Best Practices Guide

Access Manager 3.2 SP1

October 2012

Legal Notice

Contents

About This Guide

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 (TIDs), and online help for further instruction regarding each of the guidelines offered here.

This guide includes the following topics:

Audience

This guide is intended for Access Manager administrators.

Feedback

We want to hear your comments and suggestions about this guide and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Documentation Updates

For the most recent version of the *Best Practices Guide*, visit the NetIQ Access Manager Documentation Web site (https://www.netiq.com/documentation/novellaccessmanager32/).

Additional Documentation

For information about the other Access Manager devices and features, see the following:

- *NetIQ Access Manager 3.2 SP1 Administration Console Guide*
- *NetIQ Access Manager 3.2 Identity Server Guide*
- *NetIQ Access Manager 3.2 Policy Guide*
- *NetIQ Access Manager 3.2 J2EE Agent Guide*
- *NetIQ Access Manager 3.2 SP1 SSL VPN Server Guide*
- *NetIQ Access Manager 3.2 Event Codes*
- *NetIQ Access Manager 3.2 SP1 Installation Guide*

- *NetIQ Access Manager 3.2 SP1 Setup Guide*
- *Performance and Sizing Guidelines* (https://www.netiq.com/documentation/novellaccessmanager32/resources/performance_sizing/performance_sizing.pdf)

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

---

1 Design Considerations

This section describes the architectural suggestions for Access Manager.

For more information about additional security setups, see Chapter 4, “Enabling Additional Security,” on page 21.

1.1 Access Manager Component Deployment

The components of Access Manager include the Administration Console, Identity Server, SSL VPN, Access Gateway, and J2EE Agents.

Administration Console: Manages the Identity Server, SSL VPN, 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: The 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.

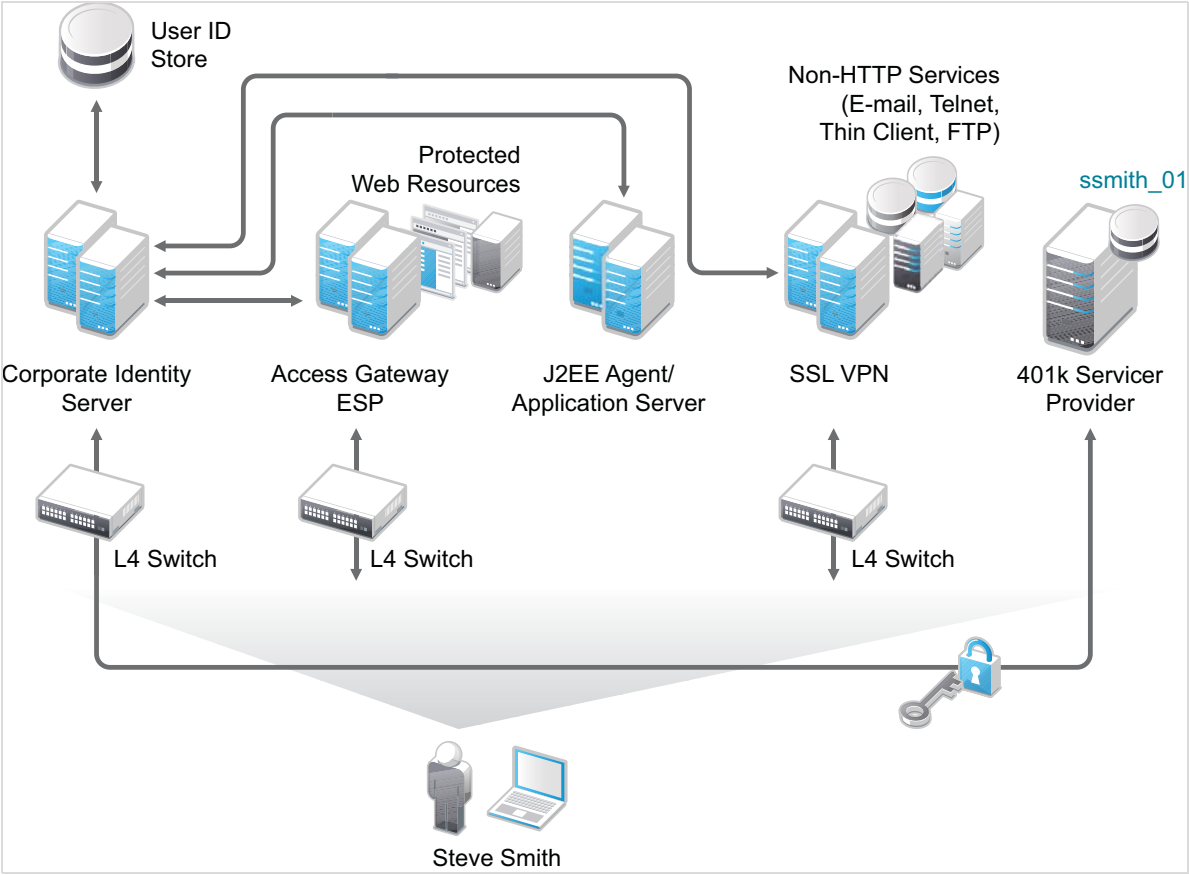
SSL VPN: Provides access to non-http servers. The SSL VPN depends on the Identity Server or the Access Gateway for validating the users.

J2EE Agents: Provides fine-grained access control to Java applications. Access Manager provides JBoss, WebLogic, and IBM WebSphere server agents for Java 2 Enterprise Edition (J2EE) application servers.

Depending on the number of users, you would need to create a cluster of components such as Identity Servers, Access Gateways, and SSL VPN Servers. Even if one node is sufficient to support all the load, NetIQ recommends to have at least two nodes in each component cluster to provide the failover support.

For more information, see “Clustering and Fault Tolerance” in the *NetIQ Access Manager 3.2 SP1 Setup Guide*.

The following diagram illustrates how the 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 *Performance and Sizing Guidelines* (http://www.novell.com/docrep/2012/02/access_manager_performance_and_sizing_guidelines_white_paper.pdf).

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.
  - The 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 3.2 SP1 Setup Guide*.
- Ensure that the LDAP time out setting in the 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 minutes.

- 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 the Identity Server.
- Set the TCP idle time in the Access Gateway lower than the LDAP time out to clear the connection table in the Access Gateway. If this time is not set, Linux fills the connection table making it almost impossible to login if the sessions are not cleared.

1.2 Firewall Settings

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

For more information, see "Configuring the Administration Console Firewall" in the *NetIQ Access Manager 3.2 SP1 Installation Guide* and "Setting Up Firewalls" in the *NetIQ Access Manager 3.2 SP1 Setup 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 3.2 SP1 Setup Guide*.

1.4 Configuring a Back Channel Traffic

The default behavior for the Identity Server and the 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 5.1.3, "Configuring a Specific IP Address for Proxied Requests," on page 30 and Section 5.2.2, "Configuring a Specific IP Address for Proxied Requests," on page 34.

1.5 Network Time Protocol

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

For a Windows Access Gateway Service, use the Date and Time option in the Control Panel. 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 3.2 SP1 Setup Guide*.

2 Configuration Tips

This chapter describes miscellaneous techniques for configuring Access Manager.

2.1 Configuring Administration Console

2.1.1 Creating Multiple Admin Accounts

The Administration Console is installed with one admin user account. We recommend you to have more than one administrator account. In case a user forgets the password, you have other administrator user accounts to access the 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 an account for each administrator and make the user security equivalent to the admin user. This also ensures that you have more than one user who has full access to the Administration Console.

For more information, see “Creating Multiple Admin Accounts” in the *NetIQ Access Manager 3.2 SP1 Administration Console Guide*.

2.1.2 Installing Secondary Versions of the 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 Versions of the Administration Console” in the *NetIQ Access Manager 3.2 SP1 Setup Guide*.

2.2 Applying the Configuration

2.2.1 Backing Up and Restoring Configuration

NetIQ recommends that you 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 "Backing Up and Restoring" in the *NetIQ Access Manager 3.2 SP1 Administration Console Guide*.

2.2.2 Exporting and Importing Configuration

You can export and import the configuration changes only for the Access Gateway and policies.

For more information about exporting or importing the Access Gateway configuration, see "Exporting and Importing an Access Gateway Configuration" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

For more information about exporting or importing the policies configuration, see "Importing and Exporting Policies" in the *NetIQ Access Manager 3.2 Policy Guide*.

3 Common Configuration Tasks

This chapter provides information about several common tasks that can be performed in Access Manager.

3.1 Configuring User Stores

User stores are LDAP directory servers which are used to authenticate the 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.

The Identity Server has built-in support to interact with eDirectory, Active Directory, and Sun One Directory. The 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 3.2. For more information, see the Developer documentation. (http://developer.novell.com/documentation/nacm32/nacm_enu/data/bfg38fg.html)

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

For more information, see “Configuring Identity User Stores” in the *NetIQ Access Manager 3.2 Identity Server 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 Advanced Local Authentication Procedures” in the *NetIQ Access Manager 3.2 Identity Server Guide* and (http://www.novell.com/communities/node/8727/integrating-novell-access-manager-actividentity-4tress-aaa-server-66).

For more information about extending the authentication mechanisms, see *Identity Server Authentication API in the Novell Access Manager 3.2 Developer Kit (http://developer.novell.com/documentation/nacm32/nacm_enu/index.html?page=/documentation/nacm31/nacm_enu/data/bookinfo.html)* .

3.3 Customizing Login Pages, Logout Pages, and Messages

You can customize the login and logout page, and error messages for the Access Manager Components.

For more information about the customizing the login page, logout page, and error messages in the Identity Server, see "Customizing Login Pages, Logout Pages, and Messages" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

For more information about customizing the error messages and error pages in the Access Gateway, see "Customizing Error Messages and Error Pages on Access Gateway" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

For more information about customizing logout requests in the Access Gateway, see "Customizing Logout Requests" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

For more information about customizing the home page, exit page, and error messages in the SSL VPN, see "Customizing SSL VPN User Interface" in the *NetIQ Access Manager 3.2 SP1 SSL VPN Server 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 "Setting Up Federation" in the *NetIQ Access Manager 3.2 SP1 Setup Guide*.

3.5 Associating the Access Gateway with the Identity Server

We recommend you to enable SSL for communication between the Access Gateway and the Identity Server.

For more information, see"Configuring SSL Communication with the Browsers and the Identity Server " in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

3.6 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 the policies that you should use to enforce protection. The authentication procedures and the 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 the 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, identityijection/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 3.2 SP1 Access Gateway Guide*.

3.7 Setting Up Google Applications

You can configure Access Manager to provide the single sign-on services to the Google applications by using Security Assertion Markup Language (SAML) 2.0.

For more information, see *Integrating Google Apps and Novell Access Manager using SAML2* (http://www.novell.com/communities/node/8645/integrating-google-apps-and-novell-access-manager-using-saml2).

3.8 Protecting SharePoint 2010

3.8.1 Protecting SharePoint Using the Domain-Based Multi-Homing Proxy Service

You can configure Access Manager to provide protected access to SharePoint by using a domain-based proxy service and single sign-on access by using identity injection. You can access Sharepoint with a URL similar to this: *https://<Published DNS name>:<port number if any>/path*. For example, *https://shpt.multibox-mag.com/default.aspx*.

Perform the following configurations:

1. Configure the proxy service type as Domain-Based Multi-Homing.

   For example, the published DNS Name = shpt.multibox-mag.com.

   For more information, see "Configuring the Domain-Based Proxy Service" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

2. Configure the following Web servers options:

   - **Web Server Host Name:** Specify the actual host name of the SharePoint server.
   - **Connect Port:** Specify the port that the Access Gateway should use to communicate with Web servers.

   For more information, see "Configuring the Web Servers of a Proxy Service" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

3. Create new HTML Rewriter profiles: one Word profile and one Character profile.

   For more information about how to create a new rewriter profile, see "Creating or Modifying a Rewriter Profile" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

   - Create a Word rewriter and enter the following values:

     And Document Content-Type Header is: click *New*, then specify the following type:

     ```
     application/x-vermeer-rpc
     ```

     Variable or Attribute Name to Search for Is: Create the following two new attributes:

     ```
     formvalue
     ```

     ```
     value
     ```

   - Create a Character rewriter. In the *Additional Strings to Replace* section, specify the search and replace strings as shown in Table 3-1, then click *OK*.

     NOTE: win2k8-r2-64bit:32274 in tables Table 3-1 and Table 3-2 is referring to Sharepoint server's domain name and the port in which it is configured. Change it with your Sharepoint server's domain name and the port number.

Table 3-1 *Search and Replace strings*

Search String	Replace String
\u0022http:\u002f\u002fwin2k8-r2-64bit:32274	\u0022https://shpt.multibox-mag.com
http%253A%252F%252Fwin2k8-r2-64bit%253A32274	https://shpt.multibox-mag.com
http%3A%2F%2Fwin2k8-r2-64bit%2Ecom%3A32274	https%3A%2F%2Fshpt.multibox-mag.com
http%3a%2f%2fwin2k8-r2-64bit%3a32274	https://shpt.multibox-mag.com
http:%2f%2fwin2k8-r2-64bit	https://shpt.multibox-mag.com
http:\u00252F\u00252Fwin2k8-r2-64bit	https://shpt.multibox-mag.com
http\u00253A\u00252F\u00252Fwin2k8-r2-64bit\u00253A32274	https://shpt.multibox-mag.com

Save and enable this rewriter profile and move it to the top of the ordered list of profiles for this accelerator.

4 Configure the protected resources: pr-private, pr-public, and pr-other.

For more information, see "Configuring Protected Resources" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

- Protected resource: pr-private
  - **Authentication Procedure:** Secure Name/Password – Form type contract
  - **URL Path:** /default.aspx
  - **Identity Injection:** Enabled (injects Credential Profile LDAP name and password into the Authorization headers)
- Protected resource: pr-public
  - **Authentication Procedure:** None
  - **URL Path:** /
- Protected resource: pr-other
  - **Authentication Procedure:** WebDAV

    Create an authentication procedure with the following settings:

    Contract: Secure Name/Password - Form

    Non-Redirected Login: enabled

    Realm: Sharepoint

    Redirect to Identity Server When No Authentication Header is Provided: disabled
  - **URL Path:** /*
  - **Identity Injection:** Enabled (injects Credential Profile LDAP name and password into the Authorization headers)

3.8.2 Protecting SharePoint for the Path-Based Multi-Homing Proxy Service

You can configure Access Manager to provide protected access to SharePoint using a path-based proxy service with the *Remove Path on Fill* option enabled, and single sign-on access by using identity injection. You can access Sharepoint with a URL similar to this: *https://<Published DNS name>:<port number if any>/path*. For example, *https://multibox-mag.com/shpt/default.aspx*.

When the *Remove Path on Fill* option is enabled, SharePoint access requires the following additional entries in the Advanced Options section for Global, Master and path-based service.

Advanced options required in the global settings include:

- NAGGlobalOptions AllowMSWebDavMiniRedir=on

Advanced options required in the master service include:

- NAGHostOptions primaryWebdav=/shpt
- NAGHostOptions webdavPath=/_vti_inf.html
- NAGHostOptions webdavPath=/_vti_bin/_vti_aut/author.dll
- NAGHostOptions webdavPath=/_vti_bin/shtml.dll/_vti_rpc
- NAGHostOptions webdavPath=/_vti_bin/_vti_aut/author.dll
- NAGHostOptions webdavPath=/_vti_bin/_vti_adm/admin.dll
- NAGHostOptions webdavPath=/_vti_bin/owssvr.dll

Advanced options required in the path-based service include:

- NAGChildOptions WebDav=/shpt

Perform the following configurations:

1. Configure the proxy service type as Path-Based Multi-Homing. For example, Published DNS Name= shpt.multibox-mag.com)

   - **Path List:** /shpt

     Remove Path on Fill: Select the check box.

     Reinsert Path in "set-cookie" Header: Select the check box.

   For more information, see "Configuring a Path-Based Multi-Homing Proxy Service" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

2. Configure the following options for Web servers:

   - **Web Server Host Name:** Enter the actual host name of the SharePoint server.
   - **Connect Port:** Enter the port that the Access Gateway should use to communicate with the Web servers.

   For more information, see "Configuring the Web Servers of a Proxy Service" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

3. Create new HTML Rewriter profiles: one Word profile and one Character profile.

   For more information about how to create a new rewriter profile, see "Creating or Modifying a Rewriter Profile" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

   - Create a Word rewriter. Keep the default values except the following:

     And Document Content-Type Header Is: click *New*, then specify the following type:

     ```
     application/x-vermeer-rpc
     ```

     Rewrite Inbound Query String Data: Select the check box.

Rewrite Inbound POST Data: Select the check box.

Rewrite Inbound Headers: Select the check box.

Enable Rewriter Actions: Select the check box.

Variable or Attribute Name to Search for Is: Specify the following attributes:

```
ctx.displayFormUrl
ctx.editFormUrl
ctx.HttpPath
ctx.imagesPath
ctx.listUrlDir
editPrmsUrl
formvalue
L_Menu_BaseUrl
sDialogUrl
strHelpUrl
strImageAZ
strImagePath
value
webUrl
WPSC.WebPartPage.WebServerRelativeURL
```

Java Script Method of Search for is: Specify the following attributes:

```
insertitem
ProcessDefaultNavigateHierarchy
UpdateFormDigest
```

String to Search for is: Specify the following attributes:

```
Search=/_layouts/images
Replace=$path/_layouts/images
Search=/sites
Replace=$path/sites
Search=\u002f_layouts\u002fimages
Replace=$path\u002f_layouts\u002fimages
```

- Create a Character rewriter and enter the following values:.

  And Document Content-Type Header Is: application/x-vermeer-rpc

  Additional Strings to Replace: Specify the search and replace strings as shown in Table 3-2, then click *OK*

Table 3-2 *Search and Replace strings*

Search String	Replace String
\u0022http:\u002f\u002fwin2k8-r2-64bit:32274	\u0022https://multibox-mag.com/shpt
\u002f_layouts	/shpt\u002f_layouts
\u002f_vti_bin	/shpt\u002f_vti_bin
event,'/_layouts	event,'/shpt/_layouts
http%253A%252F%252Fwin2k8-r2-64bit%253A32274	https://multibox-mag.com/shpt
http%3A%2F%2Fwin2k8-r2-64bit%2Ecom%3A32274	https%3A%2F%2Fmultibox-mag.com/shpt
http%3a%2f%2fwin2k8-r2-64bit%3a32274	https%3a%2f%2fmultibox-mag.com/shpt
http:%2f%2fwin2k8-r2-64bit	https://multibox-magcom/shpt
http:\u00252F\u00252Fwin2k8-r2-64bit	https://multibox-mag.com/shpt
http\u00253A\u00252F\u00252Fwin2k8-r2-64bit\u00253A32274	https://multibox-mag.com/shpt
	webUrl=/ webUrl=/shpt

Save and enable this rewriter profile and move it to the top of the ordered list of profiles for this accelerator.

4 Configure the protected resources: pr-private, pr-public, and pr-other.

For more information, see "Configuring Protected Resources" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

- Protected resource: pr-private
  - **Authentication Procedure:** Secure Name/Password – Form type contract
  - **URL Path:** /shpt/default.aspx
  - **Identity Injection:** Enabled (injects Credential Profile LDAP name and password into the Authorization headers)
- Protected resource: pr-public
  - **Authentication Procedure:** None
  - **URL Path:** /shpt
- Protected resource: pr-other
  - **Authentication Procedure:** WebDAV

    Create an authentication procedure with the following settings:

    Contract: Secure Name/Password - Form

    Non-Redirected Login: enabled

    Realm: Sharepoint

    Redirect to Identity Server When No Authentication Header is Provided: disabled
  - **URL Path:** /shpt/*
  - **Identity Injection:** Enabled (injects Credential Profile LDAP name and password into the Authorization headers)

4 Enabling Additional Security

4.1 Protecting the Administration Console

The Administration Console and Identity Server are sometimes installed on the same machine. The Identity Server must be accessible and the services provided by Access Manager must be available on the Internet. This might cause a security issue with the Administration Console.

Perform the following steps to secure the Administration Console:

1. Make a copy of the `server.xml` file.
2. Edit the `server.xml` file.

   Linux: `/opt/novell/nam/idp/conf`

   Windows: `\Program Files (x86)\Novell\Tomcat\conf`
3. Look for the end of the `<Host>` block.
4. Before the last line (before `</Host>`), insert the following lines:

   ```
   <Context path="/nps">
              <Valve className="org.apache.catalina.valves.RemoteAddrValve"
              allow="xxx.yyy.zzz.www" />
           </Context>
   ```

   The syntax for the allow directive, which can also be changed to a deny directive, is a comma-separated IP regular expressions list (Perl regex format). A simple example is as follows:

   ```
   allow="192.168.10[1-3].[0-9]*"
   ```

   This allows you to access the following IP addresses: 192.168.101.0/24, 192.168.102.0/24, 192.168.103.0/24.

4.2 Enabling Secure Cookies

The Access Gateway and the embedded service provider (ESP) of the Access Gateway both use session cookies in their communication with the browser.

For more information about how to protect these cookies from being intercepted by hackers, see " Enabling Secure Cookies" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

By default, the Identity Server and ESP cluster cookies do not have any secure or HTTPOnly flags.

To set the cluster cookies in the Identity Server, you must add the following parameter in the NIDP `web.xml` and restart Tomcat:

Add the following parameters in `web.xml` after the `ldapLoadThreshold context param`:

```
<context-param>
        <param-name>secureClusterCookie</param-name>
        <param-value>true</param-value>
</context-param>
<context-param>
        <param-name>httponlyClusterCookie</param-name>
        <param-value>true</param-value>
</context-param>
```

To set the cluster cookies in ESP, you must add the following parameter in the NESP `web.xml` and restart Tomcat:

Add the following parameters in the *web.xml* below the `ldapLoadThreshold context param`:

```
<context-param>
        <param-name>httponlyClusterCookie</param-name>
        <param-value>true</param-value>
</context-param>
```

NOTE: The secure cookies cannot be configured for ESP cluster because the communication between the Access Gateway and NESP is over HTTP on the loopback interface.

4.3 Configuring the 256-bit SSL Communication

By default, Access Manger supports the 128-bit SSL communication among the Administration Console, Identity Server, SSL VPN, and browsers. The supported ciphers include:

- SSL_RSA_WITH_RC4_128_MD5
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_KRB5_WITH_3DES_EDE_CBC_SHA
- TLS_KRB5_WITH_RC4_128_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- SSL_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

To enable the strong 256-bit ciphers:

1. Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6 from Sun's Java website.
2. Extract the zip file and replace the policy jars in `/opt/novell/java/jre/lib/security/`.
3. Modify the `server.xml` file located in `/opt/novell/nam/adminconsole/conf/`.
4. Add the 256-bit ciphers to the cipher attribute of `<Connectors>`.

   For the list of 256-bit ciphers, see *Java ™ Cryptography Architecture*

Sun Providers Documentation (http://docs.oracle.com/javase/6/docs/technotes/guides/security/SunProviders.html#SunJSSEProvider).

4.4 Disabling Phishing

You can configure the Access Gateway ESP to disable the ESP phishing by implementing a context parameter in the `web.xml` file for ESP.

1. Open the `web.xml` file located in `/opt/novell/nam/mag/webapps/nesp/WEB-INF`.
2. Add the following entry:

```
<context-param>
   <param-name>phishingCheck</param-name>
   <param-value>standard</param-value>
</context-param>
```

3. Restart the Tomcat.

4.5 Configuring Whitelist

The whitelist feature allows you to restrict target URLs to URLs that match the domains in the whitelist.

For information about how to configure a whitelist, see "Configuring Whitelist of Target URLs" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

4.6 Preventing IP Spoofing

An attacker can spoof a non-secure browser into sending a JSESSION cookie that contains a valid user session. To stop this from happening, you need to configure the Identity Server to use SSL. For configuration information, see "Configuring Secure Communication on the Identity Server" in the *NetIQ Access Manager 3.2 SP1 Setup Guide* and "Securing the Identity Server Cookie" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

4.7 Preventing the Error Page to Show the Tomcat Version

Accessing a non-existing page or providing wrong credentials on a protected page throws an HTTP 401 error with Tomcat version. This issue happens on the Windows platform in the following scenarios:

- When the Identity Server is the only component installed on the Windows server.
- The Access Gateway Service on Windows.

To prevent the error pages to display the Tomcat version:

1. Go to `C:\Program Files\Novell\Tomcat\lib` and run `"C:\Program Files\Java\jdk1.7.0_03\bin\jar" -xf catalina.jar`
2. Move catalina.jar to some other folder.
3. Go to `C:\Program Files\Novell\Tomcat\lib\org\apache\catalina\util` and edit the `serverInfo.properties` file:
   - **3a** Remove `Apache Tomcat/7.0.23` from the line `server.info=`.
   - **3b** Remove `7.0.23.0` from the line`server.number=`.
   - **3c** Remove `Nov 20 2011 07:36:25` from the line `server.built=`.
4. Go to `C:\Program Files\Novell\Tomcat\lib` and run `jar -cf catalina.jar META-INF org`.

4.8 Setting an Optimal Secure Socket Layer Configuration With Ciphers

IMPORTANT: The settings specified in this section indicate an SSL configuration that provides an optimal level of security. If you plan on making any changes in the cipher information, ensure you test the configuration before you deploy it in your production setup.

In addition to setting up the Secure Socket Layer (SSL), using a cipher suite provides additional security to client-server communications from Identity Server, Access Gateway to the Web browsers.

Specifying SSL Configuration for Identity Server :

You can force all client communication with the Identity Server to use 128-bit encryption by modifying the `server.xml` file used by Tomcat. If the browser is unable to supported the encryption level specified in this file, the user is not allowed to authenticate.

1. At a command prompt, change to the Tomcat configuration directory:

   Linux: `/opt/novell/nam/idp/conf`

   Windows Server 2008: `\Program Files (x86)\Novell\Tomcat\conf`
2. To the `server.xml` file, add the cipher suites you want to support. You can add or remove ciphers from this list based on your needs.For 128-bit encryption, add the following line:

   ```
   ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA,
   TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
   TLS_DHE_DSS_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA,
   SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,
   TLS_KRB5_WITH_3DES_EDE_CBC_SHA, TLS_KRB5_WITH_RC4_128_SHA
   "
   ```

   This is a comma-separated list of the JSSE names for the TLS cipher suites.

   IMPORTANT: If you enter a cipher name incorrectly, Tomcat reverts to the default values, which allow the weak ciphers to be used.

   For a complete list of supported cipher suites and their requirements, see The SunJSSE Provider (http://java.sun.com/javase/6/docs/technotes/guides/security/SunProviders.html#SunJSSEProvider).
3. To activate the cipher list, restart Tomcat.

   Linux: Enter one of the following commands:

```
/etc/init.d/novell-idp restart

rcnovell-idp restart
```

Windows: Enter the following commands:

```
net stop Tomcat7

net start Tomcat7
```

4 (Conditional) If you have multiple Identity Servers in your cluster configuration, repeat these steps on each Identity Server.

Specifying SSL Configuration for Access Gateway :

To set up a cipher list from the ciphers provided by OpenSSL, C*lick Devices* > *Access Gateways* > *Edit* > *Advanced Options* and add the following configuration:

```
SSLProtocol All -SSLv2

SSLHonorCipherOrder On

SSLCipherSuite

ECDHE-RSA-AES256-SHA384:AES256-
SHA256:RC4:HIGH:MEDIUM:!LOW:!EXP:!SSLv2:!aNULL:!EDH:!AESGCM:!eNULL:!NULL
```

This configuration indicates the Access Gateway to disable SSLv2 and select the following ciphers for optimal security:

```
RC4-SHA                 SSLv3 Kx=RSA      Au=RSA  Enc=RC4(128)  Mac=SHA1
RC4-MD5                 SSLv3 Kx=RSA      Au=RSA  Enc=RC4(128)  Mac=MD5
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH       Au=RSA  Enc=Camellia(256) Mac=SHA1
DHE-DSS-CAMELLIA256-SHA SSLv3 Kx=DH       Au=DSS  Enc=Camellia(256) Mac=SHA1
CAMELLIA256-SHA         SSLv3 Kx=RSA      Au=RSA  Enc=Camellia(256) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH       Au=RSA  Enc=Camellia(128) Mac=SHA1
DHE-DSS-CAMELLIA128-SHA SSLv3 Kx=DH       Au=DSS  Enc=Camellia(128) Mac=SHA1
CAMELLIA128-SHA         SSLv3 Kx=RSA      Au=RSA  Enc=Camellia(128) Mac=SHA1
DHE-RSA-AES256-SHA      SSLv3 Kx=DH       Au=RSA  Enc=AES(256)  Mac=SHA1
DHE-DSS-AES256-SHA      SSLv3 Kx=DH       Au=DSS  Enc=AES(256)  Mac=SHA1
AES256-SHA              SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
DHE-RSA-AES128-SHA      SSLv3 Kx=DH       Au=RSA  Enc=AES(128)  Mac=SHA1
DHE-DSS-AES128-SHA      SSLv3 Kx=DH       Au=DSS  Enc=AES(128)  Mac=SHA1
AES128-SHA              SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
EDH-RSA-DES-CBC3-SHA    SSLv3 Kx=DH       Au=RSA  Enc=3DES(168) Mac=SHA1
EDH-DSS-DES-CBC3-SHA    SSLv3 Kx=DH       Au=DSS  Enc=3DES(168) Mac=SHA1
DES-CBC3-SHA            SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=SHA1
```

5 Performance Tuning

This chapter describes how to optimize the performance of the Identity Server, the Access Gateway, and policies.

5.1 Tuning the Identity Server for Performance

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

5.1.1 Basic Tuning Options

The following Access Manager components and features can affect the performance of the 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 misconfigured, 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 handles the traffic correctly, but the system can run up to 50% slower than when persistence is enabled. For tips on how to set up the L4 switch, see “Configuration Tips for the L4 Switch ” in the *NetIQ Access Manager 3.2 SP1 Setup Guide*.

Enabled Protocols: On the General Configuration page (click *Devices* > *Identity Servers* > *Edit*), 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 (click *Devices* > *[Name of Cluster]*), 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 the 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, you should specify the minimum number of peers.

Limit User Sessions: On the General Configuration page (click *Devices* > *Identity Servers* > *Edit*), you can select to limit the number of sessions a user can have. When a user is limited to a specific number of sessions, the 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 (click *Devices* > *Identity Servers* > *Edit* > > *Local* > *Contracts* > *[Name of Contract]*), you need to specify an authentication time-out. 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. You need to analyze your needs. Are you really interested in who logged in, or are you more interested in who failed to log in?

5.1.2 Disabling User Profile Objects

If you are not using 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 every 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 the Administration Console, the ndsd process (Linux) or the NDS Server (Windows) is running at 100%.
- Running the backup utility is very slow.
- Logging in to the Administration Console is very slow.

To discover whether profile objects are causing a slowdown, open an LDAP browser (or in the 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, the 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, make the following modifications to your Identity Server configuration:

1. In the Administration Console, click *Devices* > *Identity Servers* > *Edit* > *Liberty* > *Web Service Provider*.
2. Disable the following profiles:
   - Personal Profile
   - Employee Profile
   - Custom Profile
3. Either 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 either with the *Extended Schema User References* option or with the *Novell Secret Store User Store 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 about these options, see"Configuring a User Store for Secrets" in the *NetIQ Access Manager 3.2 Identity Server Guide*.
4. Click *OK* twice, then update the Identity Server.
5. Disable the use of the user profile objects:
   - **5a** Log in to the Identity Server machine as the `root` user.
   - **5b** Open the `web.xml` file.

     Linux: `/opt/novell/nam/idp/webapps/nidp/WEB-INF/`

     Windows Server 2008: `\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEB-INF/`
   - **5c** Add the following lines to the file:

     ```
     <context-param>
       <param-name>cpAuthorityType</param-name>
       <param-value>memory</param-value>
     </context-param>
     ```
   - **5d** Restart Tomcat.

     Linux: Enter the following command:

     `/etc/init.d/novell-idp restart` Or

     rcnovell-idp restart

     Windows: Enter the following commands:

     `net stop Tomcat7`

     `net start Tomcat7`
   - **5e** Make this change on each Identity Server in the cluster.

5.1.3 Configuring a Specific IP Address for Proxied Requests

The default behavior for the 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.

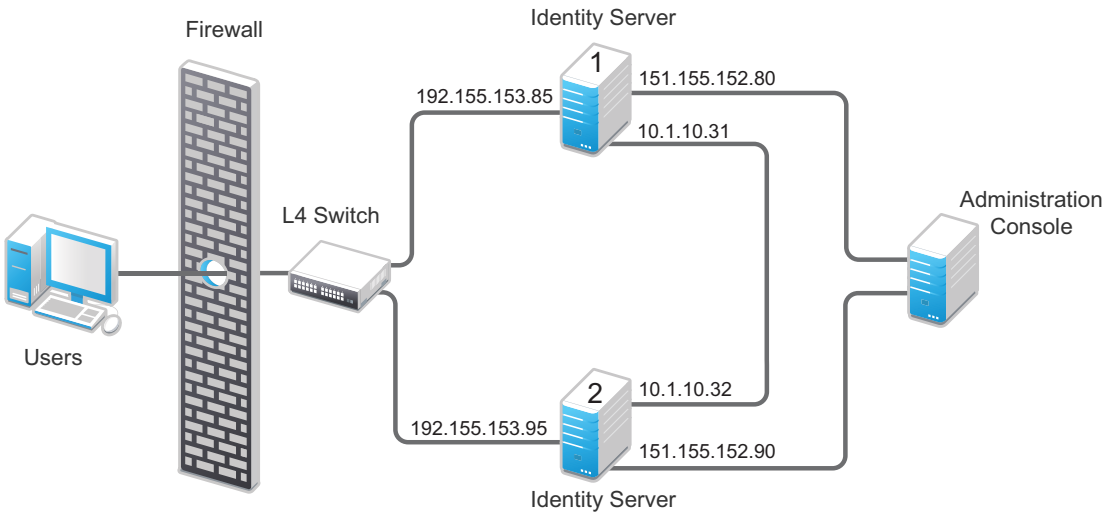
In version 3.1 SP2 IR1 and later, you can specify the IP address that an Identity Server uses for proxied requests to other members of the cluster. A proxied request is sent to another member of a cluster when the request is not sent to the authoritative server.

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 the Identity Server and the Administration Console for management tasks. This includes configuration updates, health checks, and statistics. To configure this IP address, log in to the Administration Console, then click *Devices* > *Identity Servers* > *[Name of Identity Server].*

Figure 5-1 on page 30 illustrates a configuration with a two-member cluster. The L4 switch sends client traffic to the 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 the Administration Console.

Figure 5-1 *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, click *Devices* > *Identity Servers* > *Name of Identity Server*.)
   - IP address or IP address with port that is available to use for proxied requests.
2. Log in to the Identity Server as the `root` user.
3. Change to the `WEB-INF` directory:

   Linux: `/opt/novell/nam/idp/webapps/nidp/WEB-INF/`

Windows Server 2008: `\Program Files (x86)\Novell\Tomcat\webapps\nps\WEB-INF/`

4 Open the `web.xml` file for editing.

5 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>
```

6 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 the Identity Server. You cannot specify a port with this entry.
- Replace *unused* with just a space. If you configure this feature for the Access Gateway, this IP address entry is used for the reverse proxy IP address. The 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 5-1 on page 30, 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 5-1 on page 30 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>
```

7 Save the file.

8 Restart Tomcat:

Linux: `/etc/init.d/novell-idp restart` Or

`rcnovell-idp restart`

Windows: Enter the following commands:

```
net stop Tomcat7
net start Tomcat7
```

9 Repeat Step 2 through Step 7 for each cluster member, modify the `<param-value>` element to contain the addresses for other members of the cluster.

5.1.4 Configuring Java Memory Allocations

The Tomcat configuration file controls the amount of memory that Tomcat can allocate for Java. If you have installed your 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:

- "Modifying Java Parameters on Linux" on page 32
- "Modifying Java Parameters on Windows" on page 32

Modifying Java Parameters on Linux

1. Log in to the Identity Server as the `root` user.
2. Open the Tomcat configuration file for editing.

   `/opt/novell/nam/idp/conf/tomcat7.conf`
3. For the Access Gateway Service, 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.
4. Find the following line in the file:

   ```
   JAVA_OPTS="${JAVA_OPTS} -Dnids.freemem.threshold=10"
   ```
5. If required you can change the `-Dnids.freemem.threshold` value to a value between 5 and 15. 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.
6. Save your changes, then restart Tomcat.
7. Repeat these steps for each Identity Server in your cluster.

Modifying Java Parameters on Windows

1. Log in to the Identity Server as the administrator.
2. Open the Tomcat configuration utility from `/Program Files (x86)/Novell/Tomcat/bin/tomcat7w.exe`.
3. Click the *Java* tab.
4. In the *Java options* section, find the following line:

   ```
   -Dnids.freemem.threshold=10
   ```

   If the line does not exist, you need to add it.
5. If required change the `-Dnids.freemem.threshold` value to a value between 5 and 15. 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 `stdout.log` file.

6 Change the *Maximum memory pool* size to 2048.

   This allows Java to use 2 GB of memory.

7 Save your changes, then restart Tomcat.

8 Repeat these steps for each Identity Server in your cluster.

5.2 Tuning the Access Gateway for Performance

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

5.2.1 Basic Tuning Options

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

Maximum Number of User Sessions: NetIQ recommends 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 Section 5.2.4, "Java Memory Allocations," on page 37.

LDAP Attributes: If you have policies that 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 3.2 Identity Server 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 the Access Gateway cache these pages. For information on cache configuration options, see "Configuring Caching Options" in the *NetIQ Access Manager 3.2 SP1 Access Gateway 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 misconfigured, 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. For tips on how to set up the L4 switch, see "Configuration Tips for the L4 Switch " in the *NetIQ Access Manager 3.2 SP1 Setup 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 the 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 3.2 SP1 Access Gateway Guide*.

Access Gateway Service: See Section 5.2.5, "Performance Tips," on page 38.

5.2.2 Configuring a Specific IP Address for Proxied Requests

The default behavior for the 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.

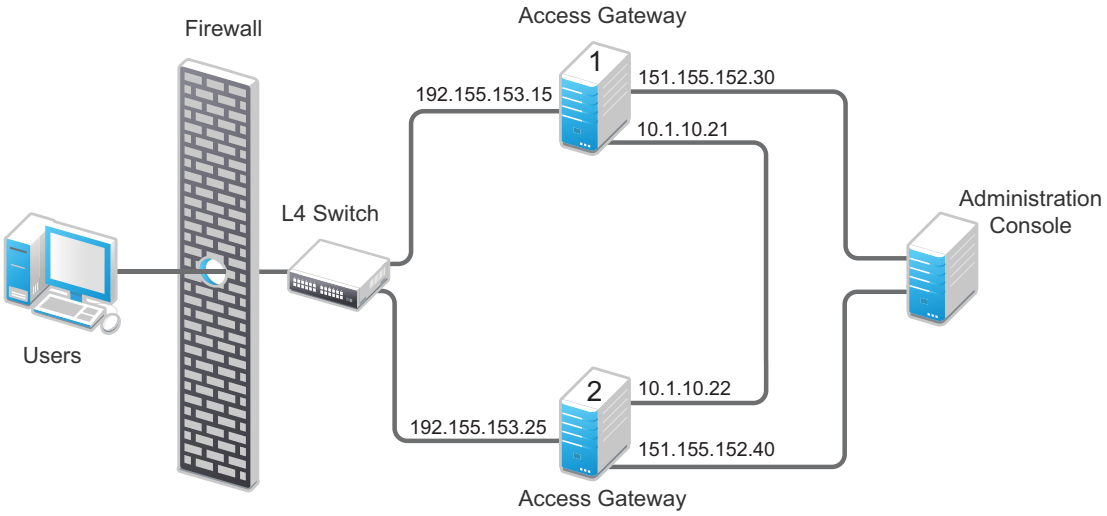
In version 3.1 SP2 IR1 and later, you can specify the IP address that an Access Gateway uses for proxied requests to other members of the cluster. A proxied request is sent to another member of a cluster when the request is not sent to the authoritative server.

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 the Access Gateway and the Administration Console for management tasks. This includes configuration updates, health checks, and statistics. To modify this IP address, log in to the Administration Console, then click *Devices > Access Gateways > [Name of Access Gateway]*.

Figure 5-2 illustrates a configuration with a two-member cluster. The L4 switch sends client traffic to the 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 the Administration Console.

Figure 5-2 *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, click *Devices* > *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 *Devices* > *Access Gateways* > *Name of Access Gateway*.
   - IP address or IP address with port that is available to use for proxied requests.
2. Log in to the Access Gateway as the `root` user.
3. Change to the `WEB-INF` directory:

   Linux: `/opt/novell/nam/mag/webapps/nesp/WEB-INF/`

   Windows: `\Program Files\Novell\Tomcat\webapps\agm\WEB-INF/`
4. Open the `web.xml` file for editing.
5. Add a 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 the Access Gateway. You cannot specify a port with this entry.

- Replace *Reverse_Proxy_IP* with the IP address of the reverse proxy of the 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 5-2, 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 5-2 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>
```

6 Save the file.

7 Restart Tomcat:

Linux: `/etc/init.d/novell-mag restart`

Windows: Enter the following commands:

```
net stop "Apache Tomcat"
net start "Apache Tomcat"
```

8 Repeat Step 2 through Step 7 for each cluster member, modify the `<param-value>` element to contain the addresses for other members of the cluster.

5.2.3 Configuring the Access Gateway ESP to Reduce the 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 the Access Gateway enabled policies.

For more information about how to configure a new attribute set, see "Configuring Attribute Sets" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

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

---

4 In the Administration Console, click *Devices* > *Identity Servers* > *Servers* > *Edit* > *Liberty*, then select the 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 the Identity Server and the selected ESP.

For more information about how to add the attribute set, see "Configuring the Attributes Sent with Authentication" in the *NetIQ Access Manager 3.2 Identity Server 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 more information, see"Using the Refresh Data Option" in the *NetIQ Access Manager 3.2 Policy Guide*.

This refresh rate determines how often the 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 the Access Gateway proxy and the ESP.

7 Inject the 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.

5.2.4 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:

- "Modifying Java Parameters on Linux" on page 37
- "Modifying Java Parameters on Windows" on page 38

Modifying Java Parameters on Linux

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

1 Log in to the Access Gateway as the `root` user.

2 Open the Tomcat configuration file for editing.

```
/opt/novell/nam/mag/conf/tomcat7.conf
```

3 For the Access Gateway Service, 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.

4 Find the following line in the file:

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

5 If required change the `-Dnids.freemem.threshold` value to a value between 5 and 15. 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.

6 Save your changes, then restart Tomcat.

7 Repeat these steps for each Access Gateway in your cluster.

Modifying Java Parameters on Windows

1 Log in to the Access Gateway as the administrator.

2 Open the Tomcat configuration utility.

```
/Program Files/Novell/Tomcat/bin/tomcat7w.exe
```

3 Click the *Java* tab.

4 In the *Java options* section, find the following line:

```
-Dnids.freemem.threshold=10
```

   If the line does not exist, you need to add it.

5 If required change the `-Dnids.freemem.threshold` value to a value between 5 and 15. 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 `stdout.log` file.

6 Change the *Maximum memory pool* size to 2048.

   This allows Java to use 2 GB of memory.

7 Save your changes, then restart Tomcat.

8 Repeat these steps for each Access Gateway in your cluster.

5.2.5 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. Click *Devices* > *Access Gateways* > *Edit* > *Advanced Options* and add the following command:

```
DiskCacheMonitorStats off
```

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

Click *Devices* > *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" (http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslciphersuite).

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.

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

5.2.6 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.

5.2.7 Configuring Apache to Use Syslog in Linux

For the Access Gateway Appliance, configure Apache to use the Syslog utility to write error logs in `/var/log/novell-apache2/error_log`. The Syslog utility allows you to write the httpd threads to the log file simultaneously instead of the default behavior that is sequential.

1. Add the following lines into the `/etc/syslog-ng/syslog-ng.conf` file:

```
filter f_user       {facility(user);};
destination agsmessages {file("/var/log/novell-apache2/error_log");};
log {source(src); filter(f_user); destination(agsmessages); flags(final); };

filter f_local6     {facility(local6);};
destination httpheaders {file("/var/log/novell-apache2/httpheaders");};
log {source(src); filter(f_local6); destination(httpheaders); flags(final);};

filter f_local5     {facility(local5);};
destination soapmessages{file("/var/log/novell-apache2/soapmessages");};
log {source(src); filter(f_local5); destination(soapmessages); flags(final);
};
```

2. Restart the Syslog service by running the following command:

   `/etc/init.d/syslog restart` Or

   `rcsyslog restart`

3. Configure httpd to use Syslog in `/etc/opt/novell/apache2/conf/httpd.conf`.

   Change the `ErrorLog` directive to `ErrorLog syslog:user`.

   Sample snippet of the working httpd.conf for ErrorLog:

```
<IfModule !mpm_winnt_module>
 ErrorLog syslog:user
</IfModule>

<IfModule mpm_winnt_module>
 ErrorLog "/var/log/novell-apache2/error_log"
</IfModule>
```

4. Restart the Apache service running the following command:

   `/etc/init.d/novell-apache2 restart` Or

   `rcapache2 restart`

5.3 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 3.2 Identity Server Guide*.

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

6 Best Practices for Certificates

Access Manager allows you to manage centrally stored certificates used for digital signatures and data encryption. eDirectory resides on the 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.

6.1 Getting the Certificate Expiration Notification

You can receive advance notification by running a bash script in the 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.

This script should be configured 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
```

6.1.1 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.com admin2@novell.com admin3@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.

6.2 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 more information about how to renew the certificates, see *Recreating Server Certificates on OES Linux* (http://wiki.novell.com/index.php/Recreating_Server_Certificates_on_OES_Linux).

7 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 Novell Support for help in diagnosing configuration problems.

For more information, see "Running the Diagnostic Configuration Export Utility" in the *NetIQ Access Manager 3.2 SP1 Administration Console Guide*.

Troubleshooting the Administration Console: See "Troubleshooting the Administration Console" in the *NetIQ Access Manager 3.2 SP1 Administration Console Guide*.

Troubleshooting the Identity Server: See "Troubleshooting Identity Server and Authentication" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

Troubleshooting the Access Gateway: See "Troubleshooting the Access Gateway" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

Troubleshooting the SSL VPN: See "Troubleshooting SSL VPN Configuration" in the *NetIQ Access Manager 3.2 SP1 SSL VPN Server Guide*.