Quest

Quest® InTrust 11.4.1

Preparing for Auditing TPAM

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.

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

InTrust Preparing for Auditing TPAM
Updated - April 2019
Version - 11.4.1

Contents

TPAM Auditing Overview

In enterprises Quest Total Privileged Access Management (TPAM) appliance controls privileged identity management and privileged access control in order to meet highest compliance and security requirements. Providing comprehensive auditing of privileged user activity across all of the systems managed by TPAM is vital for raising individual accountability and achieving compliance goals set by external regulations and internal security policy requirements. InTrust complements TPAM auditing capabilities by collecting logs produced by TPAM and correlating them with other native logs residing on Windows and Unix/Linux systems.

InTrust can help you track sys-admin and user activity recorded by TPAM, password and session requests from TPAM users, and also monitor TPAM appliance state. This is enabled through configuring InTrust to collect TPAM logs transmitted to a Syslog server.

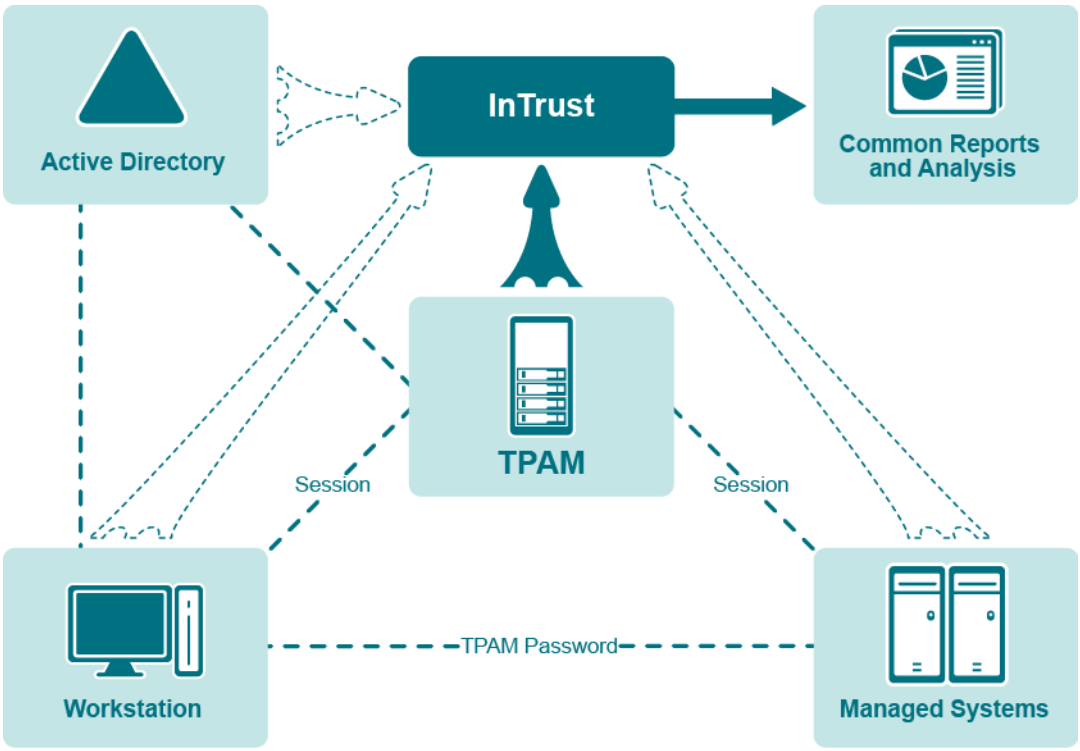
To integrate InTrust with TPAM, use the InTrust Knowledge Pack for TPAM that is provided.

Benefits of Using InTrust

When integrated with TPAM, 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 TPAM 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 TPAM 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 TPAM
    - 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 TPAM and related systems work together.



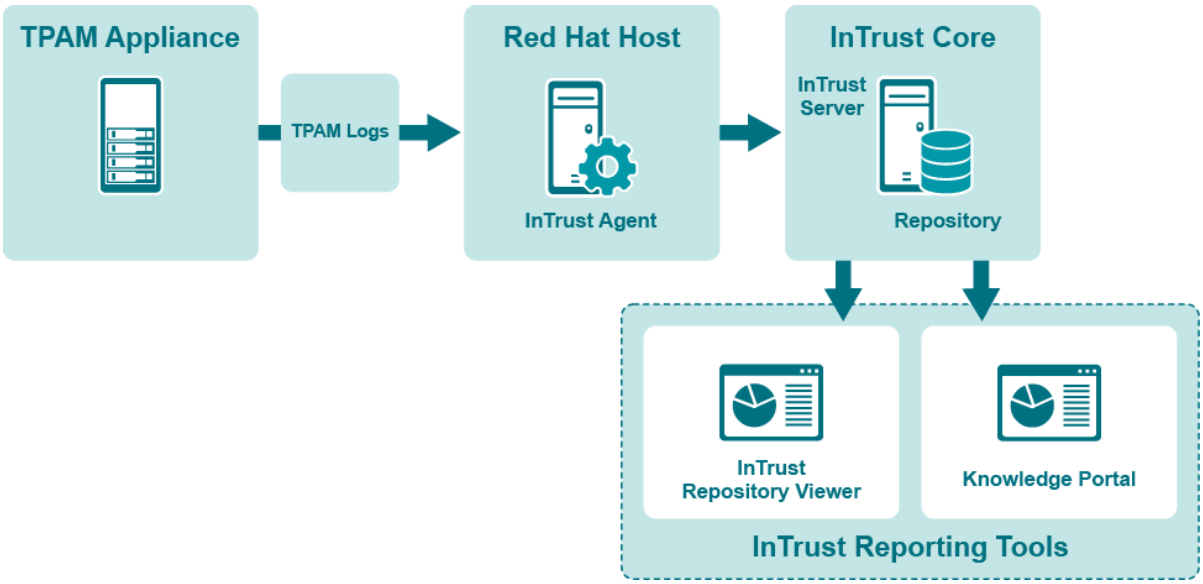
Note that in addition to collecting TPAM logs, InTrust can also collect logs from related systems, such as hosts managed by TPAM, workstations from which users connect to TPAM and Active Directory domain controllers where TPAM users reside. For more information about that, refer to the corresponding InTrust documentation.

How Integration Works

Communication between the components takes place as follows:

1. TPAM logs such as user and sys-admin activity are forwarded to a Red Hat or Oracle Linux host with installed InTrust agent acting as a Syslog listener.
2. Then logs are parsed on InTrust side and put into the InTrust repository.
3. TPAM events in InTrust Repository are normalized into a common representation not requiring expert knowledge of events.
4. As a result, data from TPAM can be tracked using one of the following:
    - Repository Viewer (for ad-hoc searches and forensic analysis)
    - Quest Knowledge Portal (for interactive and schedule based reporting)

This scenario is shown in the following diagram.


TPAM Appliance
TPAM Logs
Red Hat Host
InTrust Agent
InTrust Core
InTrust Server
Repository
InTrust Repository Viewer
Knowledge Portal
InTrust Reporting Tools

Getting Started

Step 1. Install InTrust with TPAM Knowledge Pack

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

> **CAUTION: The Linux Knowledge Pack must be installed for InTrust in addition to the TPAM Knowledge Pack.**

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

Predefined Objects

The TPAM Knowledge Pack installation brings the following objects to InTrust:

- Data source: “TPAM through Red Hat Linux Syslog”
- Gathering policy: “TPAM: All Syslog Events”
- Task: TPAM Syslog - daily collection“”
- Site: “TPAM hosts”

Step 2. Configure TPAM Log Forwarding

InTrust takes advantage of the Syslog logging system on TPAM appliance. Syslog provides data for auditing activities.

In order to collect TPAM logs using InTrust, TPAM administrator should configure TPAM to forward log messages to a Linux host running one of the supported by InTrust versions of Red Hat Enterprise Linux or

Oracle Linux on which you plan to install the InTrust agent later. That Linux host with the InTrust agent will act as a Syslog listener.

For information on how to configure the logs to be sent to the Syslog server, refer to TPAM documentation.

IMPORTANT: TPAM provides the **Include Source: ApplianceName in syslog message** option in its Syslog configuration settings. For InTrust to be able to collect TPAM events, this option must be turned off. If it is enabled, matching will fail for the resulting Syslog messages.

Step 3. Allow Syslog Reception on Linux Host

You need to permit the Syslog daemon to receive logs from the TPAM appliance on the Red Hat or Oracle Linux host to which you forwarded logs on step 2. For that, perform the *Enabling Reception of External Syslog Messages* procedure described in the Syslog Configuration topic

After this, you should be ready to receive events from TPAM.

Step 4. Install the Agent

You need to install an InTrust agent on the Red Hat Enterprise Linux or Oracle Linux host to which you forwarded logs on step 2. For details, see Installing Agents Manually on Linux Computers.

Step 5. Establish a Connection with InTrust Server

To establish a connection between an agent and an InTrust server, see the procedure in the Establishing a Connection with the Server topic.

Step 6. Add Agent to Site on InTrust Server

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

1. In **Quest InTrust Manager | Configuration | Sites | Unix Network**, right-click the **TPAM hosts** node and then click **Add | Computer**.
2. Type in the name of agent previously installed on step 4.

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 7. Enable Schedule for Daily Collection Task

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

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

Step 8. Run Daily Collection Task

To start collecting events that the Linux host receives from the TPAM appliance, right-click **Syslog - daily collection** in the left pane and then click **Run**.

This task collects all events from TPAM appliance 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 Scenarios topic.

Usage Scenarios

This chapter describes typical situations in a production environment and how InTrust with the TPAM Knowledge Pack help handle them, as follows:

- Observing TPAM Session Requests
- Tracking User Activity in Environment

Information in this section implies that you are familiar with InTrust repositories and Repository Viewer. For detailed information on browsing InTrust repositories with Repository Viewer, refer to Understanding InTrust Repositories and Searching for Events in Repository Viewer.

Observing TPAM Session Requests

Suppose for a security reason you need to check whether and when (if applicable) a specific user had access to a particular host through TPAM session. Given that you have configured TPAM and InTrust intercommunication as described in the Getting Started topic, you can solve this task as follows:

1. Open Repository Viewer to browse data stored in your repository
2. Use the predefined search named TPAM session requests (last 24 hours) located under **Auditing Unix and Linux | Auditing TPAM**. This search will find all events related to TPAM session requests which were generated during last 24 hours. Events are grouped by the Target field which represent managed host the request was referred to.
3. To look for a particular user, target or time period, or for all of them at the same time, you need to narrow down the search scope by configuring the following parameters of the search filter:
    - To define a user or a set of users, use the **Who** field from **Normalized Strings**
    - To set managed hosts requests were referred to, use the **Target** field from **Named Insertion Strings**.
    - To limit time period, use the **When** field from **Normalized Strings**
4. Finally, to execute search, click the **Go** button. The events providing all necessary information according to your search criteria will be shown in the events grid.

Tracking User Activity in Environment

One of the greatest benefits of using InTrust in your environment is that you get the ability to consolidate various log sources and view them in InTrust Repository Viewer.

Information on user and admin activity from TPAM complements information from the other sources such as events from Active Directory domain controllers where TPAM users reside, the user session events tracked on workstations or any other sources supported by InTrust for log collection. Combining such information sources together allows getting complete trace of user activity in your environment.

Suppose you need to correlate Syslog events from TPAM with events from Windows event log to completely track activity of a particular user in your environment, such as

- Account logon and authentication events
- Events from TPAM Syslog and from Syslog of managed systems

For that purpose, you can create a custom Search Folder which includes all necessary data sources in InTrust Repository Viewer and use the Who field from Normalized Strings as well as any other filter parameters as follows:

1. In InTrust Repository Viewer create a new search folder. For that, right-click **Custom Search Folders** and select **Create Search Folder**.
2. Add a **Custom** filter parameter and specify the following query as its value:
   ```
   ((striequ(Log,"security")) and ((striequ(What,"logon")) or (striequ
   (What,"Kerberos Authentication")))) or (striequ(Log,"syslog")) or (striequ
   (Log,"TPAM"))
   ```
3. Select users you are interested in using the **Who** field.
4. After that configure layout according to your needs using fields from **Normalized Strings**, such as **When**, **What**, **Where from**, and other fields.

Now you can track when the selected users logon to their Windows computers, when they access TPAM and which activities they perform through TPAM.

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