho para a pasta que você deseja usar para montar os pontos de recuperação.
Tipo de montagem	Especifique a maneira de acessar os dados do ponto de recuperação montado: • Apenas leitura • Apenas leitura com gravações anteriores • Gravável
Idioma	Selecione o idioma no qual você deseja que a LMU seja exibida. Você pode selecionar dentre as seguintes opções: • Inglês • Francês • Alemão • Português • Espanhol • Chinês simplificado • Japonês • Coreano
Atualização automática	Selecione e insira o tempo durante o qual o LMU deve atualizar sua conexão com um Core para obter as informações mais recentes.
Mostrar Core local	Se o LMU estiver instalado em uma máquina do Core, selecione para mostrar esse Core.

Opção	Descrição
Mostrar notificações pop-up	Selecione para permitir que o LMU notifique-o sobre eventos e alertas por meio de pop-ups na área de trabalho.
Abrir a pasta de montagem no Windows Explorer se a montagem for bem-sucedida	Selecione essa opção para poder procurar o conteúdo de um ponto de recuperação montado.

3. Clique em **Salvar**.

Como editar definições de conexão do Core no Local Mount Utility

Para editar as definições que você estabeleceu quando adicionou um Core ao LMU, conclua o procedimento a seguir.

NOTE: Esse procedimento não se aplica ao Core localhost. Ele só se aplica a máquinas Core remotas.

1. Na interface do usuário do Local Mount Utility, clique com o botão direito do mouse no Core cujas definições você deseja editar e em **Editar Core**.
2. Na caixa de diálogo **Editar Core**, você pode alterar as definições descritas na tabela a seguir.

Tabela 166. Definições do Core

Opção	Descrição
Nome do host	O nome do Core a partir do qual você deseja montar pontos de recuperação. **NOTE:** Se você estiver instalando o LMU em uma máquina do Rapid Recovery Core, o LMU adicionará automaticamente a máquina localhost.
Porta	O número da porta utilizada para comunicar-se com o Core. O número de porta padrão é 8006.
Usar minhas credenciais de usuário do Windows	Selecione esta opção se as credenciais que você usa para acessar o Core são as mesmas que suas credenciais do Windows.
Usar credenciais específicas	Selecione esta opção se as credenciais que você usa para acessar o Core são diferentes das suas credenciais do Windows.
Nome de usuário	O nome de usuário usado para acessar a máquina do Core. **NOTE:** Essa opção só permanecerá disponível se você escolher usar credenciais específicas.
Senha	A senha usada para acessar a máquina do Core.

Opção	Descrição
	NOTE: Essa opção só permanecerá disponível se você escolher usar credenciais específicas.

3. Depois que você fizer as alterações, clique em **OK**.

Reconectar a um Core

Se você perder a conexão com uma máquina do Rapid Recovery Core, é possível restabelecer a conexão clicando em **Refresh** (Atualizar) na tela inicial do LMU.

Como remover uma máquina Rapid Recovery Core do Local Mount Utility

Conclua o procedimento a seguir para remover um Core do LMU.

NOTE: Essa opção não está disponível para um Rapid Recovery Core localizado em e rotulado como o localhost.

1. Na interface do usuário do Local Mount Utility, clique com o botão direito do mouse que você deseja remover e clique em **Remover Core**.
2. Para confirmar um comando, clique em **Sim** na caixa de diálogo.

   A LMU remove o Core e as máquinas protegidas na árvore de navegação.

Trabalhar com máquinas protegidas no Local Mount Utility

Com o Local Mount Utility (LMU), você pode montar e procurar pontos de recuperação em máquinas protegidas sem precisar estar conectado no Rapid Recovery Core Console associado a essa máquina. Para obter mais informações, consulte os procedimentos a seguir:

- Montar um ponto de recuperação usando o Local Mount Utility
- Usar o Local Mount Utility para explorar um ponto de recuperação montado
- Atualizar pontos de recuperação
- Desmontar pontos de recuperação no Local Mount Utility

Montar um ponto de recuperação usando o Local Mount Utility

Com o LMU, você pode montar qualquer ponto de recuperação associado a uma máquina Core conectada, inclusive máquinas protegidas, máquinas replicadas e máquinas "apenas pontos de recuperação".

Antes de montar um ponto de recuperação, o Local Mount Utility (LMU) deve se conectar ao Core em que o ponto de recuperação está armazenado. Conforme descrito no procedimento Adicionar uma máquina Core ao Local Mount Utility, o número de Cores que podem ser adicionados ao LMU é ilimitado.

1. No LMU, selecione a máquina na qual você deseja montar um ponto de recuperação.
2. Selecione o ponto de recuperação que você deseja montar e selecione uma das seguintes opções:

Opção	Descrição
Montagem	Esta opção permite montar o ponto de recuperação usando a seleção padrão das opções do LMU. Para obter mais informações, consulte Alterar as opções do Local Mount Utility.
Montagem avançada...	Essa opção abre a caixa de diálogo **Montagem avançada**.

3. Se você tiver selecionado **Montagem avançada**, conclua as opções descritas na tabela a seguir.

Tabela 167. Opções de montagem avançada

Opção	Descrição
Caminho do ponto de montagem	Digite ou navegue até o local que será usado para montar os pontos de recuperação.
Tipo de montagem	Selecione uma das opções a seguir: • Montagem de apenas leitura • Montagem gravável • Montagem de apenas leitura com gravações anteriores Para obter descrições de cada opção, consulte Etapa 4.

- Clique em **Montar**.

O LMU abre automaticamente a pasta que contém o ponto de recuperação montado. A coluna Montagem local na página Pontos de recuperação do LMU indica como o ponto de recuperação foi montado.

Usar o Local Mount Utility para explorar um ponto de recuperação montado

A exploração de um ponto de recuperação abre os dados de backup em uma janela do Windows Explorer e permite pesquisar em volumes e pastas o item ou os itens que você deseja recuperar.

Você pode recuperar itens copiando-os para o local preferido usando um gerenciador de arquivos, como o Windows Explorer (ou programaticamente usando APIs do Windows). Conclua o procedimento a seguir para explorar um ponto de recuperação montado atualmente.

NOTE: Este procedimento não é necessário se você estiver explorando um ponto de recuperação imediatamente após montá-lo, pois a pasta que contém o ponto de recuperação abre automaticamente após a conclusão do procedimento de montagem.

1. Na interface do usuário do Utilitário de montagem local, clique em **Montagens ativas**.

A janela Montagens ativas é aberta e exibe todos os pontos de recuperação montados.

2. Expanda a árvore de navegação para revelar os pontos de recuperação montados para cada máquina e seus volumes.
3. Clique em **Explorar** próximo do volume que você deseja explorar.

Atualizar pontos de recuperação

Se a opção estiver habilitada, o Local Mount Utility (LMU) recebe atualizações em tempo real do Core e das máquinas protegidas. Se essa opção estiver desabilitada, para ver os pontos de recuperação mais recentes de uma máquina, você deve clicar periodicamente em **Refresh** (Atualizar) na tela inicial do LMU.

Desmontar pontos de recuperação no Local Mount Utility

Execute o procedimento a seguir para desmontar os pontos de recuperação que estão montados no Local Mount Utility (LMU).

1. Na interface do usuário do LMU, clique no Core ou na máquina protegida associada ao montar o ponto ou pontos de recuperação.
2. Siga umas destas etapas:
   - Para desmontar todos os pontos de recuperação montados do Core selecionado ou da máquina protegida de uma só vez, clique em **Desmontar todos** e, em seguida, em **Sim** na caixa de diálogo.
   - Para desmontar um único ponto de recuperação, selecione o ponto de recuperação na lista e, em seguida, clique em **Desmontar**.

   O ponto ou os pontos de recuperação são desmontados.

Referências do Core Console

Este apêndice contém as tabelas de referência que descrevem muitas das funções e ícones disponíveis no Rapid Recovery Core Console. Serve como um suplemento para o capítulo Core Console do *Guia do usuário do Rapid Recovery*.

Como ver a interface do usuário do Core Console

Core Console é a interface do usuário por meio da qual os usuários interagem com o Rapid Recovery. Ao efetuar login no Rapid Recovery Core Console, você vê os elementos a seguir.

Tabela 168. Elementos de UI incluídos no Core Console

Descrições dos menus e das informações que são exibidos no Core Console.

Elemento de UI	Descrição
Área de imagem corporativa	Para ambientes típicos, o lado superior esquerdo do Core Console tem o nome do produto completo, inclusive o logotipo da Quest. Clicar em qualquer lugar na área da marca resulta na abertura de uma nova guia do navegador da Web, exibindo a documentação no site de suporte do produto.
Barra de botões	A barra de botões, exibida à direita da área da marca, contém botões acessíveis de qualquer lugar do Core Console. Esses botões abrem assistentes para realizar tarefas comuns, como proteger uma máquina, realizar uma restauração do ponto de recuperação; criar, conectar ou importar um arquivo; ou replicar desse Core de origem para um Core de destino. Cada botão da barra de botões é descrito mais detalhadamente na tabela Tabela 169.
Contagem de tarefas em execução	Mostra quantos trabalhos estão em execução no momento. Esse valor é dinâmico, com base no estado do sistema. Ao clicar no menu suspenso, você vê um resumo do status de todos os trabalhos em execução. Clicando no **X** de qualquer trabalho, você pode escolher cancelar esse trabalho.
Menu suspenso de Ajuda	O menu **Ajuda** inclui as seguintes opções: • **Ajuda**. Links para ajuda dentro do produto, que se abre em uma janela do navegador à parte. • **Documentação**. Links para a documentação técnica do Quest no site da Rapid Recovery. • **Suporte**. Links para o site do Rapid Recovery, fornecendo acesso ao Live Chat, aos tutoriais em vídeo, aos artigos da base de conhecimento do Suporte de proteção de dados da Quest, às perguntas frequentes e muito mais. • **Guia de início rápido**. O Guia de início rápido é um fluxo guiado de tarefas sugeridas para configurar e usar o Rapid Recovery. O guia é aberto automaticamente cada vez que você efetua login no Core Console, a menos que você desabilite essa função. É possível abrir o Guia de Início Rápido no menu Ajuda a qualquer momento. Para obter

Elemento de UI	Descrição
	mais informações sobre esse recurso, consulte Noções básicas sobre o Guia de início rápido. • **Enviar uma ideia**. Se você tiver sugestões de recursos ou melhorias, selecione esta opção para abrir o portal de ideias da Quest, onde você pode descrever de forma rápida e fácil suas ideias e solicitar uma análise dos gerentes de produto para a possível inclusão em uma versão futura do Rapid Recovery. • **Sobre**. Abre a caixa de diálogo Sobre o Rapid Recovery. As informações incluem o componente do Rapid Recovery; informações sobre a versão, ID do Core; um hyperlink para contribuições de terceiros; e uma descrição do software.
Data e hora do servidor	A hora atual da máquina que executa o serviço Rapid Recovery Core é exibida no canto superior direito do Core Console. Quando você passa o mouse sobre a hora, a data do servidor também é exibida. Essa é a data e hora gravada pelo sistema para eventos como registro em log, programação e geração de relatórios. Por exemplo, ao aplicar as programações de proteção, o horário exibido no Core Console é usado. Isso é verdadeiro mesmo que o fuso horário seja diferente no server de banco de dados ou na máquina cliente onde o navegador está sendo executado.
Barra de ícones	A barra de ícones inclui uma representação gráfica das principais funções acessíveis no Core Console. Ela é exibida no lado esquerdo da interface do usuário (UI), logo abaixo da área da marca. O clique no item apropriado da barra de ícones leva você até a seção correspondente da UI, onde você pode gerenciar essa função. Cada um dos ícones da barra é descrito mais detalhadamente na tabela Tabela 170.
Área de navegação esquerda	A área de navegação esquerda é exibida no lado esquerdo da interface do usuário, abaixo da barra de ícones. • A área de navegação esquerda contém o filtro de texto e o menu Máquinas. • Se você adicionou replicação a esse Core, esta área contém um menu Máquinas replicadas. • Se há máquinas que foram removidas da proteção, mas cujos pontos de recuperação foram salvos, esta área contém um menu Apenas pontos de recuperação. • Se você adicionou grupos personalizados, esta área contém um menu Grupo personalizado. • Caso você tenha anexado um arquivo, essa área contém um menu de arquivos anexados. Você pode ativar ou desativar a exibição da área de navegação esquerda. Isso é útil quando é preciso ver mais conteúdo na área de navegação principal da UI. Para ocultar esta seção, clique na borda cinza entre as áreas de navegação esquerda e de navegação principal. Para mostrar este elemento de UI novamente, clique na borda cinza outra vez. Cada um dos elementos na área de navegação esquerda é descrito mais detalhadamente na tabela Tabela 172.
Ajuda sensível ao contexto	 No Rapid Recovery Core Console, sempre que você clica no ícone de Ajuda (um ponto de interrogação azul), uma janela de navegador redimensionável é aberta com dois quadros. O quadro à esquerda contém uma árvore de navegação mostrando os tópicos do *Guia do usuário do Rapid Recovery*. O frame direito exibe o conteúdo para o tópico de ajuda selecionado. A qualquer momento, a árvore de navegação de ajuda se expande para exibir a localização do tópico selecionado em sua hierarquia. É possível procurar em

Elemento de UI	Descrição
	todos os tópicos do *Guia do usuário* utilizando esse recurso de ajuda sensível ao contexto. Feche o navegador quando você terminar de pesquisar tópicos. Você pode também abrir a ajuda pela opção **Ajuda** do menu **Ajuda**.

Barra de botões

Os detalhes sobre a barra de botões são exibidos na tabela a seguir.

Tabela 169. Botões e menus da barra de botões

Descrições das ações disponíveis para cada menu e botão na barra de botões do Core Console.

Elemento de UI	Descrição
Barra de botões: Botão Proteger e menu	O botão **Proteger** abre o Assistente de proteção de máquina, no qual você pode proteger uma única máquina no Rapid Recovery Core. Além disso, para outras opções de proteção, você pode acessar o menu suspenso próximo a esse botão, que inclui as opções a seguir. • A opção **Proteger máquina** é outro método para iniciar o assistente de proteção de máquina para proteger uma única máquina. • A opção **Proteger cluster** permite que você se conecte a um cluster de servidor. • A opção **Proteger diversas máquinas** abre o Assistente de proteção de diversas máquinas a fim de permitir que você proteja duas ou mais máquinas simultaneamente. • A opção **Implantar software do agente** permite instalar o software Rapid Recovery Agent em uma ou mais máquinas simultaneamente. Essa função usa o Assistente de implantação do software do agente.
Barra de botões: Botão Restaurar e menu	O botão **Restaurar** abre o assistente Restaurar máquina, que permite restaurar dados a partir de pontos de recuperação salvos de uma máquina protegida. Além disso, para outras opções de restauração ou exportação, você pode acessar o menu suspenso próximo a esse botão, que inclui as opções a seguir. • A opção **Restaurar máquina** é outro método para abrir o Assistente de restauração de máquina a fim de restaurar dados. • A opção **Montar ponto de recuperação** abre o Assistente de montagem, que permite montar ponto de recuperação em uma máquina protegida. • O botão **Exportação do VM** abre o Assistente de exportação. Nesse assistente você pode criar uma máquina virtual usando pontos de recuperação salvos no Rapid Recovery Core. Você pode criar uma exportação única ou definir parâmetros para uma VM que é continuamente atualizada após cada snapshot de uma máquina protegida.
Barra de botões: Botão Arquivar e menu	O botão **Arquivar** abre o Assistente de arquivo. Nesse assistente você pode criar um arquivo único usando pontos de recuperação ou criar um arquivo e salvar continuamente nesse arquivo com base em um programa definido por você.

Elemento de UI	Descrição
	Além disso, para outras opções de arquivamento, você pode acessar o menu suspenso próximo a esse botão, que inclui as opções a seguir. • A opção **Criar arquivo** é outro método para abrir o Assistente de criação de arquivo para criar um arquivo único ou arquivar continuamente. • A opção **Importar arquivo** abre o Assistente de importação de arquivo, que permite importar arquivo. • A opção **Anexar arquivo** monta um arquivo para você poder ler o conteúdo como um sistema de arquivos.
Barra de botões: Botão Replicar 	O botão **Replicar** abre o Assistente de replicação. Nesse assistente você pode especificar um Core de destino, selecionar máquinas protegidas no Core de origem e replicar pontos de recuperação de máquinas protegidas para o Core de destino especificados por você. Você pausar a replicação ao defini-la, ou a replicação pode começar imediatamente. Além disso, você pode especificar se uma unidade de seeding será usada para copiar dados para pontos de recuperação existentes para o Core de destino.

Barra de ícones

Os detalhes sobre a barra de ícone são exibidos na tabela a seguir.

Tabela 170. Barra de ícones

Descrições das ações disponíveis para cada menu na barra de ícones do Core Console.

Elemento de UI	Descrição
Barra de ícones	A barra de ícones inclui uma representação gráfica das principais funções acessíveis no Core Console. Quando você clica em um item, é conduzido para a seção correspondente da interface de usuário, onde pode gerenciar aquela função. Os ícones da barra de ícones são:
Barra de ícones: Ícone Inicial 	**Inicial**. Clique no ícone Inicial para navegar até a página Inicial do Core.
Barra de ícones: Ícone Replicação 	**Replicação**. Clique no ícone Replicação para visualizar ou gerenciar a replicação de entrada ou de saída.
Barra de ícones: Ícone Standby virtual 	**Standby virtual**. Clique no ícone Standby virtual para exportar informações de um ponto de recuperação para uma máquina virtual inicializável.
Barra de ícones: Ícone Eventos 	**Eventos**. Clique no ícone Eventos para visualizar um registro de todos os eventos relacionados ao Rapid Recovery Core.

Elemento de UI	Descrição		
Barra de ícones: Ícone Definições			**Definições**. Clique no ícone Definições para visualizar ou gerenciar definições do Rapid Recovery Core. Você pode fazer cópia de segurança ou restaurar definições da configuração da restauração do núcleo. Você pode fazer definições gerais para controlar portas ou exibir aspectos. Além disso, você pode configurar definições nas seguintes categorias: atualizações automáticas; trabalhos noturnos; definições da fila de transferência; definições de tempo limite do cliente; definições de cache de deduplicação DVM; definições do Replay Engine e definições de implantação. Você pode visualizar ou alterar conexões do banco de dados; definições do servidor de SMTP; contas de armazenamento em nuvem e alterar definições de fonte para relatórios. Você pode determinar definições de capacidade de anexação SQL; definições de trabalho do núcleo; definições de licença; definições SNMP e definições vSphere.
Barra de ícones: Ícone Mais			**Mais**. Clique no ícone Mais para acessar outros recursos importantes. Cada um tem o próprio ícone, listado abaixo.
Barra de ícones: Ícone Mais	Informações do sistema		**Informações do sistema**. Clique em Informações do sistema para exibir dados sobre o servidor do Rapid Recovery Core. Você pode ver o nome de host, OS, arquitetura e memória do Core. Você pode ver o nome exibido no Core Console. Também pode visualizar o nome de domínio totalmente qualificado do Core na rede e o caminho para os metadados de cache e para o cache de deduplicação. Para obter mais informações sobre como alterar o nome de exibição, consulte Noções básicas sobre as informações do sistema do Core. Para obter mais informações sobre cache de deduplicação, consulte Noções básicas sobre o cache de deduplicação e locais de armazenamento. Para obter informações sobre como ajustar as definições, consulte Configurar definições de cache de deduplicação DVM.
Barra de ícones: Ícone Mais	Arquivos		**Arquivos**. O Rapid Recovery permite gerenciar arquivos de informações no Core. Você pode visualizar informações sobre arquivos anexados ou programados e adicionar, verificar ou importar arquivos.
Barra de ícones: Ícone Mais	Montagens		**Montagens**. Permite mostrar e desmontar montagens locais e mostrar e desconectar montagens remotas.
Barra de ícones: Ícone Mais	CDs de inicialização		**CDs de inicialização**. Permite gerenciar CDs de inicialização, normalmente usados em uma bare metal restore (BMR). Você pode criar a imagem ISO de um CD de inicialização, excluir uma imagem existente ou clicar no caminho da imagem para abrir ou salvá-la.

Elemento de UI	Descrição		
Barra de ícones: Ícone Mais	Repositórios		**Repositórios**. Permite mostrar e gerenciar repositórios associados ao Core.
Barra de ícones: Ícone Mais	Chaves de criptografia		**Chaves de criptografia**. Permite mostrar, gerenciar, importar ou adicionar chaves de criptografia que você pode aplicar a máquinas protegidas. Caso não estejam sendo usadas, você pode excluir as chaves de criptografia.
Barra de ícones: Ícone Mais	Contas de nuvem		**Contas de nuvem**. Permite mostrar e gerenciar conexões entre o seu Core e as contas de armazenamento em nuvem.
Barra de ícones: Ícone Mais	Pesquisa de arquivos		**Pesquisa de arquivos**. Permite pesquisar arquivos específicos nos pontos de recuperação que você pode restaurar em um disco local.
Barra de ícones: Ícone Mais	Política de retenção		**Política de retenção**. Permite mostrar e modificar a política de retenção de núcleo, inclusive por quanto tempo manter pontos de recuperação antes de avançar e finalmente excluí-los.
Barra de ícones: Ícone Mais	Notificações		**Notificações**. Permite configurar notificações sobre eventos do Core, determinar definições do servidor de SMTP para notificações de e-mail e configurar redução de repetição para suprimir notificações repetidas sobre o mesmo evento.
Barra de ícones: Ícone Mais	Restauração do correio		**Restauração de e-mail**. Permite pesquisar em bancos de dados do servidor Exchange dados para localizar e restaurar mensagens de e-mail.
Barra de ícones: Ícone Mais	Downloads		Downloads. Você pode baixar instalador da web do software do agente, o utilitário de montagem local ou os arquivos MIB que contêm informações do evento a serem usadas em um navegador SNMP.
Barra de ícones: Ícone Mais	Relatórios		Relatórios. Permite acessar relatórios do Core ou agendar relatórios para serem gerados continuamente.
Barra de ícones: Ícone Mais	Log do Core		Log do Core. Permite baixar o arquivo de log do Core para fins de diagnóstico.

Menu de navegação à esquerda

O conjunto completo de menus que podem aparecer na área de navegação esquerda está descrito na tabela a seguir:

Tabela 171. Opções do menu de navegação à esquerda

Descrições das opções disponíveis para os tipos de máquinas listadas na área de navegação à esquerda.

Elemento de UI	Descrição
Menu Máquinas	O menu Máquinas (anteriormente Máquinas protegidas) aparece como primeiro menu na área de navegação esquerda, se uma ou mais máquinas estiverem protegidas em seu Core. Quando você clica em uma máquina específica exibida nesse painel, uma página Resumo será exibida, mostrando informações resumidas sobre essa máquina selecionada. Para obter mais informações sobre o que você pode realizar na página Resumo, consulte Visualização das informações de resumo de uma máquina protegida.
Menu de máquinas replicadas	Se você visualizar o nome de um outro Rapid Recovery Core como um menu de navegação de nível superior, o Core no qual você esta visualizando o Console do Core é um Core de destino. O menu recebe o nome do Core de origem e cada máquina listada sob ele representa uma máquina do Core de origem que está replicada neste destino. Se este Core de destino replica os pontos de recuperação de mais de um Core de origem, cada Core de origem será exibido como seu próprio menu navegável na área de navegação à esquerda. Quando você clica em uma máquina específica exibida em um menu de máquinas replicadas, uma página Resumo será exibida, mostrando informações resumidas sobre a máquina selecionada replicada. Para obter mais informações sobre replicação, consulte Replicação.
Menu Apenas pontos de recuperação	Se você visualizar um menu APENAS PONTOS DE RECUPERAÇÃO, o seu Core manterá os pontos de recuperação para uma máquina que esteja protegida ou replicada. Considerando que aquela máquina não continuará a capturar novos snapshots, os pontos de recuperação anteriormente capturados em seu Core permanecerão. Esses pontos de recuperação podem ser usados para recuperação em nível de arquivo, mas não podem ser usados para realizar um bare metal restore, restaurar volumes inteiros ou adicionar dados de snapshot.
Menu de grupos personalizados	Se você criou quaisquer grupos personalizados, um menu de grupos personalizados será exibido no menu de navegação. Os grupos personalizados são contêineres lógicos usados para agrupar máquinas (por exemplo, por função ou organização ou por localização geográfica). Os grupos personalizados podem conter objetos heterogêneos (máquinas protegidas, máquinas replicadas e assim por diante). Você pode definir o rótulo para um grupo personalizado; como outros menus, o nome é exibido no menu com todas as letras maiúsculas. Você pode executar ações para, por exemplo, itens em um grupo personalizado, clicando na seta à direita do título do grupo personalizado. Por exemplo, você pode forçar um snapshot para cada máquina protegida em um grupo personalizado. Para obter mais informações sobre como criar e gerenciar grupos personalizados, consulte Noções básicas sobre grupos personalizados.
Menu Arquivos anexados	 Se você anexar qualquer arquivo em seu Core, cada arquivo será listada no menu de navegação à esquerda. Seu rótulo é o nome do arquivo. Cada máquina incluída no arquivo está contida nesta lista.

Os detalhes sobre os elementos na área de navegação à esquerda são exibidos na tabela a seguir.

Tabela 172. Área de navegação à esquerda e menus

Descrições dos menus disponíveis para os tipos de máquinas listadas na área de navegação à esquerda.

Elemento de UI	Descrição
Filtro de texto de	 Filtro de texto é um campo de texto que permite filtrar os itens exibidos nos menus Máquinas, Máquinas replicadas e Máquinas "apenas pontos de recuperação". Caso

Elemento de UI	Descrição
menus das máquinas	você digite os critérios neste filtro, apenas as máquinas que atendam aos critérios são exibidas nos menus apropriados.
Detalhes de Expandir e contrair 	Clique na seta à direita do filtro de texto para expandir e contrair detalhes dos menus Máquinas, Máquinas replicadas e Máquinas "apenas pontos de recuperação".
Menu Máquinas     	O menu Máquinas aparece na área de navegação esquerda da UI. Neste menu, você pode ver as máquinas protegidas, clusters protegidos ou máquinas replicadas configurados no Core. Se houver grupos protegidos ou máquinas apenas com pontos de recuperação, eles também serão exibidos como parte desse menu. **NOTE:** Se um hipervisor vSphere/ESXi tiver máquinas sob proteção, o host também aparecerá nesse menu, com as VMs como filhas, mesmo se o host não estiver protegido. Você pode minimizar ou expandir a visualização de qualquer uma das máquinas protegidas no Core clicando na seta no lado esquerdo do rótulo desse menu. O ícone exibido retrata o tipo de máquina: • Um ícone de máquina simples retrata uma máquina física ou uma VM protegida com software Rapid Recovery Agent instalado. O mesmo ícone é usado para mostrar uma máquina “apenas pontos de recuperação”. • Um ícone de várias máquinas retrata um cluster protegido. • Um ícone de máquina dupla oco retrata uma VM VMware usando proteção sem agente. • Um ícone de máquina tripla oco retrata um host vCenter VMware. • Um ícone mostrando dois servidores empilhados retrata um host do Hyper-V. • Um ícone mostrando um único servidor retrata uma VM protegida sem agente do Hyper-V. Caso você clique no menu Máquinas, a página Máquinas será exibida, mostrando todas as máquinas protegidas nesse Core no painel Máquinas. Para obter mais informações, consulte Visualização do menu Máquinas protegidas.
Menu Máquinas replicadas	Caso você esteja replicando máquinas de outro Rapid Recovery Core, o nome desse Core é exibido como um menu à parte no menu Máquinas. Cada máquina replicada nesse core de destino pelo núcleo de origem listado é exibida nesse menu. Para cada máquina replicada, o ícone indica o tipo de máquina replicada. Por exemplo, em caso de replicação de uma máquina única, o ícone mostra uma máquina. Em caso de replicação de um cluster de servidor, o ícone representa um cluster. Você pode minimizar ou expandir a visualização de qualquer uma dessas máquinas replicadas clicando na seta no lado esquerdo do rótulo desse menu. No menu Máquinas replicadas, você pode executar ações em todas as máquinas replicadas. Se você clicar no menu Máquinas replicadas, a página Máquinas é exibida. Essa página mostra todas as máquinas protegidas em outro Core (de origem) que são replicadas para este Core de destino. Para obter mais informações, consulte Ver máquinas replicadas no menu de navegação.

Elemento de UI	Descrição
Menu Apenas pontos de recuperação	Se alguma máquina que estava protegida anteriormente no Core tiver sido removida da proteção sem que seus pontos de recuperação tenham sido excluídos, o menu Apenas pontos de recuperação aparecerá. Não há ícone de menu. Cada uma das máquinas protegidas anteriormente com pontos de recuperação retidos é exibida nessa lista. A máquina “apenas pontos de recuperação” mostra um ícone padrão de máquina protegida. Você pode minimizar ou expandir a visualização de qualquer uma das máquinas "apenas pontos de recuperação" clicando na seta no lado esquerdo do rótulo desse menu. No menu Apenas pontos de recuperação, você pode remover os pontos de recuperação de todas as máquinas que têm apenas pontos de recuperação neste Core. Quando você clica no menu Apenas pontos de recuperação, a página Máquinas aparece, mostrando as máquinas cujos pontos de recuperação foram salvos. Para obter mais informações, consulte Visualizar o menu Apenas pontos de recuperação.
Menu Grupos personalizados	Se o Core inclui algum grupo personalizado, a área de navegação esquerda inclui um menu Grupo personalizado. Cada um dos objetos nesse grupo personalizado é exibido nessa lista. Você pode minimizar ou expandir a visualização de qualquer um dos grupos personalizados no Core clicando na seta no lado esquerdo do rótulo desse menu. No menu Grupos personalizados, você pode executar ações com itens semelhantes no grupo. Caso você clique no menu Grupos personalizados, a página Máquinas é exibida, mostrando um painel para cada um dos objetos do Rapid Recovery exibidos no grupo: máquinas protegidas, máquinas replicadas e máquinas “apenas pontos de recuperação”. Para obter mais informações, consulte Visualizar o menu Grupos personalizados.
Menu Arquivos anexados	Caso você tenha anexado qualquer arquivo ao Core, a área de navegação à esquerda inclui um menu para cada arquivo anexado. Cada uma das máquinas protegidas incluídas no arquivo é exibida nessa lista. O rótulo do menu usa o nome especificado quando o arquivo foi salvo. Você pode minimizar ou expandir a visualização de qualquer um dos arquivos anexados no Core clicando na seta no lado esquerdo do rótulo desse menu. No menu de arquivos anexados, você pode realizar ações para itens semelhantes no grupo. Caso você clique no menu de arquivos anexados, a página Máquinas é exibida, mostrando um painel para cada um dos objetos do Rapid Recovery exibidos no grupo: máquinas protegidas, máquinas replicadas e máquinas "apenas pontos de recuperação". Para obter mais informações, consulte Visualizar o menu Grupos personalizados.

Visualizar máquinas protegidas

A partir da página **Início** do Rapid Recovery Core Console, na visualização Tabelas de resumo, você poderá ver informações de resumo de quaisquer máquinas protegidas pelo Core no painel Máquinas protegidas.

NOTE: Um agente de software atua em nome do usuário para executar ações específicas. As máquinas protegidas também são chamadas de agentes, porque executam o software Rapid Recovery Agent para facilitar a criação de cópias de segurança e a replicação de dados no Rapid Recovery Core.

Você pode ver o status, o nome de exibição de cada máquina, o repositório que ela utiliza, a data e a hora do último instantâneo, quantos pontos de recuperação existem no repositório para a máquina e a quantidade total de espaço de armazenamento que os instantâneos usam no repositório.

Para gerenciar os aspectos da máquina protegida, comece navegando até a máquina que você deseja ver, configurar ou gerenciar. Na página **Início**, há três maneiras de navegar até uma máquina protegida:

- Você pode clicar no endereço IP ou nome de exibição de qualquer máquina protegida do painel Máquinas protegidas. Isso leva você para a página Resumo da máquina protegida selecionada.
- Na área de navegação à esquerda, você pode clicar no título do menu **Máquinas protegidas**. A página **Protected Machines** (Máquinas protegidas) aparece. Nessa página, você pode ver informações resumidas sobre cada máquina. Para ver uma descrição detalhada dessa página, consulte Visualização das informações de resumo de uma máquina protegida.
- Na área de navegação à esquerda, no menu Máquinas protegidas, você pode clicar no endereço IP ou nome de exibição de qualquer máquina protegida. Isso leva você para a página **Resumo** da máquina protegida selecionada. Para ver uma descrição detalhada dessa página, consulte Visualização das informações de resumo de uma máquina protegida.

Visualizar eventos de uma máquina protegida

Na página **Eventos**, você pode visualizar os trabalhos que ocorreram ou estão em progresso na máquina protegida selecionada. Os botões na parte superior da página permitem navegar para listas de trabalhos em cada uma das três categorias de atividades:

- **Tarefas.** Um trabalho que deve ser realizado pelo Rapid Recovery para que funcione corretamente.
- **Alertas.**Ama notificação relacionada a uma tarefa ou evento que inclui erros e aviso.
- **Registro.**Uma combinação de todas as tarefas e alertas de máquinas protegidas.

A tabela a seguir contém descrições de cada elemento da página **Eventos**.

Tabela 173. Elementos da página Eventos

Elemento de UI	Descrição
Pesquisar palavra-chave	Permite pesquisar um item específico dentro de cada categoria. Disponível somente para tarefas.
De	Para restringir os resultados, você pode inserir uma data de início da pesquisa. Disponível somente para tarefas.
Para	Para restringir os resultados, você pode inserir uma data de término da pesquisa. Disponível somente para tarefas.
Ícones de status	Cada ícone representa um status diferente do trabalho. Para alertas e tarefas, clicar em um dos ícones permite filtrar a lista por esse status, gerando, essencialmente, um

Elemento de UI	Descrição
	relatório. Quando você clica no ícone uma segunda vez, o filtro desse status é removido. Você pode filtrar por mais de um status. Os status são: • **Ativo.**Um trabalho em progresso. • **Enfileirado.** Um trabalho que está aguardando a conclusão de outro trabalho para poder começar. • **Aguardando.**Um trabalho que está aguardando sua aprovação ou conclusão, como uma unidade de propagação. (Para obter mais informações sobre unidades de propagação, consulte Replicação.) • **Concluído.**Um trabalho que foi concluído com êxito. • **Com falha.** Um trabalho que teve uma falha e não foi concluído.
Ícone de serviço	Este botão adiciona trabalhos de serviços à lista de trabalhos. Quando você clica nesse ícone, um ícone de serviço menor aparece em cada ícone de status, permitindo filtrar por trabalhos de serviço que possuam esses status (se houver). Exemplos de trabalhos de serviços são a exclusão de arquivos de índice ou a remoção de uma máquina da proteção.
Lista suspensa Tipo de exportação	A lista suspensa inclui os formatos para os quais você pode exportar o relatório de eventos. Disponível somente para tarefas. Ela inclui os seguintes formatos: • PDF • HTML • CSV • XLS • XLSX
(ícone Exportar)	Converte o relatório de eventos para o formato selecionado. Disponível somente para tarefas.
Seleção de página	Os relatórios de eventos podem incluir vários trabalhos em múltiplas páginas. Os números e as setas na parte inferior da página **Eventos** permitem navegar pelas páginas adicionais do relatório.

O página **Eventos** exibe todos os eventos em uma tabela. A seguinte tabela lista as informações exibidas para cada item.

Tabela 174. Informações detalhadas da tabela de resumo de eventos

Elemento de UI	Descrição
Status	Exibe o status da tarefa, alerta ou item de registro. Disponível para alertas ou itens de registro, clique no cabeçalho para filtrar os resultados por status.
Nome	Nome está disponível somente para tarefas. Esse campo de texto lista o tipo de tarefa que foi concluída nessa máquina protegida. Os exemplos incluem transferência de volumes, manutenção de repositório, execução, realização de verificação de capacidade de montagem, realização de verificação de soma de verificação e assim por diante.
Hora inicial	Disponível para tarefas, alertas e itens de registro. Exibe a data e a hora de início do trabalho ou da tarefa.

Elemento de UI	Descrição
Hora final	Disponível somente para tarefas. Exibe a data e a hora de conclusão do trabalho ou da tarefa.
Detalhes do trabalho	Disponível somente para tarefas. Abra a caixa de diálogo **Monitorar tarefa ativa** de maneira que você possa visualizar os detalhes do trabalho ou da tarefa específico(a). Esses detalhes incluem um ID do trabalho, taxa de transferência de dados do core (se relevante), tempo decorrido para conclusão do trabalho, trabalho total em quantidade de gigabytes e tarefas subordinadas associadas ao trabalho.
Mensagem	Disponível para alertas e itens de registro. Esse campo de texto fornece uma mensagem descritiva do alerta ou do item de registro.

Visualizar o menu Mais de uma máquina protegida

O menu **Mais** oferece opções adicionais para ajudar a gerenciar a máquina protegida selecionada. Para acessar essas ferramentas, clique no menu suspenso Mais e selecione uma das opções descritas na tabela a seguir.

Tabela 175. Ferramentas acessíveis na opção Mais de uma máquina protegida

Elemento de UI	Descrição
Informações do sistema	Mostra informações sobre a máquina protegida, informações do sistema, volumes, processadores, adaptadores de rede e endereços IP referentes a essa máquina. Para obter mais informações, consulte Visualização das informações do sistema de uma máquina protegida.
Montagens	No painel Montagens locais, você pode visualizar ou desmontar volumes montados localmente. No painel Montagens remotas, você pode visualizar ou desmontar volumes montados usando o Local Mount Utility. Para obter informações sobre a desmontagem de volumes, consulte Desmontar pontos de recuperação. Para obter mais informações sobre a montagem local de um ponto de recuperação, consulte Montar um ponto de recuperação ou Montar um volume de ponto de recuperação em máquina Linux, respectivamente.
Política de retenção	Permite especificar uma política de retenção para a máquina selecionada. Você pode optar por usar a política padrão do Core ou diferenciar a política de retenção apenas para esta máquina. Para obter mais informações, consulte Personalizar as definições de política de retenção de uma máquina protegida.
Notificações	Permite especificar um grupo de notificação personalizado para os eventos relacionados à máquina selecionada. Isso não altera as notificações já definidas no Core. Para obter mais informações, consulte Configurar grupos de notificação.
Log do Agent	Permite baixar e visualizar o arquivo de log de uma máquina protegida usando o software Rapid Recovery Agent. Para obter mais informações, consulte Download e visualização do arquivo de log de uma máquina protegida.

Third-party contributions

This product contains the third-party components listed below. For third-party license information, go to http://quest.com/legal/license-agreements.aspx. Source code for components marked with an asterisk (*) is available at http://opensource.quest.com.

Table 176. List of third-party contributions

Component	License or acknowledgment	Notes
AlphaFS 2.0.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
AlphaVSS 1.2.4000	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
ANTLR 3.3.3	BSD ANTLR 3	Copyright (c) 2003-2007, Terence Parr A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
ANTLR 4.0.2	BSD ANTLR 4	Copyright (c) 2012 Terence Parr and Sam Harwell A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
AWS SDK for .NET 3.3.37	Apache 2.0	A copy of this license can be found at Apache 2.0.
Azure SDK for .NET 2.4	Apache 2.0	A copy of this license can be found at Apache 2.0
Bootstrap 3.0.0	Apache 2.0	Bootstrap.js by @fat & @mdo Copyright 2012 Twitter, Inc. A copy of this license can be found at Apache 2.0
Bundletransformer 1.9.138	Apache 2.0	Copyright (c) 2012-2015 Andrey Taritsyn A copy of this license can be found at Apache 2.0
Caliburn.Micro 2.0.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Castle Windsor 2.5.2	Apache 2.0	A copy of this license can be found at Apache 2.0.
Chromium 43.0.2312	Chromium BSD License N/A	Copyright 2014 The Chromium Authors. All rights reserved. A copy of this license can be found at Chromium BSD License N/A.

Component	License or acknowledgment	Notes
CLAP 4.2	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Common Library for Hyak Code Generator 1.0.2	Apache 2.0	A copy of this license can be found at Apache 2.0.
curlpp 0.7.2	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
EcmaScript.Net 1.0.1	Mozilla Public License (MPL) 1.1	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Far Manager 3.0.4242	Far Manager BSD License N/A	Copyright (c) 1996 Eugene Roshal Copyright (c) 2000 Far Group All rights reserved. A copy of this licenses can be found at Far Manager BSD License N/A.
fio 2.18*	GPL (GNU General Public License) 2.0	This component is not used in the application. It is provided with the product for customer convenience. A copy of this license can be found at GPL (GNU General Public License) 2.0.
FlotCharts 0.8.3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Google APIs Client Library for .NET 1.9.2	Apache 2.0	Copyright 2011 Google Inc A copy of this license can be found at Apache 2.0.
HTML Renderer 1.5.0.6	BSD CodePlex	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
html5-placeholder-shim.jquery.js 1.0.58	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
ISOLINUX 4.05 20120131*	GPL (GNU General Public License) 2.0	A copy of this license can be found at GPL (GNU General Public License) 2.0.
JavaScriptEngineSwitcher 1.2.4	Apache 2.0	Copyright (c) 2013-2015 Andrey Taritsyn A copy of this license can be found at Apache 2.0.
jqGrid 4.4.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jqrowl 1.2.6	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Component	License or acknowledgment	Notes
JQuery 1.8.2	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery File Upload Plugin 5	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery knob 1.2.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Templates 1.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Templates 1.0.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
JQuery UI 1.9.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Validation 1.9.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Viewport 1.0.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Viewport 1.0.0.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.fileDownload 1.3.3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.hotkeys 0.7.9	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.mCustomScrollbar 3.0.7	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquerey.mousewheel 3.1.12	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.splitter 0.14.0	GNU LGPL Version 3, 29 June 2007	Copyright (C) 2010-2013 Jakub Jankiewicz A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.tagsinput 1.3.3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Json.NET 4.5	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Component	License or acknowledgment	Notes
jsTree 1.0-rc3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.11.3*	GNU LGPL Version 3, 29 June 2007	Copyright © 2006–2015 SUSE LLC and contributors. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.12*	GNU LGPL Version 3, 29 June 2007	Copyright © 2002 Red Hat, Inc. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.15*	GNU LGPL Version 3, 29 June 2007	Copyright © 2015 Canonical Ltd. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.17*	GNU LGPL Version 3, 29 June 2007	Copyright © 2002 Red Hat, Inc. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.19*	GNU LGPL Version 3, 29 June 2007	Copyright © 2006–2015 SUSE LLC and contributors. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Libc.so.6 2.7*	LGPL (GNU Lesser General Public License) 2.1	A copy of this license can be found at LGPL (GNU Lesser General Public License) 2.1.
libext2fs 1.42.12*	GNU Lesser General Public License 2.1	Copyright (C) 1993, 1994, 1995, 1996 Theodore Ts'o. A copy of this license can be found at LGPL (GNU Lesser General Public License) 2.1.
libssh2 1.4.3	BSD-style N/A	Portions Copyright 2002-2010 Atsuhiko Yamanaka, JCraft,Inc. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Log4Net 1.2.10	Apache 2.0	A copy of this license can be found at Apache 2.0.
MarkdownSharp 1.13	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
matchMedia 2.72	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
memtest86+ 4.20*	GPL (GNU General Public License) 2.0	A copy of this license can be found at GPL (GNU General Public License) 2.0.
Microsoft Azure Compute	Apache 2.0	A copy of this license can be found at Apache 2.0.

Component	License or acknowledgment	Notes
Management Library 12.0.0		
Microsoft Reactive Extensions for .NET 2.1	Apache 2.0	A copy of this license can be found at Apache 2.0.
Moment.js 2.6.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
MongoDB 2.0.6*	GNU Affero GPL 3.0	A copy of this license can be found at GNU AFFERO GENERAL PUBLIC LICENSE
MongoDB 10gen driver 2.4.1	Apache 2.0	A copy of this license can be found at Apache 2.0.
Mono 5.2*	LGPL (GNU Lesser General Public License) 2.1	Copyright (C) 1991, 1999 Free Software Foundation, Inc. A copy of this license can be found at LGPL (GNU Lesser General Public License) 2.1.
MsieJavaScriptEngine 1.4.3*	Mozilla Public License (MPL) 1.1	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
NBD various*	GPL (GNU General Public License) 2.0	This component is not used in the application. It is provided with the product for customer convenience. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
NDesk.Options 0.2.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Newtonsoft.Json.dll 6.0.8	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
NLog 4.4.12	BSD - Kowalski 2011	Copyright (c) 2004-2011 Jaroslaw Kowalski <jaak@jkowwalski.net>. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
OpenSSL 1.1.0e	OpenSSL 1.0	This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). Copyright (c) 1998-2016 The OpenSSL Project. All rights reserved. A copy of this license can be found at OpenSSL 1.0.
OpenStack.NET 1.4.0.2	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Component	License or acknowledgment	Notes
PowerCollections 2007*	Eclipse Public License 1.0	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Prism 4.0	Microsoft patterns & practices license N/A	Contains software or other content adapted from Microsoft patterns & practices ObjectBuilder, © 2006 Microsoft Corporation. All rights reserved. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
ProductionStackTrace 1.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Protobuf-net 2.0.0.627	Apache 2.0	A copy of this license can be found at Apache 2.0.
PuTTY 0.63	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Quartz.NET 2.1.2	Apache 2.0	A copy of this license can be found at Apache 2.0.
Raphaël—JavaScript Library 2.1.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
RazorGenerator 2.1	Apache 2.0	A copy of this license can be found at Apache 2.0.
Resize Floating Popup Control Revision 3	Code Project Open License (CPOL) 1.02	A copy of this license can be found at Code Project Open License (CPOL) 1.02 .
respond.js 1.3.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
SignalR 1.2.2	Apache 2.0	Copyright (c) .NET Foundation. All rights reserved. A copy of this license can be found at Apache 2.0.
SimpleRestServices 1.2.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
SimpleRestServices 1.3.0.3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Sparsehash 1.11	BSD CodePlex	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
SSH.Net 2013.4.7	BSD CodePlex	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Component	License or acknowledgment	Notes
TextFileEncodingDetector 1.0	BSD TextFileEncodingDetector 1.0	Copyright 2002-2008 Xiph.org Foundation Copyright 2002-2008 Jean-Marc Valin Copyright 2005-2007 Analog Devices Inc. Copyright 2005-2008 Commonwealth Scientific and Industrial Research Organisation (CSIRO) Copyright 1993, 2002, 2006 David Rowe Copyright 2003 EpicGames Copyright 1992-1994 Jutta Degener, Carsten Bormann A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
trip 2.1.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Tri-state tree view Revision 9 (30-May-2011)	Code Project Open License (CPOL) 1.02	A copy of this license can be found at Code Project Open License (CPOL) 1.02 .
Virtual Box SDK 4.2.14*	LGPL (GNU Lesser General Public License) 2.1	c 2004-2015 Oracle Corporation A copy of this license can be found at LGPL (GNU Lesser General Public License) 2.1.
WebGrease 1.5.2	Apache 2.0	A copy of this license can be found at Apache 2.0.
Yahoo! UI Library: YUI Compressor .Net 2.7.0	BSD CodePlex	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
zlib 1.2.5	zlib 1.2.5	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Apache 2.0

License Text

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places:

within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Chromium BSD License N/A

License Text

Copyright 2014 The Chromium Authors. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code Project Open License (CPOL) 1.02

License Text

Preamble

This License governs Your use of the Work. This License is intended to allow developers to use the Source Code and Executable Files provided as part of the Work in any application in any form.

The main points subject to the terms of the License are:

Source Code and Executable Files can be used in commercial applications;

Source Code and Executable Files can be redistributed; and

Source Code can be modified to create derivative works.

No claim of suitability, guarantee, or any warranty whatsoever is provided. The software is provided "as-is".

The Article(s) accompanying the Work may not be distributed or republished without the Author's consent

This License is entered between You, the individual or other entity reading or otherwise making use of the Work licensed pursuant to this License and the individual or other entity which offers the Work under the terms of this License ("Author").

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CODE PROJECT OPEN LICENSE ("LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HEREIN, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE AUTHOR GRANTS YOU THE RIGHTS CONTAINED HEREIN IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO ACCEPT AND BE BOUND BY THE TERMS OF THIS LICENSE, YOU CANNOT MAKE ANY USE OF THE WORK.

Definitions.

"Articles" means, collectively, all articles written by Author which describes how the Source Code and Executable Files for the Work may be used by a user.

"Author" means the individual or entity that offers the Work under the terms of this License.

"Derivative Work" means a work based upon the Work or upon the Work and other pre-existing works.

"Executable Files" refer to the executables, binary files, configuration and any required data files included in the Work.

"Publisher" means the provider of the website, magazine, CD-ROM, DVD or other medium from or by which the Work is obtained by You.

"Source Code" refers to the collection of source code and configuration files used to create the Executable Files.

"Standard Version" refers to such a Work if it has not been modified, or has been modified in accordance with the consent of the Author, such consent being in the full discretion of the Author.

"Work" refers to the collection of files distributed by the Publisher, including the Source Code, Executable Files, binaries, data files, documentation, whitepapers and the Articles.

"You" is you, an individual or entity wishing to use the Work and exercise your rights under this License.

Fair Use/Fair Use Rights. Nothing in this License is intended to reduce, limit, or restrict any rights arising from fair use, fair dealing, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

License Grant. Subject to the terms and conditions of this License, the Author hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

You may use the standard version of the Source Code or Executable Files in Your own applications.

You may apply bug fixes, portability fixes and other modifications obtained from the Public Domain or from the Author. A Work modified in such a way shall still be considered the standard version and will be subject to this License.

You may otherwise modify Your copy of this Work (excluding the Articles) in any way to create a Derivative Work, provided that You insert a prominent notice in each changed file stating how, when and where You changed that file.

You may distribute the standard version of the Executable Files and Source Code or Derivative Work in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution.

The Articles discussing the Work published in any form by the author may not be distributed or republished without the Author's consent. The author retains copyright to any such Articles. You may use the Executable Files and Source Code pursuant to this License but you may not repost or republish or otherwise distribute or make available the Articles, without the prior written consent of the Author.

Any subroutines or modules supplied by You and linked into the Source Code or Executable Files this Work shall not be considered part of this Work and will not be subject to the terms of this License.

Patent License. Subject to the terms and conditions of this License, each Author hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, import, and otherwise transfer the Work.

Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

You agree not to remove any of the original copyright, patent, trademark, and attribution notices and associated disclaimers that may appear in the Source Code or Executable Files.

You agree not to advertise or in any way imply that this Work is a product of Your own.

The name of the Author may not be used to endorse or promote products derived from the Work without the prior written consent of the Author.

You agree not to sell, lease, or rent any part of the Work. This does not restrict you from including the Work or any part of the Work inside a larger software distribution that itself is being sold. The Work by itself, though, cannot be sold, leased or rented.

You may distribute the Executable Files and Source Code only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy of the Executable Files or Source Code You distribute and ensure that anyone receiving such Executable Files and Source Code agrees that the terms of this License apply to such Executable Files and/or Source Code. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute the Executable Files or Source Code with any

technological measures that control access or use of the Work in a manner inconsistent with the terms of this License.

You agree not to use the Work for illegal, immoral or improper purposes, or on pages containing illegal, immoral or improper material. The Work is subject to applicable export laws. You agree to comply with all such laws and regulations that may apply to the Work after Your receipt of the Work.

Representations, Warranties and Disclaimer. THIS WORK IS PROVIDED "AS IS", "WHERE IS" AND "AS AVAILABLE", WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OR GUARANTEES. YOU, THE USER, ASSUME ALL RISK IN ITS USE, INCLUDING COPYRIGHT INFRINGEMENT, PATENT INFRINGEMENT, SUITABILITY, ETC. AUTHOR EXPRESSLY DISCLAIMS ALL EXPRESS, IMPLIED OR STATUTORY WARRANTIES OR CONDITIONS, INCLUDING WITHOUT LIMITATION, WARRANTIES OR CONDITIONS OF MERCHANTABILITY, MERCHANTABLE QUALITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTY OF TITLE OR NON-INFRINGEMENT, OR THAT THE WORK (OR ANY PORTION THEREOF) IS CORRECT, USEFUL, BUG-FREE OR FREE OF VIRUSES. YOU MUST PASS THIS DISCLAIMER ON WHENEVER YOU DISTRIBUTE THE WORK OR DERIVATIVE WORKS.

Indemnity. You agree to defend, indemnify and hold harmless the Author and the Publisher from and against any claims, suits, losses, damages, liabilities, costs, and expenses (including reasonable legal or attorneys' fees) resulting from or relating to any use of the Work by You.

Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL THE AUTHOR OR THE PUBLISHER BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK OR OTHERWISE, EVEN IF THE AUTHOR OR THE PUBLISHER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Termination.

This License and the rights granted hereunder will terminate automatically upon any breach by You of any term of this License. Individuals or entities who have received Derivative Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 6, 7, 8, 9, 10 and 11 will survive any termination of this License.

If You bring a copyright, trademark, patent or any other infringement claim against any contributor over infringements You claim are made by the Work, your License from such contributor to the Work ends automatically.

Subject to the above terms and conditions, this License is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, the Author reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

Publisher. The parties hereby confirm that the Publisher shall not, under any circumstances, be responsible for and shall not have any liability in respect of the subject matter of this License. The Publisher makes no warranty whatsoever in connection with the Work and shall not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. The Publisher reserves the right to cease making the Work available to You at any time without notice

Miscellaneous

This License shall be governed by the laws of the location of the head office of the Author or if the Author is an individual, the laws of location of the principal place of residence of the Author.

If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this License, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

This License constitutes the entire agreement between the parties with respect to the Work licensed herein. There are no understandings, agreements or representations with respect to the Work not specified herein. The Author

shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Author and You.

Far Manager BSD License N/A

License Text

Copyright (c) 1996 Eugene Roshal

Copyright (c) 2000 Far Group

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions

are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

EXCEPTION:

Far Manager plugins that use only the following header files from this distribution (none or any): farcolor.hpp, farkeys.hpp, plugin.hpp, farcolorW.pas, farkeysW.pas and pluginW.pas; can be distributed under any other possible license with no implications from the above license on them.

GNU AFFERO GENERAL PUBLIC LICENSE

Version 3, 19 November 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/> Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU Affero General Public License is a free, copyleft license for software and other kinds of works, specifically designed to ensure cooperation with the community in the case of network server software.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, our General Public Licenses are intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

Developers that use our General Public Licenses protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License which gives you legal permission to copy, distribute and/or modify the software.

A secondary benefit of defending all users' freedom is that improvements made in alternate versions of the program, if they receive widespread use, become available for other developers to incorporate. Many developers of free software are heartened and encouraged by the resulting cooperation. However, in the case of software used on network servers, this result may fail to come about. The GNU General Public License permits making a modified version and letting the public access it on a server without ever releasing its source code to the public.

The GNU Affero General Public License is designed specifically to ensure that, in such cases, the modified source code becomes available to the community. It requires the operator of a network server to provide the source code of the modified version running there to the users of that server. Therefore, public use of a modified version, on a publicly accessible server, gives the public access to the source code of the modified version.

An older license, called the Affero General Public License and published by Affero, was designed to accomplish similar goals. This is a different license, not a version of the Affero GPL, but Affero has released a new version of the Affero GPL which permits relicensing under this license.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU Affero General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component,

and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from

a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms. "Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available

network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Remote Network Interaction; Use with the GNU General Public License.

Notwithstanding any other provision of this License, if you modify the Program, your modified version must prominently offer all users interacting with it remotely through a computer network (if your version supports such interaction) an opportunity to receive the Corresponding Source of your version by providing access to the Corresponding Source from a network server at no charge, through some standard or customary means of facilitating copying of software. This Corresponding Source shall include the Corresponding Source for any work covered by version 3 of the GNU General Public License that is incorporated pursuant to the following paragraph.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the work with which it is combined will remain governed by version 3 of the GNU General Public License.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU Affero General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU Affero General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU Affero General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU Affero General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.> Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU Affero General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Affero General Public License for more details.

You should have received a copy of the GNU Affero General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If your software can interact with users remotely through a computer network, you should also make sure that it provides a way for users to get its source. For example, if your program is a web application, its interface could display a "Source" link that leads users to an archive of the code. There are many ways you could offer source, and different solutions will be better for different programs; see section 13 for the specific requirements.

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU AGPL, see <http://www.gnu.org/licenses/>.

GPL (GNU General Public License) 2.0

License Text

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its

contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS"

WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

LGPL (GNU Lesser General Public License) 2.1

License Text

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is

especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will

automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

OpenSSL 1.0

License Text

License

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

==========

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

/

Sobre nós

Somos mais do que um nome

Estamos em uma jornada para fazer com que a tecnologia da informação trabalhe ainda mais por você. É por isso que criamos soluções de software voltadas para a comunidade que ajudam você a gastar menos tempo com administração de TI e mais tempo em inovação para os negócios. Ajudamos a modernizar seu data center, implantar as soluções na nuvem de forma mais rápida e fornecer a experiência, a segurança e a acessibilidade necessárias para desenvolver seus negócios orientados aos dados. Aliados ao convite da Quest para que a comunidade global participe dessa inovação e ao nosso firme compromisso para garantir a satisfação do cliente, continuamos a oferecer soluções que causam impacto real na vida dos nossos clientes e deixam um legado do qual nos orgulhamos. Estamos desafiando o panorama atual transformando a nossa empresa em uma nova empresa de software. E, como seu parceiro, trabalhamos incansavelmente para garantir que sua tecnologia da informação seja projetada para e por você. Essa é a nossa missão, e estamos juntos nisso. Bem-vindo à nova Quest. Você foi convidado a participar da inovação™.

Nossa marca, nossa visão. Juntas.

Nosso logotipo reflete nossa história: inovação, comunidade e suporte. Uma parte importante dessa história começa com a letra Q. É um círculo perfeito, que representa nosso compromisso com a precisão e a força tecnológica. O espaço no próprio Q simboliza nossa necessidade de adicionar a parte que falta (você) à comunidade, à nova Quest.

Contato com a Quest

Para perguntas sobre vendas ou outras questões, acesse https://www.quest.com/contact.

Recursos de suporte técnico

O suporte técnico está disponível para clientes da Quest com um contrato de manutenção válido e clientes que estão usando versões de teste. Acesse o Portal de suporte da Quest em https://support.quest.com.

O Portal de suporte fornece ferramentas de autoajuda, que você pode usar para resolver problemas de forma rápida e independente, 24 horas por dia, 365 dias por ano. O Portal de suporte permite que você:

- Envie e gerencie uma solicitação de serviço.
- Visualize artigos da Base de conhecimento.
- Inscreva-se para receber notificações de produtos.
- Faça o download de software e documentação técnica.
- Assista a vídeos de instruções.
- Participar de discussões comunitárias.
- Converse com engenheiros de suporte on-line.
- Visualize serviços para ajudá-lo com o nosso produto