Quest®

Quest® InTrust 11.3.2

Preparing for Auditing and Monitoring Solaris

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.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation 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.

Legend

! **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

i **IMPORTANT**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

InTrust Preparing for Auditing and Monitoring Solaris
Updated - June 2018
Version - 11.3.2

Contents

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.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation 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.

Legend

! **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

i **IMPORTANT**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

InTrust Preparing for Auditing and Monitoring Solaris
Updated - June 2018
Version - 11.3.2

Contents

Solaris Auditing and Monitoring Overview

The Solaris Knowledge Pack expands the auditing and reporting capabilities of InTrust to Oracle (formerly, Sun) Solaris. The Knowledge Pack enables InTrust to work with Syslog, text logs, and the Solaris Audit log.

The following table shows what you can audit and monitor on Solaris:

Data Source	Gathering	Real Time Monitoring
Syslog messages	X	X
Text logs of any format	X	
Configuration file modification	X	X
Solaris audit logs generated by Basic Security Module (BSM)	X	

For Solaris Syslog, there is an agent-free approach to gathering, which is not covered in this guide. It involves Syslog forwarding to an InTrust server. For details about this method, see Setting Up Gathering of Syslog Data.

Requirements

For details about Solaris versions that InTrust can audit and monitor, see Solaris Events.

Installation

The Solaris Knowledge Pack must be installed on top of an existing InTrust installation. The following objects are included:

- Data sources:
  - Solaris Syslog
  - Solaris Audit Log
  - Solaris Accounts Monitoring
  - Solaris Text Files Monitoring
  - Gathering policies:
  - Solaris: Security: Common Syslog Security Events

    - Solaris: Security: Failed Logons
    - Solaris: Security: Successful Logons
    - Solaris: Security: SU Activity
    - Solaris: Security: Reboots
    - Solaris: All Syslog Messages
    - Solaris: logins/logouts from Audit Log
    - Solaris: process execution events from Audit Log
    - Solaris: filesystem events from Audit Log
    - Solaris: All Events from Audit Log
    - Solaris: Accounts monitoring
    - Solaris: Text files monitoring
- Import policies:
    - Solaris: Security: Common Syslog Security Events
    - Solaris: Security: Failed Logons
    - Solaris: Security: Successful Logons
    - Solaris: Security: SU Activity
    - Solaris: Security: Reboots
    - Solaris: All Syslog Messages
    - Solaris: logins/logouts from Audit Log
    - Solaris: process execution events from Audit Log
    - Solaris: filesystem events from Audit Log
    - Solaris: All Events from Audit Log
    - Solaris: Accounts monitoring
    - Solaris: Text files monitoring
- Consolidation policies:
    - Solaris Logs Consolidation
    - Solaris Logs Consolidation for the Last Month
- Tasks:
    - Solaris Syslog—daily collection of important security events
    - Solaris audit log daily collection
    - Solaris configuration changes daily collection
    - Solaris weekly reporting
- "Solaris hosts" site
- "Solaris: security" Real-time monitoring policies:

- Predefined reports belonging to the following categories (for complete list of reports and report descriptions, refer to the InTrust Reports for Sun Solaris document):
  - Administrative Activity
  - Forensic Analysis
  - Normal User Activity

Installing Agents

InTrust agents must be installed manually on Solaris hosts. For details, see Installing Agents Manually on Solaris Computers.

Preparing Audit Trails

InTrust takes advantage of the following logging systems available on Solaris:

- Syslog
- Basic Security Module (BSM)

Syslog provides data for auditing and real-time monitoring activities. Basic Security Module data is used only for auditing.

This topic describes the configuration requirements that InTrust imposes on these systems.

Configuring Syslog

Syslog is an important logging facility in Solaris. Syslog functionality is provided by the syslogd daemon, which accepts messages from various sources that support logging, and either writes these messages to files or passes them on to other hosts in the network.

The InTrust agent processes the message flow before it arrives at syslogd's input. However, the agent catches only the local messages; it does not catch messages redirected from other computers over the network. Therefore, do not rely on syslogd’s message redirection feature if you audit and monitor Syslog with InTrust. InTrust support for the Solaris Syslog depends on local messages.

It is up to you how you configure syslogd logging. This configuration does not affect the operation of the InTrust agent, which provides all the Syslog data that InTrust accepts.

Configuring Basic Security Module

Basic Security Module (BSM) in Solaris provides logging capability and stores system events in the Solaris Audit log. This section describes how to prepare BSM for InTrust operations.

To enable Basic Security Module Auditing

1. Switch to run level 1 (System Maintenance Mode) using the following command:
   ```
   /usr/sbin/init 1
   ```

2. Enable BSM auditing with the following command:

   ```
   /etc/security/bsmconv
   ```

   When the system prompts you for confirmation, enter **Y**.

   If you want to customize logging options, edit the Basic Security Module configuration files at this stage. The configuration files are listed further on.

3. Reboot the system.

   When the system is rebooted, a message similar to the following will be displayed during the startup process to indicate that auditing has been enabled:

   ```
   starting audit daemon
   Configured 233 kernel events.
   ```

   At this point, auditing is enabled, and a log file should be present in the **/var/audit** directory.

If BSM functionality is no longer required on a Solaris system, you can disable it using the **bsmunconv** command.

> **NOTE:** When the **bsmconv** command is run, it disables the **Stop-a** keyboard sequence by adding **set abort_enable = 0** to the **/etc/system** file. Disabling the ability of a user or administrator to stop a system through a keyboard **Stop-a** or equivalent command over a serial port may not be appropriate for all environments.

BSM Configuration Files

The following table describes the BSM configuration files. For detailed information about configuring BSM, visit http://www.oracle.com/technetwork/indexes/documentation/index.html.

File	Description
audit_class	An audit class is a group of audit events. All audit classes are defined in the **/etc/security/audit_class** file. All audit events are assigned to audit classes in the/etc/security/audit_event file. Audit classes are recorded in the audit trail if they are turned on globally in the audit_control file, or are assigned to a specific user in the audit_user database. These audit classes are used by the audit_control, audit_user, and audit_event files, as well as in the audit mask.
audit_control	The **/etc/security/audit_control** file describes system parameters for auditing. These parameters include the following: • Audit trail storage directory (or directories) • Minimum free space warning value • Audit flags assigned to user and system processes It is possible to audit only failed audit events or only successful audit events. For example, you can specify that a successful attempt to allocate memory should not be recorded but that a failed attempt should be recorded. This can be specified in either the **audit_control** or **audit_user** files.

File	Description
audit_event	The **/etc/security/audit_event** file defines the audit events and assigns each event to one or more audit classes. For additional information on the **audit_event** file, refer to the **audit_event** man page.
audit_user	The **/etc/security/audit_user** file enables you to specify additional auditing for individual users. Access to this database follows the rules for the password database specified in **/etc/nsswitch.conf**.

NOTE: The InTrust agent does not modify the contents of token fields it retrieves from the Solaris Audit log. However, information in these fields is not sufficient if you store Solaris Audit log data in a centralized way.

The agent complements this information by adding InTrust-specific fields to tokens. These fields are filled in by resolving the values of some fields for the current Solaris host.

InTrust Configuration

After you have taken all the necessary configuration steps on the target Solaris hosts, the InTrust Manager snap-in takes over all auditing and real-time monitoring operations. This section describes Solaris-specific settings that are not explained in the other InTrust documentation.

Data Sources

The “Solaris Syslog” and “Solaris Audit Log” data sources represent the Solaris audit trails—Syslog and Basic Security Module log, respectively. The "Solaris text files monitoring" and “Solaris accounts monitoring” data sources work with files that are not audit trails.

Solaris Syslog

Syslog auditing and real-time monitoring is based on the flow of data intended for the syslogd daemon. The “Solaris Syslog” data source is used to analyze the data flow and capture only the necessary portions of it.

This data source uses a list of regular expressions. When the data source is working, it applies the expressions, in the order specified, to each message. The order of the regular expressions matters because message processing stops as soon as the message matches one of the expressions.

When parsing takes place, pairs of parentheses are used in regular expressions to break messages up into numbered fields.

For example, the following regular expression:

```
^(.{15}) ([-[:alnum:]_.]+) (su)(\[[0-9]*\]){0,1}: \[ID ([0-9]+) [a-z]+\.[a-z]+\] ('su
(.*)' succeeded for (.*) on (.*))
```

matches the following message:

```
Dec 16 07:29:28 r5 su: [ID 366847 auth.notice] 'su root' succeeded for jsmith
on /dev/pts/1
```

The result is an event with the following fields:

Field Name	Field Number	Field Contents
Computer	<2>	r5
Description	<6>	‘su root’ succeeded for jsmith on /dev/pts/1
Event ID	<5>	366847
Event Source	<3>	su
Insertion String #1	<6>	‘su root’ succeeded for jsmith on /dev/pts/1
Insertion String #11	<7>	root
Insertion String #12	<8>	jsmith

The last regular expression in the predefined data source is designed to match any message. This ensures that the message is not lost. The result of this regular expression is an event where the Description and Insertion String #1 fields both contain the descriptive part of the message, if a descriptive part is present.

It is not recommended that you modify predefined regular expressions in the data source. These expressions are required for the reports that come with the Solaris Knowledge Pack. These reports will ignore any data resulting from the use of custom regular expressions.

If you create a custom Syslog data source with your own regular expressions, make sure you use customized reports based on the data that these regular expressions help capture.

> CAUTION: **Including a lot of complex regular expressions in the data source may slow down Syslog processing significantly.**

Text File-Monitoring Data Sources

The “Solaris text files monitoring” and “Solaris accounts monitoring” scripted data sources are designed to parse specified files. Real-time monitoring rules use these data sources to monitor the files for changes.

CAUTION: These scripted data sources are not designed for general-purpose auditing and monitoring of text-based logs. They should be used only on configuration files that preferably do not exceed 100 kilobytes. To collect large text-based logs, use Custom Text Log Events data sources, as described in the Auditing Custom Logs with InTrust document.

To specify the file paths, edit the appropriate parameters of the data sources. For example, to monitor the /etc/hosts.allow and /etc/hosts.deny files, take the following steps:

1. Open the properties of the “Solaris text files monitoring” data source.
2. On the **Parameters** tab, select the **TextFiles** parameter and click **Edit**.
3. Supply “**/etc/hosts.allow**” and “**/etc/hosts.deny**” in the dialog box that appears.

Similarly, you can edit the UsersFile and GroupsFile parameters of the “Solaris accounts monitoring” data source if the location of the passwd and groups files differs from the default on your Solaris hosts.

> NOTE: Monitoring the **passwd** and **groups** files makes sense if your Solaris environment does not use a directory solution. With a directory in place, information in these files is not important or representative.

External Events Data Sources

The External Events data source type is not represented by any predefined data sources. It is different from other data source types in that it generates event records with fields that you define and hands them over to the InTrust agent to process.

Data sources of this type are represented by a command-line utility on the agent side and an InTrust data source object on the InTrust server side.

This command-line utility forces special events on the InTrust agent running on the same computer. The agent stores the events in its backup cache. From there, the events can be captured by the gathering or real-time monitoring engine.

To create an External Events data source

1. Right-click the **Configuration | Data Sources** node and select **New Data Source**.
2. In the New Data Source Wizard, select the **External Events** data source type.
3. Complete the remaining steps.

For details about External Events data source settings, see Configuring Data Sources.

Script Event Provider Data Sources

InTrust provides an additional option to create a custom data source using the Script Event Provider.

This functionality allows you to create a script that starts with pre-set frequency. Under some conditions that are specified in this script events are generated and then are passed to the InTrust agent. Events are stored in the agent's backup cache. From there, the events can be captured by the gathering or real-time monitoring engine.

You can specify in the certain script: what information is stored and how it is ordered in the certain events, what conditions are required for event generation.

To create a custom data source with Script Event Provider

1. Right-click the **Configuration | Data Sources** node and select **New Data Source**.
2. In the New Data Source Wizard, select the **Script Event Provider** data source type.
3. On the Script step select the script language and enter your script text using XML editor.
4. On the same step specify a frequency of the script running.
5. Complete the remaining steps.

Auditing, Reporting, and Real-Time Monitoring

Solaris auditing, reporting, and real-time monitoring is similar to working with any other system supported by InTrust. There is only one important difference that refers to active scheduling of the InTrust tasks—see the warning note below.

> ! CAUTION: **An active schedule is required to make the agent cache events. If the schedule is disabled, no events are stored. Since all data sources described above (except "Solaris Audit Log") use events caching, it is recommended that you use at least one task for the cache-enabled data sources that run regularly. If you want to gather data only on demand, you must still enable the schedule for your task or tasks, but set it to a point in the future or in the past.**

The other Solaris auditing, reporting and real-time monitoring operations do not have special requirements, and you can perform them as described in the Auditing Guide and Real-Time Monitoring Guide.

Use Scenarios

This topic describes typical situations in a production environment and outlines how InTrust helps handle them:

- Syslog Configuration Monitoring
- Tracking Resource Access

For information about specific procedures, such as creating tasks and jobs or activating rules, see the Auditing Guide and Real-Time Monitoring Guide.

Syslog Configuration Monitoring

Suppose you use a finely-tuned Syslog audit policy in your environment. Your audit configuration has proven efficient and reliable, and you do not want anyone but a few trusted administrators to be able to change it. Even so, you want to know immediately if the audit policy is modified in any way.

Use InTrust real-time monitoring capabilities to enable immediate notification. Syslog audit configuration is defined in the **syslog.conf** file, so the solution in this case is to monitor this file with InTrust and send an alert whenever the file is modified.

Enable the “Syslog.conf file modified” rule and supply the appropriate file paths as the rule's parameter.

Tracking Resource Access

In this scenario, one of your Solaris hosts stores production-critical files. You want to be notified whenever these files are accessed. Take the following steps to track access to your files using InTrust:

1. Make sure that Basic Security Module policy is configured to capture file-related events.
2. Create a weekly InTrust task that includes gathering of relevant Solaris Audit log events and reporting on them.
   If you like, you can store the gathered data in an InTrust repository. You can also include a notification job to inform you of task completion.
   Include the “File access” report in the reporting job, and supply the appropriate paths in the Files filter. The resulting reports are stored in the local folder that is specified during InTrust installation (for details see the Deployment Guide).

Now you can use Knowledge Portal to view a weekly report indicating who accessed your critical files, when they were accessed, and whether they were modified.

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product