Quest

Quest® InTrust 11.4.1

Preparing for Auditing and Monitoring Linux

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 and Monitoring Linux
Updated - April 2019
Version - 11.4.1

Contents

Linux Auditing and Monitoring Overview

The Linux Knowledge Pack expands the auditing and reporting capabilities of InTrust to SuSE Linux Enterprise Server, Red Hat Enterprise Linux, Oracle Linux and Debian GNU/Linux. The Knowledge Pack enables InTrust to work with Syslog and text logs.

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

Data Source	Gathering	Real-Time Monitoring
Syslog messages	X	X
Text logs of any format	X	
Configuration file modification	X	X

Requirements

For details about Linux distribution versions that InTrust can audit and monitor, see the following topics:

- Red Hat Enterprise Linux Events
- SUSE Linux Events
- Oracle Linux Events
- Debian GNU/Linux Events
- Ubuntu Linux Events

To prepare a Linux host, you need to install an InTrust agent and adjust the configuration of the Syslog flavor used. Currently, agents must be installed manually on each Linux host you want to cover.

An alternative agent-free approach, which is not covered in this topic, is to use Syslog forwarding to an InTrust server. For details about this method, see Setting Up Gathering of Syslog Data.

Installation

The Linux Knowledge Pack is installed on top of an existing InTrust installation. The following objects are included:

- Data sources:
  - Redhat Linux Syslog
  - Redhat Linux Accounts Monitoring
  - Redhat Linux Text Files Monitoring
  - SuSE Linux Accounts Monitoring
  - SuSE Linux Syslog
  - SuSE Linux Text Files Monitoring
- Gathering policies:
  - Redhat Enterprise Linux: Common Security Events
  - Redhat Enterprise Linux: All Syslog Messages
  - Redhat Enterprise Linux: Accounts Monitoring
  - Redhat Enterprise Linux: Text files Monitoring
  - SuSE Linux Enterprise Server: Common Security Events
  - SuSE Linux Enterprise Server: All Syslog Messages
  - SuSE Linux Enterprise Server: Accounts Monitoring
  - SuSE Linux Enterprise Server: Text Files Monitoring
- Import policies:
  - Redhat Enterprise Linux: Common Security Events
  - Redhat Enterprise Linux: All Syslog Messages
  - Redhat Enterprise Linux: Accounts Monitoring
  - Redhat Enterprise Linux: Text Files Monitoring
  - SuSE Linux Enterprise Server: Common Security Events
  - SuSE Linux Enterprise Server: All Syslog Messages
  - SuSE Linux Enterprise Server: Accounts Monitoring
  - SuSE Linux Enterprise Server: Text Files Monitoring

- Consolidation policies:
    - Redhat Linux Log Consolidation
    - Redhat Linux Log Consolidation for the Last Month
    - SuSE Linux Log Consolidation
    - SuSE Linux Log Consolidation for the Last Month
    - Real-time monitoring policies:
    - Redhat Linux: security
    - SuSE Linux: security
- Tasks:
    - Redhat Linux daily collection of security events
    - Redhat Linux weekly reporting
    - SuSE Linux daily collection of security events
    - SuSE Linux weekly reporting
- Sites:
    - Redhat Linux hosts
    - SuSE Linux hosts

NOTE: To work with Oracle Linux and Debian GNU/Linux, use the data sources, policies and sites designed for Red Hat Enterprise Linux.

Installing Agents

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

Syslog Configuration

InTrust takes advantage of the Syslog logging system on Linux computers. Syslog provides data for auditing and real-time monitoring activities.

Syslog functionality is provided by a 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. There are multiple implementations of the daemon, including **rsyslog** and **syslog-ng**; these systems and keep their configuration files in different locations and have different sets of options.

When you install the InTrust agent on the Linux host, the necessary entries are automatically added to Syslog configuration. You do not have to modify any InTrust-related settings manually. However, if you use classic **syslogd**, it is up to you how you configure redirection of messages to other destinations.

NOTE: Prior to InTrust 11.3.2, a few manual Syslog configuration steps could be necessary to make Syslog gathering and real-time monitoring work. If you install the agent as part of an upgrade from version 11.3.1 or earlier to the current version, the new agent detects and updates the manual configuration. This activity is captured by Syslog. To confirm that it was successful, find Syslog messages that contain the string "SyslogConf::fix_rsyslog_file".

Preventing Skipping of Forwarded Messages

Reception of forwarded Syslog messages relies on named pipes, which have limited capacity. If a pipe opened for incoming messages becomes full, then messages will be skipped. This is a difficult situation to diagnose, but if you know or suspect it is happening on your message-receiving host, you can try increasing the pipe size.

The following is a sample Perl script that sets the maximum capacity for the pipe required by InTrust. Run it (or a variation of it) on the InTrust agent host that captures Syslog messages.

```
#!/usr/bin/perl

use Fcntl;

use constant

{

    F_SETPIPE_SZ => 1031,

    F_GETPIPE_SZ => 1032,

};

######################################################################
```

```
$MaxPipeBufPath = "/proc/sys/fs/pipe-max-size";
sysopen(Handle, $MaxPipeBufPath, O_RD) or die "sysopen failed: $!";
$MaxPipeBuf = readline(Handle) or die "readline failed: $!";
close Handle;
print "\n" . "max pipe buffer size = " . $MaxPipeBuf . "\n";
######################################################################
$FilePath = "/var/log/intrust_syslog";
sysopen(Handle, $FilePath, O_RD);
$CurrBuf = fcntl(Handle, F_GETPIPE_SZ, 0) or die "fcntl failed: $!";
print "current pipe buffer size = " . $CurrBuf . "\n";
######################################################################
if( int($CurrBuf) < int($MaxPipeBuf) )
{
    fcntl(Handle, F_SETPIPE_SZ, int($MaxPipeBuf) ) or die "fcntl failed: $!";
    print "new pipe buffer size = " . fcntl(Handle, F_GETPIPE_SZ, 0) . "\n";
}
######################################################################
close Handle;
```

InTrust Configuration

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

Auditing, Reporting, and Real-Time Monitoring

Linux 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. Since all Data Sources described above 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 Linux auditing, reporting and real-time monitoring operations do not have special requirements.

The following are details about the Linux-related data sources in InTrust.

Redhat Linux Syslog and SuSE Linux Syslog Data Sources

The “Redhat Linux Syslog” and the “SuSE Linux Syslog” data sources represent the Syslog audit trails.

Syslog auditing and real-time monitoring is based on the flow of data intended for the syslogd or syslog-ng daemons. The “Redhat Linux Syslog” (“SuSE Linux Syslog”) data source is used to analyze the data flow and capture only the necessary portions of it.

The 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)(\([^[]+\)){0,1}(\[[0-9]+\]){0,1}: (session opened for user (.*) by ([^()]*)\(.*\))
```

matches the following message:

```
Dec 16 12:10:47 es7 su(pam_unix)[23200]: session opened for user root by jsmith (uid=508)
```

The result is an event with the following fields:

Field Name	Field Number	Field Contents
Computer	<2>	es7
Description	<6>	session opened for user root by jsmith(uid=508)
Event ID	2	2
Event Source	<3>	su
Insertion String #1	<6>	session opened for user root by jsmith(uid=508)
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 Linux 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 “Redhat Linux text files monitoring”(or “SuSE Linux text files monitoring”) and “Redhat Linux accounts monitoring”(or “SuSE Linux 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 “Redhat Linux 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 “Redhat Linux accounts monitoring” data source if the location of the passwd and groups files differs from the default on your Linux hosts.

NOTE: Monitoring the **passwd** and **groups** files makes sense if your Linux 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 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 how frequently the script should run.
5. Complete the remaining steps.

Use Scenarios

This topic describes typical situations in a production environment and how InTrust helps handle them. 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 make sure the appropriate file paths are supplied 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. To view the resulting reports use the Knowledge Portal web application.

Take the following steps:

1. Make sure that syslogd or syslog-ng is running.
2. Create an InTrust task that gathers Syslog events from the appropriate site (gathering job), builds reports based on the gathered data (reporting job).The resulting reports are stored in the local folder that is specified during InTrust installation.
3. A good report for this scenario is "Multiple failed login attempts".
   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.
4. Schedule the task to run every morning at a convenient time.

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