opentext™

Access Manager CE 24.2 (v5.1)

Best Practices Guide

May 2024

Legal Notice

Contents

About this Book and the Library 5

1 Design Considerations 7

1.1 Access Manager Component Deployment . . . 7
1.2 Firewall Settings . . . 9
1.3 Configuring Domain Name Server . . . 9
1.4 Configuring a Back Channel Traffic . . . 9
1.5 Network Time Protocol . . . 9

2 Configuration Tips 11

2.1 Tips for Configuring Administration Console . . . 11
2.1.1 Creating Multiple Administrator Accounts . . . 11
2.1.2 Installing Secondary Versions of Administration Console . . . 11
2.2 Applying the Configuration . . . 11
2.2.1 Backing Up and Restoring Configuration . . . 12
2.2.2 Exporting and Importing Configuration . . . 12

3 Common Configuration Tasks 13

3.1 Configuring User Stores . . . 13
3.2 Setting Up Strong Authentication . . . 13
3.3 Customizing Login Pages, Logout Pages, and Messages . . . 14
3.4 Setting Up Federations . . . 14
3.5 Associating Access Gateway with Identity Server . . . 14
3.6 Setting Up Google Applications . . . 14
3.7 Best Practices for Configuring Protected Resources . . . 15
3.8 Configuring Single Sign-On For Office 365 Services . . . 16
3.9 Protecting SharePoint 2013 and 2016 . . . 16
3.10 Configuring the Persistent Authentication . . . 16
3.11 Configuring Support for Access Manager on Google Chrome Browser . . . 16

4 Performance Tuning 19

4.1 Tuning Identity Server for Performance . . . 19
4.1.1 Basic Tuning Options . . . 19
4.1.2 Disabling User Profile Objects . . . 20
4.1.3 Configuring a Specific IP Address for Proxied Requests . . . 21
4.1.4 Configuring Java Memory Allocations . . . 23
4.2 Tuning Access Gateway for Performance . . . 24
4.2.1 Basic Tuning Options . . . 24
4.2.2 Configuring a Specific IP Address for Proxied Requests . . . 25
4.2.3 Configuring Access Gateway ESP to Reduce Access Gateway Load and Improve Performance . . . 27
4.2.4 Java Memory Allocations . . . 28

4.2.5 Performance Tips 29
4.2.6 Setting Cache Store Size in Access Gateway Appliance 29
4.3 Tuning the Policy Performance 29

5 Best Practices for Certificates 31

5.1 Getting the Certificate Expiration Notification 31
5.2 Renewing the Expired eDirectory Certificates 33

6 Troubleshooting 35

About this Book and the Library

The purpose of this Best Practices Guide is to help administrators with configuration guidelines to obtain the best performance with Access Manager components. It is not a comprehensive instruction set. Administrators using this guide should consult product documentation, technical information documents (TID), and online help for further instruction regarding each of the guidelines offered here.

Intended Audience

This guide is intended for Access Manager administrators.

Other Information in the Library

You can access other information resources in the library at the following locations:

- Access Manager Product Documentation (https://www.microfocus.com/documentation/access-manager/index.html)
- Access Manager Developer Resources (https://www.microfocus.com/documentation/access-manager/developer-documentation-5.0/)

NOTE: Contact namsdk@opentext.com for any query related to Access Manager SDK.

---

1 Design Considerations

This section describes the architectural suggestions for Access Manager.

- Section 1.1, “Access Manager Component Deployment,” on page 7
- Section 1.2, “Firewall Settings,” on page 9
- Section 1.3, “Configuring Domain Name Server,” on page 9
- Section 1.4, “Configuring a Back Channel Traffic,” on page 9
- Section 1.5, “Network Time Protocol,” on page 9

For information about additional security setups, see *NetIQ Access Manager CE 24.2 (v5.1) Security Guide* .

1.1 Access Manager Component Deployment

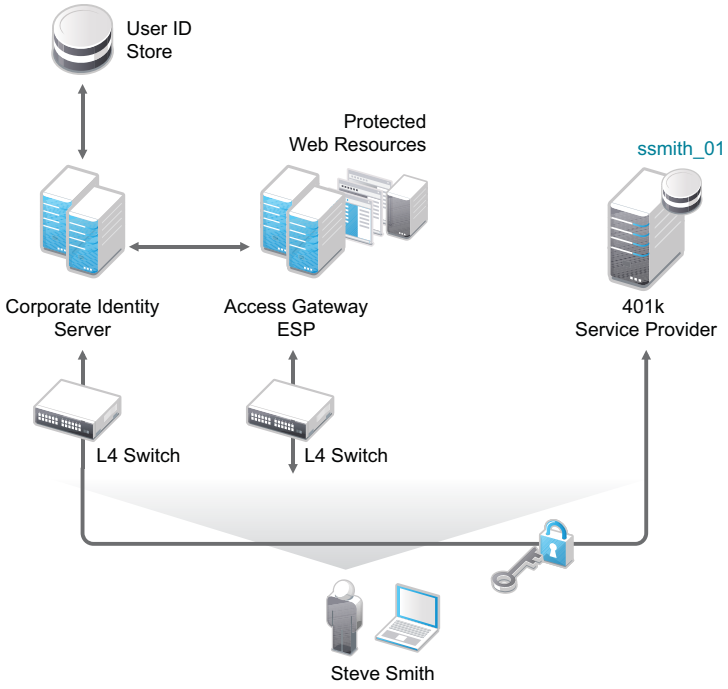
The components of Access Manager include Administration Console, Identity Server, and Access Gateway.

Administration Console: Manages Identity Server and Access Gateway.

Identity Server: Provides authentication functionality for the users and it uses the back-end LDAP servers to validate the user credentials.

Access Gateway: Access Gateway protects web servers and contacts Identity Server for users authentication. It also gets user attributes from Identity Server and passes on to the web servers.

The following diagram illustrates how Access Manager components are integrated with each other:



The recommended number of components nodes that are required are based on the concurrent user sessions. For more information, see *NetIQ Access Manager Performance and Sizing Guidelines* .

The following are the recommended configurations for the Access Manager components:

- Enable Sticky-Bit on the Layer 4 (L4) switch.

  Each L4 switch has a slightly different method and terminology for the sticky bit or persistence bind. This bit allows a client that has established a session to be directed to the same Identity Server or Access Gateway for all requests sent during the session. This minimizes the need to forward session information between Access Gateways or between Identity Servers and thus maximizes performance.
- L4 health check recommendations:
  - Heartbeat URL checks should occur every 30 seconds.
  - Access Manager devices should be removed from the service after three failures.

    For more information, see “Configuration Tips for the L4 Switch ” in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.
- Ensure that the LDAP time out setting in Identity Server, Active Directory (if using it as a user store), Web servers, and the L4 switch are all set to the same value. Based on an average user session, the recommended value is 15-20 seconds.
- To improve the performance of Identity Servers, ensure that Identity Server can perform a reverse lookup on the LDAP user store’s IP address. If the LDAP user store’s IP addresses are not part of the DNS server, make an entry in the hosts file of Identity Server.
- Set the TCP idle time in Access Gateway lower than the LDAP time out to clear the connection table in Access Gateway. If this time is not set, Linux fills the connection table making it almost impossible to log in if the sessions are not cleared.

1.2 Firewall Settings

Before you install other Access Manager components and import them into Administration Console, or before you log in to Administration Console from a client machine, you must first configure the firewall on Administration Console.

For more information, see "Configuring the Administration Console Firewall" and "Setting Up Firewalls" in the *NetIQ Access Manager CE 24.2 (v5.1) Installation and Upgrade Guide*.

1.3 Configuring Domain Name Server

Access Manager devices know each other by their IP addresses, and some requests require them to match an IP address with the device DNS name.

For more information, see "Configuring Name Resolution" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

1.4 Configuring a Back Channel Traffic

The default behavior for Identity Server and Access Gateway is to use the same IP address for incoming client requests, for proxied requests, and for management tasks. You can improve performance by separating this traffic into separate pools via IP addresses. You can also use the IP addresses to route the traffic so that it remains behind the firewall.

For more information, see Section 4.1.3, "Configuring a Specific IP Address for Proxied Requests," on page 21 and Section 4.2.2, "Configuring a Specific IP Address for Proxied Requests," on page 25.

1.5 Network Time Protocol

For trusted authentication to work, the time must be synchronized between Identity Server and Access Gateway and the time difference must be within one minute of each other. For Identity Server or Access Gateway Service, use YaST to verify the time settings.

If you have a Network Time Protocol server, configure the Access Manager machines to use it.

For more information, see "Verifying Time Synchronization" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

2 Configuration Tips

In this Chapter

- Tips for Configuring Administration Console
- Applying the Configuration

2.1 Tips for Configuring Administration Console

- Section 2.1.1, “Creating Multiple Administrator Accounts,” on page 11
- Section 2.1.2, “Installing Secondary Versions of Administration Console,” on page 11

2.1.1 Creating Multiple Administrator Accounts

Administration Console is installed with one administrator user account. It is recommended to have more than one administrator account. If a user forgets the password, you have other administrator user accounts to access Administration Console and to reset the password. If you have multiple administrators, you might want to create a user account for each one so that log files reflect the modifications of each administrator. The easiest way to do this is to create a new user as a trustee of the tree root with [Entry Rights] for Supervisor and inheritable rights assignment. This also ensures that you have more than one user who has full access to Administration Console.

For more information, see “Managing Administrators” in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

2.1.2 Installing Secondary Versions of Administration Console

You can create fault tolerance by installing up to two secondary consoles. NetIQ recommends that you install at least one secondary console.

For more information, see “Installing Secondary Administration Console” in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

2.2 Applying the Configuration

- Section 2.2.1, “Backing Up and Restoring Configuration,” on page 12
- Section 2.2.2, “Exporting and Importing Configuration,” on page 12

2.2.1 Backing Up and Restoring Configuration

It is recommended to back up your Access Manager configuration before you make changes to the configuration. Later, you can restore the Access Manager configuration.

For more information, see “Back Up and Restore” in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

2.2.2 Exporting and Importing Configuration

You can export and import Access Manager configuration changes through Advanced File Configurator.

For more information, see “Exporting and Importing Configurations” in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

3 Common Configuration Tasks

In this Chapter

- Configuring User Stores
- Setting Up Strong Authentication
- Customizing Login Pages, Logout Pages, and Messages
- Setting Up Federations
- Associating Access Gateway with Identity Server
- Setting Up Google Applications
- Best Practices for Configuring Protected Resources
- Configuring Single Sign-On For Office 365 Services
- Protecting SharePoint 2013 and 2016
- Configuring the Persistent Authentication
- Configuring Support for Access Manager on Google Chrome Browser

3.1 Configuring User Stores

User stores are LDAP directory servers which are used to authenticate end users. You must specify an initial user store when creating an Identity Server configuration. You must use the same procedure for setting up the initial user store, adding a user store, or modifying an existing user store.

Identity Server has built-in support to interact with eDirectory, Active Directory, and Sun One Directory. Identity Server also provides a framework to plug in other user stores.

The LDAP Server Plug-In is available in the NetIQ Access Manager Developer Kit. For more information, see the *Access Manager 5.0 SDK Guide*.

For all Identity Servers to communicate with the user store over SSL, you need to import the trusted root of the user store into Identity Server's trust store.

For more information, see “Configuring Identity User Stores” in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

3.2 Setting Up Strong Authentication

You can enable strong authentication by using other methods such as x509 or NESCM to increase the security than using the form based method. You can also use multi-factor for more security.

For more information, see “Configuring Authentication” in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

For more information about extending the authentication mechanisms, see Identity Server Authentication API in the *Access Manager 5.0 SDK Guide*.

3.3 Customizing Login Pages, Logout Pages, and Messages

You can customize the login and logout pages, and error messages for the Access Manager components.

For information about customizing the login page, logout page, and error messages in Identity Server, see "Customizing User Portal".

For more information about customizing the error messages and error pages in Access Gateway, see "Customizing Error Messages and Error Pages on Access Gateway".

For more information about customizing logout requests in Access Gateway, see Customizing Logout Requests.

NOTE: After modifying a JSP file to customize the login page, logout page, and error messages, you need to sanitize the JSP file to prevent XSS attacks. See "Cross-site Scripting Attacks" in the NetIQ Access Manager CE 24.2 (v5.1) Security Guide .

3.4 Setting Up Federations

Federation allows a user to associate two accounts with each other. This allows the user to log into one account and access the resources of the other account without logging in to the second account. It is one method to provide single sign-on when a user has accounts in multiple user stores.

You can set up two types of federation:

- Persistent: Permanent federation among accounts. Set up this federation when you want a user account at the service provider to be associated with a user account at the identity provider after authentication.
- Transient: Temporary federation among accounts. Federation expires with the session.

For more information, see "Configuring Authentication" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

3.5 Associating Access Gateway with Identity Server

It is recommended to enable SSL for communication between Access Gateway and Identity Server. See "Configuring SSL Communication with Browsers and Access Gateway " in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

3.6 Setting Up Google Applications

You can configure Access Manager to provide the single sign-on services to the Google applications by using SAML 2.0.

For more information, see "Setting Up Google Applications" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

Access Manager also provides an easy way to configure this federation by using a connector. For more information, see *Access Manager CE 24.2 (v5.1) Applications Configuration Guide*.

3.7 Best Practices for Configuring Protected Resources

A protected resource configuration specifies the directories on the web server that you want to protect. The protected resource configuration specifies the authorization procedures and policies for enforcing protection. Authentication procedures and policies (Authorization, Identity Injection, and Form Fill) enable the single sign-on environment for the user. The type of protection a resource requires depends upon the resource, the Web server, and the conditions you define for the resource.

You can select the following types of protection:

Authentication Procedures: Specifies the type of credentials the user must use to log in such as name and password or secure name and password. You can select None for the procedure, which allows the resource to be a public resource, with no login required. In addition to selecting the contract, you can also configure how the authentication procedure handles subsequent authentication requests from an application.

Authorization Policy: Specifies the conditions a user must meet to be allowed access to a protected resource. You define the conditions, and Access Gateway enforces the Authorization policies. For example, you can assign roles to your users, and use these roles to grant and deny access to resources.

Identity Injection Policy: Specifies the information that must be injected into the HTTP header. If the Web application has been configured to look for certain fields in the header and the information cannot be found, the Web application determines whether the user is denied access or redirected. The Web application defines the requirements for Identity Injection. The Identity Injection policies allow you to inject the required information into the header.

Form Fill Policy: Allows you to manage forms that Web servers return in response to client requests. Form fill allows you to pre-populate fields in a form on first login and then securely save the information in the completed form to a secret store for subsequent login. The user is prompted to re-enter the information only when something changes, such as a password.

These policies allow you to design a custom access policy for each protected resource:

- Resources that share the same protection requirements can be configured as a group. You set up the policies, and then add the URLs of each resource that requires these policies.
- A resource that has specialized protection requirements can be set up as a single protected resource. For example, a page that uses Form Fill is usually set up as a single protected resource.

Avoid configuring a policy for a protected resource with a path /* unless it is required. We recommend that configure the policy for protected resources with specific paths. For example, identityinjection/subpath/* or acl/credentialprofile/*.

While configuring a Form Fill policy, try to provide the details such as **Page Matching Criteria** and **Form Name**, so that it matches only the specified form not the other pages. Also, if possible, configure the Form Fill policy for a page instead of a path.

For more information about how to configure a protected resource, see“Configuring Protected Resources” in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

3.8 Configuring Single Sign-On For Office 365 Services

Access Manager is compatible with Microsoft Office 365 and provides single sign-on access to Office 365 services.

For more information, see "Configuring Single Sign-On for Office 365 Services" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

Access Manager also provides an easy way to configure this federation by using a connector. For more information, see *Access Manager CE 24.2 (v5.1) Applications Configuration Guide*.

3.9 Protecting SharePoint 2013 and 2016

You can enable SSO to SharePoint Server 2013 or SharePoint 2016 by using WS Federation claims-based authentication. In this configuration, Access Manager works as a WS Federation claims provider for SharePoint Server.

Access Manager contains a set of claims. Each claim represents a specific information about a user, such as username, group memberships, and role on the network. SharePoint versions 2013 and 2016 support claims-based authentication by obtaining the security token from the user and using the information within the claims to determine access to resources.

For information about how to protect SharePoint, see "Configuring SSO to SharePoint Server" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

3.10 Configuring the Persistent Authentication

You can use the persistent authentication only for applications that do not require very high security. It is recommended to configure the CryptoKey as class level property for the contract. The CryptoKey must be long and random to keep the user information secure.

For information about how to configure the persistent authentication, see "Persistent Authentication" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

3.11 Configuring Support for Access Manager on Google Chrome Browser

Google Chrome version 80 introduces a change in how cookies are handled in web browser. To support this Chrome version, perform the following steps:

For Identity Server

1. Open Identity Server's web.xml.
2. Uncommont the `ResponseCookieProcessor` filter configuration to set the `<param-name>` in the file.

You must change the value from *Active* to *True*.

```
<filter>
       <filter-name>ResponseCookieProcessor</filter-name>
       <filter-
class>com.novell.nidp.servlets.filters.cookie.ResponseCookieProcessor</filter-
class>
       <description> This filter is used to edit Response cookies before
delivering to the client.</description>
       <init-param>
              <param-name>Active</param-name>
              <param-value>False</param-value>
       </init-param>
       <init-param>
              <param-name>SameSiteLevel</param-name>
              <param-value>None</param-value>
       </init-param>
   </filter>
   <filter-mapping>
       <filter-name>ResponseCookieProcessor</filter-name>
       <url-pattern>/*</url-pattern>
 </filter-mapping>
```

For information about how to open and edit a file, see "Modifying Configurations" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

For Access Gateway:

1. On the **Home** page, click **Access Gateways** > **Edit** > **Advanced Options**.
2. Add the following Global Advanced Options:
   - `NAGGlobalOptions SameSiteCookie=on`. This option sets `SameSite=None` to all Set-Cookie headers coming from Access Gateway.
   - `NAGGlobalOptions SameSiteOption <input-string>.`

     Instead of using the default value *None* for the SameSite value, you can set it to *Lax* or *Strict*. For example, `NAGGlobalOptions SameSiteOption "SameSite=Strict"` or `NAGGlobalOptions SameSiteOption "SameSite=Lax"`.
3. (Optional) On the **Home** page, click **Access Gateways** > **Edit** > **[Name of Reverse Proxy]** > **[Name of Proxy Service]** > **Advanced Options**.
4. Add the following options at proxy service level:
   - NAGHostOptions SameSiteCookie=*on*
   - NAGHostOptions SameSiteOption SameSite=<*input-string*>. <*input-string*> can be *Strict* or *Lax*.

     For more information about these options, see Access Gateway Advanced Options in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

4 Performance Tuning

- Section 4.1, “Tuning Identity Server for Performance,” on page 19
- Section 4.2, “Tuning Access Gateway for Performance,” on page 24
- Section 4.3, “Tuning the Policy Performance,” on page 29

4.1 Tuning Identity Server for Performance

Use the following information to improve the performance of your Identity Server cluster.

- Section 4.1.1, “Basic Tuning Options,” on page 19
- Section 4.1.2, “Disabling User Profile Objects,” on page 20
- Section 4.1.3, “Configuring a Specific IP Address for Proxied Requests,” on page 21
- Section 4.1.4, “Configuring Java Memory Allocations,” on page 23

4.1.1 Basic Tuning Options

The following Access Manager components and features can affect the performance of Identity Server cluster.

LDAP User Stores: This critical component can be a major cause for slowness, depending upon configuration, hardware, and the layout of the directory. Configure search contexts to avoid LDAP searches that traverse the entire tree.

L4 Switch: If the switch is slow or mis-configured, it can severely impact performance. You need to make sure the switch has ample capacity to handle the traffic. If possible, clustered Identity Servers should be plugged directly into the switch or segmented accordingly. It is also critical that you enable sticky bit/persistence on the L4 switch. When this feature is not enabled, the product may not handle the traffic correctly.

For tips on how to set up the L4 switch, see “Configuration Tips for the L4 Switch ” in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

Enabled Protocols: On the Configuration page (click **Identity Servers** > [cluster name] > **Configuration** > **General**), you can select which protocols to enable. The Liberty protocol needs to be enabled, but each additional protocol adds a little processing overhead. Do not enable protocols unless you are using them.

Session Failover: On the Cluster Details page (**Identity Servers** > dot menu of the cluster > **Cluster Details**), you can set up session failover so that if an Identity Server in the cluster goes down, the user does not lose any session data. This feature adds some overhead, because Identity Servers need to share some authentication information. You need to balance the need to preserve user session data with the increase in authentication traffic. For best performance, specify the minimum number of peers.

Limit User Sessions: On the General Configuration page (click **Identity Servers** > [cluster name] > **Configuration** > **General**, you can select to limit the number of sessions a user can have. When a user is limited to a specific number of sessions, Identity Servers must check with the other servers in the cluster before establishing a new session. This check adds a little overhead to each new authentication request.

Authentication Timeouts: For each contract, specify an authentication time-out (**Identity Servers** > [cluster name] > **Authentication** > **Contracts** > **[Name of Contract]**). Short time-outs generate more authentication traffic. Carefully consider the security requirements for your resources and set limits that meet the requirements. If you need to verify only users those are actively using a session, have all these protected resources use the same contract, or have them share the same activity realm.

Logging: You need to manage the size and number of log files as well as the logging level. You should increase the log level to Debug only when you are troubleshooting a problem. As soon as the problem is resolved, you should reduce the log level. You should also have a schedule to check the number and size of the log files and to remove the older log files.

Auditing: You need to carefully select the events that you audit. Selecting all events that are available for the Access Manager components can impact performance. For example, the Login Provided event generates an event every time a user authenticates. If you have many users, this one event could impact performance. Analyze your needs. Are you really interested in who logged in, or are you more interested in who failed to log in?

4.1.2 Disabling User Profile Objects

If you do not use the default configuration for storing Form Fill secrets and you have not enabled persistent federation between identity and service providers, you can disable the creation of objects under the LibertyUserProfile container in the configuration data store. The default behavior is to create an object in this container for each user accessing the system, and the login process checks for a matching user in this container.

If you have thousands of users, the following symptoms might indicate that the user profile objects are slowing down the login process:

- On Administration Console, the ndsd process is running at 100%.
- Running the backup utility is very slow.
- Logging in to Administration Console is very slow.

To discover whether profile objects are causing a slowdown, open an LDAP browser (or in Administration Console, select the **View Objects** task in the menu bar). Expand the following objects: novell > accessManagerContainer > nids > cluster. Expand the SCC objects, and look for objects stored in LibertyUserProfile objects.

- If you have only a few hundred of these objects, user profile objects are not slowing the authentication process.
- If you have thousands of these objects, user profile objects are probably causing a slowdown. You can speed up authentication by disabling the use of these objects. When you do this, Identity Server no longer creates objects in the LibertyUserProfile container, and it does not try to match an authenticating user with a profile object.

To prevent the creation and use of user profile objects, modify the Identity Server configuration as follows:

1. In Administration Console, on the **Home** page, click **Identity Servers > Edit Cluster > Liberty > Web Service Provider**.
2. Disable the following profiles:
   - Personal Profile
   - Employee Profile
   - Custom Profile
3. Disable the Credential Profile (which also disables using Form Fill or Identity Injection with credentials) or enable the Credential Profile and modify its default configuration:
   - **3a** Click **Credential Profile**.
   - **3b** Select to store secrets with the **Extended Schema User References** option.

     When the Credential Profile is enabled, the default behavior is to create user profile objects and store the secrets there. You must configure one of these other options to store the secrets. For more information, see"Configuring a User Store for Secrets" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.
4. Click **OK** > **OK** and update Identity Server.
5. Disable the use of the user profile objects:
   - **5a** Open Identity Server's web.xml.

     For information about how to open and modify a file, see "Modifying Configurations" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.
   - **5b** Add the following lines to the file:

```
<context-param>
 <param-name>cpAuthorityType</param-name>
 <param-value>memory</param-value>
</context-param>
```

4.1.3 Configuring a Specific IP Address for Proxied Requests

The default behavior for Identity Server is to use the same IP address for incoming client requests, for proxied requests, and for management tasks. You can improve performance by separating this traffic into separate pools via IP addresses. You can also use the IP addresses to route the traffic so that it remains behind the firewall.

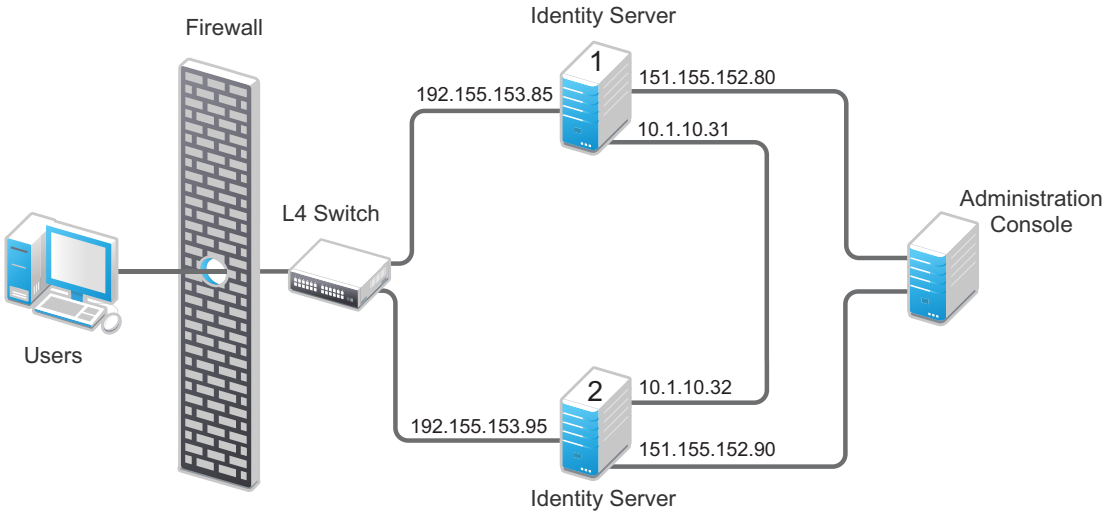
You can specify the IP address that an Identity Server uses for proxied requests to other members of the cluster. A proxied request is sent to another member of a cluster when the request is not sent to the authoritative server.

An authoritative server is the cluster member that holds the authentication information for a given user session. For a request associated with a given session to be processed, it must be routed or proxied to the authoritative cluster member. If an L4 switch sends a request to a non-authoritative cluster member, that cluster member proxies that request to the authoritative cluster member.

You can also specify the IP address for the communication that takes place between Identity Server and Administration Console for management tasks. This includes configuration updates, health checks, and statistics. To configure this IP address, log in to Administration Console, then click **Identity Servers** > dot menu of the server > **Server Details**.

Figure 4-1 illustrates a configuration with a two-member cluster. The L4 switch sends client traffic to Identity Servers by using the IP addresses that start with 192. The IP addresses that start with 10 are used to route proxied requests to the cluster members. The IP addresses starting with 151 are used for the management traffic with Administration Console.

Figure 4-1 *Two-Member Identity Server Cluster*



To specify the IP address for the proxied requests on the SOAP channel:

1. Gather the required information. For each Identity Server in the cluster, you need the following information:
   - Management IP address. (To get this value or modify the value, on the **Home** page, click **Identity Servers** > **Configuration** > **Name**.
   - IP address or IP address with port that is available to use for proxied requests.
2. Open Identity Server's web.xml.

   For information about how to open and edit a file, see "Modifying Configurations" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.
3. Add a proxyAddessMap parameter entry to the file.

   ```
   <context-param>
       <param-name>proxyAddressMap</param-name>
       <param-value>Managament_IP, unused, Proxied_Request_IP
           </param-value>
   </context-param>
   ```
4. Adjust the `<param-value>` element as necessary.

The <param-value> element specifies the IP addresses that are used by the other members of the cluster. It is a comma-separated list of IP addresses. You need a value entry for each member of the cluster, except the cluster member you configure. A member does not send proxied requests to itself, so you do not need to add it. Each value entry must contain three IP addresses:

- Replace *Management_IP* with the management IP address of Identity Server. You cannot specify a port with this entry.
- Replace *unused* with just a space. If you configure this feature for Access Gateway, this IP address entry is used for the reverse proxy IP address. Identity Server does not have a reverse proxy.
- Replace *Proxied_Request_IP* with the address to use for the proxied requests (also called the SOAP back channel). You can specify a port with entries, such as `151.155.152.90:445`.

For Identity Server 1 in Figure 4-1, the entry should look similar to the following lines:

```
<context-param>
   <param-name>proxyAddressMap</param-name>
   <param-value>151.155.152.90,10.1.10.32</param-value>
</context-param>
```

If your cluster has three or more members, you need to add addresses for the other members. The following example shows an entry for Identity Server 1 in Figure 4-1 if the cluster contains a third member:

```
<context-param>
   <param-name>proxyAddressMap</param-name>
   <param-value>151.155.152.90,10.1.10.32,
       151.155.152.100,10.1.10.33</param-value>
</context-param>
```

After sending the change to devices, click **Update All** on the Identity Servers page to apply the configuration change. This action restarts services.

4.1.4 Configuring Java Memory Allocations

The Tomcat configuration file controls the amount of memory that Tomcat can allocate for Java. If you have installed Identity Server on a machine with the recommended 4 GB of memory, you can modify two parameters in this file to improve performance under heavy load:

1. Open Identity Server's tomcat.conf.

   For information about how to open and modify a file, see "Modifying Configurations" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

2. Find the following line in the file:

   ```
   JAVA_OPTS="-server -Xmx2048m -Xms512m -Xss128k
   ```

   This `-Xmx` value is ideal for a system with 4 GB of memory. If the system has more physical memory, increase the `-Xmx` value. For example, if the system has 8 GB of memory, increase `-Xmx` to 4096.

3. Find the following line in the file:

   ```
   JAVA_OPTS="${JAVA_OPTS} -Dnids.freemem.threshold=10"
   ```

4 Change the `-Dnids.freemem.threshold` value to a value between 5 and 15 based on your requirement. The default value is 10.

This prevents user sessions from using up all the memory and ensures that there is free memory available so that the other internal Java processes can continue to function. When this threshold is reached, the user receives a 503 Server Busy message and a threshold error message is logged to the `catalina.out` file.

For example, the threshold value is 10. When the memory goes above 90% used, the user receives a 503 Server Busy message.

4.2 Tuning Access Gateway for Performance

Use the following information to improve the performance of your Access Gateway cluster.

- Basic Tuning Options
- Configuring a Specific IP Address for Proxied Requests
- Configuring Access Gateway ESP to Reduce Access Gateway Load and Improve Performance
- Java Memory Allocations
- Performance Tips
- Setting Cache Store Size in Access Gateway Appliance

4.2.1 Basic Tuning Options

The following Access Manager components and features can affect the performance of Access Gateway cluster:

Maximum Number of User Sessions: It is recommended that you keep the maximum number of user sessions per Access Gateway to 48,000. If your Access Gateways are exceeding this number or getting close to it, you can add another Access Gateway to the cluster.

If you want to support more than 48,000 sessions per Access Gateway, you need to modify the Java memory parameters. For configuration information, see Java Memory Allocations.

LDAP Attributes: If policies use LDAP attributes, configure the embedded service provider (ESP) to obtain these attribute values at authentication. When a policy needs to be evaluated for a user, the values are then available in cache. If the values are not in cache, an LDAP query must be sent to retrieve them. If the user then accesses another resource that requires different LDAP attributes, another query must be sent. For configuration information, see "Sending Attributes to the Embedded Service Provider" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

Web Servers: Web servers or services can be a major cause of slowness because they process the most information. You need to examine the content on the Web servers. If users are requesting static pages with multiple images, you need to improve the performance by having Access Gateway cache these pages. For information about cache configuration options, see "Configuring Cache Options" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

If your Web servers serve dynamic content, you can upgrade that Web servers to faster hardware, or you can add another server to the group of Web servers serving the dynamic content.

L4 Switch: If the switch is slow or mis-configured, it can severely impact performance. You need to make sure the switch has ample capacity to handle the traffic. If possible, clustered Access Gateways should be plugged directly into the switch or segmented accordingly. It is also critical that you enable sticky bit/persistence on the L4 switch. When this feature is not enabled, the product handles the traffic correctly, but the system can run up to 50% slower than when persistence is enabled.

See "Configuration Tips for the L4 Switch " in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

Policies: You need to implement the Authorization, Identity Injection, and Form Fill policies so that they execute as quickly as possible. For example, a Form Fill policy impacts performance when the form matching criteria are set up so that an entire directory of files must be searched before the form is found. Also, when policies are assigned to a protected resource, one policy with ten actions executes faster than ten policies with one action in each policy.

Logging: You need to manage the size and number of log files as well as the logging level. You should increase the log level to Debug only when you troubleshoot a problem. As soon as the problem is resolved, you should reduce the log level. You should also have a schedule to check the number and size of the log files and to remove the older log files.

Auditing: You need to carefully select the events that you audit. Selecting all events that are available for the Access Manager components can impact performance. For example, the URL Accessed event of Access Gateway generates an event every time a user accesses a resource. If you have many users and many resources that these users access, selecting this event could impact performance. You need to analyze your needs to see if you need to audit all URLs accessed. If you need to audit only a few URLs, you can use proxy service logging to gather the information. See "Configuring Logging for a Proxy Service"in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

Access Gateway Service: See Section 4.2.5, "Performance Tips," on page 29.

4.2.2 Configuring a Specific IP Address for Proxied Requests

The default behavior for Access Gateway is to use the same IP address for incoming client requests, for proxied requests, and for management tasks. You can improve performance by separating this traffic into separate pools via IP addresses. You can also use the IP addresses to route the traffic so that it remains behind the firewall.

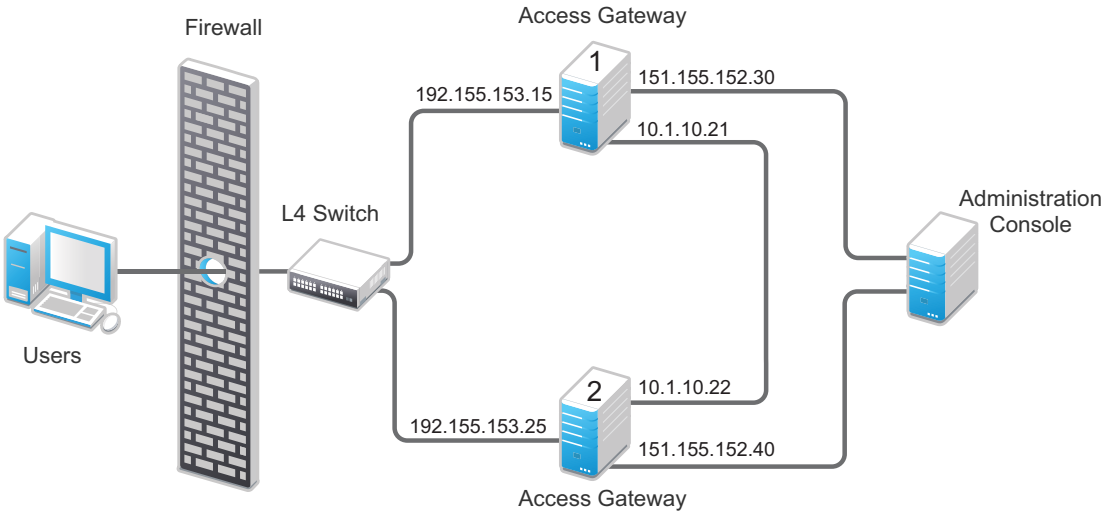
You can specify the IP address that an Access Gateway uses for proxied requests to other members of the cluster. A proxied request is sent to another member of a cluster when the request is not sent to the authoritative server.

An authoritative server is the cluster member that holds the authentication information for a given user session. For a request associated with a given session to be processed, it must be routed or proxied to the authoritative cluster member. If an L4 switch sends a request to a non-authoritative cluster member, that cluster member proxies that request to the authoritative cluster member.

You can also specify the IP address for the communication that takes place between Access Gateway and Administration Console for management tasks. This includes configuration updates, health checks, and statistics. To modify this IP address, log in to Administration Console, on the **Home** page, click **Access Gateways > [Name of Access Gateway]**.

Figure 4-2 illustrates a configuration with a two-member cluster. The L4 switch sends client traffic to Access Gateways by using the IP addresses that start with 192. The IP addresses that start with 10 are used to route proxied requests to the cluster members. The IP addresses starting with 151 are used for the management traffic with Administration Console.

Figure 4-2 *Two-Member Access Gateway Cluster*



To specify the IP address for the proxied requests on the SOAP channel:

1. Gather the required information. For each Access Gateway in the cluster, you need the following information:
   - IP address of the authenticating reverse proxy. To get this value, on the **Home** page, click **Access Gateways** > **Edit**. Select the reverse proxy that is used for authentication. Use the **Cluster Member** drop-down list to display the IP address for the various cluster members.
   - Management IP address. To get this value or modify the value, click **Access Gateways** > **Name of Access Gateway**.
   - IP address or IP address with port that is available to use for proxied requests.
2. Open Access Gateway's web.xml.

   For information about how to open and modify a file, see "Modifying Configurations" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.
3. Add the proxyAddessMap parameter entry to the file.

   ```
   <context-param>
       <param-name>proxyAddressMap</param-name>
       <param-value>Managament_IP, Reverse_Proxy_IP, Proxied_Request_IP
           </param-value>
   </context-param>
   ```

   The `<param-value>` element specifies the IP addresses that are used by other members of the cluster. It is a comma-separated list of IP addresses. You need a value entry for each member of the cluster, except the cluster member you configure. A member does not send proxied requests to itself, so you do not need to add it. Each value entry must contain three IP addresses:
   - Replace *Management_IP* with the management IP address of Access Gateway. You cannot specify a port with this entry.

- Replace *Reverse_Proxy_IP* with the IP address of the reverse proxy of Access Gateway. You cannot specify a port with this entry.
- Replace *Proxied_Request_IP* with the address to use for the proxied requests (also called the SOAP back channel). You can specify a port with this entry, such as `151.155.152.30:445`.

For Access Gateway 1 in Figure 4-2, the entry should look similar to the following lines:

```
<context-param>
   <param-name>proxyAddressMap</param-name>
   <param-value>151.155.152.40,192.155.153.25,10.1.10.22</param-value>
</context-param>
```

If your cluster has three or more members, you need to add addresses for the other members. The following example shows an entry for Access Gateway 1 in Figure 4-2 if the cluster contained a third member.

```
<context-param>
   <param-name>proxyAddressMap</param-name>
   <param-value>151.155.152.40,192.155.153.25,10.1.10.22,
       151.155.152.50,192.155.153.35,10.1.10.23</param-value>
</context-param>
```

4.2.3 Configuring Access Gateway ESP to Reduce Access Gateway Load and Improve Performance

1. Identify all policies that are enabled for each defined protected resource.
2. Go through each of these policies and note the attributes that are required by this policy.

   For example, you might find that single policy is enabled for one protected resource and the policy requires the following attributes: all user roles, LDAP cn, LDAP roomNumber, LDAP mail, and LDAP title.
3. Define an attribute set that contains all attributes required by Access Gateway enabled policies.

   For information about how to configure a new attribute set, see "Configuring Attribute Sets" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

   NOTE: The local attribute must include the attribute that Identity Server evaluates. Ignore the Remote Attribute option for communications between Identity Server and embedded service provider (ESP).

   ---
4. In Administration Console, on the **Home** page, click **Identity Servers** > **Servers** > **Edit** > **Liberty**, then select Access Gateway or Access Gateway cluster configuration for which you want to use the newly defined attribute set.
5. Add the newly defined attribute set to the Liberty relationship between Identity Server and the selected ESP.

   For information about how to add the attribute set, see "Configuring the Attributes Sent with Authentication" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.
6. Define the attribute refresh rate for the policy.

   The LDAP attribute for an Identity Injection or Form Fill policy can be configured to refresh its value according to a specified interval.

For information, see“Using the Refresh Data Option” in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

This refresh rate determines how often Access Gateway proxy must go back to the ESP to determine whether the data is valid. For performance purposes, you should define the **Session** setting for retrieving the attributes only one time during the session. This reduces the communication between Access Gateway proxy and the ESP.

7 Inject Identity Server user name and password to the back-end Web server.

If the policy requires the credential profile user name and password to be sent to the back-end Web server, the attribute map must include the credential profile details. Unlike regular LDAP attributes, these credential profile attributes must be mapped to a Remote Attribute name.

The Remote Attribute name is case-sensitive.

You need to map the UserName, userPassword, and userDN credential profile attributes. When you define the attributes to send to the back-end Liberty ESP, you need to send the UserName and userPassword. The userDN can be left in the available list because it was already sent in a SAML assertion by default at authentication time.

4.2.4 Java Memory Allocations

The Tomcat configuration file controls the amount of memory that Tomcat can allocate for Java. If you have installed your Access Gateway on a machine with the recommended 4 GB of memory, you can modify two parameters in this file to improve performance under heavy load:

On Access Gateway Appliance, you need to modify just the free memory threshold for best performance. On Access Gateway Service, you need to modify the free memory threshold and the amount of memory that Java can use.

1 Open Access Gateway’s tomcat.conf.

For information about how to open and modify a file, see “Modifying Configurations” in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

2 Find the following line in the file:

```
JAVA_OPTS="-server -Xmx2048m -Xms512m -Xss128k
```

This `-Xmx` value is ideal for a system with 4 GB of memory. If the system has more physical memory, increase the `-Xmx` value. For example, if the system has 8 GB of memory, increase `-Xmx` to 4096.

3 Find the following line in the file:

```
JAVA_OPTS="${JAVA_OPTS} -Dnids.freemem.threshold=10"
```

4 Change the `-Dnids.freemem.threshold` value to a value between 5 and 15 based on your requirement. The default value is 10.

This prevents user sessions from using up all the memory and ensures that there is free memory available so that the other internal Java processes can continue to function. When this threshold is reached, the user receives a 503 Server Busy message and a threshold error message is logged to the `catalina.out` file.

For example, the threshold value is 10. When the memory goes above 90% used, the user receives a 503 Server Busy message.

4.2.5 Performance Tips

Caching: Use a high performance disk system for the cache directory, such as tempfs on Linux.

You can improve the speed of adding files to cache and retrieving them from cache if you turn off gathering cache statistics. On the **Home** page, click **Access Gateways > Edit > Advanced Options** and add the following command:

```
DiskCacheMonitorStats off
```

SSL Terminator: Install an SSL terminator between the browsers and Access Gateway. This reduces the amount of rewriting required when the browsers are using SSL and the Web servers protected by Access Gateway are not configured for SSL.

Click **Home** > **Access Gateways** > **Edit** > **Reverse Proxy / Authentication**. Enable the **Behind Third Party SSL Terminator** option.

SSL Cipher Suites: Use the advanced options from Apache to set the cipher suites that you want to allow. Some cipher suites take longer than others to process.

For more information, see "SSLCipherSuite Directive".

Statistics: If additional performance is desired and statistics are not important, you can unload the `mod_status` module. If you unload the `mod_status` module, extended information is not gathered.

To unload the module, open the httpd.conf file in the `apache` directory, and add a comment symbol (#) to the line that loads the `mod_status` module in the `Load Module` section.

For information about how to open and modify a file, see "Modifying Configurations" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

If you turn on debug mode, the mod_status module is automatically loaded to gather as much information as possible.

4.2.6 Setting Cache Store Size in Access Gateway Appliance

To set the disk space of cache, in megabytes, use the `DiskCacheMonitorCacheStoreSize` parameter in the `/etc/opt/novell/ag/mod_disk_cache_monitor.conf` configuration file.

This parameter is by default set to 1024 megabytes.

For information about how to open and modify a file, see "Modifying Configurations" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

4.3 Tuning the Policy Performance

Authorization and Identity Injection policies allow you to select conditions, one of which is Roles. If you have thousands of users accessing your resources, you might want to design most of your policies to use roles. Roles are evaluated when a user logs in, and the roles assigned to the user are cached as long as the session is active. When the user accesses a resource protected by a policy that uses role conditions, the policy can be immediately evaluated because the user's role values are available. This is not true for all conditions; the values for some conditions must be retrieved from

the user store. For example, if the policy uses a condition with an LDAP attribute, the user's value must be retrieved from the LDAP user store before the policy can be evaluated. On a system with medium traffic, this delay is not noticed. On a system with high traffic, the delay might be noticeable.

However, you can design your policies to have the same results without retrieving the LDAP attribute value at resource access. You can create a Role policy for the LDAP attribute and have users assigned to this role at authentication when they match the attribute value requirements. When users access resources, they gain immediate access or are immediately denied access because their role assignments are cached.

If the same LDAP attribute policy is used to grant access to multiple resources, chances that a user notices a delay are minimal. The first time a policy is evaluated for a user, the data required for the policy is cached and is therefore immediately available the next time it is requested.

Another option available for LDAP, Credential Profile, Liberty User Profile, and Shared Secret attributes is to have the attribute values sent with the assertion at authentication. You configure an attribute set for the attributes, and then configure the service provider for these attributes. For more information, see "Configuring the Attributes Sent with Authentication" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

As you design your policies, experiment and find the type that works best for your network and your customers.

5 Best Practices for Certificates

Access Manager allows you to manage centrally stored certificates used for digital signatures and data encryption. eDirectory resides on Administration Console and is the main certificate store for all of the Access Manager components.

All digital certificates have an expiration date. Most of the client and server applications check this date before using the certificate's contents. You can create a script to set up advance notification of when the certificates expire.

You can also renew the expired certificates.

- Section 5.1, "Getting the Certificate Expiration Notification," on page 31
- Section 5.2, "Renewing the Expired eDirectory Certificates," on page 33

5.1 Getting the Certificate Expiration Notification

You can receive advance notification by running a bash script in Administration Console. This script retrieves all the server certificate expiration dates through LDAP and checks the dates against the current month and year. If the certificate expires within the same month or it has already expired, you get a notification through an email. If the certificate is going to expire on the same day that the script is run, you get a special warning to repair the certificates immediately.

Configure this script to run on the first day of the month at midnight. If the server certificate expired on the first day of the month before the start of the work day (for example, at 1 a.m.), the administrators should have already received an email.

Sample Bash Script:

```
DOMAIN=novell.com
ADMIN="admin1@novell.com admin2@novell.com admin3@novell.com"
LDAPHOST=LDAPHOST.novell.com
Organization='o=novell'
CERTLOG=/tmp/CERTLOG.log
mkdir -p /tmp/
ldapsearch -h$LDAPHOST -p389 -x -b "$Organization" |
grep -B1 nDSPKINotAfter > $CERTLOG
NUMOFLINES=`cat $CERTLOG | wc -l`
i=2
while [ $i -le $NUMOFLINES ]; do
VAR1=`cat $CERTLOG | head -n$i | tail -n2`
EXPIRY=`echo $VAR1 | sed -e 's/nDSPKINotAfter: /~/' | cut -d~ -f2`
EXPIRY_YYYYMM=`echo $EXPIRY | cut -c-6`
CURRENT_YYYYMM=`date +%Y%m`
if [ $EXPIRY_YYYYMM -le $CURRENT_YYYYMM ]; then
EXPIRY_DATE=`echo $EXPIRY | cut -c-8`
EXPIRY_DAY=`echo $EXPIRY | cut -c7-8`
EXPIRY_MTH=`echo $EXPIRY | cut -c5-6`
EXPIRY_YEAR=`echo $EXPIRY | cut -c1-4`
CURRENT_DATE=`date +%Y%m%d`
```

```
CERTNAME=`echo $VAR1 | sed -e 's/nDSPKINotAfter: /~/' | cut -d~ -f1`
if [ $EXPIRY_DATE == $CURRENT_DATE ]; then
echo "Please use iManager to repair the Certificate IMMEDIATELY" |
mail -r $HOST@$DOMAIN -s "Server Certificate will expire TODAY!! -->
$CERTNAME" $ADMIN
else
echo "Please use iManager to repair the Certificate" |
mail -r $HOST@$DOMAIN -s "Server Certificate will expire
on $EXPIRY_DAY-$EXPIRY_MTH-$EXPIRY_YEAR (DD-MM-YYYY) -->
$CERTNAME" $ADMIN
fi
fi
((i=$i+3))
done
```

Implementing the Solution

1 Modify the following variables in the sample bash script according to your environment:

Variable	Description
DOMAIN=novell.com	This is the domain name of your company. Ensure that it is valid because the notification email is sent using this domain.
ADMIN="admin1@novell.comadmin2@novell.comadmin3@novell.com"	These are the email addresses of administrators who will receive the email alerts. Use a space to separate the addresses.
LDAPHOST=LDAPHOST.novell.com	This is the domain name or IP address of the eDirectory server or OES that contains a replica of all server organizational units (OUs). **NOTE:** This server should allow LDAP searches through port 389. To allow LDAP through port 389, open **iManager** > **LDAP** > **LDAP options** > **LDAP Group** > **SERVERNAME** > clear the **Require TLS for Simple Binds with Password** option. If port 389 is not allowed, change the script to use 636 (look for the ldapsearch command within the script).
Organization='o=novell'	This is the name of the organization configured on the eDirectory tree. If your servers are located across multiple organizations, use the tree name instead. For example, Organization='T=novell-tree'

2 Configure crontab to run this script on the first day of every month at midnight.

For example, modify the `/etc/crontab` file to include the following line:

```
0 0 1 * * root /usr/local/bin/check_certexpire.sh 2>/dev/null
```

3 Configure postfix to enable sending email messages:

3a Ensure that the postfix service is started by entering the following command:.

```
/etc/init.d/postfix status
```

The status should show that the service is running.

3b Ensure that the postfix service is started at run time by entering the following command:

```
chkconfig postfix on
```

3c Edit the `/etc/postfix/main.cf` file and ensure that the following line is included:

```
transport_maps = hash:/etc/postfix/transport
```

3d Find out the IP address or DNS address of your SMTP server. For example, 10.1.1.1.

3e Edit the `/etc/postfix/transport` file and ensure that the following line is included:

```
* smtp:10.1.1.1
```

3f Change the IP address to the address of your SMTP server.

3g Enter the following command:

```
/sbin/postmap /etc/postfix/transport
```

4 Verify that this command updates the `/etc/postfix/transport.db` file.

5 Try sending an email to yourself by entering the following command on the server.

```
echo "this is a test email" | mail -r $HOST@yourcompany.com -s "This is a test subject" youremail@yourcompany.com
```

Change *yourcompany.com* to your company's domain and *youremail* to your actual email address. Leave $HOST as it is.

5.2 Renewing the Expired eDirectory Certificates

The secondary Administration Console stops working when the eDirectory certificates expire. You must renew the expired certificates. To create new certificates for the configuration store or for the eDirectory server, run the `ndsconfig upgrade` command.

For information about how to renew certificates, see Creating Server Certificate Objects.

6 Troubleshooting

This chapter provides the details that help you in debugging the Access Manager issues.

Diagnostic Utility: You can use the `amdiag.sh` tool as a diagnostic utility to identify issues. This tool creates a a LDIF file in an addition to an XML Dump file.The XML file or LDIF file (if required) can then be sent to NetIQ Support for help in diagnosing configuration problems.

For more information, see "Diagnostic Configuration Export Utility" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

Troubleshooting Administration Console: See "Troubleshooting Administration Console" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

Troubleshooting Identity Server: See "Troubleshooting Identity Server and Authentication" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.

Troubleshooting Access Gateway: See "Troubleshooting Access Gateway" in the *NetIQ Access Manager 24.2 (v5.1) Administration Guide*.