Audit Logging

Active IQ Unified Manager 9.11

NetApp
July 19, 2022

Table of Contents

Audit Logging

You can detect whether the audit logs have been compromised with using Audit Logs. All the activities performed by a user are monitored and logged in the Audit Logs. The audits are performed for all user interface and publicly exposed APIs' functionalities of Active IQ Unified Manager.

You can use the Audit Log: File View to view and access all the audit log files available in your Active IQ Unified Manager. The files in the Audit Log: File View are listed based on their creation date. This view displays information of all the audit log that are captured from the installation or upgrade to the present in the system. Whenever you perform an action in Unified Manager, the information is updated and is available in the logs. The status of each log file is captured using the "File Integrity Status" attribute which gets actively monitored to detect tampering or deletion of the log file. The audit logs can have one of the following states when the audit logs are available in the system:

State	Description
ACTIVE	File in which logs are being currently logged.
NORMAL	File which is inactive, compressed and stored in the system.
TAMPERED	File which has been compromised by a user who has manually edited the file.
MANUAL_DELETE	File which got deleted by an authorized user.
ROLLOVER_DELETE	File which got deleted due to Rolling off based on Rolling Configuration Policy.
UNEXPECTED_DELETE	File which got deleted due to unknown reasons.

The Audit Log page includes the following command buttons:

- Configure
- Delete
- Download

The **DELETE** button enables you to delete any of the audit logs listed in the Audit Logs view. You can delete an audit log and optionally provide a reason to delete the file which helps in future to determine a valid delete. The REASON column lists the reason along with the name of the user who performed the delete operation.

Deleting a log file will cause deletion of file from the system but the entry in the DB table will not be deleted.

You can download the audit logs from Active IQ Unified Manager using the **DOWNLOAD** button in the Audit Logs section and export the audit log files. The files that are marked "NORMAL" or "TAMPERED" are downloaded in a compressed `.gzip` format.

When a full Autosupport bundle is generated, the support bundle includes both archived and active audit log files. But when a light support bundle is generated, it includes only the active audit logs. The archived audit logs are not included.

Configuring audit logs

You can use the **Configure** button in the Audit Logs section to configure rolling policy for Audit Log files and to also enable remote logging for the Audit Logs.

You can set the values in the **MAX FILE SIZE** and **AUDIT LOG RETENTION DAYS** as per the desired amount and frequency of data that you want to store in the system. The value in the field **TOTAL AUDIT LOG SIZE** is the size of the total audit log data present in the system. The roll over policy is determined by the values in the field **AUDIT LOG RETENTION DAYS**, **MAX FILE SIZE**, and **TOTAL AUDIT LOG SIZE**. When the size of the audit log backup reaches the value configured in **TOTAL AUDIT LOG SIZE**, then the file that was archived first is deleted. This means that the oldest file is deleted. But the file entry continues to be available in the database and is marked as “Rollover Delete”. The **AUDIT LOG RETENTION DAYS** value is for the number of the days the audit log files are preserved. Any file older than the value set in this field is rolled over.

Steps

1. Click **Audit Logs** > > **Configure**.
2. Enter values in the **MAX FILE SIZE**, **TOTAL AUDIT LOG SIZE**, and **AUDIT LOG RETENTION DAYS**.

   If you want to enable remote logging, then you should select the **Enable Remote Logging**.

Enabling remote logging of audit logs

You can select the **Enable Remote Logging** checkbox on the Configure Audit Logs dialog box to enable remote audit logging. You can use this feature to transfer audit logs to a remote Syslog server. This will enable you to manage your audit logs when there are space constraints.

The remote logging of audit logs provides a tamper-proof backup in case the audit log files on the Active IQ Unified Manager server are tampered.

Steps

1. In the **Configure Audit Logs** dialog box, select the **Enable Remote Logging** checkbox.

   Additional fields to configure remote logging are displayed.

2. Enter the **HOSTNAME** and **PORT** of the remote server you want to connect to.
3. In the **SERVER CA CERTIFICATE** field, click **BROWSE** to select a public certificate of the target server.

   The certificate should be uploaded in `.pem` format. This certificate should be obtained from the target Syslog server and should not have expired. The certificate should contain the selected “hostname” as part of the `SubjectAltName` (SAN) attribute.

4. Enter the values for the following fields: **CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

   The values should be in milliseconds for these fields.

5. Select the required Syslog format and TLS protocol version in the **FORMAT** and **PROTOCOL** fields.
6. Select the **Enable Client Authentication** checkbox if the target Syslog server requires certificate based authentication.

   You will need to download client authentication certificate and upload it to the Syslog server before saving the Audit Log configuration, otherwise the connection will fail. Depending on the type of Syslog server, you might need to create a hash of the client authentication certificate.

   Example: syslog-ng requires a <hash> of the certificate to be created using the command `openssl x509 -noout -hash -in cert.pem`, and then you should symbolically link the client authentication certificate to a file named after the <hash> .0.

7. Click **Save** to configure the connection with your server and enable remote logging.

   You will be redirected to the Audit Logs page.