

Quest®



Appliance de gestion des systèmes KACE® 11.1

## **Notes de publication**



# Table des matières

<b>Notes de publication de l'appliance de gestion des systèmes Quest® KACE® 11.1.....</b>	<b>3</b>
À propos de l'appliance de gestion des systèmes KACE 11.1.....	3
Nouvelles fonctionnalités.....	3
Améliorations.....	5
Problèmes résolus.....	6
Problèmes recensés.....	10
Configuration requise.....	12
Licence du produit.....	12
Instructions d'installation.....	13
Préparation de la mise à jour.....	13
Mise à jour du serveur de l'appliance de gestion des systèmes KACE à partir d'une mise à jour annoncée.....	14
Téléchargement et application manuelle d'une mise à jour.....	15
Tâches à effectuer après la mise à jour.....	15
Vérification du bon déroulement de la mise à jour.....	15
Vérification des paramètres de sécurité.....	16
Ressources supplémentaires.....	16
Globalisation.....	17
Qui nous sommes.....	17
Ressources du support technique.....	17
Mentions légales.....	18

# Notes de publication de l'appliance de gestion des systèmes Quest® KACE® 11.1

---

Ce document fournit des informations sur la version 11.1 de l'appliance de gestion des systèmes KACE.

## À propos de l'appliance de gestion des systèmes KACE 11.1

L'appliance de gestion des systèmes KACE est une appliance virtuelle conçue pour automatiser la gestion des périphériques, le déploiement des applications, l'application des correctifs, la gestion du parc informatique et la gestion des tickets du Service Desk. Pour plus d'informations sur la série d'appliances de gestion des systèmes KACE, consultez la page <https://www.quest.com/products/kace-systems-management-appliance/>. Cette version contient de nouvelles fonctions, des résolutions de problèmes et des améliorations relatives à la sécurité.



**REMARQUE:** Il s'agit du seul document traduit pour cette version. Toutefois, les variantes localisées n'incluent pas les informations sur les problèmes résolus, les améliorations et les problèmes connus. D'autres guides, tels que le *guide de l'administrateur* et l'aide relative au produit ne sont pas localisés pour le moment, et les documents de la version 10.2 sont inclus.

## Nouvelles fonctionnalités

Cette version de l'appliance de gestion des systèmes KACE comprend les fonctionnalités suivantes.

### Communications de l'appareil

- **Ajout de la barre d'état système de l'agent KACE :** plus de fonctionnalités ajoutées à l'icône de l'agent dans la barre d'état système, comme l'ouverture de liens. Les administrateurs système peuvent définir jusqu'à dix liens qui apparaissent dans le nouvel élément de menu **Raccourcis**. Cet élément de menu apparaît uniquement lorsqu'un ou plusieurs liens sont définis dans les paramètres de communication de l'agent, dans la section Raccourcis de l'icône d'état de l'agent.

Les liens URI (Uniform Resource Identifier) standard sont pris en charge, tels que les URL HTTP, SSH et FTP. En cliquant sur ce lien, votre système lance l'application associée à la ressource sélectionnée. Par exemple, lorsque vous cliquez sur un lien de type HTTP, votre système ouvre le lien dans le navigateur par défaut.

- **Inventaire Hyper-V :** des informations d'inventaire et des commandes d'appareil connexes ont été ajoutées dans cette version pour les données relatives à Virtual Machine Manager et MS Hyper-V, pour les appareils gérés par l'agent. Les détails de l'inventaire comprennent une liste des machines virtuelles et des

hôtes Hyper-V à répertorier. Cette fonction est similaire à celle de l'inventaire VMware proposée à partir de la version 10.0.

- **Mises à jour de la prise en charge des systèmes d'exploitation** : l'appliance prend désormais en charge les versions suivantes des systèmes d'exploitation sur les appareils gérés par l'agent :
  - MS Windows 10 20H2
  - MS Windows Server 2019 20H2
  - macOS 11.0
    - Lors de la connexion à **Console utilisateur** à l'aide de HTTPS à partir d'un système macOS 11.0, l'appliance ne peut pas déterminer l'identifiant unique (KUID) de l'agent associé à ce système. Cela a un impact sur la liste *Mes appareils* et les installations de la bibliothèque de logiciels. La cause première de ce problème est la nouvelle exigence de macOS 11.0 selon laquelle tous les paramètres de confiance des certificats doivent être approuvés par l'utilisateur. Ce problème entraîne également l'apparition de l'entrée suivante dans le fichier `konea.log` de l'agent :

```
|ERROR|ssl_darwin.go:107:AddCertAsTrustedRoot |
SecTrustSettingsSetTrustSettings failed|{"err":"The authorization was
denied since no user interaction was possible."}
```
    - L'appliance ne prend pas en charge les correctifs du système d'exploitation pour cette version. L'application de correctif est possible. L'application de correctif au niveau du système d'exploitation pour les appareils macOS 11.0 est possible avec le Cloud KACE Mobile Device Manager (MDM), si vous disposez d'un abonnement.

#### Application de correctif

- **Mises à niveau du package Linux** : l'appliance vous permet maintenant d'automatiser le processus d'installation et de gestion des mises à jour des packages Linux qui tiennent le système d'exploitation Linux à jour sur vos appareils Linux RedHat, SUSE, Ubuntu, CentOS et Raspbian gérés. Ces mises à niveau améliorent les performances globales de vos appareils Linux gérés et les protègent contre les failles de sécurité potentielles.

Utilisez cette fonctionnalité pour créer des calendriers de mise à niveau qui vous permettent soit de détecter les mises à niveau des packages, soit de détecter et de mettre à niveau tous les packages concernés. Vous pouvez vérifier la liste des mises à niveau de package disponibles après une action de planification de détection uniquement, pour chaque version de Linux.

Le processus de mise à niveau repose sur l'hypothèse que vos appareils Linux gérés pointent vers les référentiels de packages appropriés. Seuls les packages incluant des mises à jour de sécurité sont identifiés. L'appliance ne tente pas de détecter ou de mettre à niveau tous les packages, ni de mettre à niveau l'ensemble du système d'exploitation vers la dernière version.

**i** **REMARQUE:** Raspbian Linux ne fait pas de distinction entre les mises à jour régulières et les mises à jour de sécurité. La détection et la mise à niveau des packages pour les appareils Raspbian gérés entraîne l'installation de tous les packages mis à jour sur ces appareils.

- **Intégration avec le nouveau catalogue de mises à jour matérielles Dell** : à partir de cette version, l'appliance utilise une nouvelle version du catalogue matériel Dell. Le processus de détection et de déploiement des mises à jour matérielles est très similaire à celui utilisé pour l'application des correctifs aux appareils. Commencez par créer des mises à jour programmées pour détecter et/ou déployer les mises à jour matérielles. Vous pouvez vérifier la liste des mises à jour Dell disponibles sur la page du catalogue. Cette page répertorie les mises à jour pour lesquelles des fichiers de signature existent sur l'appliance.
  - Cette fonctionnalité requiert la dernière version de l'agent KACE pour fonctionner sur les appareils Dell gérés.
  - Les données existantes liées aux mises à jour matérielles Dell, telles que l'historique des planifications, ne sont pas migrées depuis les versions antérieures de l'appliance.
  - Les rapports utilisateur associés aux mises à jour matérielles Dell et créés avec une version précédente de l'appliance ne sont pas migrés vers la version 11.1.

## Infrastructure

- **Oval pour Linux et Mac** : dans cette version, l'appliance étend la prise en charge d'Oval au-delà du seul MS Windows existant en utilisant la plus vaste et la meilleure sélection de données CVE au monde.
- **Alertes de renouvellement de licence** : lorsque la maintenance de l'appliance expire, certaines fonctionnalités, telles que la prise en charge des correctifs, ne sont plus disponibles. Cela entraîne une alerte d'erreur sur le tableau de bord Accueil. Pour renouveler votre licence, rendez-vous sur <https://support.quest.com/contact-us/renewals>.

## Service Desk

- **Hiérarchie des catégories de tickets du Service Desk** : la console de l'administrateur a été améliorée pour vous permettre de simplifier la configuration des catégories et sous-catégories pour le Service Desk. Vous pouvez créer et modifier les nœuds de catégories et sous-catégories de tickets à l'aide d'un widget arborescent. L'arborescence vous permet de mieux comprendre et gérer les relations entre les catégories. Vous pouvez facilement ajouter de nouveaux nœuds de catégorie, les renommer, les supprimer ou les trier, selon vos besoins. Une fonction de recherche est également disponible, pour trouver rapidement une catégorie ou une sous-catégorie spécifique.
- **Possibilité de spécifier le préfixe du ticket du Service Desk** : à partir de cette version, vous pouvez utiliser un préfixe différent pour chaque file d'attente afin d'organiser le workflow de votre Service Desk et de les associer aux catégories applicables, telles que `HELP` : pour le centre d'assistance ou `HDREQ` : pour les demandes de matériel et de logiciels.
- **Prise en charge du service Microsoft 365 GCC High** : vos identifiants OAuth pour MS Office 365 vous permettent désormais de définir votre type de client Azure AD et l'URL du point de terminaison, afin d'acquérir les jetons pour le Cloud national associé à votre environnement. Lorsque vous sélectionnez un OAuth pour Office 365 pour les e-mails entrants du Service Desk, vous pouvez utiliser un service d'API Microsoft 365 applicable, tel que Microsoft 365 GCC, Microsoft 365 GCC High et autres. Microsoft 365 GCC High, en particulier, est utilisé dans les environnements de haute sécurité.

# Améliorations

La liste ci-dessous répertorie les améliorations apportées à cette version.

Amélioration	ID du problème
Windows Installer now preserves the <code>NoHooks userinit</code> registry setting during upgrade.	K1A-2393
Managed Installation can continue if the Agent disconnects.	K1A-2392
KACE Agent no verifies the Konea tunnel and alerts the server if broken.	K1A-2384
The user is alerted when reboot is pending and patching operations are skipped as a result.	K1A-2381
11.1 KACE macOS agents use PKG installer file rather than DMG disk image.	K1A-2374
API access can now be restricted through the <i>Access Control List Details</i> page.	K1-30596
This version includes the ability to sort by custom ticket fields in KACE GO.	K1-30562

Amélioration	ID du problème
SAML-enabled systems can now be locked down to allow access only to SAML-authenticated users and the local <code>admin</code> user.	K1-30246
This version includes an option to reject SAML users who do not already have an account on the appliance.	K1-30211
<i>Approval Status</i> column is added to the <i>Quarantine</i> list and <i>Quarantine Detail</i> pages.	K1-30105
In the <i>General Settings</i> page, an option is added to indicate interest in participation in a future Beta program.	K1-30071
The appliance now includes the ability to select an Azure AD <i>GCC High account</i> during the creation of credentials for a Office365 OAuth account, and to set the URL endpoint for a <code>.us</code> domain.	K1-22281
In the email notification text editor, the <b>\$</b> button now allows insertion of tokens.	K1-22082
Added the ability to select a <i>single-tenant</i> Azure AD account type during the creation of credentials for a Office365 OAuth account.	K1-21914
User's manager can now be reset to <i>Unassigned</i> either manually through the <b>Console d'administration</b> , or during LDAP import with an empty manager mapped field.	K1-19328
Discovery schedules for devices associated with an Active Directory server, now include a new option for enabling the appliance to use a secure port for LDAP communication, <b>Use Secure LDAP (LDAPS)</b> . This check box is available in the <i>Active Directory</i> section on the <i>Discovery Schedule Detail</i> page, when you select <b>Active Directory</b> as the <i>Discovery Type</i> .	N/A
Access Control List restrictions can be now applied based on sub-domains. You can specify the sub-domain name on the <i>Access Control List</i> page, in the <i>IP Address/Domain</i> column of the <i>Allow List</i> .	N/A

## Problèmes résolus

La liste ci-dessous répertorie les problèmes résolus dans cette version.

### Resolved Service Desk issues

Problème résolu	ID du problème
Creating a Service Desk process template that included a separator could result in an error when used from the User Portal.	K1-30698
<i>Time Closed</i> , <i>Time Stalled</i> and <i>Time Opened</i> are not updated for a parent ticket with approvals.	K1-30685
When copying text from a Word application to a ticket, the formatting could not be retained.	K1-30545

Problème résolu	ID du problème
When duplicating a process, the ticket template was not duplicated.	K1-30460
Tickets with very long summary fields could result in an error when the <i>Tickets</i> list page loads.	K1-23726
Default ticket template is not set when creating a new ticket by email.	K1-23422
Unexpected rendering behavior (scrolling) could be seen when viewing ticket details when multiple categories and sub-categories are present.	K1-22645
In the Service Desk list view, <i>Time Open</i> and <i>Time Opened</i> are renamed to <i>Time Since Last Opened</i> and <i>Last Opened</i> , respectively.	K1-22630
Emails sent with display names with a comma or multi-language character to a Service Desk queue through POP3 was not handled correctly, in some cases.	K1-22610
Image was broken using several variables in email templates.	K1-21347
<i>Email On Event</i> ticket notification emails were formatted differently than Custom Ticket Rule emails.	K1-21198
Default value was not displayed on ticket detail page for drop-down fields with <i>Always Required</i> option.	K1-21187
Service Desk: Token emails from Gmail to Gmail leaved behind empty spaces.	K1-21186
When a ticket is submitted by email with embedded dark colors, the text was hidden if the <b>Console d'administration</b> is also set to a dark theme.	K1-21147
Process parent ticket did not close if child tickets were closed from <i>Tickets</i> list view.	K1-21143
Service Desk email notifications broke if templates exceeded character limits.	K1-21118
Advanced Search: Filters did not work as expected when using Unassigned Owner.	K1-21116
Advanced Search in <i>Tickets</i> list: Filters did not work as expected when using <i>Status</i> and <i>Process Status</i> .	K1-21107
Populating a Service Desk ticket multi-selection custom field with double quotes in the select value resulted in unexpected behavior.	K1-21094
Ticket attachment links sent in email notifications did not work as expected in some cases.	K1-19964

#### Resolved KACE Agent issues

Problème résolu	ID du problème
CentOS receives all updates with the Linux Update feature. The security filter is not available for the Linux Package Upgrades page.	K1A-3810

<b>Problème résolu</b>	<b>ID du problème</b>
KACE Agent 11.0 failed to download file from HTTPS source, impacting use of replication shares that are accessed through the HTTPS protocol.	K1A-2330
Client certificate install operation could timeout on newly provisioned Windows devices, preventing the agent from receiving any commands from the appliance until a reconnect event happened.	K1A-2329
VMM managed Hyper-V host was not added to appliance during VMM inventory when the Agent is installed on some Hyper-V hosts.	K1A-2328
Replication did work when password had an '@' symbol.	K1A-2326
macOS 11.0 (Big Sur): Installing KACE Agent with the Agent Status icon enabled resulted in warnings during installation.	K1A-2318
<code>konea.exe</code> and <code>clientidentifier.exe</code> could crash in some environments.	K1A-2291
Recurring Alert messages kept spawning new Windows on endpoint.	K1A-2289
Wake-on-LAN (WoL) through relay did not display error when the relay agent selected was down.	K1A-2285
Tokens were treated as invalid by agents (error: Agent token signed by another server) if the appliance database became out of sync with the file system.	K1-30642
SNMP inventory data from Dell servers could cause inventory to fail.	K1-30615
In the <b>Console d'administration système</b> , on the <i>Agent Token Detail</i> page, <i>Organization</i> is represented with its ID instead of name.	K1-29969
Offline KScripts did not run when scheduled for <i>Run on the instance/day of week</i> .	K1-21173
MSI Policy wizard script could fail to set the registry value correctly.	K1-21049
Scripting option <i>Allow run without a logged-in user</i> cleared still allowed script to run.	K1-19576
SMB URLs did not properly handle passwords with special characters.	K1-17342

#### Resolved Inventory issues

<b>Problème résolu</b>	<b>ID du problème</b>
SNMP inventory mistakenly identified non-hex strings as hex strings, causing incorrect values in some cases.	K1-30668
Dell Warranty retrieval errors were not logged to the new <code>dell_warranty_log</code> error file.	K1-30531
Overdue Service Desk widgets included tickets that were not yet overdue.	K1-30480

Problème résolu	ID du problème
In the <b>Quarantine</b> list page, it was not possible to view the details of a quarantined device.	K1-24508
Viewing script logs from the <i>Device Detail</i> page displayed blank logs.	K1-21349
<b>Reset Tries</b> button in <i>Windows Feature Updates Status</i> on <i>Device Detail</i> page did not always work.	K1-21172
<i>Gateway IP Address</i> was not an available column on the <i>Devices</i> list page.	K1-21131
Machine deletion could lead to software installation counts being inaccurate.	K1-20437
No history was tracked when Smart Label was edited.	K1-17612

#### Other resolved issues

Problème résolu	ID du problème
The <i>Windows Feature Update Summary</i> page did not correctly list all updates, in some cases.	K1-30887
Knowledge Base articles with multiple labels could be hidden for users.	K1-30671
LDAP Import: Scheduled imports set to <i>None</i> could still run automatically.	K1-30666
<i>Compliance by Patch</i> and <i>Compliance by Machine</i> widgets sometimes did not display correct values.	K1-30630
Images did not appear correctly in knowledge base articles, in some cases.	K1-30565
Emails with multiple CC's sent to a Service Desk queue through a POP3 server could not be handled correctly.	K1-30533
File attachments of type .eml or .msg were missing from tickets submitted by email.	K1-30527
Managed Installation with <b>Override default installation</b> configured would show <b>Default installation</b> set after saving.	K1-30481
An error could be seen while creating custom view on the <i>Quarantine</i> page in the <b>Console d'administration système</b> .	K1-29978
<b>Do not associate file</b> Managed Installation option was not displayed correctly after saving.	K1-29927
In some cases, the network settings for the proxy settings were not honored by the Credential manager when using an Office365 OAuth account.	K1-29063
Access to the <b>Console d'administration</b> could be disrupted when changing an organization's virtual IP address or host name.	K1-25452

Problème résolu	ID du problème
Email sent to Service Desk queues that use a multi-part MIME format could fail to parse correctly.	K1-22656
When a non-administrative queue owner attempts to retrieve the list of Service desk tickets using the API, tickets they did not submit could be omitted from the results.	K1-22653
SFTP- and FTP-specific <i>Offboard Backup Transfer Settings</i> fields containing backslashes caused offboard backup failure.	K1-22608
The <i>Object History</i> page sometimes failed to load when it contained Windows Feature Update data.	K1-21575
Agent upstream tunnel client certificate validation failed when an aging konea certificate was archived.	K1-21354
In KACE GO it was not possible to accept barcode searches that have embedded spaces or new line characters.	K1-21195
SAML LDAP attribute mapping option could cause authentication failures.	K1-21193
Asset import did not change Assignee information.	K1-21185
Code can now be saved in the <i>Notes</i> field of KScripts.	K1-21184
Monitoring: Create Ticket in Profile configuration did not select proper queue ID.	K1-21175
Search on <i>Device Issues</i> page did not function as expected.	K1-21169
SAML: Editing SP Metadata for <code>NameIDFormat</code> did not save changes.	K1-21139
Unexpected behavior observed when trying to map and update <i>Manager</i> field using SAML.	K1-21102
Default role for new users did not always honor the role chosen in <i>Settings</i> .	K1-21082
<i>Alternate location</i> for Managed Installation was not used behind a replication share.	K1-21016
Location was unassigned on asset when a new or previously removed device connects.	K1-20468
The <b>Generate Self-Signed Certificate</b> button was incorrectly enabled before the configuration information was saved in the SSL wizard.	K1-18300

## Problèmes recensés

L'existence des problèmes suivants est connue à la date de cette publication.

Problème recensé	ID du problème
KACE Agent for SUSE 11.1 requires <code>libxslt</code> to be installed in order to install. This is a newly introduced dependency.	K1A-3813
Disk Usage history is not recorded by a macOS KACE Agent of an APFS file system.	K1A-3805
The appliance reports the MS Windows 10 build number 20H2 through its technical release version of 2009.	K1A-3803
Dell Updates: Custom View does not report any results when Smart Label is a criteria.	K1-31860
Email attachments in <code>.eml</code> and <code>.msg</code> file format are marked as <i>discarded</i> if subject contains slashes <code>'/</code> .	K1-31786
Linux package upgrades: <i>Deploy All</i> can push some updates that change system configuration which requires manual reconfiguration, such as on Ubuntu 18.04LTS (Desktop version with UI).	K1-31770
KACE GO: Non-admin queue owners cannot to set ticket device/asset to arbitrary device.	K1-31764
Windows Feature Update (WFU) schedule fails when using a deployment type of <i>Detect and Stage</i> type and the Agent version is 10.2.	K1-31743
Wake-on-LAN (WoL) options are not present in the <b>Choose Action</b> menu on the <i>Device Detail</i> page for supported devices.	K1-31729
Duplicating patch schedule from list of schedules does not work as expected.	K1-31714
Duplicating Dell Updates schedule from list of schedules does not work as expected.	K1-31713
Users with no queue permissions cannot see tickets they are CC-ed on.	K1-31710
Downloading status count is not displayed in <i>Patch Schedules</i> list page.	K1-31066
<i>Managed Installation Detail</i> page incorrectly shows that PKG files cannot be used.	K1-30820
Patching step with reboot in <i>Task Chain</i> shows Failed status.	K1-30812
Patch schedule with On-Demand Deploy ends Task Chain task when staging is completed.	K1-30811
Patch schedule information is not showing correctly after disabling a patch schedule.	K1-30733
Schedule information is not showing correctly after disabling a Linux package upgrade schedule.	K1-30725
Pasting an image into a knowledge base article causes other pasted images to reset alignment and justification.	K1-30721

Problème recensé	ID du problème
Package download process incorrectly updates offline <i>Last Modified</i> instead of <i>Last Update</i> status.	K1-30588
Invalid filters (Smart Labels) can be saved, resulting in Smart Labels that never populate.	K1-20268

## Configuration requise

La version minimale requise pour installer l'appliance de gestion des systèmes KACE 11.1 est la version 11.0. Si votre appliance exécute une version antérieure, vous devez d'abord effectuer la mise à jour vers la version indiquée avant de procéder à l'installation.

La version minimale requise pour effectuer la mise à niveau de l'agent KACE est la version 10.2. Nous vous recommandons d'utiliser la dernière version de l'agent avec l'appliance de gestion des systèmes KACE 11.1.



**REMARQUE:** Le package RPM de l'agent KACE peut être installé sur les appareils SUSE Linux gérés uniquement lorsque le package `libxslt-tools` est installé avant le package de l'agent.

Pour vérifier le numéro de version de l'appliance, connectez-vous à la page **Console d'administration** et cliquez sur **Besoin d'aide**. Dans le panneau Aide qui s'affiche, en bas, cliquez sur le bouton entouré « i ».

Avant de procéder à la mise à niveau vers la version 11.1 ou d'installer cette version, vérifiez que votre système répond aux exigences minimales. Ces exigences figurent dans les spécifications techniques de l'appliance de gestion des systèmes KACE.

- Pour les appliances virtuelles : rendez-vous sur <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-virtual-appliances/>.
- Pour KACE en tant que service : rendez-vous sur <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-kace-as-a-service/>.

## Licence du produit

Aucune licence supplémentaire n'est requise si vous possédez une licence de produit de l'appliance de gestion des systèmes KACE.

Si vous utilisez l'appliance de gestion des systèmes KACE pour la première fois, vous trouverez les informations relatives à la licence dans le guide d'installation de l'appliance. Rendez-vous sur [Ressources supplémentaires](#) pour accéder au guide approprié.



**REMARQUE:** les licences de produit correspondant à la version 11.1 doivent être utilisées exclusivement sur les appliances de gestion des systèmes KACE qui exécutent la version 11.1 ou une version ultérieure. Les licences correspondant à la version 11.1 ne peuvent être utilisées avec des appliances exécutant une version antérieure, comme la version 10.0.

# Instructions d'installation

Vous pouvez appliquer cette version à partir d'une mise à jour annoncée ou en téléchargeant et en appliquant manuellement un fichier de mise à jour. Pour obtenir des instructions, reportez-vous aux rubriques suivantes :

- [Préparation de la mise à jour](#)
- [Mise à jour du serveur de l'appliance de gestion des systèmes KACE à partir d'une mise à jour annoncée](#)
- [Téléchargement et application manuelle d'une mise à jour](#)
- [Tâches à effectuer après la mise à jour](#)



**REMARQUE:** afin de garantir la précision de la découverte des logiciels et du nombre d'installations pour les appareils exécutant un logiciel en particulier, à partir de la version 7.0 de l'appliance de gestion des systèmes KACE, le catalogue de logiciels se réinstallera après chaque mise à niveau.

## Préparation de la mise à jour

Avant de procéder à la mise à jour du serveur de l'appliance de gestion des systèmes KACE, suivez ces recommandations :

- **Vérifiez la version du serveur de l'appliance de gestion des systèmes KACE :**

La version minimale requise pour installer l'appliance de gestion des systèmes KACE 11.1 est la version 11.0. Si votre appliance exécute une version antérieure, vous devez d'abord effectuer la mise à jour vers la version indiquée avant de procéder à l'installation.

Pour vérifier le numéro de version de l'appliance, connectez-vous à la page **Console d'administration** et cliquez sur **Besoin d'aide**. Dans le panneau Aide qui s'affiche, en bas, cliquez sur le bouton entouré « i ».

- **Vérifiez la version de votre agent KACE.**

La version minimale requise pour effectuer la mise à niveau de l'agent KACE est la version 10.2. Nous vous recommandons d'utiliser la dernière version de l'agent avec l'appliance de gestion des systèmes KACE 11.1.



**REMARQUE:** Le package RPM de l'agent KACE peut être installé sur les appareils SUSE Linux gérés uniquement lorsque le package `libxslt-tools` est installé avant le package de l'agent.

- **Effectuez une sauvegarde avant de commencer.**

Sauvegardez votre base de données et vos fichiers, et enregistrez vos sauvegardes sur un support extérieur au serveur de l'appliance de gestion des systèmes KACE, pour pouvoir y accéder ultérieurement. Pour des instructions sur la sauvegarde de votre base de données et de vos fichiers, consultez le document **Administrator Guide** (Guide de l'administrateur) à l'adresse <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/>.

- **Appliances installées avant la version 7.0.**

Pour les appliances initialement installées avant la version 7.0 qui n'ont pas été réimaginees (appliances physiques) ou réinstallées (virtuelles), Quest Software recommande fortement d'exporter, de recréer (une installation d'image ou de machine virtuelle à partir d'un fichier OVF) et réimporter la base de données avant de mettre à niveau vers la version 11.1. Pour plus d'informations, rendez-vous sur <https://support.quest.com/kace-systems-management-appliance/kb/111810/how-to-re-image-the-k1000-appliance>.

Si la version de votre appliance a de nombreuses versions de retard, l'article suivant contient des conseils utiles concernant la mise à niveau : <https://support.quest.com/kace-systems-management-appliance/kb/155574/upgrading-a-kace-systems-management-appliance-that-is-multiple-versions-behind-upgrade-path-6-x-to-10-0->.

Les raisons pour lesquelles vous devriez réimager l'appliance sont nombreuses. La nouvelle disposition du disque, par exemple, offre une meilleure compatibilité avec la version 11.1. Elle présente également une meilleure sécurité et de meilleures performances.

Pour déterminer si votre système bénéficierait d'une telle mise à niveau, vous pouvez utiliser un fichier `KBIN` pour déterminer l'âge exact de votre appliance et de la disposition de son disque. Pour télécharger le fichier `KBIN`, consultez <https://support.quest.com/kace-systems-management-appliance/kb/210267/how-to-run-the-kace-systems-management-appliance-configuration-report>.

- **Assurez-vous que le port 52 231 est disponible.**

Avant toute mise à niveau `.kbin`, le port 52 231 doit être disponible afin que la page de la console de mise à niveau KACE soit accessible. Si la mise à niveau est lancée sans que ce port ne soit disponible, vous ne pourrez pas suivre la progression de la mise à niveau. Quest KACE vous recommande fortement d'autoriser le trafic vers l'appliance via le port 52231 depuis un système de confiance et de suivre la mise à niveau à l'aide de la Console de mise à niveau. Sans accès à la Console de mise à niveau, la mise à niveau renvoie vers une page inaccessible qui indique dans le navigateur une expiration du délai de réponse. La personne en charge peut alors croire à un plantage du système dû à la mise à niveau, la conduisant à redémarrer alors que la mise à niveau est en réalité toujours en cours. En cas de doute sur la progression de la mise à niveau, contactez le support KACE et **ne redémarrez pas l'appliance**.

## Mise à jour du serveur de l'appliance de gestion des systèmes KACE à partir d'une mise à jour annoncée

Vous pouvez effectuer la mise à jour du serveur de l'appliance de gestion des systèmes KACE en appliquant une mise à jour annoncée, dans la section *Tableau de bord* ou *Mises à jour de l'appliance* de la page **Console d'administration**.

**MISE EN GARDE:** Ne redémarrez jamais le serveur de l'appliance de gestion des systèmes KACE manuellement pendant une mise à jour.

1. Sauvegardez votre base de données et vos fichiers. Pour obtenir des instructions, consultez le **Guide de l'administrateur**, <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/>.
2. Accédez au *Panneau de configuration* de l'appliance :
  - Si le composant **Organisation** n'est pas activé sur votre appliance, cliquez sur **Paramètres**.
  - Si le composant **Organisation** est activé sur l'appliance, procédez comme suit : connectez-vous à la page **Console d'administration système** de l'appliance à l'adresse : `http://nom_hôte_KACE_SMA/system` ou sélectionnez **Système** dans la liste déroulante figurant en haut à droite de la page, puis cliquez sur **Paramètres**.
3. Dans la barre de navigation de gauche, cliquez sur **Mises à jour de l'appliance** pour afficher la page *Mises à jour de l'appliance*.
4. Cliquez sur **Rechercher des mises à jour**.  
Le journal présente les résultats de la vérification.
5. Lorsqu'une mise à jour est disponible, cliquez sur **Mise à jour**.

**IMPORTANT:** au cours des dix premières minutes, certains navigateurs peuvent donner l'impression de se bloquer pendant la décompression et la vérification de la mise à jour. Pendant cette procédure, ne quittez pas la page, ne l'actualisez pas et ne cliquez sur aucun des boutons du navigateur de cette page car ces actions interrompraient la procédure. Une fois la mise à jour décompressée et vérifiée, la page *Journaux* s'ouvre. Ne redémarrez jamais l'appliance manuellement pendant la procédure de mise à jour.

La version 11.1 est appliquée et le serveur de l'appliance de gestion des systèmes KACE redémarre. La progression s'affiche dans la fenêtre du navigateur et sur la page **Console d'administration**.

6. Une fois la mise à niveau du serveur terminée, mettez à niveau tous de vos agents vers la version 11.1.

## Téléchargement et application manuelle d'une mise à jour

Si vous disposez d'un fichier de mise à jour fourni par Quest, vous pouvez le télécharger manuellement pour mettre à jour le serveur de l'appliance de gestion des systèmes KACE.

**!** **MISE EN GARDE: Ne redémarrez jamais le serveur de l'appliance de gestion des systèmes KACE manuellement pendant une mise à jour.**

1. Sauvegardez votre base de données et vos fichiers. Pour obtenir des instructions, consultez le **Guide de l'administrateur**, <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/>.
2. Connectez-vous au site Web de Quest à l'adresse <https://support.quest.com/kace-systems-management-appliance/download-new-releases> à l'aide de vos informations d'identification, téléchargez le fichier `.kbin` du serveur de l'appliance de gestion des systèmes KACE correspondant à la version 11.1 GA (disponibilité générale) et enregistrez localement ce fichier.
3. Dans la barre de navigation de gauche, cliquez sur **Mises à jour de l'appliance** pour afficher la page *Mises à jour de l'appliance*.
4. Dans la section *Mettre à jour manuellement* :
  - a. Cliquez sur **Parcourir** ou sur **Sélectionner un fichier**, puis accédez au fichier de mise à jour.
  - b. Cliquez sur **Mise à jour**, puis sur **Oui** pour confirmer.

La version 11.1 est appliquée et le serveur de l'appliance de gestion des systèmes KACE redémarre. La progression s'affiche dans la fenêtre du navigateur et sur la page **Console d'administration**.

5. Une fois la mise à niveau du serveur terminée, mettez à niveau tous de vos agents vers la version 11.1.

## Tâches à effectuer après la mise à jour

Après la mise à jour, vérifiez que celle-ci s'est déroulée avec succès et vérifiez les paramètres selon les besoins.

## Vérification du bon déroulement de la mise à jour

Pour vous assurer que la mise à jour s'est déroulée avec succès, vérifiez le numéro de version de l'appliance de gestion des systèmes KACE.

1. Accédez au *Panneau de configuration* de l'appliance :
  - **Si le composant Organisation n'est pas activé sur votre appliance, cliquez sur Paramètres.**
  - **Si le composant Organisation est activé sur l'appliance, procédez comme suit : connectez-vous à la page Console d'administration système de l'appliance à l'adresse : `http://nom_hôte_KACE_SMA/system` ou sélectionnez **Système** dans la liste déroulante figurant en haut à droite de la page, puis cliquez sur Paramètres.**
2. Pour vérifier la version actuelle, cliquez sur **Besoin d'aide** en haut à droite de la page, puis dans le panneau Aide qui s'affiche, en bas, cliquez sur le bouton entouré « i ».

## Vérification des paramètres de sécurité

Afin de renforcer la sécurité, l'accès à la base de données via HTTP et FTP est désactivé pendant la mise à jour. Si vous utilisez cette méthode pour accéder aux fichiers de base de données, vous devrez modifier les paramètres de sécurité après la mise à jour.

1. Accédez au *Panneau de configuration* de l'apppliance :
    - Si le composant **Organisation** n'est pas activé sur votre appliance, cliquez sur **Paramètres**.
    - Si le composant **Organisation** est activé sur l'apppliance, procédez comme suit : connectez-vous à la page **Console d'administration système de l'apppliance** à l'adresse : `http://nom_hôte_KACE_SMA/system` ou sélectionnez **Système** dans la liste déroulante figurant en haut à droite de la page, puis cliquez sur **Paramètres**.
  2. Dans la barre de navigation de gauche, cliquez sur **Paramètres de sécurité** pour afficher la page *Paramètres de sécurité*.
  3. Dans la section supérieure de la page, modifiez les paramètres suivants :
    - **Activer les fichiers de sauvegarde sécurisés** : décochez cette case pour permettre aux utilisateurs d'accéder aux fichiers de sauvegarde de base de données via HTTP sans authentification.
    - **Activer l'accès à la base de données** : cochez cette case pour permettre aux utilisateurs d'accéder à la base de données sur le port 3306.
    - **Activer la sauvegarde via FTP** : cochez cette case pour permettre aux utilisateurs d'accéder aux fichiers de sauvegarde de base de données via FTP.
- !** **MISE EN GARDE:** la modification de ces paramètres n'est pas recommandée car elle réduit la sécurité de la base de données.
4. Cliquez sur **Enregistrer**.
  5. **Mises à niveau KBIN uniquement.** Renforcez l'accès par mot de passe racine (2FA) à l'apppliance.
    - a. Dans la Console d'administration système, cliquez sur **Paramètres > Support**.
    - b. Sur la page *Support*, sous *Outils de dépannage*, cliquez sur **Authentification à deux facteurs**.
    - c. Sur la page *Authentification à deux facteurs du support*, cliquez sur **Remplacer la clé secrète**.
    - d. Enregistrez les jetons et placez ces informations dans un endroit sûr.

## Ressources supplémentaires

Des informations supplémentaires sont disponibles parmi les sources suivantes :

- Documentation du produit en ligne (<https://support.quest.com/kace-systems-management-appliance/11.1/technical-documents>)
    - **Spécifications techniques** : informations concernant les exigences minimales d'installation et de mise à niveau vers la dernière version du produit.
- Pour les appliances virtuelles** : rendez-vous sur <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-virtual-appliances/>.

**Pour KACE en tant que service** : rendez-vous sur <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-kace-as-a-service/>.

- **Guides d'installation** : instructions d'installation des appliances virtuelles. Rendez-vous sur <https://support.quest.com/kace-systems-management-appliance/11.1/technical-documents> pour accéder à la documentation relative à la version la plus récente.
- **Guide de l'administrateur** : instructions concernant l'utilisation de l'appliance. Rendez-vous sur <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/> pour accéder à la documentation relative à la version la plus récente.

## Globalisation

Cette section contient des informations concernant l'installation et le fonctionnement de ce produit dans les configurations autres qu'en langue anglaise utilisées, par exemple, par des personnes extérieures à l'Amérique du Nord. Cette section ne remplace pas les informations relatives aux plateformes et configurations prises en charge que vous retrouverez dans d'autres parties de la documentation du produit.

Cette version est au format Unicode et est compatible avec tous les jeux de caractères. Dans cette version, tous les composants du produit doivent être configurés afin d'utiliser les mêmes codages de caractères, ou des codages compatibles, et ils doivent être installés de manière à utiliser les mêmes options locales et régionales. Cette version peut être utilisée dans les régions suivantes : Amérique du Nord, Europe Occidentale et Amérique Latine, Europe Centrale et Orientale, Asie Orientale, Japon.

La version est disponible dans les langues suivantes : allemand, espagnol, français, japonais, portugais (Brésil).

## Qui nous sommes

Quest crée des solutions logicielles qui rendent tangibles les avantages des nouvelles technologies, dans un environnement IT de plus en plus complexe. De la gestion des bases de données et des systèmes à la gestion d'Active Directory et d'Office 365, en passant par la résilience de la cybersécurité, Quest aide ses clients à relever, dès maintenant, leur prochain défi IT. Dans le monde entier, plus de 130 000 entreprises, dont 95 % des entreprises du classement Fortune 500, comptent sur Quest pour assurer une gestion et un suivi proactifs de leur prochaine initiative, pour trouver la solution aux prochains défis complexes de Microsoft et pour garder une longueur d'avance sur la prochaine menace. Quest Software. Quand le présent rencontre le futur. Pour plus d'informations, visitez le site [www.quest.com](http://www.quest.com).

## Ressources du support technique

Le support technique est disponible pour les clients Quest disposant d'un contrat de maintenance valide et les clients qui utilisent des versions d'évaluation. Vous pouvez accéder au portail du support technique Quest à l'adresse <https://support.quest.com/fr-fr/>.

Ce portail propose des outils d'auto-dépannage qui vous permettront de résoudre des problèmes rapidement et sans aide extérieure, 24 h/24 et 365 j/an. Il permet d'effectuer les opérations suivantes :

- Soumettre et gérer une demande de service
- Consulter les articles de la base de connaissances
- Vous inscrire pour recevoir des notifications sur les produits
- Télécharger des logiciels et de la documentation technique
- Visionner des vidéos de procédure
- Participer aux discussions de la communauté
- Discuter en ligne avec des ingénieurs du support technique
- Découvrir des services capables de vous aider avec votre produit

## Mentions légales

© 2021 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (<https://www.quest.com>) for regional and international office information.

### Brevets

Chez Quest Software, nous sommes fiers de notre technologie avancée. Des brevets et des brevets en attente peuvent s'appliquer à ce produit. Pour obtenir les informations les plus récentes sur les brevets applicables à ce produit, visitez notre site Web à l'adresse <https://www.quest.com/legal>.

### Trademarks

Quest, the Quest logo, Join the Innovation, and KACE are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. All other trademarks and registered trademarks are property of their respective owners.

### Légende



**MISE EN GARDE:** une icône MISE EN GARDE indique un risque de dommage causé au matériel ou de perte de données si les instructions ne sont pas respectées.



**IMPORTANT, REMARQUE, CONSEIL, MOBILE ou VIDÉO:** une icône d'information indique la présence de renseignements supplémentaires.

Notes de publication de l'appliance de gestion des systèmes KACE

Date de mise à jour : avril 2021

Version logicielle - 11.1