Managing authentication

Active IQ Unified Manager 9.13

NetApp
February 12, 2024

Table of Contents

Managing authentication

You can enable authentication using either LDAP or Active Directory on the Unified Manager server and configure it to work with your servers to authenticate remote users.

For enabling remote authentication, setting up authentication services, and adding authentication severs, see the previous section on **Configuring Unified Manager to send alert notifications**.

Editing authentication servers

You can change the port that the Unified Manager server uses to communicate with your authentication server.

What you'll need

You must have the Application Administrator role.

Steps

1. In the left navigation pane, click **General** > **Remote Authentication**.
2. Check the **Disable Nested Group Lookup** box.
3. In the **Authentication Servers** area, select the authentication server that you want to edit, and then click **Edit**.
4. In the **Edit Authentication Server** dialog box, edit the port details.
5. Click **Save**.

Deleting authentication servers

You can delete an authentication server if you want to prevent the Unified Manager server from communicating with the authentication server. For example, if you want to change an authentication server that the management server is communicating with, you can delete the authentication server and add a new authentication server.

What you'll need

You must have the Application Administrator role.

When you delete an authentication server, remote users or groups of the authentication server will no longer be able to access Unified Manager.

Steps

1. In the left navigation pane, click **General** > **Remote Authentication**.
2. Select one or more authentication servers that you want to delete, and then click **Delete**.
3. Click **Yes** to confirm the delete request.

   If the **Use Secure Connection** option is enabled, then the certificates associated with the authentication server are deleted along with the authentication server.

Authentication with Active Directory or OpenLDAP

You can enable remote authentication on the management server and configure the management server to communicate with your authentication servers so that users within the authentication servers can access Unified Manager.

You can use one of the following predefined authentication services or specify your own authentication service:

- Microsoft Active Directory

  You cannot use Microsoft Lightweight Directory Services.

- OpenLDAP

You can select the required authentication service and add the appropriate authentication servers to enable the remote users in the authentication server to access Unified Manager. The credentials for remote users or groups are maintained by the authentication server. The management server uses the Lightweight Directory Access Protocol (LDAP) to authenticate remote users within the configured authentication server.

For local users who are created in Unified Manager, the management server maintains its own database of user names and passwords. The management server performs the authentication and does not use Active Directory or OpenLDAP for authentication.

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.

State	Description
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.

The audit log files are archived periodically and saved to the database for reference. Before archival, the audit logs are digitally signed for maintaining the security and integrity.

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.

> The **Connection Timeout** value can affect the configuration. If the configuration takes longer time to respond than the defined value, it can lead to configuration failure due to a connection error. To establish a successful connection, increase the **Connection Timeout** value, and try the configuration again.

Remote Authentication page

You can use the Remote Authentication page to configure Unified Manager to communicate with your authentication server to authenticate remote users who attempt to

log into the Unified Manager web UI.

You must have the Application Administrator or Storage Administrator role.

After you select the Enable remote authentication checkbox, you can enable remote authentication using an authentication server.

- **Authentication Service**

  Enables you to configure the management server to authenticate users in directory service providers, such as Active Directory, OpenLDAP, or specify your own authentication mechanism. You can specify an authentication service only if you have enabled remote authentication.

  - **Active Directory**
    - Administrator Name

      Specifies the administrator name of the authentication server.

    - Password

      Specifies the password to access the authentication server.

    - Base Distinguished Name

      Specifies the location of the remote users in the authentication server. For example, if the domain name of the authentication server is ou@domain.com, then the base distinguished name is **cn=ou,dc=domain,dc=com**.

    - Disable Nested Group Lookup

      Specifies whether to enable or disable the nested group lookup option. By default this option is disabled. If you use Active Directory, you can speed up authentication by disabling support for nested groups.

    - Use Secure Connection

      Specifies the authentication service used for communicating with authentication servers.

  - **OpenLDAP**
    - Bind Distinguished Name

      Specifies the bind distinguished name that is used along with the base distinguished name to find remote users in the authentication server.

    - Bind Password

      Specifies the password to access the authentication server.

    - Base Distinguished Name

      Specifies the location of the remote users in the authentication server. For example, if the domain name of the authentication server is ou@domain.com, then the base distinguished name is **cn=ou,dc=domain,dc=com**.

    - Use Secure Connection

Specifies that Secure LDAP is used for communicating with LDAP authentication servers.

- **Others**
  - Bind Distinguished Name

    Specifies the bind distinguished name that is used along with the base distinguished name to find remote users in the authentication server that you have configured.

  - Bind Password

    Specifies the password to access the authentication server.

  - Base Distinguished Name

    Specifies the location of the remote users in the authentication server. For example, if the domain name of the authentication server is ou@domain.com, then the base distinguished name is **cn=ou,dc=domain,dc=com**.

  - Protocol Version

    Specifies the Lightweight Directory Access Protocol (LDAP) version that is supported by your authentication server. You can specify whether the protocol version must be automatically detected or set the version to 2 or 3.

  - User Name Attribute

    Specifies the name of the attribute in the authentication server that contains user login names to be authenticated by the management server.

  - Group Membership Attribute

    Specifies a value that assigns the management server group membership to remote users based on an attribute and value specified in the user's authentication server.

  - UGID

    If the remote users are included as members of a GroupOfUniqueNames object in the authentication server, this option enables you to assign the management server group membership to the remote users based on a specified attribute in that GroupOfUniqueNames object.

  - Disable Nested Group Lookup

    Specifies whether to enable or disable the nested group lookup option. By default this option is disabled. If you use Active Directory, you can speed up authentication by disabling support for nested groups.

  - Member

    Specifies the attribute name that your authentication server uses to store information about the individual members of a group.

  - User Object Class

    Specifies the object class of a user in the remote authentication server.

- Group Object Class

  Specifies the object class of all groups in the remote authentication server.

  The values that you enter for the *Member*, *User Object Class*, and *Group Object Class* attributes should be the same as those added in your Active Directory, OpenLDAP, and LDAP configurations. Otherwise, the authentication might fail.

- Use Secure Connection

  Specifies the authentication service used for communicating with authentication servers.

If you want to modify the authentication service, ensure that you delete any existing authentication servers and add new authentication servers.

Authentication Servers area

The Authentication Servers area displays the authentication servers that the management server communicates with to find and authenticate remote users. The credentials for remote users or groups are maintained by the authentication server.

- **Command buttons**

  Enables you to add, edit, or delete authentication servers.

  - Add

    Enables you to add an authentication server.

    If the authentication server that you are adding is part of a high-availability pair (using the same database), you can also add the partner authentication server. This enables the management server to communicate with the partner when one of the authentication servers is unreachable.

  - Edit

    Enables you to edit the settings for a selected authentication server.

  - Delete

    Deletes the selected authentication servers.

- **Name or IP Address**

  Displays the host name or IP address of the authentication server that is used to authenticate the user on the management server.

- **Port**

  Displays the port number of the authentication server.

- **Test Authentication**

  This button validates the configuration of your authentication server by authenticating a remote user or group.

While testing, if you specify only the user name, the management server searches for the remote user in the authentication server, but does not authenticate the user. If you specify both the user name and password, the management server searches and authenticates the remote user.

You cannot test the authentication if remote authentication is disabled.

Copyright information

Trademark information