Quest

Quest® InTrust 11.4

# Preparing for Auditing and Monitoring HP-UX

### 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 and Monitoring HP-UX
Updated - October 2018
Version - 11.4

# Contents

# HP-UX Auditing and Real-Time Monitoring Overview

The HP-UX Knowledge Pack for expands the auditing and reporting capabilities of InTrust to HP-UX. The Knowledge Pack enables InTrust to work with HP-UX Syslog, text logs, and audit log.

The following table shows what you can audit and monitor on HP-UX:

| Data Source | Gathering | Real-Time Monitoring |
|---|---|---|
| Syslog messages | Yes | Yes |
| Text logs of any format | Yes | No |
| Configuration file modification | Yes | Yes |
| HP-UX audit logs | Yes | No |

# Setup



# Requirements

For details about HP-UX versions compatible with the InTrust Knowledge Pack for HP-UX, see HP-UX Events.

# Installation

The HP-UX Knowledge Pack must be installed to enable HP-UX support in InTrust. The following is a list of included objects:

- Data Sources
    - HP-UX Syslog
    - HP-UX Audit Log
    - HP-UX Account Monitoring
    - HP-UX Text file monitoring

- Gathering Policies
    - HP-UX Syslog: Security: Common Syslog Security Events
    - HP-UX Syslog: Security: Failed Logins
    - HP-UX Syslog: Security: Successful Logins
    - HP-UX: Security: SU Activity
    - HP-UX: Security: Reboots
    - HP-UX: All Syslog Messages
    - HP-UX: Login/logoff from Audit Log
    - HP-UX Audit Log: Process execution
    - HP-UX Audit Log: Failed file access
    - HP-UX: All Events from Audit Log
    - HP-UX Audit Log: Account management
    - HP-UX Audit Log: Audit management
    - HP-UX: Account monitoring
    - HP-UX: Text file monitoring
    - HP-UX: Security: Common Audit Log Security Events
    - HP-UX: Audit Log: Administrative activity
- Import Policies
    - HP-UX: Security: Common Syslog Security Events
    - HP-UX: All Syslog messages
    - HP-UX: Security: Failed logins
    - HP-UX: Security: Successful logins
    - HP-UX: Security: su activity
    - HP-UX: Security: Reboots
    - HP-UX: Logins/logouts from Audit Log
    - HP-UX: Process execution events from Audit Log
    - HP-UX: Audit Log: Failed file access
    - HP-UX: All events from Audit Log
    - HP-UX: Account monitoring
    - HP-UX: Text file monitoring
    - HP-UX: Security: Common Audit Log Security Events
    - HP-UX: Audit Log: Administrative activity
    - HP-UX: Audit Log: Account management
    - HP-UX: Audit Log: Audit management

- Consolidation Policies
  - HP-UX logs consolidation
  - HP-UX logs consolidation for the last month
- Tasks
  - HP-UX Syslog - daily collection of common security events
  - HP-UX Audit Log - daily collection of common security events
  - HP-UX configuration changes daily collection
  - HP-UX weekly reporting
- Rules
  - 'su root' succeeded
  - Multiple failed logins
  - Login authentication failed
  - Failed 'su' attempt
  - Successful login by root
  - User account created
  - User account removed
  - Group created
  - Group removed
  - User added to the group
  - User removed from the group
  - Syslog.conf file modified
  - Text file modified
- Reports
  - HP-UX login statistics
  - HP-UX user logons
  - HP-UX failed login attempts
  - HP-UX multiple failed login attempts
  - HP-UX process execution
  - All HP-UX syslog events
  - Account Management
  - HP-UX User management
  - HP-UX Group management
  - HP-UX Group membership management
  - System configuration management
  - HP-UX configuration files modifications
  - HP-UX Audit control

- Other
    - "HP-UX hosts" site
    - "HP-UX: security" real-time monitoring policy

To install the Knowledge Pack, launch InTrust setup on the InTrust server, and select the corresponding option.

The reporting server you use must have the same reports that are available in the Knowledge Pack that you install on the InTrust server. For that, install the HP-UX Report Pack on the reporting server you want to use for preparing HP-UX-related reports.

# Getting Started

The related topics explain the steps you need to take to set up HP-UX auditing and monitoring, as follows:

1. Install the InTrust agent on each HP-UX host.
2. Adjust the configuration of Syslog, if necessary.
3. Complete the configuration in InTrust Manager.

# Agent Setup

For detailed instructions, see Installing Agents Manually.

# Configuring Syslog

Syslog is an important logging facility in HP-UX. 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** message redirection feature if you audit and monitor Syslog with InTrust. InTrust support for the HP-UX 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 HP-UX Audit Log

The HP-UX audit system does not require additional configuration for the InTrust agent to work with the audit log. The agent is aware of the two current binary audit log files.

Note that if you change the locations of the audit log files, the agent will no longer work with the old files, which may still contain important data.

# InTrust Configuration

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

For more details, see the topics about the specific data sources:

- HP-UX Syslog
- HP-UX Audit Log
- Text File Monitoring Data Sources
- Script Event Provider Data Sources

The “HP-UX Syslog” and “HP-UX Audit Log” data sources represent the HP-UX audit trails. The "HP-UX Text File Monitoring" and “HP-UX Account Monitoring” data sources work with files that are not audit trails.

# HP-UX Syslog

Syslog auditing and real-time monitoring is based on the flow of data intended for the **syslogd** daemon. The “HP-UX 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}) ((?:[[:digit:]][[:alpha:]])?):?([-[:alnum:]_.]+) (su): ((\+)
([[:alnum:]\?]+) (.*)-(.*))
```

matches the following message:

```
Mar 5 19:19:02 6E:spb9460 su: + 2 user2-root
```

The result is an event with the following fields:

| Field Name | Field Number | Field Contents |
|---|---|---|
| Computer | 3 | spb9460 |
| Description | 5 | + 4 user2-root |
| Event Source | 4 | su |
| Insertion String #1 | 5 | + 4 user2-root |
| Insertion String #11 | 9 | root |
| Insertion String #12 | 7 | 4 |

| Field Name | Field Number | Field Contents |
|---|---|---|
| Insertion String #14 | 2 | 6E |
| Insertion String #8 | 8 | user2 |

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 HP-UX 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.**

# HP-UX Audit Log

In InTrust Manager, the HP-UX Audit log is represented by the “HP-UX Audit Log” data source. Use this data source in any gathering, consolidation and import policies that need to work with Audit log data.

For information about the format of the resulting event records, see Data Collected from Audit Log.

# Text File Monitoring Data Sources

The “HP-UX Account Monitoring” and “HP-UX Text File 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 Auditing Custom Logs with InTrust.**

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 “HP-UX Text File 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 “HP-UX account monitoring” data source if the location of the **passwd** and **groups** files differs from the default on your HP-UX hosts.

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

# Script Event Provider Data Sources

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

This functionality allows to create a script that starts with pre-set frequency. Under some conditions that are specified in this script, events are generated and then 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 the following in the script: what information is stored and how it is ordered in 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

HP-UX 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. For information 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. All data sources described above except "HP-UX Audit Log" use event caching, so 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.**
>
> **Caching is not used for the "HP-UX Audit Log" data source, so you do not need an active schedule just to gather audit log data.**

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

# Use Scenarios

The following are typical situations in a production environment, and InTrust helps handle them:

- Syslog Configuration Monitoring
- Tracking Security Incidents

For information about specific procedures, such as creating tasks and jobs or activating rules, see the InTrust Auditing 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 Security Incidents

You want to receive daily information about possible security issues in your environment, such as brute force attack attempts.

You can achieve this by scheduling gathering and reporting jobs with InTrust.

Take the following steps:

1. Make sure that **syslogd** is running.
2. Create an InTrust task that gathers Syslog events from the appropriate site (gathering job) and builds reports based on the gathered data (reporting job).The resulting reports are stored in the local folder that is specified during InTrust installation (for details, see the *Specifying reporting settings* section in Installing the First Server in InTrust Organization in the InTrust Deployment Guide).
3. A good report for this scenario is “HP-UX Multiple failed login attempts”.
4. It is up to you whether you want to store the gathered data in an InTrust repository. You can also include a notification job to get notified of task completion.
5. Schedule the task to run every morning at a convenient time.

# Data Collected from Audit Log

This topic describes the format that Audit log data is stored in. Native tools are used for converting Audit log to text, and the text entries are transformed into event records for the repository or audit database. Each event record has a fixed number of fields, which are described in the following table. These fields are always present, even if their values are empty.

| Field | Details |
|---|---|
| EventID | Event ID |
| EventType | Success (0x0008) or failure (0x0010) |
| UserName | The user that generated the event |
| Description | The body of the event |
| Insertion String #1 | Process ID (PID) |
| Insertion String #2 | Parent process ID (PPID) |
| Insertion String #3 | Audit ID (AID)<br>ID assigned to the initiator account by the audit system and found in all events that this account generates |
| Insertion String #4 | Real UID (RUID)<br>UID of the user that initially logged into the system |
| Insertion String #5 | Real GID (RGID)<br>GID of the user that initially logged into the system |
| Insertion String #6 | Effective UID (EUID)<br>UID of the initiator account at the time of the event; the effective UID may have changed since the user initially logged in |
| Insertion String #7 | Effective GID (EGID)<br>GID of the initiator account at the time of the event; the effective GID may have changed since the user initially logged in |
| Insertion String #8 | Number of the TTY device where the event was generated |
| Insertion String #9 | String description of the event |

| Field | Details |
| --- | --- |
| Insertion String #10 | String description of the real GID (specified by Insertion String #5) |
| Insertion String #11 | String description of the effective GID (specified by Insertion String #7) |

## 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