Syslog Configuration for Auditing

Access Manager 4.2
Contents

1. Introduction ................................................................. 3
2. How Access Manager auditing works with Syslog ................................. 3
3. Linux: Configuring Access Manager and Syslog ................................... 4
   3.1 Linux Configuration Steps ..................................................... 4
   3.2 Advanced RSyslog Configuration ............................................... 7
       3.2.1 Caching of Audit Events ................................................... 8
       3.2.2 Configuring SSL Communication ......................................... 8
   3.3 Troubleshooting .................................................................... 10
4. Windows: Configuring Syslog .......................................................... 11
   4.1 Configuration Steps Overview .................................................. 11
   4.2 Syslog Agents .................................................................... 11
1. Introduction

Access Manager 4.2 release supports Syslog as the audit channel for forwarding the audit messages to the remote audit server. The traditional NetIQ Platform Agent for auditing is discontinued in the 4.2 release and the customers are encouraged to move to Syslog for auditing.

This whitepaper covers:

- How Access Manager auditing works with Syslog
- Configuring Syslog for Access Manager Auditing
- Advanced configurations like caching and SSL
- Troubleshooting

2. How Access Manager auditing works with Syslog

Syslog Agent

The Access Manager components can be configured to send the audit messages to syslog. A local syslog agent runs on each device to collect the audit messages and forward them to the centralized syslog server. On Linux, rsyslog is auto-configured as the local syslog agent and communicates with TCP port 1290.

Windows does not include a syslog agent. However, many free and paid versions of the syslog client for Windows are available in the market. Administrators should procure one and install it manually on each system.

Syslog Server

The central auditing server can be Sentinel or any syslog server. The IP and port of this server can be configured on the Administration Console’s Auditing UI.
Note: NAM Auditing over syslog is supported only on TCP.

3. Linux: Configuring Access Manager and Syslog

3.1 Linux Configuration Steps
Perform the following steps to configure Access Manager auditing using syslog:

1. Install RSyslog on each Access Manager server.
2. Configure the centralized audit server – Sentinel or third party syslog server.
3. Install or Upgrade Access Manager to 4.2.
5. Configure Syslog on the Administration Console System (cannot be done through UI)
6. Optional: Manually configure caching of messages and/or SSL for syslog (see [Advanced RSyslog Configuration](#)).

Step 1: Install RSyslog

This is a pre-requisite for the install/upgrade of Access Manager.

**Distributed Access Manager Setup (Non-Appliance)**

Trying to install/upgrade Access Manager 4.2 without RSyslog will result in the following error:

```
DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT (y/n) ?:y
Checking for RPMs: expat fontconfig freetype2 glib2 libjpeg libpng12-0 libtiff5
Missing rpm: rsyslog-module-gtls
Install the missing rpms before proceeding. Terminating Installation.
```

Install the latest rsyslog package from the respective operating system's repository.

SLES:

```
zypper in rsyslog-module-gtls
```

Redhat:

Use the “rpm –ivh <rpm name>” or the yum command to install the rsyslog module.

**NAM Appliance and MAG Appliance**
The rsyslog rpm is available in the update channel in the pattern NetIQ-Access-Manager. The base operating system of the appliance has to be upgraded to SLES11 SP4 and the rsyslog rpm has to be installed before upgrading Access Manager to 4.2.

1. Upgrade the base operating system by following the instructions on the documentation site.

2. Install rsyslog using the command:

   ```
   zypper in -t pattern NetIQ-Access-Manager
   ```

3. Confirm that the rpm is available using the command:

   ```
   rpm -qa | grep -i syslog
   ```

**Note:**

Repeat this step on each Access Manager component – Administration Console, Identity Server and Access Gateway.

**Step 2: Install / Upgrade to Access Manager 4.2**

Follow the usual steps to install or upgrade to Access Manager 4.2.

**Step 3: Configure the Centralized Audit Server**

If you are using Sentinel as the centralized audit server, an updated NAM collector that supports Syslog is available and can be downloaded from the site:

https://www.netiq.com/support/sentinel/plugins/

If you plan to use any other Syslog as your centralized audit server, configure it and make sure that it is reachable.

**Note:** To test this feature, the syslog agent running on the Administration Console can also be used as the centralized syslog server. All the audit events will be written to /var/log/NAM_Audits.log file. This is not recommended for production systems.

**Step 4: Configure Auditing**

Access Manager must be configured to use Syslog.

1. Login to the Administration Console.
2. On the dashboard, click Auditing.
3. In the **Audit Messages Using** field:
   - Select **Syslog**.
   - For Sentinel, select **Send to Sentinel**.
   - For all other syslog servers, select **Send to Third Party**. The audit messages are sent in JSON format to the configured Syslog server.

4. **Server Listening Address**: Specify the IP address or DNS name of the syslog server.
   
   When the configuration is saved, the local syslog agents running on each system are automatically updated to point to the configured IP of the remote syslog server. The only exception is that the syslog agent of the Administration Console cannot be modified using the UI for security reasons and hence must be manually updated (see next section).

5. **Server Public NAT Address**: If the auditing server is in the private network, then you have to enter the Public NAT IP Address of the auditing server using which devices can reach the auditing server.

6. **Port**: Specify the syslog server port:
   - For Sentinel server, the default port is 1468.
   - For third party syslog servers, specify the configured port of that server.

7. Save the changes.

**Step 5: Configuring the Administration Console for auditing with Syslog**

In the case of a standalone Administration Console (with no other Access manager components installed), the configuration changes done on the Auditing UI are not applied to the local files for security reasons. These files must manually updated by logging into the system.

To configure the Administration Console for auditing with syslog, perform the following:

**Syslog Agent Configuration**
1. Configure the local syslog agent to communicate with TCP port 1290 by adding the following in the /etc/rsyslog.d/nam.conf file:

```
$InputTCPServerRun 1290
```

2. Configure the local agent to forward the Audit messages to the remote syslog server at 172.16.50.50 on port 1468. This can be done by adding the following to the nam.conf file:

```
$template ForwardFormat,"<%PRI%%TIMESTAMP::date-rfc3164% %HOSTNAME% %syslogtag:1:32%msg::sp-if-no-1st-sp%msg\n" local0.* @@172.16.50.50:1468;ForwardFormat
```

Now, the /etc/rsyslog.d/nam.conf file should have:

```
$InputTCPServerRun 1290
$template ForwardFormat,"<%PRI%%TIMESTAMP::date-rfc3164% %HOSTNAME% %syslogtag:1:32%msg::sp-if-no-1st-sp%msg\n" local0.* @@172.16.50.50:1468;ForwardFormat
```

**Access Manager Auditing Configuration**

3. Configure the auditing settings for Access Manager by editing the /etc/Auditlogging.cfg file.

```
LOGDEST=syslog # syslog or PA
FORMAT=JSON # JSON or CSV
SERVERIP=127.0.0.1 # Don’t change.
SERVERPORT=1290 # Don’t change.
```

LOGDEST: Set to “syslog” to send the audit messages to the local syslog agent.
FORMAT: Set to “CSV” if using Sentinel. Set to “JSON” for all other remote syslog servers.
SERVERIP: Use the default 127.0.0.1 to send the messages to the local syslog agent.
SERVERPORT: Use the default 1290 on which the local syslog agent is communicating.

4. Restart the Administration Console using the command: /etc/init.d/novell-ac restart.

### 3.2 Advanced RSyslog Configuration

RSyslog supports additional features that can be beneficial in a production environment. You have to configure them manually if required.
3.2.1 Caching of Audit Events

RSyslog supports queuing to cache the audit events if the remote syslog server is not reachable. When the remote syslog server is reachable again, the queued events are then relayed to the server. This ensures that there is no loss of any audit events. The complete guide for the RSyslog’s Queues is available at [http://www.rsyslog.com/doc/v8-stable/concepts/queues.html](http://www.rsyslog.com/doc/v8-stable/concepts/queues.html)

Add the following to `/etc/rsyslog.d/nam.conf` to cache in-memory:

```plaintext
$WorkDirectory /rsyslog/work  # Default location for work (spool) files
$ActionQueueType LinkedList  # Use asynchronous processing
$ActionQueueFileName example_fwd  # Set file name, also enables disk mode
$ActionResumeRetryCount -1  # Infinite retries on insert failure
$ActionQueueSaveOnShutdown on  # Save in-memory data if rsyslog shuts down.
```

Note:

1. Making any changes on the Auditing UI will overwrite all manual changes done to the nam.conf file.
2. The changes must be manually done on each component – Administration Console, Identity Server and Access Gateway.

3.2.2 Configuring SSL Communication

We can configure the secure TLS channel auditing between the Access Manager component and the remote Audit server mechanism.

The detail guides on the steps are available at:


Configuration steps:

1. Generate the Certificate Authority (CA) Certificate
   - Create a Private Key
     ```bash
certtool --generate-privkey --outfile ca-key.pem
     ```
   - Create the self-signed certificate
2. Generate the certificate for local syslog client (private Key)
   • Create a private key for syslog agent
     ```
     certtool --generate-privkey --outfile rslclient-key.pem --bits 2048
     ```
   • Generate a certificate request for the syslog client.
     ```
     certtool --generate-request --load-privkey rslclient-key.pem --outfile request.pem
     ```
   • Generate the certificate and sign it with the CA private key.
     ```
     certtool --generate-certificate --load-request request.pem --outfile rslclient-cert.pem --load-ca-certificate ca.pem --load-ca-privkey ca-key.pem
     ```

3. Generate the certificate for Remote syslog Server (private Key)
   • Remove the previously generated request.pem.
   • Create a private key for Syslog server.
     ```
     certtool --generate-privkey --outfile rslserver-key.pem --bits 2048
     ```
   • Generate a certificate request for the rsyslog Server
     ```
     certtool --generate-request --load-privkey rslserver-key.pem --outfile request.pem
     ```
   • Generate the machine certificate and sign it with the CA private key.
   • Copy certificates from CA to rsyslog server and rsyslog client.
     ```
     certtool --generate-certificate --load-request request.pem --outfile rslserver-cert.pem --load-ca-certificate ca.pem --load-ca-privkey ca-key.pem
     ```
• Configure the Syslog server for TLS. Sample nam.conf file entries for:

```plaintext
# Increase the amount of open files rsyslog is allowed, which includes open tcp sockets
# This is important if there are many clients.
# http://www.rsyslog.com/doc/rsconf1_maxopenfiles.html
$MaxOpenFiles 2048

# make gtls driver the default
$DefaultNetstreamDriver gtls

# certificate files generated on RHEL6 and stored in /root
$DefaultNetstreamDriverCAFile /etc/pki/rsyslog/ca.pem
$DefaultNetstreamDriverCertFile /etc/pki/rsyslog/rslserver-cert.pem
$DefaultNetstreamDriverKeyFile /etc/pki/rsyslog/rslserver-key.pem

#### GLOBAL DIRECTIVES ####
$ActionSendStreamDriverAuthMode x509/name
$ActionSendStreamDriverMode 1 # run driver in TLS-only mode
```

• Configure the syslog agent for TLS. Sample /etc/rsyslog.d/nam.conf for:

```plaintext
# make gtls driver the default
$DefaultNetstreamDriver gtls

# certificate files
$DefaultNetstreamDriverCAFile /etc/pki/rsyslog/ca.pem
$DefaultNetstreamDriverCertFile /etc/pki/rsyslog/rslclient-cert.pem
$DefaultNetstreamDriverKeyFile /etc/pki/rsyslog/rslclient-key.pem

#### GLOBAL DIRECTIVES ####
$ActionSendStreamDriverAuthMode x509/name
$ActionSendStreamDriverMode 1 # run driver in TLS-only mode
```

Note:

1. Making any changes on the Auditing UI will overwrite the manual changes done to the nam.conf file.
2. The changes must be manually done on each component – Administration Console, Identity Server and Access Gateway.

3.3 Troubleshooting

**Audit events are not reaching the remote server.**

• Check if the rsyslog package is installed properly in the NAM device
- Check if the local TCP port 1290 is communicating with the local NAM device
- Check if the remote syslog server’s IP address and port numbers provided in the Administration Console UI is reflecting in /etc/rsyslog.d/nam.conf
- Check if the remote audit server is reachable from the NAM devices

Audit events are not parsed properly from the Sentinel server

- Check if in the Administration Console, the Send to Sentinel option is selected as the remote audit Server
- Ensure that you are using the latest NAM Collector for Sentinel available from https://www.netiq.com/support/sentinel/plugins/

Audit events are received in CSV format instead of JSON format in the remote non-Sentinel syslog audit server

- Check if in the Administration Console Send to Third Party option is selected as the remote audit server.

4. Windows: Configuring Syslog

4.1 Configuration Steps Overview
To configure Access Manager auditing using syslog, perform the following steps:

1. Configure the centralized audit server – Sentinel or third party syslog server.
2. Install a Windows Syslog agent on each Access Manager server. Configure it to send messages to the centralized syslog server.
3. Install or Upgrade Access Manager to 4.2.
4. Configure Access Manager auditing – audit server type, IP and port. See the section 4 of the Linux Configuration Steps.
5. Configure the nam.conf file on each Access Manager server to send messages to the local syslog agent.

4.2 Syslog Agents
The Access Manager distribution does not include a syslog agent for Windows. However, many free and paid versions of the agents are available in the market. An Administrator can manually procure and install these agents on each Access Manager component – Administration Console, Identity Server and Access Gateway.

Check the NetIQ Cool Solutions page for an example configuration using Syslog-ng as an agent on Windows.