Quest

Quest® InTrust 11.4.1

Preparing for Auditing and Monitoring IBM AIX

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 IBM AIX
Updated - June 2019
Version - 11.4.1

Contents

IBM AIX Auditing and Real-Time Monitoring Overview

The InTrust Knowledge Pack for IBM AIX expands the auditing and reporting capabilities of InTrust to IBM AIX. The Knowledge Pack enables InTrust to work with IBM AIX Syslog, text logs, and Audit log.

IMPORTANT: The Knowledge Pack for AIX is not distributed with InTrust 11.4.1. However, version 11.4 of the Knowledge Pack is fully compatible, and you can download it from from https://support.quest.com/download-install-detail/6097173.

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

Data source	Gathering	Real-Time Monitoring
Syslog messages	Yes	Yes
Text logs of any format	Yes	No
Configuration file modification	Yes	Yes
AIX audit logs	Yes	No

Setup

Requirements

For details about IBM AIX versions compatible with the InTrust Knowledge Pack for IBM AIX, see IBM AIX Events.

Installation

To enable AIX support in InTrust, the AIX Knowledge Pack must be installed on the InTrust server.
The Knowledge Pack is installed as part of the main InTrust installation. The following objects are included:

- Data sources:
  - AIX Audit Log
  - AIX Syslog
  - AIX Accounts Monitoring
  - AIX Text Files Monitoring
- Gathering policies:
  - AIX: Common Security Events
  - AIX: All Syslog Messages
  - AIX: Accounts monitoring
  - AIX: Text files monitoring
  - AIX: All Events from Audit Log
  - AIX: filesystem events from Audit Log
  - AIX: logins/logouts from Audit Log
  - AIX: process execution events from Audit Log
  - AIX: system object events from Audit Log

- Import policies:
    - AIX: Common Security Events
    - AIX: All Syslog Messages
    - AIX: Accounts monitoring
    - AIX: Text files monitoring
    - AIX: All Events from Audit Log
    - AIX: filesystem events from Audit Log
    - AIX: logins/logouts from Audit Log
    - AIX: process execution events from Audit Log
    - AIX: system object events from Audit Log
- Consolidation policies:
    - AIX logs consolidation
    - AIX logs consolidation for the last month
- Tasks:
    - AIX logs—daily collection
    - AIX configuration changes daily collection
    - AIX weekly reporting
- “AIX hosts” site
- “AIX: security” real-time monitoring policy
- Reports:
    - AIX login statistics
    - AIX successful logins
    - AIX su activity
    - AIX failed login attempts
    - AIX multiple failed login attempts
    - All AIX syslog events
    - AIX User management
    - AIX Group management
    - AIX Group membership management
    - AIX Configuration files modifications
    - AIX File Permission Changes
    - AIX Password Changes
    - AIX Reboots

- 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

To install the Knowledge Pack, launch its setup package on the InTrust server.

Getting Started

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

1. Install the InTrust agent on each AIX 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 AIX. 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 **syslog.conf** file specifies where syslogd sends a message depending on the parameters of the message. For a detailed description of this file's format, see the **syslog.conf** man page.

When you install the InTrust agent on the AIX host, the necessary entries are automatically added to **syslog.conf**. You do not have to modify any message redirection settings manually. However, as long as you do not modify InTrust-related settings, it is up to you how you configure redirection of messages to other destinations.

Configuring AIX Audit Log

The AIX audit system provides logging capability and handles system events in the following two ways:

- Writes event records to log files in "bin mode"
- Redirects messages to the specified destination in "stream mode"

The InTrust agent on the AIX computer relies on stream mode for event records.

Auditing starts according to audit system settings, including the following:

- Accounts to be audited
- Types of events to be audited for those accounts

If your auditing is already configured the way you need, then you do not need to do any further configuration. However, you might still need to configure or adjust the audit settings, as described in the related topics. In this case you primarily need to edit the two settings listed above.

Editing Audit Log Configuration Files

AIX audit uses the settings in the following files:

- /etc/security/audit/config
- /etc/security/audit/events
- /etc/security/audit/objects
- /etc/security/audit/bincmds
- /etc/security/audit/streamcmds

This section briefly describes only settings that specify auditable accounts and events. For detailed information about these and other settings, refer to the audit system man pages (**man audit**) and the *Accounting and Auditing on AIX 5L* IBM Red Book.

The settings in question are configured in the **/etc/security/audit/config** file.

If you did not enable system audit compatibility with the agent during setup, take the following additional steps to enable the InTrust agent to capture Audit log events:

1. 1 In the start stanza of the file, set the **streammode** option to **on**:
   `streammode = on`
2. 2 In the **streams** stanza, set the **cmds** option to the***<agent_installation_directory>*/InTrustStreamCmds** file, which was created during setup. For example:
   `cmds = /export/home/1604/InTrustStreamCmds`

The **/etc/security/audit/config** file also includes definitions of audit classes and assignments of those classes to individual user accounts.

This part of the file looks similar to the following:

```
...

classes:

general=USER_SU,PASSWORD_Change,FILE_Unlink,FILE_Link,FILE_Rename,FS_Chdir,FS_
Chroot,PORT_Locked,PORT_Change,FS_Mkdir,FS_Rmdir

objects=S_ENVIRON_WRITE,S_GROUP_WRITE,S_LIMITS_WRITE,S_LOGIN_WRITE,S_PASSWD_READ,S_
PASSWD_WRITE,S_USER_WRITE,AUD_CONFIG_WR

...

users:

root = general,objects,kernel,files

...
```

Auditing is configured on a per-user basis. Each audited account is assigned an audit class, which is a grouping of auditable event types. Audit classes are defined in the **classes** stanza and associated with individual users in the **users** stanza.

You can use default AIX audit class presets, or define your own classes, and associate them with the users whose activity you want to audit. For details on event syntax and any other configuration options, refer to AIX documentation.

After editing the **/etc/security/audit/config** file, restart system audit.

Auditing, Reporting, and Real-Time Monitoring

AIX 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 event caching, it is recommended that you use at least one task for the 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 AIX 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.

InTrust Configuration

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

Data Sources

The “AIX Syslog” and “AIX Audit Log” data sources represent the AIX audit trails. The "AIX Text Files Monitoring" and “AIX Accounts Monitoring” data sources work with files that are not audit trails.

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

AIX Syslog

Syslog auditing and real-time monitoring is based on the flow of data intended for the **syslogd** daemon. The “AIX 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 AIX 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.

AIX Audit Log

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

In addition to native Audit log events, the InTrust agent writes the following two events:

Event ID	Meaning
60000	The InTrust agent detected that AIX system audit had been stopped
60001	The InTrust agent detected that AIX system audit had been started (either before or after the start of the agent itself)

For information about the format of the resulting event records, see Audit Log Event Format.

Text File-Monitoring Data Sources

The “AIX Accounts Monitoring” and “AIX Text Files 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.

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 “AIX 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 “AIX accounts monitoring” data source if the location of the passwd and groups files differs from the default on your AIX hosts.

NOTE: Monitoring the passwd and groups files makes sense if your AIX 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 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.

Use Scenarios

This section describes typical situations in a production environment and outlines how InTrust helps handle them. For information about specific procedures, such as creating tasks and jobs or activating rules, see the InTrust Auditing Guide.

- Syslog Configuration Monitoring
- Tracking Security Incidents

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 the Installing the First Server in InTrust Organization topic in the Deployment Guide).
3. A good report for this scenario is “AIX 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.

Audit Log Event Format

This section describes the format to which the InTrust agent converts the Audit log trails it receives. A typical Audit log trail is like this:

```
Wed Jun 20 15:37:16 2007 FS_Mkdir jsmith OK smbd root 450648 245934 819443
00C8967E4C000000

mode: 755 dir: tmp/data
```

From these trails, the agent produces event records for the 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
ProviderName	For all events, the value of this field is empty.
Priority	For all events, the value of this field is 2, meaning Normal.
LocalTime	The local time of the event.
GMT	The time of the event represented in GMT format.
DataSourceName	For all events, the value of this field is "AIX 5L Audit Log".
HostName	The name of the AIX host where the InTrust agent captured the event.
DataSourceId	InTrust's internal ID of the agent's AIX auditing engine. For all events, the value of this field is "{B0CAB4B0-F676-4E2A-A345-A6071279D8FC}"
Insertion String 1	Event name such as FS_Rmdir, FILE_Unlink and so on.
Insertion String 2	User account under which the program ran. This may not be the same as the user account that opened the login session.
Insertion String 3	Auditing status according to system audit.
Insertion String 4	Name of the program that caused the event. For events 60000 and 60001, the value is "InTrust collector for AIX audit log".
Insertion String 5	User account that first opened the login session. In the course of the session, the account may have been substituted.
Insertion String 6	Process ID of the program that caused the event.
Insertion String 7	Process ID of the program's parent process.
Insertion String 8	Thread ID of the program that caused the event.
Insertion String 9	CPU ID used by the program.

Field	Details
Insertion String 10	Same as Insertion String 2.
Insertion String 11	Same as Insertion String 5.
Insertion String 12	The formatted but unmodified contents of the audit trail.
Description	Events 60000 and 60001 provide their own descriptions. For other events, the value is the same as Insertion String 12.
UserName	Same as Insertion String 5.
Category	Same as Insertion String 1.
Source	Same as Insertion String 4.
TimeGenerated	Event generation time in GMT format.
TimeWritten	Event record time in GMT format.
EventType	For event 60000, the value of this field is 2, meaning Warning. For all other events, the value is 4, meaning Information.
EventID	Can be 0, 60000 or 60001. For all native Audit log events, the value of this field is 0. Events with the IDs 60000 and 60001 are not native events. They are generated by the agent when it detects system audit stop and start, respectively.
PlatformID	The ID of the AIX platform; 640 for all events.

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