IBM AIX

Contents

IBM AIX DSMs

IBM® Security QRadar® provides the IBM AIX Audit and IBM AIX Server DSMs to collect and parse audit or operating system events from IBM AIX devices.

IBM AIX Server DSM overview

The IBM AIX Server DSM collects operating system and authentication events using syslog for users that interact or log in to your IBM AIX appliance.

The following table identifies the specifications for both IBM AIX DSM Server:

Table 1. IBM AIX Server DSM specifications

Specification	Value
Manufacturer	IBM
DSM names	IBM AIX Server
RPM file names	`DSM-IBMAIXServer-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	V5.X, V6.X, and V7.X
Protocol type	Syslog
QRadar recorded event types	Login or logoff events Session opened or session closed events Accepted password and failed password events Operating system events
Automatically discovered?	Yes
Includes identity?	Yes
More information	IBM website (http://www.ibm.com/)

To integrate IBM AIX Server events with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the latest version of the IBM AIX Server DSM.
2. Configure your IBM AIX Server device to send syslog events to QRadar.
3. Configure a syslog-based log source for your IBM AIX Server device. Use the following protocol-specific parameters:

Paramater	Description
Log Source Type	IBM AIX Server
Protocol Configuration	Syslog

Note: For more information about the remaining parameters, see the *Managing Log Sources Guide*.

Configuring your IBM AIX Server device to send syslog events to QRadar

Procedure

1. Log in to your IBM AIX appliance as a root user.
2. Open the `/etc/syslog.conf` file.
3. To forward the system authentication logs to QRadar, add the following line to the file:

   `auth.info @QRadar_IP_address`

   A tab must separate auth.info and the IP address of QRadar. For example:

   ```
   ##### begin /etc/syslog.conf
   mail.debug /var/adm/maillog
   mail.none /var/adm/maillog
   auth.notice /var/adm/authlog
   lpr.debug /var/adm/lpd-errs
   kern.debug /var/adm/messages
   *.emerg;*.alert;*.crit;*.warning;*.err;*.notice;*.info /var/adm/messages
   auth.info            @<10.100.100.1>
   ##### end /etc/syslog.conf
   ```
4. Save and exit the file.
5. Restart the syslog service:

   `refresh -s syslogd`

IBM AIX Audit DSM overview

The IBM AIX Audit DSM collects detailed audit information for events that occur on your IBM AIX appliance.

The following table identifies the specifications for the IBM AIX Audit DSM:

Table 2. IBM AIX Audit DSM specifications

Specification	Value
Manufacturer	IBM
DSM names	IBM AIX Audit
RPM file names	DSM-IBMAIXAudit-*QRadar_version-build_number*.noarch.rpm
Supported versions	V6.1 and V7.1
Protocol type	Syslog Log File Protocol
QRadar recorded event types	Audit events
Automatically discovered?	Yes
Includes identity?	No
More information	IBM website (http://www.ibm.com/)

To integrate IBM AIX Audit events with QRadar, complete the following steps:

1. Download the latest version of the IBM AIX Audit DSM.
2. For syslog events, complete the following steps:

a. Configure your IBM AIX Audit device to send syslog events to QRadar. See "Configuring IBM AIX Audit DSM to send syslog events to QRadar" on page 4.

b. If QRadar does not automatically discover the log source, add an IBM AIX Audit log source. Use the following IBM AIX Audit-specific values in the log source configuration:

Parameter	Value
Log Source Type	IBM AIX Audit
Protocol Configuration	Syslog

Note: For more information about manually adding a log source, see the *Managing Log Sources Guide*.

3. For log file protocol events, complete the following steps:

a. Configure your IBM AIX Audit device to convert audit logs to the log file protocol format.

b. Configure a log file protocol-based log source for your IBM AIX Audit device. Use the following protocol-specific values in the log source configuration:

Parameter	Value
Log Source Type	IBM AIX Audit
Protocol Configuration	Log File
Service Type	The protocol to retrieve log files from a remote server. **Important:** If you select the SCP and SFTP service type, ensure that the server that is specified in the **Remote IP or Hostname** parameter has the SFTP subsystem enabled.
Remote Port	If the host for your event files uses a non-standard port number for FTP, SFTP, or SCP, adjust the port value.
SSH Key File	If you select SCP or SFTP as the Service Type, use this parameter to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** parameter is ignored.
Remote Directory	The directory location on the remote host where the files are retrieved. Specify the location relative to the user account you are using to log in. **Restriction:** For FTP only. If your log files are in a remote user home directory, leave the remote directory blank to support operating systems where a change in the working directory (CWD) command is restricted.
FTP File Pattern	The FTP file pattern must match the name that you assigned to your AIX audit files with the **-n** parameter in the audit script. For example, to collect files that start with AIX_AUDIT and end with your time stamp value, type `AIX_Audit_*`.

Parameter	Value
FTP Transfer Mode	ASCII is required for text event logs that are retrieved by the log file protocol by using FTP.
Processor	NONE
Change Local Directory?	Leave this check box clear.
Event Generator	LineByLine The Event Generator applies more processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

Note: For more information about the remaining parameters, see the *Managing Log Sources Guide*.

Configuring IBM AIX Audit DSM to send syslog events to QRadar

To collect syslog audit events from your IBM AIX Audit device, redirect your audit log output from your IBM AIX device to the IBM Security QRadar Console or Event Collector.

About this task

On an IBM AIX appliance, you can enable or disable classes in the audit configuration. The IBM AIX default classes capture a large volume of audit events. To prevent performance issues, you can tune your IBM AIX appliance to reduce the number of classes that are collected. For more information about audit classes, see your IBM AIX appliance documentation.

Procedure

1. Log in to your IBM AIX appliance.
2. Open the audit configuration file:
   `/etc/security/audit/config`
3. Edit the Start section to disable the **binmode** element and enable the **streammode** element:
   ```
   binmode = off
   streammode = on
   ```
4. Edit the Classes section to specify which classes to audit.
5. Save the configuration changes.
6. Open the `streamcmds` file:
   `/etc/security/audit/streamcmds`
7. Add the following line to the file:
   `/usr/sbin/auditstream | auditpr -h eclrRdi | /usr/bin/logger -p local0.debug`
8. Save the configuration changes.
9. Edit the syslog configuration file to specify a debug entry and the IP address of the QRadar Console or Event Collector:
   `*.debug @ip_address`

Tip: A tab must separate *.debug from the IP address.

10. Save the configuration changes.
11. Reload your syslog configuration:
    ```
    refresh -s syslogd
    ```
12. Start the audit script on your IBM AIX appliance:
    ```
    audit start
    ```

What to do next

The IBM AIX Audit DSM automatically discovers syslog audit events that are forwarded from IBM AIX to QRadar and creates a log source. If the events are not automatically discovered, you can manually configure a log source.

Configuring IBM AIX Audit DSM to send log file protocol events to QRadar

Configure the audit.pl script to run each time that you want to convert your IBM AIX audit logs to a readable event log format for QRadar.

Before you begin

To use the audit script, you are required to install a version of Perl 5.8 or above on your IBM AIX appliance

About this task

This procedure requires you to configure two files:

Audit configuration file

The audit configuration file identifies the event classes that are audited and the location of the event log file on your IBM AIX appliance. The IBM AIX default classes capture many audit events. To prevent performance issues, you can configure the classes in the audit configuration file. For more information about configuring audit classes, see your IBM AIX documentation.

Audit script

The audit script uses the audit configuration file to identify which audit logs to read and converts the binary logs to single-line events that QRadar can read. The log file protocol can then retrieve the event log from your IBM AIX appliance and import the events to QRadar. The audit script uses the audit.pr file to convert the binary audit records to event log files QRadar can read.

Run the audit script each time that you want to convert your audit records to readable events. You can use a cron job to automate this process. for example, you can add `0 * * * * /audit.pl` to allow the audit script to run hourly. For more information, see your system documentation.

Procedure

1. Log in to your IBM AIX appliance.
2. Configure the audit configuration file:
   a. Open the audit configuration file:
      ```
      etc/security/audit/config
      ```
   b. Edit the Start section to enable the **binmode** element.

```
binmode = on
```

c. In the Start section, edit the configuration to determine which directories contain the binary audit logs. The default configuration for IBM AIX auditing writes binary logs to the following directories:

```
trail = /audit/trail
bin1 = /audit/bin1
bin2 = /audit/bin2
binsize = 10240
cmds = /etc/security/audit/bincmds
```

In most cases, you do not have to edit the binary file in the bin1 and bin2 directories.

d. In the Classes section, edit the configuration to determine which classes are audited. For information on configuring classes, see your IBM AIX documentation.

e. Save the configuration changes.

3. Start auditing on your IBM AIX system:

```
audit start
```

4. Install the audit script:

a. Access the IBM Support website (http://www.ibm.com/support).

b. Download the `audit.pl.gz` file.

c. Copy the audit script to a folder on your IBM AIX appliance.

d. Extract the file:

```
tar -zxvf audit.pl.gz
```

e. Start the audit script:

```
./audit.pl
```

You can add the following parameters to modify the command:

Parameter	Description
-r	Defines the results directory where the audit script writes event log files for QRadar. If you do not specify a results directory, the script writes the events to the following `/audit/results/` directory. The results directory is used in the **Remote Directory** parameter in the log source configuration uses this value. To prevent errors, verify that the results directory exists on your IBM AIX system.
-n	Defines a unique name for the event log file that is generated by audit script. The **FTP File Pattern** parameter in the log source configuration uses this name to identify the event logs that the log source must retrieve in QRadar
-l	Defines the name of the last record file.
-m	Defines the maximum number of audit files to retain on your IBM AIX system. By default, the script retains 30 audit files. When the number of audit files exceeds the value of the **-m** parameter, the script deletes the audit file with the oldest time stamp.

Parameter	Description
-t	Defines the directory that contains the audit trail file. The default directory is `/audit/trail`.

What to do next

The IBM AIX Audit DSM automatically discovers log file protocol audit events that are forwarded from IBM AIX to QRadar and creates a log source. If the events are not automatically discovered, you can manually configure a log source.

Index

C

I