Quest® InTrust 11.6.0

Preparing for Auditing One Identity Privilege Manager for Sudo

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 One Identity Privilege Manager for Sudo
Updated - November 2023
Version - 11.6.0

Contents

One Identity Privilege Manager for Sudo Auditing Overview

In enterprises One Identity Privilege Manager for Sudo helps administer Sudo and manage privileged access through **sudo** in order to meet highest compliance and security requirements. Providing comprehensive auditing of privileged access through **sudo** across all of the systems managed by Privilege Manager for Sudo is vital for raising individual accountability and achieving compliance goals set by external regulations and internal security policy requirements. InTrust complements Privilege Manager for Sudo auditing capabilities by collecting logs produced by Privilege Manager for Sudo and building reports based on collected log data.

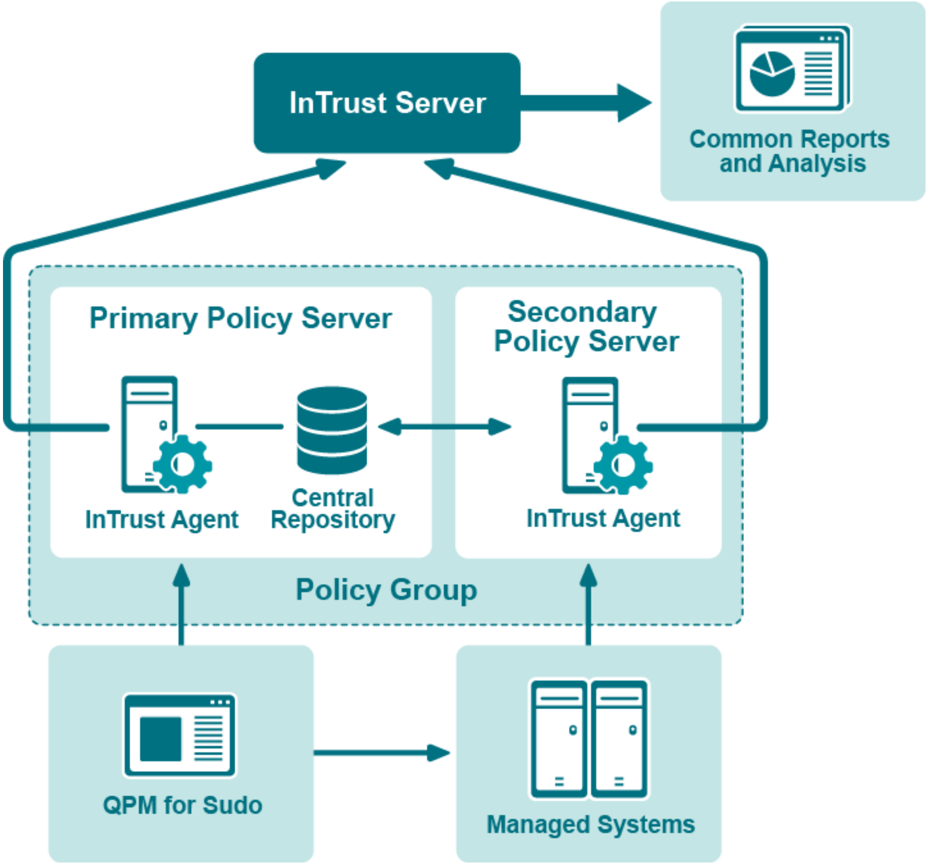
To integrate InTrust with Privilege Manager for Sudo, use the InTrust Knowledge Pack for One Identity Privilege Manager for Sudo that is provided.

Benefits of Using InTrust

When integrated with Privilege Manager for Sudo, InTrust brings new, powerful means of automating and streamlining your auditing workflow:

- **Long-term data storage, archival, and backup.** With InTrust, you can use file-based or Centera-based repositories to store Privilege Manager for Sudo logs in a compressed form for any period of time; extract events from the repository for on-going reporting needs. These features help organizations comply with external regulations and internal policies.
- **Exploration and representation** of Privilege Manager for Sudo logs in InTrust Repository Viewer with the following benefits:
  - Quick and interactive full-text search
  - Fields detection and field-based search
  - Grouping, sorting and charting of information
- **Consolidation of various log sources** to allow comprehensive analysis of privileged users activity, such as
  - Logon events from Windows DCs and logon session events from Windows workstations
  - Events from native logs residing on UNIX/Linux hosts managed by Privilege Manager for Sudo
  - Changes to Active Directory, File Systems, Exchange objects and other infrastructure components and IT data captured by the Change Auditor family of products.

The following figure shows how Privilege Manager for Sudo and InTrust work together:



How Integration Works

Communication between the components takes place as follows:

1. InTrust agent installed on Privilege Manager for Sudo master host transmits all Syslog events from the host to InTrust default repository.
2. Privilege Manager for Sudo events in InTrust Repository events in InTrust Repository are normalized into a common representation not requiring expert knowledge of events.
3. As a result, data from Privilege Manager for Sudo can be tracked using any of the following:
   - Repository Viewer (for ad-hoc searches and forensic analysis)
   - Knowledge Portal (for interactive and schedule based reporting)

Getting Started

Step 1. Install InTrust with Privilege Manager for Sudo Knowledge Pack

First of all, you need to install InTrust in your environment. In order to work with Privilege Manager for Sudo, make sure that during setup you selected the Privilege Manager for Sudo Knowledge Pack to install with InTrust.

> ! CAUTION: **In addition to the Privilege Manager for Sudo Knowledge Pack, you need to install the Knowledge Pack for Linux or at least one of the Unix systems supported by InTrust.**

For detailed guidelines on installing InTrust, refer to the InTrust Deployment Guide.

Predefined Objects

The Privilege Manager for Sudo Knowledge Pack installation brings the following objects to InTrust:

- Data source: “Privilege Manager for Sudo Syslog”
- Gathering policy: “Privilege Manager for Sudo: All Syslog Events”
- Import policy: “Privilege Manager for Sudo: All Syslog Events”
- Tasks: “Privilege Manager for Sudo Syslog - daily collection", "Privilege Manager for Sudo weekly reporting”
- Site: “Privilege Manager for Sudo master hosts”

Step 2. Install the Agent

You need to install an InTrust agent on any Privilege Manager for Sudo master host from which you need to gather audit data. Currently, InTrust supports installing agent on master hosts running one of the following operating systems:

- Red Hat Enterprise Linux version
- Red Hat Enterprise Linux (64-bit edition) version

- SuSE Enterprise Server version 10 and 11
- SuSE Enterprise Server (64-bit edition) version 10 and 11

For details about installing the InTrust agent on any of these operating systems, see Installing Agents Manually.

Step 3. Establish a Connection with InTrust Server

See Establishing a Connection with the Server in Installing Agents Manually.

Step 4. Add Agent to Site on InTrust Server

To add the agent to your InTrust site, take the following steps:

1. In **Quest InTrust Manager | Configuration | Sites | Unix Network**, right-click the **Privilege Manager for Sudo master hosts** node and then click **Add | Computer**.
2. Type in the name of agent previously installed on step 2.

NOTE: To view agents registered for this InTrust server, open **Quest InTrust Manager | Configuration | InTrust Servers | <*Server Name*> | Agents** node in the left-pane.

3. Click **Commit** on the toolbar to apply changes.

Step 5. Enable Schedule for Daily Collection Task

To enable schedule for the daily collection task, take the following steps:

1. In **Quest InTrust Manager | Workflow | Tasks | Predefined tasks**, right-click **Privilege Manager for Sudo Syslog - daily collection** and select **Properties**.
2. Select the **Schedule Enabled** check box and click **OK**.
3. Click **Commit** button on the toolbar to apply changes.

Step 6. Run Daily Collection Task

To start collecting events from Privilege Manager for Sudo master hosts, right-click the: **Privilege Manager for Sudo Syslog - daily collection** in the left-pane and then click **Run**.

This task collects all events from Privilege Manager for Sudo and stores the events in the default repository. To view current state of the task, use the **Workflow | Sessions** node in the left pane.

When daily collection task is finished, you can open InTrust Repository Viewer and start processing event data according to your needs. For possible use case scenarios, follow information from the Usage Scenario section.

Step 7. Run Weekly Reporting Task

To import all Privilege Manager for Sudo events from the default repository to the default database and then build reports, you need to run weekly reporting task as follows:

1. Select the **Privilege Manager for Sudo - weekly reporting** task in the left pane, and then select the **Privilege Manager for Sudo reporting** on the right.
2. Open the **Delivery** tab and configure the **Export to the shared folder** and **Save report as type** options according to your needs.
3. Click the **Commit** button on the toolbar to apply changes.
4. To start building reports based on events collected on previous step, right-click the **Privilege Manager for Sudo - weekly reporting** in the left-pane and then click **Run**.

To view current state of the task, use the **Workflow | Sessions** node in the left-pane.

When weekly reporting task is finished, you can view reports stored in place, selected on the **Delivery** tab of the reporting job.

Usage Scenario

This topic describes a typical situation in a production environment and shows how InTrust with the Privilege Manager for Sudo Knowledge Pack help handle it.

Suppose you need to get information whether an unauthorized person tried to access passwords using the **passwd** command on particular hosts managed by Privilege Manager for Sudo.

To do that, in Repository Viewer open repository to which InTrust collects logs from Privilege Manager for Sudo, and then take the following steps:

1. Select the **Auditing Unix and Linux | Auditing Privilege Manager for Sudo | All events by Submit user** predefined search.
2. If necessary, perform additional configuration for the predefined search. For instance, you may change the **When** field value according to your needs.
3. Use the **Where** field to narrow down the scope of hosts on which suspicious password access might take place.
4. After that, in the Search Filter pane click **Add or Remove Parameters**, select **Named Insertion Strings** from the drop-down list and then select the **Command line** parameter. Close the **Select Filter Parameters** dialog box.
5. Specify **Contains "passwd"** as a **Command line** parameter value.

Now you can review resulting list of events to find suspicious password access events.

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

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