Migration and Upgrade Guide

Access Manager 3.2 SP1

October 2012

Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

© 2012 NetIQ Corporation and its affiliates. All Rights Reserved.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, VPN-1, Provider-1, and SiteManager-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

Access Manager, ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Cloud Manager, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PlateSpin, PlateSpin Recon, Privileged User Manager, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its affiliates in the USA. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

EXCEPT AS MAY BE EXPLICITLY SET FORTH IN THE APPLICABLE END USER LICENSE AGREEMENT, NOTHING HEREIN SHALL CONSTITUTE A WARRANTY AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY NETIQ, ITS SUPPLIERS AND LICENSORS.

Contents

About This Guide

This documentation describes how to migrate and upgrade Access Manager components from 3.1 SP4 to 3.2.

Audience

This guide is intended for network administrators, installers, and consultants who are involved in upgrading or migrating to Access Manager 3.2.

Feedback

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

Documentation Updates

For the most recent version of the *Access Manager 3.2 Upgrade and Migration Guide*, visit the Access Manager 3.2 Documentation Web site (http://www.novell.com/documentation/novellaccessmanager32/).

Additional Documentation

For documentation on Access Manager, see the Access Manager Documentation site (http://www.novell.com/documentation/novellaccessmanager32/).

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

---

1 Understanding Migration and Upgrade

A basic Access Manager installation has three Access Manager components (an Administration Console, an Identity Server, and an Access Gateway), an LDAP server, and Web servers with applications and data.

By moving to the Access Manager 3.2 release, you get all the important fixes and features that enhance the existing capabilities of the product.

The following sections in this chapter explain how to move to Access Manager 3.2.

1.1 Planning to Move to Access Manager 3.2

In this release of Access Manager, all the components are native 64-bit applications running on 64-bit architecture.

IMPORTANT: Before moving to Access Manager 3.2, ensure that you are on Access Manager 3.1 SP4 or a higher version.

This section contains details on the following:

1.1.1 General Prerequisites

Ensure that you meet the following requirements before you decide to move to Access Manager 3.2:

- ❒ You are currently on Access Manager 3.1 SP4 or a higher version. If your current version of Access Manager is not 3.1 SP4, see Access Manager 3.1 Installation Guide (http:////www.novell.com/documentation/novellaccessmanager31/installation/?page=/documentation/novellaccessmanager31/installation/data/bookinfo.html).
- ❒ All the components are configured to the same Network Time Protocol (NTP) server. This is required to synchronize the time across all components.

- ❒ You have physical access to the server or server console (in case of VMWare setups) as a root user and are familiar with firewall configurations. The required ports also must be opened in the firewall. For more information on the ports, see Section 2.1, "Port Details," on page 13.
- ❒ You have read and understood the network requirements. For details, see "Installation Requirements " in the *NetIQ Access Manager 3.2 SP1 Installation Guide*

1.1.2 Understanding Migration and Upgrade

What is Migration?

Migration is the process in which you install the latest version of Access Manager on a new server and then migrate the existing data to the new server.

During the migration process you can either provide a new IP address and host name or reuse an existing IP address.

IMPORTANT: The host name of the new 3.2 Administration Console must be different from the existing 3.1 SP4 primary and secondary Administration Consoles.

Migration can be used in the following cases:

- ❒ You are on a 32-bit architecture and you need to move to a 64-bit architecture. For example, your existing setup is on a 32-bit SLES (SUSE Linux Enterprise Server) 10 SP2 and you plan to move to a 64-bit SLES 11 SP1 or higher operating system.
- ❒ You have an existing 64-bit architecture but your operating system is 32-bit. For example, you have a 64-bit server on which a 32-bit operating system is installed.
- ❒ You plan to re-architecture your Access Manager setup. For example, you already have one Administration Console installed but you plan to add one more Administration Console to the setup.

What is Upgrade?

Upgrade is the process through which the existing components are moved to a higher version on the same machine. As the underlying operating system does not change, this process is also referred to as an in-place upgrade.

Upgrade can be used in a scenario where you are already on a 64-bit architecture setup.During the process of upgrade, the existing IP addresses and hardware are reused.

For example: If you are already on Windows 2008 64-bit platform, you can directly upgrade to Access Manager 3.2.

In addition to the migrate and upgrade process described above, you can also choose to install Access Manager 3.2 on a new 64-bit setup. After manually reconfiguring and confirming that the new 3.2 setup is working fine, you can decommission the old 3.1 SP4 setup.

IMPORTANT: To avoid service disruptions, you can install Access Manager 3.2 devices such as Identity Provider, Access Gateway Service, and SSL VPN on a new 64-bit server and then add them to the existing cluster. Once the version 3.2 setup is functional, you can de-commission the 3.1 SP4 setup.

1.1.3 Assessing Your Current Setup

Before you decide to upgrade or migrate, it is important to assess your current setup in terms of version of Access Manager and the components installed, hardware and the operating system.

- **Current Version of Access Manager:** Before you move to Access Manager 3.2, ensure that you are on Access Manager 3.1 SP4 or a higher version. If your current version of Access Manager is not 3.1 SP4, upgrade using the instructions at Access Manager 3.1 Installation Guide (http://www.novell.com/documentation/novellaccessmanager31/installation/?page=/documentation/novellaccessmanager31/installation/data/bookinfo.html)
- **Current Hardware:** If your current operating system is on a 32-bit architecture, migrate to a 64-bit architecture. This is required because all the components of Access Manager 3.2 are on 64-bit architecture.
- **Current Operating System:** You can move to Access Manager 3.2 from a SLES platform or a Windows platform.

  You are on SLES: To move to Access Manager 3.2, the operating system must be SLES 11 SP1 (64-bit) or higher. If you are on SLES 10.x, upgrade to SLES 11 SP1(64-bit) or higher.

  You are on Windows: If your current operating system is Windows 2008, you can directly upgrade to Access Manager 3.2. But if your current operating system is Windows 2003, migrate to Windows 2008 and then install Access Manager 3.1 SP4.
- **Access Manager components:** Identify the combination of Access Manager components that are currently installed in your setup. This will help you determine if you need to upgrade, migrate or do a combination of both.

  For example, assume you have Administration Console and Identity Server installed in Windows 2008 and the 3.1 SP4 Access Gateway Appliance is installed in SLES.

  In this scenario, you will first upgrade the Administration Console and the Identity Server. But the 3.1 SP4 Access Gateway Appliance needs to be migrated to 3.2 Access Gateway Appliance.

Determining Whether to Migrate or Upgrade

The following table indicates if you must migrate or upgrade based on your existing setup:

Table 1-1 *Determining the Path to Move to Access Manager 3.2*

Platforms	Windows 2003	Windows 2008	SLES
Administration Console/ Identity Server	Migrate For more information see Migrating Administration Consoles From Windows 2003 to Windows 2008	Upgrade For more information see, ◆ Upgrading the Windows Administration Console ◆ Upgrading the Windows Identity Server	Migrate For more information see, ◆ Migrating the Primary Administration Console ◆ Migrating the Secondary Administration Console ◆ Migrating Identity Server
Access Gateway Appliance	NA	NA	Migrate For more information, see Migrating 3.1 SP4 Access Gateway Appliance to 3.2 Access Gateway Appliance
Access Gateway Service	NA	Upgrade For more information, see Upgrading the Windows Access Gateway Service	Upgrade For more information see, Upgrading the 3.1 SP4 Access Gateway Service
SSL VPN	NA	NA	Migrate For more information, see Migrating SSL VPN

IMPORTANT: J2EE agents cannot be migrated or upgraded. You have to install the J2EE agents on the new Access Manager 3.2 setup. For more information see, *NetIQ Access Manager 3.2 J2EE Agent Guide*

1.1.4 IP Address Considerations

Before you migrate to the Access Manager 3.2 setup, you must decide if you want to reuse your existing IP address or use a new IP address to setup the system.

If you are already on a 64-bit architecture (Access Manager 3.1 SP4 installed on a 64-bit hardware), you can choose to reuse the existing IP address, whereas if you have decided to move to new 64-bit servers, you must use new IP addresses.

NOTE: In case of Primary Administration Console migration, you will need a new IP address, that will be temporarily used by the new 3.2 Administration Console. During the migration process, this new IP address is replaced with the original 3.1.4 Administration Console IP address.

The details on how to use both scenarios to migrate your Access Manager components is explained in Chapter 2, “Migrating Access Manager,” on page 13 .

1.2 Order of Migrating/Upgrading the Access Manager Components

Whether you need to upgrade or migrate, it is important that you move each component in the following order. Doing this will ensure that the integrity of the application and data is maintained.

1. Administration Console
2. Identity Server
3. Access Gateway Appliance
4. SSL VPN

1.3 Limitations

- Cross-platform migrations are currently not supported. For example, it is not possible to migrate from Access Manager installed in a SLES environment to a Windows environment and vice versa.
- NetIQ Access Manager Appliance (single-box solution) deployment is supported only for new installations. You cannot migrate from Access Manager 3.1 SP4 to Access Manager Appliance 3.2.
- Migration from the Access Gateway Appliance to the Access Gateway Service and vice versa is not supported.
- Cookie mangling should not be enabled in the mixed-mode cluster. The 3.1 SP4 Access Gateways do not understand mangled cookies.

2 Migrating Access Manager

Migration is the process in which you install the latest version of Access Manager on a new server and then migrate the existing data to the new server.

During the migration process you can either provide a new IP address and host name or reuse an existing IP address.

You can perform migration on a SLES 11 or a Windows 2003 server. If you are on Windows 2008, you must upgrade to Access Manager 3.2.

NOTE: If you encounter any errors while migrating, see Chapter 4, “TroubleShooting,” on page 61.

2.1 Port Details

In version 3.2, the Administration Console, Identity Server, and SSL VPN run in separate instances of tomcat. By default, each component's tomcat uses ports 8080 (http) and 8443 (https). Installing multiple components on the same server can cause a port conflict. To avoid this conflict, each component is assigned a unique port number on which the device can listen.

If a component is installed on a dedicated server no port changes are required. By default, the http port is 8080 and the https port is 8443.

The browser requests made to ports 8080/8443 are automatically redirected to the port on which the component is listening. Depending on the configuration, you must open ports 2080, 2443, and 3443 in the firewall.

The following table describes the ports for all the components of Access Manager:

Configuration	Identity Server	Administration Console	SSL VPN
Access Gateway + SSL VPN	NA	NA	8080/8443
Administration Console + SSL VPN	NA	2080/2443	8080/8443
Administration Console only	NA	8080/8443	NA
Identity Server + Administration Console	8080/8443	2080/2443	NA

Configuration	Identity Server	Administration Console	SSL VPN
Identity Server + Administration Console + SSL VPN	8080/8443	2080/2443	3080/3443
Identity Server + SSL VPN	8080/8443	NA	3080/3443
Identity Server only	8080/8443	NA	NA
SSL VPN only	NA	NA	8080/8443

2.2 Migrating Access Manager on SLES

2.2.1 Migrating Administration Consoles

Prerequisites for the Administration Console Migration

In addition to the following prerequisites, ensure that you also meet the hardware requirements for the Administration Console. For details, see "Administration Console Requirements" in the *NetIQ Access Manager 3.2 SP1 Installation Guide*.

- ❒ A new IP address, that will be temporarily used during the Primary Administration Console migration.
- ❒ Timeout Per Protected Resource (TOPPR) is enabled and applied in the Access Gateway. In the Administration Console, click *Devices* > *Access Gateways* > *Edit*, then click *Enable Timeout Per Protected Resource*.

  If the *Enable Timeout Per Protected Resource* option has already been applied, it will not be displayed on the screen.
- ❒ The primary and secondary 3.1 SP4 Administration Console time is synchronized. You can synchronize the time by enabling the Network Time Protocol (NTP) server through YaST. To do this, go to *YaST* > *Network Services* > *NTP Configuration* page.
- ❒ The new 3.2 Administration Console that you want to install should be on the same subnet as the existing 3.1 SP4 primary console.
- ❒ The health statuses for all devices in the Administration Console are green in color.

  For more information, see "Viewing Device Health" in the *NetIQ Access Manager 3.2 SP1 Administration Console Guide*.

- ❒ You have physical access to the server or server console (in case of VMWare setups) as a root user and you are familiar with iptables.

  The required ports are opened in the firewall. For more information on ports, see Section 2.1, "Port Details," on page 13.

- ❒ Note down the contracts selected under the *Satisfies contract* list of SAML2.0 and Liberty identity providers. These are under *Devices* > *Identity Servers* > *Edit* > *[Protocol]* > *[IdentityProvider]* > *Authentication Card*.

  The application interface for this feature has changed in version 3.2. You must manually configure these contracts after migration. This configuration will be effective after the Identity Server migration is done.

  (Optional) If federation is configured, see the contracts configured for 3.1 SP4, and navigate to *Administration Console* > *Devices* > *Identity Servers* > *Edit* > [*Protocol*] > [*Identity Provider*] > *Authentication Card*. The *Satisfies Contract* field lists all the configured contracts.

- ❒ The host name of the new 3.2 Administration Console should be different from the existing 3.1 SP4 primary and secondary Administration Consoles.

- ❒ Ensure that the `/etc/hosts` file of the system where you are installing Access Manager 3.2 has the host name and IP address for the new 3.2 Administration Console server. If the hostname of the Administration Console is not listed in DNS, the `/etc/hosts` file is used to resolve the hostname of the machine to a valid IP address.

WARNING: If three Administration Consoles are already installed and configured in the 3.1 SP4 setup, uninstall one secondary Administration Console before running the `install_and_migrate-3.2.sh` script.

For more information about how to deconfigure and uninstall the Administration Console, see Step 12 on page 19 and "Uninstalling the Linux Administration Console" in the *NetIQ Access Manager 3.2 SP1 Installation Guide*.

Migration Scenarios for the Administration Console

The following scenarios are supported for migrating NetIQ Access Manager from 3.1 SP4 to 3.2 on Linux.

IMPORTANT: Ensure you identify the scenario that best describes your migration environment and review the appropriate steps before you begin the process of migration.

- "The Administration Console, Identity Server, 3.1 SP4 Access Gateway Appliance, and SSL VPN Are Installed on Different Servers" on page 16
- "The Administration Console and Identity Server Are on the Same Server, and the 3.1 SP4 Access Gateway Appliance Is on a Different Server" on page 16
- "The Secondary Administration Console and Identity Server are on the Same Server" on page 16
- "The Administration Console, Identity Server, and SSL VPN Are on the Same Server" on page 16

The Administration Console, Identity Server, 3.1 SP4 Access Gateway Appliance, and SSL VPN Are Installed on Different Servers

Workflow:

1. Migrate the Administration Consoles.
2. Migrate the Identity Server.
3. Migrate the 3.1 SP4 Access Gateway Appliance to the 3.2 Access Gateway Appliance.
4. Migrate the SSL VPN from 3.1 SP4 to 3.2.

The Administration Console and Identity Server Are on the Same Server, and the 3.1 SP4 Access Gateway Appliance Is on a Different Server

Workflow:

1. Migrate the primary Administration Console.
2. Migrate the Identity Server.
3. Migrate the 3.1 SP4 Access Gateway Appliance to the 3.2 Access Gateway Appliance.

The Secondary Administration Console and Identity Server are on the Same Server

Workflow:

1. Migrate the primary Administration Console.
2. Migrate the secondary Administration Console.
3. Migrate the Identity Server.

The Administration Console, Identity Server, and SSL VPN Are on the Same Server

Workflow:

1. Migrate the Administration Consoles.
2. Migrate the Identity Server.
3. Migrate SSL VPN.

NOTE: If the device has multiple interfaces, use YaST to manually configure the primary IP address on each NIC.

To do this, go to *YaST* > *Network Devices* > *Network Settings* > *Overview*. Select the network card and click *Edit*. Enter the primary IP address. Click *Next* > *Ok* > *Quit*.

Migrating the Primary Administration Console

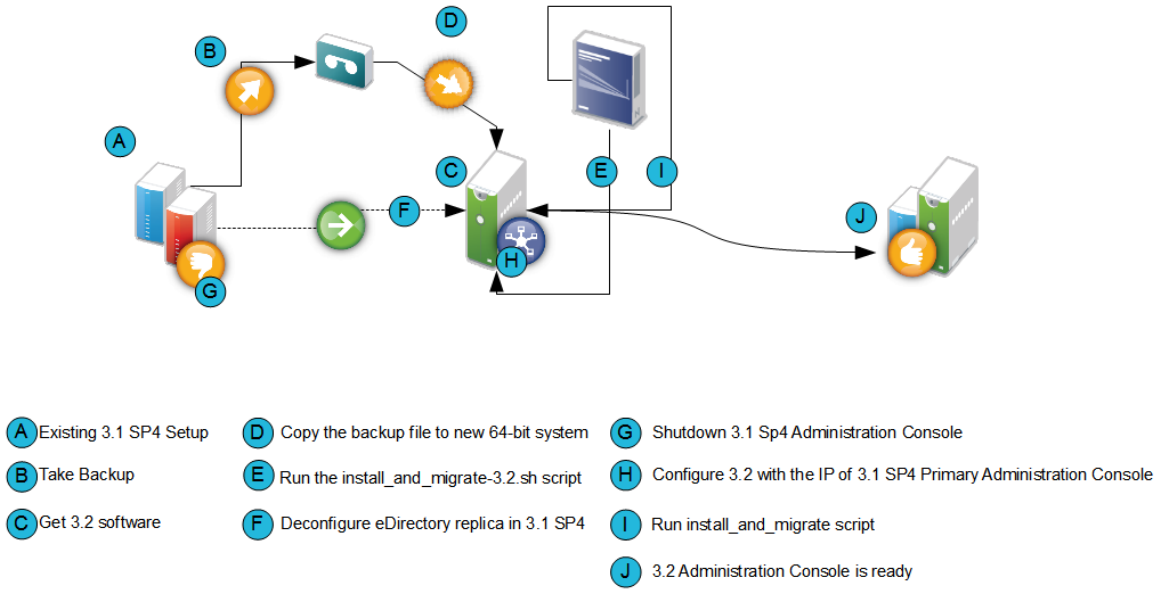
- "Migration Process" on page 17

IMPORTANT: Before you proceed with the steps for migration, ensure that you have followed the instructions in the Prerequisites for the Administration Console Migration.

If you have multiple components installed on the same system, before starting migration of any component, ensure that you read the migration prerequisites of all components.

Migration Process

Figure 2-1 *Process of Migration of the Primary Administration Console*



1 Back up the 3.1 SP4 primary Administration Console configuration by using the `/opt/novell/devman/bin/ambkup.sh` script.

   Remember the password that you enter while saving the backup file. You will need this password in Step 10.

   The NetIQ Access Manager backup file is used only for restoring the certificates. The rest of the data is synchronized through eDirectory replication.

   For more information about how to perform a backup, see "Backing Up and Restoring" in the *NetIQ Access Manager 3.2 SP1 Administration Console Guide*.

   IMPORTANT: It is strongly recommended that you review the log file to confirm if the backup process was completed without any errors.

2 Copy the backup zip file to `/tmp` or any other folder on the new 64-bit server where you plan to install the 3.2 Administration Console.

   Make a note of the location and file name in absolute format. You need to provide this information in the installation and migration script (for example, `/tmp/idpq_20120111_1314.zip`).

3 Ensure you have downloaded the software or you have the CD available.

4 Do one of the following:

   - Insert the CD into the drive, then navigate to the device. Enter the following:

     ```
     cd /media
     ```

     Browse to your CD-ROM drive.

   - If you downloaded the `AM_32_AccessManagerService_Linux64.tar.gz` file, unpack the file using the following command:

     ```
     tar -xzvf AM_32_AccessManagerService_Linux64.tar.gz
     ```

5 Browse to the `novell-access-manager` folder.

   All the files are extracted to the `novell-access-manager` folder.

6 Run the `install_and_migrate-3.2.sh` script from the folder to migrate the primary Administration Console from 3.1 SP4 to 3.2.

Ensure that you install the 3.2 Administration Console in the same subnet as the 3.1 SP4 Administration Console. For more information on the ports, see Section 2.1, "Port Details," on page 13.

7 Type `Y` and press Enter when the following message is displayed: `Would you like to continue this installation y/n? [n]:`

8 Accept the license agreement by entering `y` when the system prompts you.

9 Type `Y` and press Enter when the system displays the following message:

```
This will install NAM 3.2 as a secondary and promotes it to primary later.
During this process, the IP address of this machine will have to be changed to
the original 3.1 SP4 Administration Console IP.
Would you like to continue this installation (y/n)?
```

10 Provide the following details:

3.1 Primary Administration Console IP address: Enter the 3.1 SP4 primary IP address. Ensure that the IP address is static.

Access Manager Administration user ID: Enter the administrator user ID.

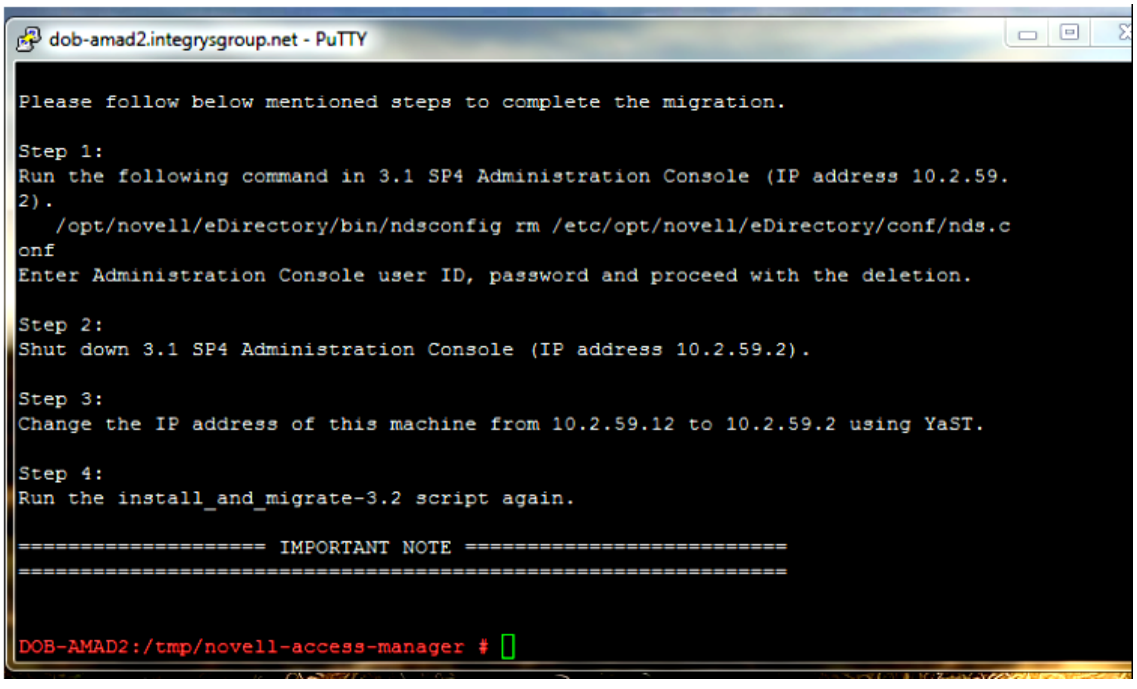
Access Manager Administration password: Enter the administrator password. Re-enter the password for verification.

Enter the backup file with absolute path: Enter the absolute path of the backup file that you created in Step 1.

Enter a password for decrypting the data: Enter the private key encryption password of the backup file. Re-enter the password for verification.

NOTE: To view installation progress, refer to the log files in `/tmp/novell_access_manager`.

After installing the 3.2 Administration Console, the system displays the following:



11 Verify if the 3.2 Access Manager server is functional. Perform one of the following steps from the 3.2 terminal:

11a Run `/opt/novell/eDirectory/bin/ndsstat -r` command. This lists all the replicas available. Verify that the status of the 3.2 replica is `On`.

11b Run `/opt/novell/eDirectory/bin/ldapsearch -A -LLL -b "ou=accessManagerContainer,o=novell" -D "cn=<username>,o=novell" -w <password>` command. This lists all the objects in the `NAM` container. You can run the same command on the 3.1 SP4 terminal to verify if the object list is complete and accurate.

12 In the Access Manager 3.1 SP4 Administration Console, run the following command to deconfigure the eDirectory replica in the 3.1 SP4 server:

```
/opt/novell/eDirectory/bin/ndsconfig rm /etc/opt/novell/eDirectory/conf/
nds.conf
```

12a Enter admin credentials in the `admin.novell` format and proceed with deletion.

The system displays the following warning:

```
Deconfiguring Novell eDirectory might cause problems in the operation of
modules dependent on eDirectory. Do you wish to continue? (y/n)
```

12b Enter `Y` to proceed with deletion.

After deletion, the following message will be displayed:

```
Deconfiguration of eDirectory server is complete.
The instance at /etc/opt/novell/eDirectory/conf/nds.conf is successfully
removed.
Stopping the service 'ndsd'... Done
```

13 Shut down the 3.1 SP4 Administration Console.

14 In the Access Manager 3.2 Administration Console, use YaST to change the IP address to the old primary Administration Console IP address:

14a Go to *YaST > Network Devices > Network Settings > Overview*.

NOTE: Launch YaST from the physical server or if you are using a virtual machine, use the console. We do not recommend that you use a remote connection for changing the IP address, since you may lose the remote connection.

14b Select the network card and click *Edit*.

14c Change the IP address to the 3.1 SP4 primary Administration Console IP address.

14d Click *Next > Ok > Quit*.

15 Run the `install_and_migrate-3.2.sh` script from the `novell-access-manager` folder again to complete the installation.

The following message is displayed:

```
Migration of NAM 3.1 SP4 to 3.2
Would you like to continue (y/n)?
```

15a Enter `Y` and the following message is displayed:

```
Installation will continue to finish the rest of the 3.2 migration tasks

Would you like to continue this installation (y/n)?
```

15b Enter `Y` and then provide the following details:

- Enter the Access Manager Administration user ID [admin].

- Enter the Access Manager Administration password.
- Re-enter the password for verification.

After migration is complete, the system displays the following message:

```
3.2 Administration Console migration completed successfully.
```

Migrating the Secondary Administration Console

To install the secondary Administration Console you can either use a new server that supports a 64-bit installer to install the secondary Administration Console or you can reuse the existing server for installation if it supports the 64-bit installer.

To migrate the secondary Administration Console to 3.2, use one of the following procedures:

- "Using a New Server for the Secondary Administration Console" on page 20
- "Reusing the Existing Server or IP Address for the Secondary Administration Console" on page 21

Using a New Server for the Secondary Administration Console

IMPORTANT: Before you install the 3.2 secondary Administration Console on a 64-bit server, it is important to de-commission the 3.1 SP4 secondary Administration Console. This process helps ensure that the number of Administration Consoles do not exceed three instances.

1. Verify if the 3.2 Access Manager server is functional. Perform one of the following steps from the 3.2 terminal:
   - **1a** Run `/opt/novell/eDirectoy/bin ndsstat -r` command. This lists all the replicas available. Verify that the status of the 3.2 replica is `On`.
   - **1b** Run `/opt/novell/eDirectory/bin/ldapsearch -A -LLL -b "ou=accessManagerContainer,o=novell" -D "cn=<username>,o=novell" -w <password>` command. This lists all the objects in the `NAM` container. You can run the same command on the 3.1 SP4 terminal to verify if the object list is complete and accurate.
2. Run the following command to delete the eDirectory replica in the 3.1 SP4 secondary Administration Console server:

   ```
   /opt/novell/eDirectory/bin/ndsconfig rm /etc/opt/novell/eDirectory/conf/nds.conf
   ```
3. Enter admin credentials in the `admin.novell` format and proceed with deletion.
4. Log in to the 3.2 primary Administration Console.
5. Click *Auditing* > *Troubleshooting*> *Other Known Device Manager Servers*.
6. Click *Remove* for this server.
7. Install the 64-bit SLES 11 SP1 or higher operating system on the new 64-bit server with a *different host name*.
   - **7a** Go to *YaST* > *Network Devices* > *Network Settings* > *Overview*.
   - **7b** Select the network card and click *Edit*.
   - **7c** Specify a different host name.

     For more information, see *SLES 11 Installation Quick Start* (http://www.suse.com/documentation/sles11/book_quickstarts/data/book_quickstarts.html).

8 Ensure you have downloaded the software or you have the CD available.

9 Do one of the following:

- Insert the CD into the drive, then navigate to the device. Enter the following:

  ```
  cd /media
  ```

  Browse to your CD-ROM drive.

- If you downloaded the `AM_32_AccessManagerService_Linux64.tar.gz` file, unpack the file using the following command:

  ```
  tar -xzvf AM_32_AccessManagerService_Linux64.tar.gz
  ```

10 Browse to the `novell-access-manager` folder.

All the files are extracted to the `novell-access-manager` folder.

Reusing the Existing Server or IP Address for the Secondary Administration Console

To use the existing server for installing the secondary Administration Console, ensure it is a 64-bit server.

1 Verify if the 3.2 Access Manager server is functional. Perform one of the following steps from the 3.2 terminal:

1a Run `/opt/novell/eDirectory/bin/ndsstat -r` command. This lists all the replicas available. Verify that the status of the 3.2 replica is `On`.

1b Run `/opt/novell/eDirectory/bin/ldapsearch -A -LLL -b "ou=accessManagerContainer,o=novell" -D "cn=<username>,o=novell" -w <password>` command. This lists all the objects in the `NAM` container. You can run the same command on the 3.1 SP4 terminal to verify if the object list is complete and accurate.

2 Run the following command to delete the eDirectory replica in the 3.1 SP4 secondary Administration Console server:

```
/opt/novell/eDirectory/bin/ndsconfig rm /etc/opt/novell/eDirectory/conf/nds.conf
```

3 Enter the admin credentials in `admin.novell` format and proceed with deletion.

4 Log in to the 3.2 primary Administration Console.

5 Click *Auditing* > *Troubleshooting*> *Other Known Device Manager Servers*.

6 Click *Remove* for this server.

7 Format the server with the 64-bit SLES 11 SP1 or higher operating system and a different host name or configure the same IP address with a different host name.

7a Go to *YaST* > *Network Devices* > *Network Settings* > *Overview*.

7b Select the network card and click *Edit*.

7c Specify a different host name.

IMPORTANT: Even after formatting the server, old certificates are not cleaned up from the user store. If you are using an existing host name during Access Manager installation, it may lead to a conflict with the existing certificates. It is recommended to use a different host name during IP address configuration.

---

8 Ensure you have downloaded the software or you have the CD available.

9 Do one of the following:

- Insert the CD into the drive, then navigate to the device. Enter the following:

```
cd /media
```

Browse to your CD-ROM drive.

- If you downloaded the `AM_32_AccessManagerService_Linux64.tar.gz` file, unpack the file using the following command:

  ```
  tar -xzvf AM_32_AccessManagerService_Linux64.tar.gz
  ```

10 Browse to the `novell-access-manager` folder.

All the files are extracted to the `novell-access-manager` folder.

11 Install the secondary Administration Console by using the `install.sh` script.

For more information about how to install the secondary Administration Console, see "Installing Secondary Versions of the Administration Console" in the *NetIQ Access Manager 3.2 Setup Guide*.

NOTE: If the secondary Administration Console migration exits stating that the Server's DIB does not contain replicas, see Section 4.3, "Migration Exits Stating That the Server's DIB Does Not Contain Replicas," on page 63.

2.2.2 Migrating Identity Server

It is recommended that you replace the Identity Servers individually. The 3.1 SP4 and 3.2 Identity Servers can coexist until the migration is complete.

Prerequisites for the Identity Server Migration

In addition to the following prerequisites, ensure that you also meet the hardware requirements for the Administration Console. For details, see "Administration Console Requirements" in the *NetIQ Access Manager 3.2 SP1 Installation Guide*.

- The Identity Server can perform a DNS resolution with the ESP (Embedded Service Provider) host name of the Access Gateway.

  For more information, see "DNS Name Resolution" in the *NetIQ Access Manager 3.2 SP1 Identity Server Guide*.

- The Identity Server time is synchronized with the time of the Administration Console. You can synchronize the time by enabling the Network Time Protocol (NTP) server through YaST. To do this, go to *YaST > Network Services > NTP Configuration*.
- You have physical access to the server or server console (in case of VMWare setups) as a root user and are familiar with firewall configurations. The required ports also must be opened in the firewall. For more information on the ports, see Section 2.1, "Port Details," on page 13.
- Determine if you want to reuse an existing IP address or use a new IP address for the migration process.
- If the services are managed by an L4 switch, remove the device that you are migrating from the L4 switch. Add the device back to the L4 switch once the migration is done successfully. This is required so that no user requests are sent by L4 switch to that device during migration.

- If you have customized any files use the `migrate_backup.sh` script to back up the files. This script is located in the `novell-access-manager` folder in the `AM_32_AccessManagerService_Linux64.tar.gz` file. Copy this script to the 3.1 SP4 machine and run the script to do the back up. It is important to take the backup regardless of whether you are reusing the same machine or a new machine.

  As part of the backup process, the files that get backed up are:

  - `/var/opt/novell/tomcat5/webapps/nidp/jsp`
  - `/var/opt/novell/tomcat5/webapps/nidp/html`
  - `/var/opt/novell/tomcat5/webapps/nidp/images`
  - `/var/opt/novell/tomcat5/webapps/nidp/config`
  - `/var/opt/novell/tomcat5/webapps/nidp/WEB-INF/lib`
  - `/var/opt/novell/tomcat5/webapps/nidp/WEB-INF/web.xml`
  - `/var/opt/novell/tomcat5/webapps/nidp/WEB-INF/classes`
  - `/var/opt/novell/tomcat5/webapps/nidp/WEB-INF/conf`
  - `/opt/novell/java/jre/lib/security/nidpkey.keytab`
  - `/opt/novell/java/jre/lib/security/bcslogin.conf`
  - `/var/opt/novell/tomcat5/webapps/nidp/classUtils`
  - `/var/opt/novell/tomcat5/conf/server.xml`
  - `/var/opt/novell/tomcat5/conf/tomcat5.conf`

- (Conditional) If the Identity Server cluster has been assigned to delegated administrators, remove them before migration and re-add them after the migration is complete.

  If you do not perform this action, the delegated administrators will not be able to log in and configure devices assigned to them. You must manually re-create these administrators and assign the respective devices.

  For more information about delegated users, "Managing Delegated Administrators" in the *NetIQ Access Manager 3.2 SP1 Administration Console Guide*.

Reusing an Existing IP Address

- "The Identity Server Is the Only Component on the Server" on page 23
- "The Identity Server and SSL VPN Are on the Same Server" on page 24

The Identity Server Is the Only Component on the Server

Workflow:

1. Back up the files if they have been changed from the default.
2. Stop and remove the 3.1 SP4 Identity Server.
3. Delete the 3.1 SP4 Identity Server which is removed from the Identity Servers cluster.
4. Uninstall the 3.1 SP4 Identity Server if you are going to use the current server to install 3.2 Identity Server.
5. Add the 3.2 Identity Server to the existing Identity Server cluster in the Administration Console.
6. Update the Identity Server and apply changes.
7. Restore the backed up files.

The Identity Server and SSL VPN Are on the Same Server

Workflow:

1. Back up the customized files.
2. Stop the 3.1 SP4 Identity Server.
3. Remove the 3.1 SP4 Identity server from the cluster.
4. Delete the 3.1 SP4 Identity Server from the Identity Servers cluster.
5. Uninstall the 3.1 SP4 Identity Server if you are going to use the current server to install 3.2 Identity Server.
6. Uninstall the 3.1 SP4 SSL VPN Server if you are going to use the current server to install 3.2 SSL VPN Server.

   WARNING: Ensure that you uninstall the SSL VPN server and do not delete the SSL VPN server object. Deleting the SSL VPN server instead of uninstalling the server will result in loss of settings.

   ---

7. Use the NetIQ Access Manager 3.2 installer to install the 3.2 Identity Server on a 64-bit SLES 11 SP1 or higher operating system.
8. Add the 3.2 Identity Server to the existing Identity Servers cluster in the Administration Console.
9. Update the Identity Server and apply changes.
10. Restore the backed up files.
11. Install SSL VPN on the same server.
12. **(Optional) For the ESP-enabled SSL VPN:** When the Identity Server and ESP-enabled SSL VPN are migrated to the same server:
    - **12a** Click *Device > SSL VPN > Edit > Authentication Configuration*.
    - **12b** In the *Embedded Service Provider Base URL* field, change the ports to 3080 and 3443 for http and https respectively.
13. **(Optional) For the traditional SSL VPN:** When the Identity Server and traditional SSL VPN are migrated to the same server:
    - **13a** Click *Access Gateway > Edit > Service.*
    - **13b** Click the SSL VPN Web server address and change the connection ports to 3080 and 3443 for http and https respectively.

      NOTE: For NetIQ Access Manager 3.2 and later, release onwards, SSL VPN will be accessible on ports 3080 (http) and 3443 (https) when installed on the same server as the Identity Server.

Using a New IP Address

- "The Identity Server Is the Only Component on the Server" on page 25
- "The Identity Server and SSL VPN Are on the Same Server" on page 25

The Identity Server Is the Only Component on the Server

Workflow:

1. Back up the customized files.
2. Use the NetIQ Access Manager 3.2 installer to install the 3.2 Identity Server on a 64-bit SLES 11 SP1 or higher operating system.
3. Add the 3.2 Identity Server to the existing Identity Server cluster in the Administration Console.
4. Update the Identity Server and apply changes.
5. Restore the backed up files.

The Identity Server and SSL VPN Are on the Same Server

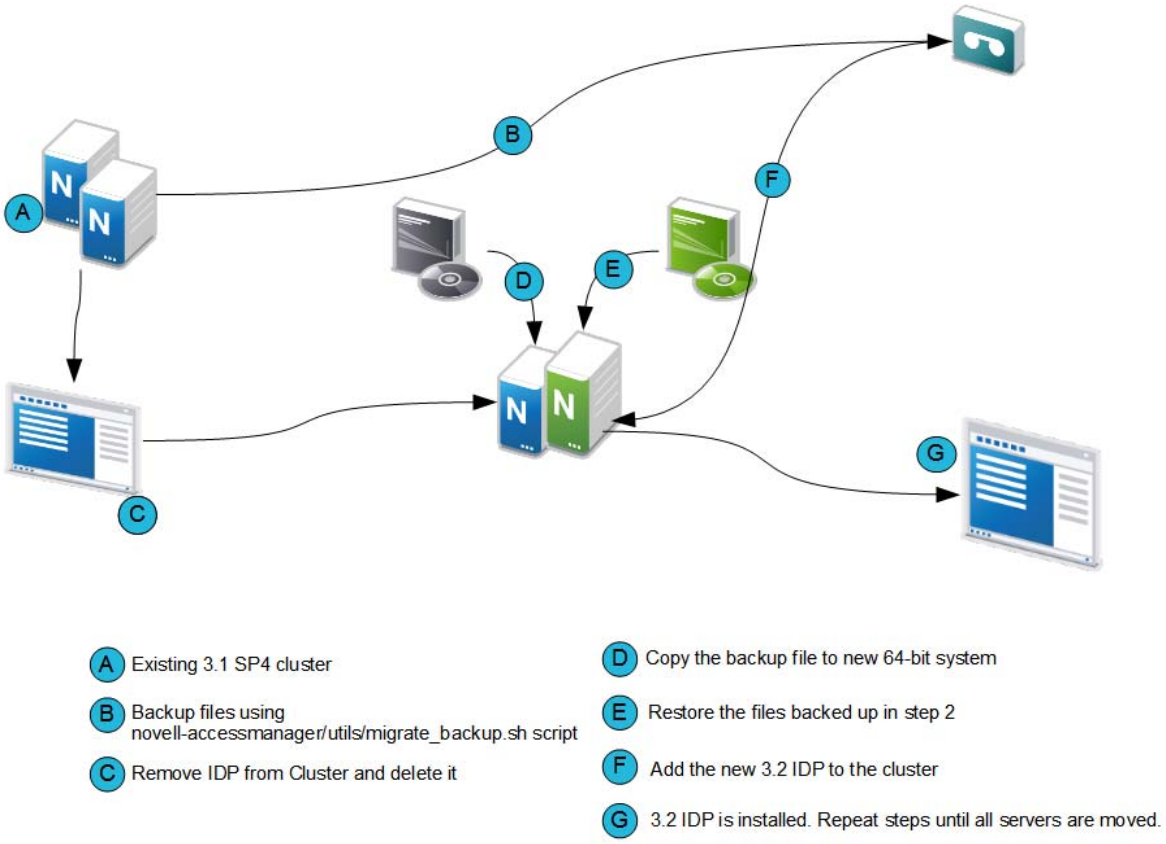
Workflow:

1. Back up the customized files.
2. Run the NetIQ Access Manager 3.2 installer on a 64-bit SLES 11 SP1 or higher operating system and install the Identity Server.
3. Add the 3.2 Identity Server to the existing Identity Servers cluster in the Administration Console.
4. Update the Identity Server and apply the changes.
5. Install SSL VPN on the same server.
6. Add the 3.2 SSL VPN to the existing SSL VPN cluster in the Administration Console.
7. Update and apply changes.
8. Restore the backed up files.
9. **(Optional) For the ESP-enabled SSL VPN:** When the Identity Server and ESP-enabled SSL VPN are migrated to the same server:
   - 9a Click *Device > SSL VPN > Edit > Authentication Configuration*.
   - 9b In the *Embedded Service Provider Base URL* field, change the ports to 3080 and 3443 for http and https respectively.
10. **(Optional) For the traditional SSL VPN:** When the Identity Server and traditional SSL VPN are migrated to the same server:
    - 10a Click *Access Gateway > Edit > Service*.
    - 10b Click the SSL VPN Web server address and change the connection ports to 3080 and 3443 for http and https respectively.

NOTE: For NetIQ Access Manager 3.2 and later, SSL VPN is accessible on ports 3080 (http) and 3443 (https) when it is installed on the same server as the Identity Server.

Process of Migration

Figure 2-2 *Process of Migrating the Identity Server*



IMPORTANT: Before you proceed with the steps for migration, ensure that you have followed the instructions in the Prerequisites for the Identity Server Migration

1. Stop the Identity Server and remove the Identity Server from the cluster configuration.
   - **1a** In the Administration Console, click *Devices* > *Identity Servers*.
   - **1b** Select the server, then click *Stop*.
   - **1c** Select the server, then choose *Actions* > *Remove from cluster*.
   - **1d** Update the cluster configuration.
2. If you are using an existing machine, delete the existing Identity Server from the Administration Console before installing the new Identity Server.
   - **2a** In the Administration Console, click *Devices* > *Identity Servers*.
   - **2b** Select the server, then click *Stop*.
   - **2c** Click *Actions* > *Delete.*
3. If the operating system is already 64-bit SLES 11 SP1 or higher, uninstall the 3.1 SP4 version and install the 3.2 Identity Server.
4. Perform a new installation of 64-bit SLES 11 SP1 or higher operating system.

   For more information, see *SLES 11 Installation Quick Start* (http://www.suse.com/documentation/sles11/book_quickstarts/data/book_quickstarts.html).

5 Ensure the following packages are installed:

- **perl-gettext, gettext-runtime:** The required library and tools to create and maintain message catalogs.
- **python:** The Python library.
- **compat:** Libraries to address compatibility issues. On SLES 11 SP1 platform, the `compat-32bit` package is available in the SLES11-Extras repository. For information on enabling this repository, see TID 7004701 (http://www.novell.com/support/kb/doc.php?id=7004701).

5a Use YaST to install the packages that have not yet been installed.

5b Use the following command to verify the installation:

```
rpm -qa | grep <package name>
```

Replace <*package name*> with the name of the package you want to verify. For example:

```
rpm -qa | grep compat
```

5c Ensure you have downloaded the software or you have the CD available.

5d Do one of the following:

- Insert the CD into the drive, then navigate to the device. Enter the following:

  ```
  cd /media
  ```

  Browse to your CD-ROM drive.
- If you downloaded the `AM_32_AccessManagerService_Linux64.tar.gz` file, unpack the file using the following command:

  ```
  tar -xzvf AM_32_AccessManagerService_Linux64.tar.gz
  ```

5e Browse to the `novell-access-manager` folder.

All the files are extracted to the `novell-access-manager` folder.

5f Run the `install.sh` script from the `novell-access-manager` folder on a 64-bit SLES 11 SP1 or higher server and choose the option to install the Identity Server.

6 Enter the following details:

- IP address of the 3.2 primary Administration Console as the primary Administration Console IP address
- Access Manager Administration User ID
- Access Manager Administration password
- Re-enter the password for verification

The system displays the following warning:

```
WARNING! In 3.2 and later, Administration Console will be accessible on ports
2080 (HTTP) and 2443 (HTTPs) when Identity Server or SSL VPN are installed on
the same machine.

Would you like to continue (y/n) ? [n]:y
```

Enter `y` to continue.

7 If local NAT is available for the Identity Server, enter the NAT IP address. For more information on configuring Network Address Translation, see "Configuring Network Address Translation" in the *NetIQ Access Manager 3.2 SP1 Installation Guide*.

8 Enter `Y` to proceed with installation.

After installation, this Identity Server device is displayed in the Administration Console.

9 Restore any customized files from the backup taken earlier as part of steps in "Prerequisites for the Identity Server Migration" on page 22.

To restore the files, copy the content of the following files to the corresponding file in the new location.

Table 2-1 *Restoring Files During IDP Migration*

Old File Location	New File Location
/var/opt/novell/tomcat5/webapps/nidp/jsp	/opt/novell/nam/idp/webapps/nidp/jsp
/var/opt/novell/tomcat5/webapps/nidp/html	/opt/novell/nam/idp/webapps/nidp/html
/var/opt/novell/tomcat5/webapps/nidp/images	/opt/novell/nam/idp/webapps/nidp/images
/var/opt/novell/tomcat5/webapps/nidp/config	/opt/novell/nam/idp/webapps/nidp/config
/var/opt/novell/tomcat5/webapps/nidp/WEB-INF/lib	/opt/novell/nam/idp/webapps/nidp/WEB-INF/lib
/var/opt/novell/tomcat5/webapps/nidp/WEB-INF/web.xml	/opt/novell/nam/idp/webapps/nidp/WEB-INF/web.xml
/var/opt/novell/tomcat5/webapps/nidp/WEB-INF/classes	/opt/novell/nam/idp/webapps/nidp/WEB-INF/classes
/var/opt/novell/tomcat5/webapps/nidp/WEB-INF/conf	/opt/novell/nam/idp/webapps/nidp/WEB-INF/conf
/opt/novell/java/jre/lib/security/bcslogin.conf	/opt/novell/java/jre/lib/security/bcslogin.conf
/opt/novell/java/jre/lib/security/nidpkey.keytab	/opt/novell/java/jre/lib/security/nidpkey.keytab
/var/opt/novell/tomcat5/webapps/nidp/classUtils	/opt/novell/nam/idp/webapps/nidp/classUtils

server.xml: If you have modified any elements or attributes in the 3.1 SP4 environment the corresponding changes will need to be applied to the 3.2 `/opt/novell/nam/idp/conf/server.xml` file.

Typical changes done to the `server.xml` in 3.1 SP4 include modifying the '`Address=`' attribute to restrict the IP address the application will listen on, or '`maxThreads=`' attribute to change the number of threads.

In the following example, 3.1 SP4 is customized to use the following ciphers.

```
<Connector NIDP_Name="connector" port="8443" address=""
ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA,, ...   ../>
```

When migrating to 3.2, copy the cipher list from your 3.1 SP4 `server.xml` and replace it in the SSL connector section of the 3.2 `server.xml` file.

tomcat5.conf: Copy any elements or attributes that you have customized in the 3.1 SP4 `tomcat5.conf` file to the 3.2 `tomcat7.conf` file.

For example, if you have included the environment variable in the 3.1 SP4 `tomcat5.conf file` to increase the heap size by using `-Xmx/Xms/Xss` settings, the variables should be copied to the 3.2 `/opt/novell/nam/idp/conf/tomcat7.conf` file.

10 Add the newly installed Identity Server to the existing Identity Servers cluster.

For more information, see "Clustering Identity Servers"in the *NetIQ Access Manager 3.2 Setup Guide.*

The cluster object stores all the existing Identity Server configurations. The newly added Identity Servers inherit these configurations.

11 On the newly added Identity Server, restart Tomcat using the `/etc/init.d/novell-idp restart` or `rcnovell-idp restart` command.

12 Repeat Step 1 through Step 11 until all the 3.1 SP4 Identity Servers are replaced with 3.2 Identity Servers.

2.2.3 Migrating 3.1 SP4 Access Gateway Appliance to 3.2 Access Gateway Appliance

Prerequisites for the Access Gateway Appliance Migration

In addition to the following prerequisites, ensure that you also meet the hardware requirements for the Administration Console. For details, see "Administration Console Requirements" in the *NetIQ Access Manager 3.2 SP1 Installation Guide*.

- ❒ Timeout Per Protected Resource (TOPPR) is enabled and applied in the Access Gateway. In the Administration Console, click *Devices* > *Access Gateways* > *Edit*, then click *Enable Timeout Per Protected Resource*.

  If the *Enable Timeout Per Protected Resource* option has already been applied, it will not be displayed on the screen.

- ❒ Access Gateway should be in a cluster before migration. If the Access Gateway is on a single device, create an access gateway cluster with a single device before migration.

  For more information, see "Managing a Cluster of Access Gateways" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

- ❒ You have physical access to the server or server console (in case of VMWare setups) as a root user and are familiar with firewall configurations. The required ports must be opened in the firewall. For more information on the ports, see Section 2.1, "Port Details," on page 13.

- ❒ Ensure that you have migrated all the Administration Consoles and Identity Servers before migrating the 3.1 SP4 Access Gateway Appliance to the 3.2 Access Gateway Appliance.

- ❒ Make a note of the IP addresses and host name of the 3.1 SP4 Access Gateway Appliance before installing the Access Gateway Appliance. The IP address used by 3.1 SP4 Access Gateway Appliance to communicate with the Administration Console will be used for installing the Access Gateway Appliance.

- ❒ Determine if you want to reuse an existing IP address or use a new IP address for the migration process.

- ❒ Ensure that you have the same number of network interfaces on the new 3.2 Access Gateway as in the 3.1 SP4 Access Gateway Appliance.

- ❒ If the services are managed by an L4 switch, remove the device that you are migrating from the L4 switch. Add the device back to the L4 switch once the migration is done successfully. This is required so that no user requests are sent by the L4 switch to that device during migration.
- ❒ If you have older versions prior to the 3.1 SP4 Access Gateway Appliance, first upgrade to 3.1 SP4 using the instructions at Access Manager 3.1 Installation Guide (http://www.novell.com/documentation/novellaccessmanager31/installation/?page=/documentation/novellaccessmanager31/installation/data/bookinfo.html)
- ❒ If you have customized any files back them up using the `migrate_backup.sh` script. This script is located in the `novell-access-manager` folder in the `AM_32_AccessManagerService_Linux64.tar.gz` file.Copy this script to the 3.1 SP4 server and run the script to back up.

  It is important to take the backup regardless of whether you are reusing the same machine or a new server.

  The files that get backed up are:

  - `/var/opt/novell/tomcat5/conf/server.xml`
  - `/var/opt/novell/tomcat5/conf/tomcat5.conf`
  - `/var/opt/novell/tomcat5/conf/web.xml`
  - `/var/opt/novell/tomcat5/webapps/nesp/WEB-INF/web.xml`
  - `/var/opt/novell/tomcat5/webapps/nesp/jsp`
  - `/var/opt/novell/tomcat5/webapps/nesp/html`
  - `/var/opt/novell/tomcat5/webapps/nesp/images`
  - `/var/opt/novell/tomcat5/webapps/nesp/config`
  - `/chroot/lag/opt/novell/bin/preapply.sh`
  - `/chroot/lag/opt/novell/bin/postapply.sh`
  - `/var/novell/errorpagesconfig/current/ErrorMessages.xml`
  - `/var/novell/ErrorPagesConfig.xml`
- ❒ If you have touch files configured in the 3.1 SP4 Access Gateway Appliance, copy the touch file migration utility files `lag2mag_touchfiles.csv` and `migrate_touchfiles.sh` to the 3.1 SP4 Access Gateway Appliance. These files are located in the `novell-access-manager/utils` folder in the `AM_AccessManagerService_Linux64.tar.gz` file.

  Use the `sh migrate_touchfiles.sh > touchfile_list` command and back up the output file `touchfile_list`.

  The `touchfile_list` file contains the options that needs to be mapped to the advanced options in Access Gateway Appliance.

  Here is an example of sample output:

```
# Global Option example
NAGGlobalOptions InPlaceSilent=on

# Virtual Host/Server Option example
NAGGlobalOptions DebugHeaders=on
```

Reusing an Existing IP Address

- "The 3.1 SP4 Access Gateway Appliance Is the Only Component on the Server" on page 31
- "The SSL VPN and 3.1 SP4 Access Gateway Appliance Are on the Same Server" on page 31

The 3.1 SP4 Access Gateway Appliance Is the Only Component on the Server

Workflow:

1. Back up any files that you have customized and note down the IP address and host name of 3.1 SP4 Access Gateway Appliance.
2. Shut down the 3.1 SP4 Access Gateway Appliance.
3. Install the Access Gateway Appliance with the IP address and host name noted in Step 1.
4. Restore the backed up files.

The SSL VPN and 3.1 SP4 Access Gateway Appliance Are on the Same Server

Workflow:

1. Back up any files that you have customized and note down the IP address and host name of 3.1 SP4 Access Gateway Appliance.
2. Shut down the 3.1 SP4 Access Gateway Appliance.
3. Install the Access Gateway Appliance with the IP address and host name noted in Step 1
4. Select Install and *Enable SSL VPN service* checkbox in the Appliance configuration page.
5. Restore the backed up files.

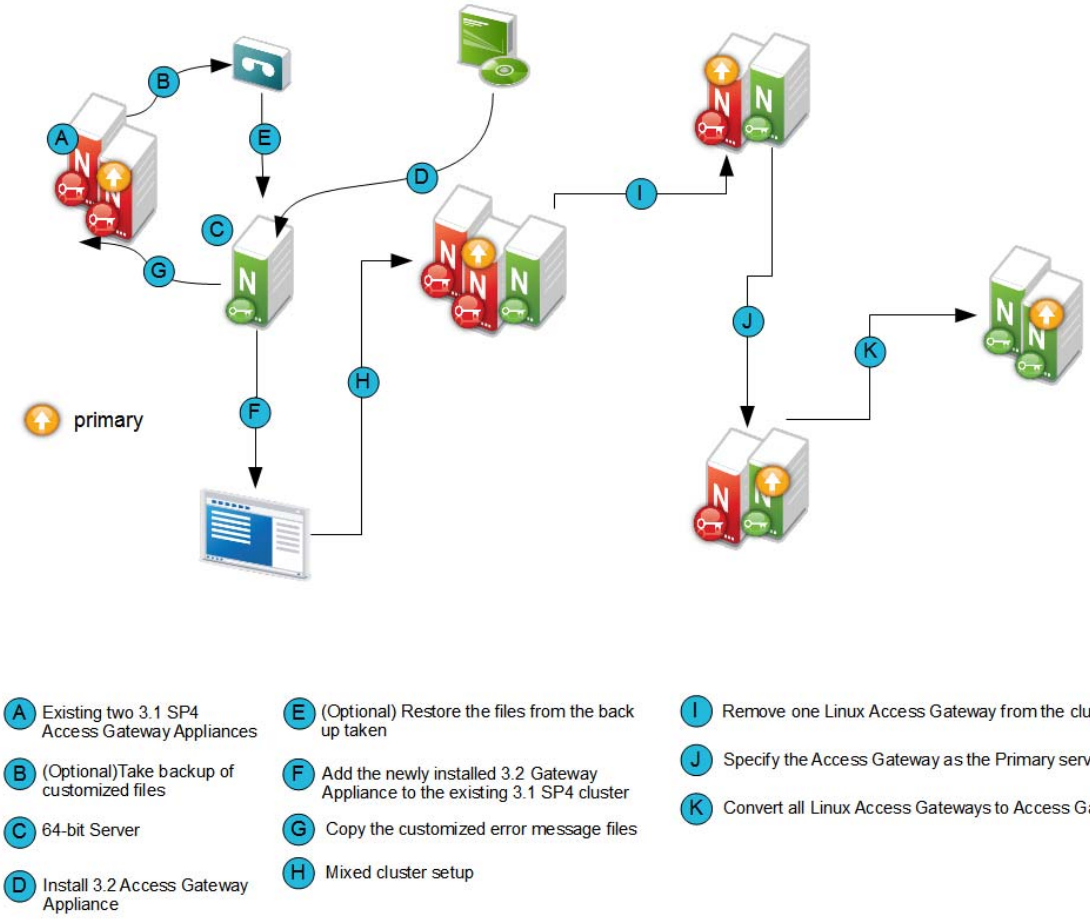
Using a New IP Address

The SSL VPN and 3.1 SP4 Access Gateway Appliance Are on the Same Server

Workflow:

1. Back up any files that you have customized.
2. Mount the Access Gateway Appliance ISO. Start the installation.
3. Select install and *Enable SSL VPN service* checkbox in the Appliance configuration page.
4. Click *Access Gateway* > *Edit* > *Service*.
5. Click the SSL VPN Web server address and change the connection ports to 3080 and 3443 for http and https respectively.
6. Restore the customized files.
7. Add the SSL VPN server to the existing SSL VPN cluster to get the configuration.

Migration Process



Migrating the 3.1 SP4 Access Gateway Appliance to 3.2 Access Gateway Appliance will not cause any disruption to the existing setup. You can add new Access Gateway Appliance nodes into the existing 3.1 SP4 Access Gateway Appliance cluster. They can co-exist together.

If you are using a different server with a different IP address, see "Use case scenario 1:" on page 32 and if you are reusing the same IP address, see "Use case scenario 2:" on page 35.

Use case scenario 1:

This scenario assumes that you have a new 64-bit server to install the 3.2 Access Gateway Appliance and explains how to migrate from 3.1 SP4 using a different IP address.

Consider that the setup includes the following components:

- Administration Console (AC 1)
- Identity Server cluster (IDP 1 and IDP2)
- 3.1 SP4 Access Gateway Appliance cluster (LAG 1 and LAG 2).

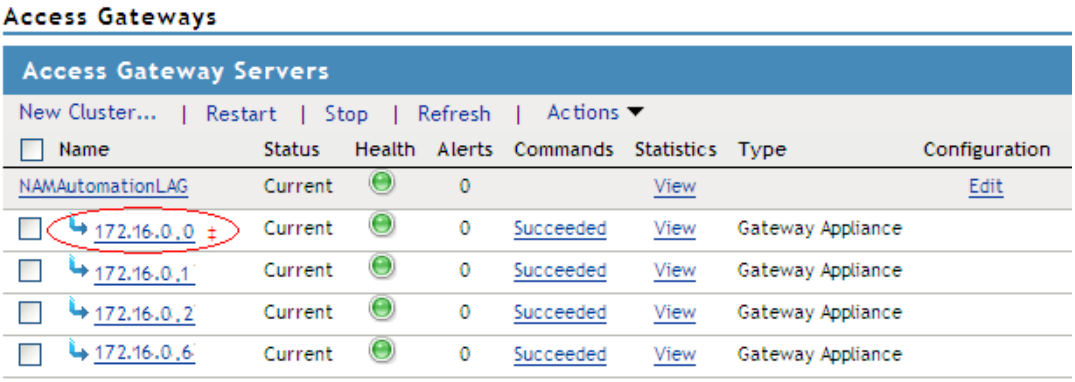
Migration Process

1 Determine which server in the 3.1 SP4 Access Gateway cluster is the primary server.

1a Login to Administration Console

1b Click *Devices* > *Access Gateways* > Select the device.

The list of servers are displayed. The primary server is indicated by a red mark beside the IP address.



2 Install the Access Gateway Appliance (AG 1). For more information, see "Installing the Access Gateway Appliance" in the *NetIQ Access Manager 3.2 SP1 Installation Guide*. While installing the Access Gateway Appliance, specify the Administration Console's (AC 1) IP address, user name and password in the Administration Console Configuration field on the Appliance Configuration page.

3 Add the newly installed Access Gateway Appliance to the 3.1 SP4 Access Gateway Appliance cluster. For more information, see "Managing Access Gateways".

4 By default, all proxy services of newly added devices to the cluster are listening on the same IP address and port. To configure each reverse proxy service to a specific IP address and port, follow the steps below.

4a Configure a primary IP Address in YaST for the remaining interfaces.

4a1 Go to `YaST > Network Devices > Network Settings > Overview`.

4a2 Select the network card and click *Edit*.

4a3 Specify the IP address.

Repeat the steps for all the interfaces.

4b Click *Devices* > *Access Gateways* > Select the device > *New IP* > click *OK*.

4c Add the secondary IP address if applicable to the interfaces from *Network Settings* > *Adapter List*.

4d Configure the DNS from *Network Settings* > *DNS*.

4e Add the Host entries (if any) from *Network Settings* > *Hosts*.

4f Set up the routing (if any) from *Network Settings* > *Gateways*.

4g Under Services, click on *Reverse Proxy/Authentication*. In the *Reverse Proxy List*, click the proxy service name. Select the newly added cluster member and select the *listening IP address* for that service.

(Optional) If you want to specify the outbound connection to the Web server, click *Web Servers*, then click *TCP Connect Options*. Select the *Cluster Member* and select the IP address from the drop down list against *Make Outbound Connection Using* if you want to select the outbound IP address to communicate with the Web server.

For more information about configuring the network settings, see "Configuring Network Settings" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

4h Restore any customized files backed up earlier as part of "Prerequisites for the Access Gateway Appliance Migration" on page 29.

Copy the content of the following files to the corresponding file in the new location.

Table 2-2 */Restoring Files during 3.2 Access Gateway Appliance Migration - Scenario 1*

Old File Location	New File Location
`/var/opt/novell/tomcat5/conf/web.xml`	`/opt/novell/nam/mag/tomcat7/conf/web.xml`
`/var/opt/novell/tomcat5/webapps/nesp/WEB-INF/web.xml`	`/opt/novell/nam/mag/tomcat7/webapps/nesp/WEB-INF/web.xml`
`/var/opt/novell/tomcat5/webapps/nesp/jsp`	`/opt/novell/nam/mag/tomcat7/webapps/nesp/jsp`
`/var/opt/novell/tomcat5/webapps/nesp/html`	`/opt/novell/nam/mag/tomcat7/webapps/nesp/html`
`/var/opt/novell/tomcat5/webapps/nesp/images`	`/opt/novell/nam/mag/tomcat7/webapps/nesp/images`
`/var/novell/errorpagesconfig/current/` (Contains error messages and error pages configuration)	`/opt/novell/nam/mag/webapps/agm/WEB-INF/config/current`
`/var/opt/novell/tomcat5/webapps/nesp/config`	`/opt/novell/nam/mag/tomcat7/webapps/nesp/config`
`/chroot/lag/opt/novell/bin/preapply.sh`	`/opt/novell/devman/jcc/scripts/presysconfig.sh`
`/chroot/lag/opt/novell/bin/postapply.sh`	`/opt/novell/devman/jcc/scripts/postsysconfig.sh`

NOTE: The names of `preapply.sh` and `postapply.sh` files are different in the 3.2 environment. To restore these files, open the file and copy paste the entire content to the files in the 3.2 environment. Refer Table 2-2 on page 34 for details of file locations.

server.xml: If you have modified any elements or attributes in the 3.1 SP4 environment the corresponding changes will need to be applied to the 3.2 `/opt/novell/nam/mag/conf/server.xml` file.

Typical changes done to the `server.xml` in 3.1 SP4 include modifying the 'Address=' attribute to restrict the IP address the application will listen on, or 'maxThreads=' attribute to modify the number of threads.

In the following example, 3.1 SP4 has customized `maxThreads` value.

```
<Connector port="9009" enableLookups="false" redirectPort="8443"
protocol="AJP/1.3" address="127.0.0.1" minSpareThreads="25"
maxThreads="300" backlog="0" connectionTimeout="20000", ...   ../>
```

Make a note of the customizations and copy paste the changed values in the 3.2 `server.xml` file.

4i If you have customized the error pages for branding purposes, you will need to redo the changes in the 3.2 setup. For details on modifying messages and customizing pages, see "Customizing the Error Pages ". The customized error messages can be restored by copying over the files as indicated in Table 2-2 on page 34.

4j In the Administration Console, copy and paste the content of the previously referenced `touchfile_list` output file, under the following:

- Global Option files to *Access Gateways* > *Edit* > *Advanced Options*.

  Example of Global Options in the `touchfile_list` file.

  ```
  # Global Option example
  NAGGlobalOptions InPlaceSilent=on
  ```

- Virtual Host/Server Option files to *Servers* > *Configuration* > *Reverse Proxy* > *Proxy Service* > *Advanced Options*.

  Example of Virtual Host/Server Options in the `touchfile_list` file.

  ```
  # Virtual Host/Server Option
  NAGGlobalOptions DebugHeaders=on
  ```

- Files under the Administration Console are already available in the Access Gateway Appliance.

  NOTE: Ensure that you do not have blank lines between each advanced option and also do not alter the content of `touchfile_list`.

  For information on the migration utility files, `lag2mag_touchfiles.csv` and `migrate_touchfiles.sh` see, "Utility Scripts" on page 67

  ---

5 Test the Access Gateway Appliance functionality by accessing Access Gateway protected resources and making sure that the pages are rendered successfully.

6 Specify AG 1 as the primary server and click *Update*. For more information, see "Changing the Primary Cluster Server".

7 Remove 3.1 SP4 Access Gateway Appliance (LAG 1) from the cluster. For more information, see "Viewing and Modifying Gateway Settings".

8 Install 3.2 Access Gateway Appliance (AG 2) as in Step 2 and add it to the 3.1 SP4 Access Gateway Appliance cluster as in Step 3.

9 After you confirm that all the services are up and running remove LAG2 from the cluster.

10 Remove 3.1 SP4 Access Gateway Appliance (LAG 2) from the cluster as in Step 7.

11 Click *OK* and *Update all*.

12 Repeat Step 2 to Step 8 (except step 4j) until you have completely migrated all the existing 3.1 SP4 Access Gateway Appliance to 3.2 Access Gateway Appliance.

After installing the Access Gateway Appliance, delete all the 3.1 SP4 Access Gateway Appliances from the Administration Console.

13 On the newly added Access Gateway server, restart Tomcat by using the `/etc/init.d/novell-mag restart` or `rcnovell-mag restart` command.

Use case scenario 2:

This scenario assumes that you have a new/existing 64-bit server to install the 3.2 Access Gateway Appliance and explains how to migrate from 3.1 SP4 using the existing IP address.

Consider that the setup includes the following components:

- Administration Console (AC 1)
- Identity Server cluster (IDP 1 and IDP 2)
- 3.1 SP4 Access Gateway Appliance cluster (LAG 1 and LAG 2)

Migration Process

1. If you have a new 64-bit server to install 3.2 Access Gateway Appliance, ensure you do the following:
   - **1a** Shut down LAG2 and
   - **1b** Have the same number of Network Interface Cards as on LAG 2 and then proceed to step 2.

     If you are reusing the existing LAG hardware, proceed to step 2.
2. Install the Access Gateway Appliance (AG 2) with the same IP address as of the 3.1 SP4 Access Gateway Appliance (LAG 2). After the installation is complete, it will take some time to sync up the configuration. Ensure that you do not modify any configuration during this time.

   When the configuration is synced up, the Access Gateway Appliance and the health of all the cluster members turns green.
3. Test the Access Gateway Appliance functionality by accessing Access Gateway protected resources and making sure pages are rendered successfully.
4. If you have customized the error pages for branding purposes, you will need to redo the changes in the 3.2 setup. For details on modifying messages and customizing pages, see "Customizing the Error Pages ". The customized error messages can be restored by copying over the files as indicated in Table 2-3 on page 37.
5. In the Administration Console, copy and paste the content of the previously referenced `touchfile_list` output file under the following:
   - Global Option files to *Access Gateways* > *Edit* > *Advanced Options*.

     Example of Global Options in the `touchfile_list` file.

     ```
     # Global Option example
     NAGGlobalOptions InPlaceSilent=on
     ```
   - Virtual Host/Server Option files to *Servers* > *Configuration* > *Reverse Proxy* > *Proxy Service* > *Advanced Options*.

     Example of Virtual Host/Server Options in the `touchfile_list` file.

     ```
     # Virtual Host/Server Option
     NAGGlobalOptions DebugHeaders=on
     ```
   - Files under the Administration Console are already available in the Access Gateway Appliance.

   NOTE: Ensure that you do not have blank lines between each advanced option and also do not alter the content of the `touchfile_list` file.

   For information on the migration utility files, `lag2mag_touchfiles.csv` and `migrate_touchfiles.sh` see, "Utility Scripts" on page 67

   ---
6. Click *OK* and *Update*.
7. Restore any customized files backed up earlier as part of "Prerequisites for the Access Gateway Appliance Migration" on page 29.

   Copy the content of the following files to the corresponding file in the new location.

Table 2-3 Restoring Files during 3.2 Access Gateway Appliance Migration -Scenario 2

Old File Location	New File Location
/var/opt/novell/tomcat5/conf/web.xml	/opt/novell/nam/mag/tomcat7/conf/web.xml
/var/opt/novell/tomcat5/webapps/nesp/WEB-INF/web.xml	/opt/novell/nam/mag/tomcat7/webapps/nesp/WEB-INF/web.xml
/var/opt/novell/tomcat5/webapps/nesp/jsp	/opt/novell/nam/mag/tomcat7/webapps/nesp/jsp
/var/opt/novell/tomcat5/webapps/nesp/html	/opt/novell/nam/mag/tomcat7/webapps/nesp/html
/var/opt/novell/tomcat5/webapps/nesp/images	/opt/novell/nam/mag/tomcat7/webapps/nesp/images
/var/novell/errorpagesconfig/current/ (Contains error messages and error pages configuration)	/opt/novell/nam/mag/webapps/agm/WEB-INF/config/current
/var/opt/novell/tomcat5/webapps/nesp/config	/opt/novell/nam/mag/tomcat7/webapps/nesp/config
/chroot/lag/opt/novell/bin/preapply.sh	/opt/novell/devman/jcc/scripts/presysconfig.sh
/chroot/lag/opt/novell/bin/postapply.sh	/opt/novell/devman/jcc/scripts/postsysconfig.sh

NOTE: The names of `preapply.sh` and `postapply.sh` files are different in the 3.2 environment. To restore these files, open the file and copy paste the entire content to the files in the 3.2 environment. Refer Table 2-2 on page 34 for details of file locations.

server.xml: If you have modified any elements or attributes in the 3.1 SP4 environment the corresponding changes will need to be applied to the 3.2 `/opt/novell/nam/mag/conf/server.xml` file.

Typical changes done to the `server.xml` in 3.1 SP4 include modifying the 'Address=' attribute to restrict the IP address the application will listen on, or 'maxThreads=' attribute to modify the number of threads.

In the following example, 3.1 SP4 has customized `maxThreads` value.

```
<Connector port="9029" enableLookups="false"  protocol="AJP/1.3"
address="127.0.0.1" minSpareThreads="25" maxThreads="300" backlog="0"
connectionTimeout="20000", ...   ../>
```

Make a note of the customizations and copy paste the changed values in the 3.2 `server.xml` file.

8 Repeat Step 1 through Step 6 except step 5 until you have completely migrated all the existing 3.1 SP4 Access Gateway Appliance to 3.2 Access Gateway Appliance.

9 On the newly added Access Gateway server, restart Tomcat by using the `/etc/init.d/novell-mag restart` or `rcnovell- mag restart` command.

NOTE: The Advanced options from the Administration Console are available only for the Access Gateway Appliance. For the 3.1 SP4 Access Gateway Appliance, you should have touch files configured.

2.2.4 Migrating SSL VPN

Prerequisites for the SSL VPN Migration

In addition to the following prerequisites, ensure that you also meet the hardware requirements for the Administration Console. For details, see "Administration Console Requirements" in the *NetIQ Access Manager 3.2 SP1 Installation Guide*.

- ❒ The high-bandwidth RPM is installed on the SSL VPN for clustering.

  For more information about how to install high bandwidth RPM, see "Installing the Key for the High-Bandwidth SSL VPN" in the *NetIQ Access Manager 3.2 SP1 Installation Guide*.

- ❒ If you are reusing the same server for migrating the SSL VPN cluster, manually uninstall the high bandwidth RPM before migration. You must then reinstall it after migration.

  For more information about how to uninstall high-band-width RPM, see "Uninstalling the RPM Key for High Bandwidth SSL VPN" in the *NetIQ Access Manager 3.2 SP1 Installation Guide*.

- ❒ If the services are managed by an L4 switch, remove the device that you are migrating, from the L4 switch. Add the device back to the L4 switch once the migration is done successfully. This is required so that no user requests are sent by the L4 switch to the device during migration.

- ❒ You have physical access to the server or server console (in case of VMWare setups) as a root user and are familiar with firewall configurations. The required ports also must be opened in the firewall. For more information on the ports, see Section 2.1, "Port Details," on page 13.

- ❒ Determine if you want to reuse an existing IP address or use a new IP address for the migration process.

- ❒ If you have customized any files back it up using the `migrate_backup.sh` script. This script is located in the `novell-access-manager` folder in the `AM_AccessManagerService_Linux64.tar.gz` file. Copy this script to the 3.1 SP4 machine and run the script to do the backup. It is important to take the backup regardless of whether you are reusing the same server or a new server.

  This script backs up the following files:

  - `/var/opt/novell/tomcat5/conf/server.xml`
  - `/var/opt/novell/tomcat5/conf/tomcat5.conf`
  - `/var/opt/novell/tomcat5/webapps/sslvpn/WEB-INF/web.xml`
  - `/var/opt/novell/tomcat5/webapps/sslvpn/WEB-INF/conf`
  - `/var/opt/novell/tomcat5/webapps/sslvpn/*.jsp`
  - `/var/opt/novell/tomcat5/webapps/sslvpn/pages*`
  - `/var/opt/novell/tomcat5/webapps/sslvpn/jsp`
  - `/var/opt/novell/tomcat5/webapps/sslvpn/html`
  - `/var/opt/novell/tomcat5/webapps/sslvpn/images`

- `/var/opt/novell/tomcat5/webapps/sslvpn/common`
- `/var/opt/novell/tomcat5/webapps/sslvpn/SSLVPNClientHelp`

NOTE: This step is required in all the SSL VPN migration scenarios even if you reuse the existing 64-bit compatible server.

Reusing an Existing IP Address

- "The SSL VPN and 3.1 SP4 Access Gateway Appliance Are on the Same Server" on page 31
- "The SSL VPN Is the Only Component on the Server" on page 39

The SSL VPN and 3.1 SP4 Access Gateway Appliance Are on the Same Server

Workflow:

1. Back up any files that you have customized.
2. Mount the Access Gateway Appliance ISO. Start the installation.
3. Provide a host name same as the one on 3.1 SP4 Access Gateway Appliance.
4. Select install. Enable SSL VPN service checkbox in the Appliance configuration page.
5. Restore the backed up files.

The SSL VPN Is the Only Component on the Server

Workflow:

1. Back up any customized files.
2. Run the `uninstall.sh` script from the existing 3.1 SP4 Access Manager installation folder.
3. Install SSL VPN.
4. Restore the backed up files.

Using a New IP Address

- "The SSL VPN and 3.1 SP4 Access Gateway Appliance Are on the Same Server" on page 39
- "The SSL VPN Is the Only Component on the Server" on page 40

The SSL VPN and 3.1 SP4 Access Gateway Appliance Are on the Same Server

Workflow:

1. Back up any customized files.
2. Mount the Access Gateway Appliance ISO and install the Access Gateway Appliance.
3. Click *Access Gateway* > *Edit* > *Service*.
4. From the administration console, click the SSL VPN Web server address and change the connection ports to 3080 and 3443 for http and https respectively.
5. Restore the customized files.
6. Add the SSL VPN server to the existing SSL VPN cluster.

The SSL VPN Is the Only Component on the Server

Workflow:

1. Back up the customized files.
2. Install SSL VPN.
3. Add the 3.2 SSL VPN to the existing SSL VPN cluster in the Administration Console.
4. Restore the backed up files.

The SSL VPN and Administration Console Are on the Same Server

Workflow:

1. Back up the customized files.
2. Migrate the Administration Console from 3.1 SP4 to 3.2
3. Migrate the Identity Server.
4. Migrate SSL VPN.
5. Restore backed up files.

The SSL VPN and Identity Server Are on the Same Server

Workflow:

1. Back up the customized files.
2. Stop the 3.1 SP4 Identity Server.
3. Remove the 3.1 SP4 Identity server from the cluster.
4. Delete the 3.1 SP4 Identity Server from the Identity Servers cluster.
5. Uninstall the 3.1 SP4 Identity Server if you are going to use the current machine to install 3.2 Identity Server.
6. Uninstall the 3.1 SP4 SSL VPN Server if you are going to use the current machine to install 3.2 SSL VPN Server.

   WARNING: Ensure that you uninstall the SSL VPN server and not delete the SSL VPN server object. Deleting the SSL VPN server instead of uninstalling the server will result in loss of settings.

   ---

7. Use the NetIQ Access Manager 3.2 installer to install the 3.2 Identity Server on a 64-bit SLES 11 SP1 or higher operating system.
8. Add the 3.2 Identity Server to the existing Identity Servers cluster in the Administration Console.
9. Update the Identity Server and apply changes.
10. Restore the backed up files.
11. Install the SSL VPN by running the NetIQ Access Manager 3.2 installer on the same server.
12. **(Optional) For the ESP-enabled SSL VPN:** When the Identity Server and ESP-enabled SSL VPN are migrated to the same server:

    12a Click *Device* > *SSL VPN* > *Edit* > *Authentication Configuration*.

    12b In the *Embedded Service Provider Base URL* field, change the ports to 3080 and 3443 for http and https respectively.

13 **(Optional) For the traditional SSL VPN:** When the Identity Server and traditional SSL VPN are migrated to the same server:

13a Click *Access Gateway > Edit > Service.*

13b Click the SSL VPN Web server address and change the connection ports to 3080 and 3443 for http and https respectively.

NOTE: For NetIQ Access Manager 3.2 and later, release onwards, SSL VPN will be accessible on ports 3080 (http) and 3443 (https) when installed on the same server as the Identity Server.

Migration Process

- "Reusing an Existing Server" on page 41
- "Migrating ESP-enabled SSL VPN or Traditional SSL VPN Server" on page 42
- "Traditional SSL VPN server installed with 3.1 SP4 Access Gateway Appliance" on page 45

IMPORTANT: Before you proceed with the steps for migration, ensure that you have followed the instructions in the "Prerequisites for the SSL VPN Migration" on page 38

Reusing an Existing Server

If the existing server supports the 64-bit installer, you can reuse the server to install the Access Manager SSL VPN 3.2.

1 Continue with the steps for the related SSL VPN migration scenarios. For more information, see "Reusing an Existing IP Address" on page 39 and "Using a New IP Address" on page 39.

2 Restore any customized files from the backup taken earlier as part of steps in "Prerequisites for the SSL VPN Migration" on page 38.

To restore the files, copy the content of the following files to the corresponding file in the new location.

Old Location	New Location
`/var/opt/novell/tomcat5/webapps/sslvpn/WEB-INF/web.xml`	`/opt/novell/nam/sslvpn/webapps/sslvpn/WEB-INF/web.xml`
`/var/opt/novell/tomcat5/webapps/sslvpn/WEB-INF/conf`	`/opt/novell/nam/sslvpn/webapps/sslvpn/WEB-INF/conf`
`/var/opt/novell/tomcat5/webapps/sslvpn/*.jsp`	`/opt/novell/nam/sslvpn/webapps/sslvpn/*.jsp`
`/var/opt/novell/tomcat5/webapps/sslvpn/pages*`	`/opt/novell/nam/sslvpn/webapps/sslvpn/pages*`
`/var/opt/novell/tomcat5/webapps/sslvpn/html`	`/opt/novell/nam/sslvpn/webapps/sslvpn/html`
`/var/opt/novell/tomcat5/webapps/sslvpn/images`	`/opt/novell/nam/sslvpn/webapps/sslvpn/images`
`/var/opt/novell/tomcat5/webapps/sslvpn/common`	`/opt/novell/nam/sslvpn/webapps/sslvpn/common`

Old Location	New Location
/var/opt/novell/tomcat5/webapps/sslvpn/SSLVPNClientHelp	/opt/novell/nam/sslvpn/webapps/sslvpn/SSLVPNClientHelp

server.xml: If you have modified any elements or attributes in the 3.1 SP4 environment the corresponding changes will need to be applied to the 3.2 `/opt/novell/nam/sslvpn/conf/server.xml` file.

Typical changes done to the `server.xml` in 3.1 SP4 include modifying the 'Address=' attribute to restrict the IP address the application will listen on, or 'maxThreads=' attribute to modify the number of threads.

In the following example, 3.1 SP4 has customized `maxThreads` value.

```
<Connector port="9029" enableLookups="false"  protocol="AJP/1.3"
address="127.0.0.1" minSpareThreads="25" maxThreads="300" backlog="0"
connectionTimeout="20000", ...   ../>
```

Make a note of the customizations and copy paste the changed values in the 3.2 server.xml file.

tomcat5.conf: Copy any elements or attributes that you have customized in the 3.1 SP4 `tomcat5.conf` file to the 3.2 `tomcat7.conf` file

For example, if you have included the environment variable in the 3.1 SP4 `tomcat5.conf file` to increase the heap size by using `-Xmx/Xms/Xss` settings, the variables should be copied to the 3.2 `/opt/novell/nam/idp/conf/tomcat7.conf` file.

3. Add the newly installed SSL VPN device to the existing SSL VPN cluster if you are not reusing the existing IP address.

   For more information, see "Clustering SSL VPN Servers"in the *NetIQ Access Manager 3.2 Setup Guide.*

   The cluster object stores all the existing SSL VPN configurations. The newly added SSL VPN servers inherit these configurations.

4. Repeat Step 2 until all the 3.1 SP4 SSL VPN Servers are replaced with 3.2 SSL VPN Servers.

5. On the newly added SSL VPN servers, restart Tomcat by using the `/etc/init.d/novell-sslvpn restart` or `rcnovell-sslvpn restart` command.

Migrating ESP-enabled SSL VPN or Traditional SSL VPN Server

You can migrate the ESP-enabled SSL VPN or traditional SSL VPN server in the following cases:

- SSL VPN server is installed independently.
- SSL VPN server is installed with the Administration Console.
- SSL VPN is installed with the Identity Server.

Migrating ESP-enabled SSL VPN or traditional SSL VPN when SSL VPN is installed independently:

IMPORTANT: Before you proceed with the steps for migration, ensure that you have followed the instructions in the "Prerequisites for the SSL VPN Migration" on page 38

1. If the operating system is 64-bit SLES 11 SP1 or higher, uninstall version 3.1 SP4 and install version 3.2 SSL VPN Server. Continue with Step 8

2. Perform a new installation of 64-bit SLES 11 SP1 or higher operating system. For more information, see SLES 11 Installation Quick Start.

3 Ensure the following packages are installed:

- **perl-gettext, gettext-runtime** The required library and tools to create and maintain message catalogs.
- **python:** The Python library.
- **compat:** Libraries to address compatibility issues. On SLES 11 SP1 platform, the `compat-32bit` package is available in the SLES11-Extras repository. For information on enabling this repository, see TID 7004701.

3a Use YaST to install the packages that have not yet been installed.

3b Use the `rpm -qa | grep` *<package name>* command to verify the installation.

Replace *<package name>* with the name of the package you want to verify. For example:

```
rpm -qa | grep compat
```

4 Ensure you have downloaded the software or you have the CD available.

5 Do one of the following:

- Insert the CD into the drive and navigate to the device. Enter the following:

  ```
  cd /media
  ```

  Browse to your CD-ROM drive.
- If you have downloaded the `AM_32_AccessManagerService_Linux.tar.gz` file, unpack the file using the `tar -xzvf AM_32_AccessManagerService_Linux.tar.gz` command.

6 Browse to the `novell-access-manager` directory. All the files are extracted to the `novell-access-manager` folder.

7 Run the `install.sh` script from the `novell-access-manager` folder on a 64-bit SLES 11 SP1 or higher server and choose the option to install the ESP-enabled SSL VPN or Traditional SSL VPN.

8 Review and accept the License Agreement.

9 If the SSL VPN machine has been configured with multiple IP addresses, select an IP address for the SSL VPN server at the prompt.

10 Specify the name of the administrator for the Administration Console.

11 Specify and confirm the administration password.

Wait while the SSL VPN server is installed on your system and imported into the Administration Console.

12 The installation ends with the following message: `Installation complete`.

13 If you are using an existing IP address, the device will be available in existing cluster. If it is installed with a new IP address, a new device will be found in the SSL VPN of the Administration Console.

14 If the existing IP address is used then wait until the health status of the device status turns green. If it is installed with a new IP address and is ESP-enabled, the health status will be in Yellow state.

15 If you are installing with a new IP address, add the device to the existing cluster and update the cluster.

16 If the export law permits and you want to install the high bandwidth version of SSL VPN, see "Traditional SSL VPN server installed with 3.1 SP4 Access Gateway Appliance" on page 45.

17 Check the SSL VPN functionality. Repeat Step 1 to Step 17 (except step 16) for the other devices in the cluster.

18 Restore any customized files from the backup taken earlier as part of steps in "Prerequisites for the SSL VPN Migration" on page 38.

To restore the files, copy the content of the following files to the corresponding file in the new location.

Old Location	New Location
/var/opt/novell/tomcat5/webapps/sslvpn/WEB-INF/web.xml	/opt/novell/nam/sslvpn/webapps/sslvpn/WEB-INF/web.xml
/var/opt/novell/tomcat5/webapps/sslvpn/WEB-INF/conf	/opt/novell/nam/sslvpn/webapps/sslvpn/WEB-INF/conf
/var/opt/novell/tomcat5/webapps/sslvpn/*.jsp	/opt/novell/nam/sslvpn/webapps/sslvpn/*.jsp
/var/opt/novell/tomcat5/webapps/sslvpn/pages*	/opt/novell/nam/sslvpn/webapps/sslvpn/pages*
/var/opt/novell/tomcat5/webapps/sslvpn/html	/opt/novell/nam/sslvpn/webapps/sslvpn/html
/var/opt/novell/tomcat5/webapps/sslvpn/images	/opt/novell/nam/sslvpn/webapps/sslvpn/images
/var/opt/novell/tomcat5/webapps/sslvpn/common	/opt/novell/nam/sslvpn/webapps/sslvpn/common
/var/opt/novell/tomcat5/webapps/sslvpn/SSLVPNClientHelp	/opt/novell/nam/sslvpn/webapps/sslvpn/SSLVPNClientHelp

server.xml: If you have modified any elements or attributes in the 3.1 SP4 environment the corresponding changes will need to be applied to the 3.2 `/opt/novell/nam/sslvpn/conf/server.xml` file.

Typical changes done to the `server.xml` in 3.1 SP4 include modifying the '`Address=`' to restrict the IP address the application will listen on, or '`maxThreads=`' attributes to modify the number of threads.

In the following example, 3.1 SP4 has customized `maxThreads` value.

```
<Connector port="9029" enableLookups="false"  protocol="AJP/1.3"
address="127.0.0.1" minSpareThreads="25" maxThreads="300" backlog="0"
connectionTimeout="20000", ...   ../>
```

Make a note of the customizations and copy paste the changed values in the 3.2 `server.xml` file.

tomcat5.conf: Copy any elements or attributes that you have customized in the 3.1 SP4 `tomcat5.conf` file to the 3.2 `tomcat7.conf` file.

For example, if you have included the environment variable in the 3.1 SP4 `tomcat5.conf file` to increase the heap size by using `-Xmx/Xms/Xss` settings, the variables should be copied to the 3.2 `/opt/novell/nam/idp/conf/tomcat7.conf` file.

Traditional SSL VPN server installed with 3.1 SP4 Access Gateway Appliance

IMPORTANT: Before you proceed with the steps for migration, ensure that you have followed the instructions in the "Prerequisites for the SSL VPN Migration" on page 38

1. Follow the steps to migrate from 3.1 SP4 Access Gateway Appliance to Access Gateway Appliance. For more information, see Section 2.2.3, "Migrating 3.1 SP4 Access Gateway Appliance to 3.2 Access Gateway Appliance," on page 29.
2. Start the installation and in the Appliance configuration screen, select the *Install and enable SSL VPN Service* check box.
3. If you have used an existing IP address, the existing SSL VPN within the cluster will be migrated to Access Manager 3.2. If it is installed with a new IP address, a new SSL VPN server will be displayed in the Administration Console.
4. The import/re-import process will take some time. Wait until the Access Gateway Appliance and the SSL VPN health status becomes green.
5. If it is not part of the SSL VPN cluster, add it to the existing cluster and update.
6. Repeat the steps for other devices in the cluster.
7. If the export law permits and you want to install the high bandwidth version of SSL VPN, see, "Traditional SSL VPN server installed with 3.1 SP4 Access Gateway Appliance" on page 45.
8. Restore any customized files from the backup taken earlier as part of steps in "Prerequisites for the SSL VPN Migration" on page 38.

   To restore the files, copy the content of the following files to the corresponding file in the new location.

Old Location	New Location
`/var/opt/novell/tomcat5/webapps/sslvpn/WEB-INF/web.xml`	`/opt/novell/nam/sslvpn/webapps/sslvpn/WEB-INF/web.xml`
`/var/opt/novell/tomcat5/webapps/sslvpn/WEB-INF/conf`	`/opt/novell/nam/sslvpn/webapps/sslvpn/WEB-INF/conf`
`/var/opt/novell/tomcat5/webapps/sslvpn/*.jsp`	`/opt/novell/nam/sslvpn/webapps/sslvpn/*.jsp`
`/var/opt/novell/tomcat5/webapps/sslvpn/pages*`	`/opt/novell/nam/sslvpn/webapps/sslvpn/pages*`
`/var/opt/novell/tomcat5/webapps/sslvpn/html`	`/opt/novell/nam/sslvpn/webapps/sslvpn/html`
`/var/opt/novell/tomcat5/webapps/sslvpn/images`	`/opt/novell/nam/sslvpn/webapps/sslvpn/images`
`/var/opt/novell/tomcat5/webapps/sslvpn/common`	`/opt/novell/nam/sslvpn/webapps/sslvpn/common`
`/var/opt/novell/tomcat5/webapps/sslvpn/SSLVPNClientHelp`	`/opt/novell/nam/sslvpn/webapps/sslvpn/SSLVPNClientHelp`
`/chroot/lag/opt/novell/bin/preapply.sh`	`/opt/novell/devman/jcc/scripts/presysconfig.sh`
`/chroot/lag/opt/novell/bin/postapply.sh`	`/chroot/lag/opt/novell/bin/postapply.sh`

server.xml: If you have modified any elements or attributes in the 3.1 SP4 environment the corresponding changes will need to be applied to the 3.2 `/opt/novell/nam/sslvpn/conf/server.xml` file.

Typical changes done to the `server.xml` in 3.1 SP4 include modifying the 'Address=' to restrict the IP address the application will listen on, or 'maxThreads=' attributes to modify the number of threads.

In the following example, 3.1 SP4 has customized `maxThreads` value.

```
<Connector port="9029" enableLookups="false"  protocol="AJP/1.3"
address="127.0.0.1" minSpareThreads="25" maxThreads="300" backlog="0"
connectionTimeout="20000", ...   ../>
```

Make a note of the customizations and copy paste the changed values in the 3.2 `server.xml` file.

tomcat5.conf: Copy any elements or attributes that you have customized in the 3.1 SP4 `tomcat5.conf` file to the 3.2 `tomcat7.conf` file

For example, if you have included the environment variable in the 3.1 SP4 `tomcat5.conf file` to increase the heap size by using `-Xmx/Xms/Xss` settings, the variables should be copied to the 3.2 `/opt/novell/nam/idp/conf/tomcat7.conf` file.

Installing the Key for the High-Bandwidth SSL VPN

You must install the high bandwidth SSL VPN if you want to add the SSL VPN servers to the cluster. Customers who are eligible to install the high bandwidth SSL VPN can install the key for the high bandwidth SSL VPN after they get the clearance to export. This key is installed only once.

In this release you do not have to upgrade the RPM every time the servlet and the server RPMs for SSL VPN are upgraded.

With Access Manager 3.1 or later, you can install the key once and upgrade it to new versions without installing the key again.

1. After you have ordered the high bandwidth version, log in to the NetIQ Customer Center and click on the link that allows you to download the RPM containing key for the high bandwidth version.
2. Download the `novl-sslvpn-hb-key-3.1.0-0.noarch.rpm` high bandwidth RPM.
3. Log in as root.
4. Enter the `/etc/init.d/novell-sslvpn stop` or `rcnovell-sslvpn stop` command to stop all services.
5. Enter the `rpm -ivh novl-sslvpn-hb-key-3.1.0-0.noarch.rpm` command to install the RPM for the high bandwidth version of SSL VPN.
6. Enter the `/etc/init.d/novell-sslvpn start` or `rcnovell-sslvpn start` command to restart all SSL VPN services.
7. Enter the `/etc/init.d/novell-sslvpn status` or `rcnovell-sslvpn status` command to check the status.

2.3 Migrating Access Manager on Windows

2.3.1 Prerequisites

- The 3.1 SP4 setup should be on Windows 2003.
- Back up your configuration. For instructions, see "Backing Up the Access Manager Configuration" in the *NetIQ Access Manager 3.2 SP1 Administration Console Guide*.

  If the upgrade fails, you need a way to recover your configuration. Because a backup can only be restored to the version on which it was created, you must restore your Access Manager components to that version. You can then restore the configuration with the backup file and work with NetIQ Technical Support to solve the upgrade problem before attempting to upgrade again.
- Back up the following files manually:
  - `C:\Program Files\Novell\Tomcat\conf\server.xml`
  - `C:\Program Files\Novell\Tomcat\conf\web.xml`
  - `C:\Program Files\Novell\Tomcat\webapps\nidp\jsp`
  - `C:\Program Files\Novell\Tomcat\webapps\nidp\WEB-INF\lib\`
  - `C:\Program Files\Novell\jre\lib\security\bcslogin.conf`
  - `C:\Program Files\Novell\Tomcat\webapps\nidp\WEB-INF\classes`
- For the Windows components (Identity Server, Administration Console, Access Gateway Appliance and Service), you should select a platform supported by Windows 2008 Server R2 Standard or Enterprise Edition.

2.3.2 Port Details

In version 3.2, the Administration Console and Identity Server run in separate instances of tomcat. By default, each component's tomcat uses ports 8080 (http) and 8443 (https). Installing multiple components on the same server can cause a port conflict. To avoid this conflict, each component is assigned a unique port number on which the device can listen.

If a component is installed on a dedicated server no port changes are required. By default, the http port is 8080 and the https port is 8443.

The following table describes the ports for the Administration Console and Identity Server:

Configuration	Identity Server	Administration Console
Administration Console only	NA	8080/8443
Identity Server + Administration Console	8080/8443	2080/2443
Identity Server only	8080/8443	NA

2.3.3 Process

- "Migrating Administration Consoles From Windows 2003 to Windows 2008" on page 48
- "Migrating the Standalone Identity Servers from Windows 2003 to Windows 2008" on page 50

Migrating Administration Consoles From Windows 2003 to Windows 2008

1. Before you proceed with the steps for migrating ensure you have followed the instructions in Section 2.3.1, "Prerequisites," on page 47.
2. Remove the Identity Server from the cluster configuration if the Identity Server is installed on the same machine as the Administration Console.
   - **2a** In the Administration Console, click *Devices* > *Identity Servers*.
   - **2b** Select the server, then click *Stop*. Wait for the Health indicator to turn red.
   - **2c** Select the server, then choose *Actions* > *Remove from Cluster*.

   NOTE: Shut down the old server to prevent duplicate IP address conflict. These IP addresses will be re-used in Step 6.
3. Copy the files that are backed up to the new 64-bit server and shut down Windows 2003. The IP address and host name will be reused in Step 6.
4. Perform a fresh installation of Windows 2008 R2 Server, 64-bit operating system on 64-bit hardware, in either Standard or Enterprise Edition with the latest patches applied.
5. If you have any secondary administration consoles, bring them down.
6. Install the 3.1 SP4 version of the Administration Console.

   Use the same IP address and DNS name as that of Windows 2003.

   For more information, see "Installing on Windows" in the *NetIQ Access Manager 3.2 SP1 Installation Guide*.
7. Restore any customized files from the backup taken earlier in "Prerequisites" on page 47.

   To restore the files, copy the content of the following files to the corresponding file in the new location.

Old File Location	New File Location
C:\Program Files\Novell\Tomcat\conf\server.xml	C:\Program Files (x86)\Novell\Tomcat\conf\server.xml
C:\Program Files\Novell\Tomcat\conf\web.xml	C:\Program Files (x86)\Novell\Tomcat\conf\web.xml
C:\Program Files\Novell\Tomcat\webapps\nidp\jsp	C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp
C:\Program Files\Novell\Tomcat\webapps\nidp\WEB-INF\lib\	C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEB-INF\lib\
C:\Program Files\Novell\jre\lib\security\bcslogin.conf	C:\Program Files (x86)\Novell\jre\lib\security\bcslogin.conf
C:\Program Files\Novell\Tomcat\webapps\nidp\WEB-INF\classes	C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEB-INF\classes

server.xml: If you have modified any elements or attributes in the 3.1 SP4 environment the corresponding changes will need to be applied to the 3.2 `C:\Program Files (x86)\Novell\Tomcat\conf\server.xml` file.

Typical changes done to the `C:\Program Files\Novell\Tomcat\conf\server.xml` in 3.1 SP4 include modifying the '`Address=`' attribute to restrict the IP address the application will listen on, or '`Ciphers=`' attribute to restrict ciphers used when communicating with application over SSL.

In the following example, 3.1 SP4 is customized to use the following ciphers.

```
<Connector NIDP_Name="connector" port="8443" address=""
ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, ...   ../>
```

When migrating to 3.2, cut and paste this cipher list from your 3.1 SP4 `server.xml` and replace it in the SSL connector section of the 3.2 `C:\Program Files (x86)\Novell\Tomcat\conf\server.xml`.

tomcat5.conf: Copy any elements or attributes that you have customized in the 3.1 SP4 `C:\Program Files\Novell\Tomcat\conf\tomcat5.conf` file to the 3.2 `C:\Program Files\Novell\Tomcat\conf\tomcat7.conf` file

For example, if you have included the environment variable in the 3.1 SP4 `tomcat5.conf file` to increase the heap size by using `-Xmx/Xms/Xss` settings, the variables should be copied to the 3.2 `tomcat7.conf` file.

8 Modify the keystore locations in the `server.xml` file:

8a Log in to the Administration Console machine as the administrator.

8b Open the `server.xml` file.

```
C:\Program Files (x86)\Novell\Tomcat\conf\server.xml
```

8c Search for the `devman.keystore` entry in the `server.xml` file

8d Change the path from

```
C:\Program Files\Novell\Tomcat\webapps\roma\WEB-INF\conf\devman.keystore
```

to

```
C:\Program Files (x86)\Novell\Tomcat\webapps\roma\WEB-INF\conf\
devman.keystore
```

8e Search for the `tomcat.keystore` entry in the `server.xml` file.

8f Change the path from

```
C:\Program Files\Novell\Tomcat\webapps\roma\WEB-INF\conf\tomcat.keystore
```

to

```
C:\Program Files (x86)\Novell\Tomcat\webapps\roma\WEB-
INF\conf\tomcat.keystore
```

8g Save the file.

8h Restart Tomcat.

```
net stop Tomcat5
net start Tomcat5
```

9 Install the 3.1 SP4 version of the Identity Server.

For more information, see "Installing on Windows" in the *NetIQ Access Manager 3.2 SP1 Installation Guide*.

10 Restore any customized files from the backup taken earlier in "Prerequisites" on page 47 as in Step 7.

11 Add the Identity Server to the cluster configuration.

For more information, see "Assigning an Identity Server to a Cluster Configuration" in the *NetIQ Access Manager 3.2 SP1 Identity Server Guide*.

12 Remove any secondary consoles from the configuration:

12a In the Administration Console, click *Auditing* > *Troubleshooting*.

12b In the *Other Known Device Manager Servers* section, click *Remove* to remove any secondary consoles.

13 Uninstall the secondary consoles. For instructions, see"Uninstalling the Windows Administration Console" in the *NetIQ Access Manager 3.2 SP1 Installation Guide*.

14 Reinstall the secondary consoles as secondary consoles to the new primary console.

For more information, see "Installing on Windows" in the *NetIQ Access Manager 3.2 SP1 Installation Guide*.

Migrating the Standalone Identity Servers from Windows 2003 to Windows 2008

1 Before you proceed with the steps for migrating ensure you have followed the instructions in Section 2.3.1, "Prerequisites," on page 47.

2 Remove the Identity Server from the cluster configuration.

2a In the Administration Console, click *Devices* > *Identity Servers*.

2b Select the server, then click *Stop*. Wait for the Health indicator to turn red.

2c Select the server, then choose *Actions* > *Remove from Cluster*.

NOTE: Shut down the old server to prevent duplicate IP address conflict. These IP addresses will be re-used in Step 6.

---

3 Perform a fresh installation of Windows 2008 R2 Server, 64-bit operating system on 64-bit hardware, in either Standard or Enterprise Edition with the latest patches applied.

4 Install the 3.1 SP4 version of the Identity Server.

Use the same IP address and DNS name for the Identity Server.

5 Restore any customized files from the backup taken earlier in "Prerequisites" on page 47.

To restore the files, copy the content of the following files to the corresponding file in the new location.

Old File Location	New File Location
C:\Program Files\Novell\Tomcat\conf\web.xml	C:\Program Files (x86)\Novell\Tomcat\conf\web.xml
C:\Program Files\Novell\Tomcat\webapps\nidp\jsp	C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp
C:\Program Files\Novell\Tomcat\webapps\nidp\WEB-INF\lib\	C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEB-INF\lib\
C:\Program Files\Novell\jre\lib\security\bcslogin.conf	C:\Program Files (x86)\Novell\jre\lib\security\bcslogin.conf
C:\Program Files\Novell\Tomcat\webapps\nidp\WEB-INF\classes	C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEB-INF\classes

6 Add the Identity Server to the cluster configuration.

For more information, see "Assigning an Identity Server to a Cluster Configuration" in the *NetIQ Access Manager 3.2 SP1 Identity Server Guide*.

3 Upgrading Access Manager

When you upgrade the Access Manager components, start the process by first backing up your configuration and then moving the Administration Console. You can then upgrade the various devices that you have imported into the Administration Console.

For instructions, see "Backing Up the Access Manager Configuration" in the *NetIQ Access Manager 3.2 SP1 Administration Console Guide*. This is useful in case upgrade fails and you need to recover your 3.1 SP4 configuration. For more information, see "Restoring the Administration Console Configuration".

We recommend that you upgrade all members of a cluster before moving to another type of device. You must upgrade the Access Manager components in the order of Administration Console, Identity Server, Access Gateway, and then SSL VPN.

3.1 Upgrading on Linux

The 3.1 SP4 Access Gateway Appliance can be upgraded to 3.2. Upgrade is not supported for other components such as the Administration Console, Identity Server, and SSL VPN. For more information on migrating those components, see Section 2.2, "Migrating Access Manager on SLES," on page 14.

3.1.1 Upgrading the 3.1 SP4 Access Gateway Service

Prerequisites for Access Gateway Service

- Manually back up the `/var/opt/novell/tomcat5/conf/tomcat5.conf` and `/var/opt/novell/tomcat5/conf/server.xml` files.

  The `ag_upgrade.sh` script takes care of backing up the remaining customized files automatically. These files get automatically backed up at the `/root/novell_access_manager.tar.gz` folder and includes apache configuration and error pages.

Process of Upgrading the 3.1 SP4 Access Gateway Service

Before you proceed with the steps for upgrading ensure you have followed the instructions in the "Prerequisites for Access Gateway Service" on page 53 section.

1. Download the `AM_32_AccessGatewayService_Linux_64.tar.gz` file from the NetIQ download site and extract it using the following command:

   ```
   tar -xzvf <AM_32_AccessGatewayService_Linux_64.tar.gz>
   ```

2. Run the `ag_upgrade.sh` script from the folder to start the upgrade.

   The `ag_upgrade.sh` script upgrades the 3.1 SP4 Access Gateway Service to version 3.2.

3. Specify the following information:

   User ID: Specify the name of the administration user for the Administration Console.

   Password and Re-enter Password: Specify and re-enter the password for the administration user account.

   The Access Gateway Service is upgraded. The following message is displayed when upgrade is complete:

   ```
   Starting Access Manager services...
   Backup of customized files are available at /root/novell_access_manager.tar.gz.
   Restore them if required.
   ```

4. View the log files. The install logs are located in the `/tmp/novell_access_manager/` directory.

5. Restore any customized files from the backup taken earlier as part of steps in "Prerequisites for Access Gateway Service" on page 53.

   To restore the files, copy the content of the following files to the corresponding file in the new location.

Old File Locations	New File Location
`/root/novell_access_manager/apache2/` (contains apache var files)	`/opt/novell/apache2/share/apache2/error`
`/root/novell_access_manager/nesp/` (contains modified error pages)	`/var/opt/novell/tomcat7/webapps/nesp/jsp/`

server.xml:

If you have modified any elements or attributes in the 3.1 SP4 environment the corresponding changes will need to be applied to the 3.2 `server.xml` file.

Typical changes done to the `server.xml` in 3.1 SP4 include modifying the '`Address=`' to restrict the IP address the application will listen on, or '`maxThreads=`' attributes to modify the number of threads.

In the following example, 3.1 SP4 has customized `maxThreads` value.

```
<<Connector port="9009" enableLookups="false" redirectPort="8443"
protocol="AJP/1.3" address="127.0.0.1" minSpareThreads="25" maxThreads="700"
backlog="0" connectionTimeout="20000, ...   ../>
```

Make a note of the customizations and copy paste the changed values in the 3.2 `server.xml` file

tomcat5.conf:

Copy any elements or attributes that you have customized in the `tomcat5.conf` file to the `tomcat7.conf` file.

For example, if you have included the environment variable to increase the heap size by using `-Xmx/Xms/Xss` attributes in the `tomcat5.conf` file, copy this variable to the 3.2 `/opt/novell/nam/idp/conf/tomcat7.conf` file.

6 Modify the required properties in `/opt/novell/nam/mag/webapps/agm/WEB-INF/agm.properties` using back up file `/root/novell_access_manager/agm/agm.properties`. If you have customized the `agm.properties` file from the backup taken in 3.1 SP4, ensure that you apply the same to the new 3.2 `/opt/novell/nam/mag/webapps/agm/WEB-INF/agm.properties` file. An example below shows the how to enable the backend webserver's webpage caching and the cache location.

```
apache.disk.cache.enabled=yes
```

```
apache.disk.cache.root=/var/cache/novell-apache2
```

7 Change the ownerships of the following files (with read access to tomcat user) using the following commands:

```
chown -R novlwww:novlwww /var/opt/novell/tomcat7/webapps/nesp/jsp/
```

```
chown -R novlwww:novlwww /opt/novell/nam/mag/webapps/agm/WEB-INF/agm.properties
```

8 On the newly added Access Gateway Service, restart Tomcat using the `/etc/init.d/novell-mag restart` or `rcnovell-mag restart` command.

3.2 Upgrading on Windows

3.2.1 Prerequisites

In addition to the following prerequisites, ensure that you also meet the hardware requirements. For more information about hardware requirements, see "Hardware Platform Requirements" in the *NetIQ Access Manager 3.2 SP1 Installation Guide*.

- ❒ The 3.1 SP4 setup should be on Windows 2008 before upgrading to version 3.2. For more information, see the *Access Manager 3.1 SP4 Installation Guide* available in the Novell Access Manager Documentation website (http://www.novell.com/documentation/novellaccessmanager31/installation/?page=/documentation/novellaccessmanager31/installation/data/bookinfo.html).
- ❒ Before upgrading, back up your configuration using the `ambkup.bat` file. For instructions, see "Backing Up the Access Manager Configuration" in the *NetIQ Access Manager 3.2 SP1 Administration Console Guide*.

  If the upgrade fails, you need a way to recover your configuration. As a backup can be restored to only the version on which it was created, you must restore your Access Manager components to that version. You can then restore the configuration with the backup file and work with NetIQ Technical Support to solve the upgrade problem before attempting to upgrade again.

3.2.2 Upgrading the Windows Administration Console

If you have installed the Administration Console and Identity Server on the same server, you must upgrade both of them at the same time. Upgrading 3.1 SP4 to 3.2 is supported only on Windows 2008.

NOTE: If your Access Manager 3.1 SP4 components are installed on Windows 2003, migrate them to 3.1 SP4 Windows 2008. For instructions, see "Migrating Administration Consoles From Windows 2003 to Windows 2008".

---

1. Manually back up your current Access Manager configuration using `ambkup.bat` file. For instructions, see "Backing Up and Restoring" in the *NetIQ Access Manager 3.2 SP1 Administration Console Guide*.
2. If the Identity Server is installed on the same server, manually back up the JSP pages and related files in the `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp` directory.
3. If you have customized the `tomcat5.conf` file or the `server.xml` file, back up these files before upgrading. These files are overwritten during the upgrade process.

   IMPORTANT: We recommend that you have your own backup of customized files.

   ---
4. Download and run `AM_32_AccessManagerService_Win64.exe` upgrade file from NetIQ.
5. Run the installation program. When the installation program detects an installed version of the Administration Console, it automatically prompts you to upgrade.
6. Read the Introduction, then click *Next*.
7. Accept the License Agreement, then click *Next.*
8. Select the component to upgrade that is currently installed, then click *Next*.
9. At the upgrade prompt, click *Continue.*
10. Specify the following information for the administrator account on the Administration Console:

    Administration user ID: Specify the name of the administration user for the Administration Console.

    Password and Re-enter Password: Specify and re-enter the password for the administration user account.
11. Decide whether you want the upgrade program to create a backup of your current configuration:
    - If you have a recent backup, click *Continue*. If you choose to not create a backup when you do not have a recent backup and you then encounter a problem during the upgrade, you may be forced to re-create your configuration.
    - If you do not have a recent backup, click *Run Config Backup*. The program creates a backup and stores it in the root of the operating system drive in the `nambkup` directory.
12. Select the *Enable SSL Renegotiation* check box if you have a mutual SSL or X509 certificate authentication configured for this server, then click *Next.*
13. Review the summary, then click *Install.*
14. If the upgrade seems to hang and you have been performing other tasks on the desktop, click the installation screen and check for a warning message. Some subcomponents of Access Manager do not send warning messages to the Installation screen when the focus of the mouse is not on the installation window.
15. When you are prompted, reboot the server.
16. View the upgrade log file found in the following location:

    `C:\Program Files(x86)\Novell\log\AccessManagerServer_InstallLog.log`

17 If the Identity Server installed on the same server, copy any custom login pages to the `C:\Program Files\Novell\Tomcat\webapps\nidp\jsp` directory.

18 Restore any customized files from the backup taken earlier.

To restore the files, copy the content of the following files to the corresponding file in the new location.

server.xml:

If you have customized the `server.xml` file from the backup taken in 3.1 SP4, ensure that you apply the same to the new 3.2 `server.xml` located at `C:\Program Files (x86)\Novell\Tomcat\conf\` directory.

An example below shows that the IP address is removed and ciphers added.

```
<Connector NIDP_Name="connector" port="8443" address=""
ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, ...   ../>
```

tomcat5.conf:

Copy any elements or attributes that you have customized in the `tomcat5.conf` file to the `tomcat7.conf` file.

For example, if you have included the environment variable to increase the heap size by using `-Xmx/Xms/Xss` settings in the `C:\Program Files (x86)\Novell\Tomcat\conf` file.

NOTE: If you have installed the Identity Server with the Administration Console and you have customized login pages, decide whether you want your customized pages restored automatically. Be aware that any new features introduced in JSP files that have the same name as your files are lost, when your file overwrites the installed file with the automatic restore.

Wait until upgrade is complete. Compare your customized file with the newly installed file and then decide whether you need to modify your file before restoring it.

For more information about the 3.2 Administration Console requirements, see "Administration Console Requirements" in the *NetIQ Access Manager 3.2 SP1 Installation Guide*.

3.2.3 Upgrading the Windows Identity Server

If you have installed only the Identity Server on the server, use the following procedure to upgrade the Identity Server.

1 Manually back up the JSP pages and related files in the `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp` directory.

IMPORTANT: We recommend that you have your own backup of the customized files.

---

2 If you have customized the `tomcat5.conf` file or the `server.xml` file at `C:\Program Files (x86)\Novell\Tomcat\conf\`, back up these files before upgrading. The registries and the file are overwritten during the upgrade process.

3 Download and run `AM_32_AccessManagerService_Win64.exe` file from Novell.

This file starts the installation program. When the program detects an installed version of the Identity Server, it automatically prompts you to upgrade.

4 On the Introduction page, click *Next*.

5 Accept the License Agreement.

6 At the upgrade prompt, click *Continue*.

7 Specify the following information for the Administration Console:

Administration user ID: Specify the name of the administration user for the Administration Console.

Password and Re-enter Password: Specify and re-enter the password for the administration user account.

8 If you have customized login pages, decide whether you want your customized pages restored automatically. Be aware that any new feature introduced in the JSP files that have the same name as your files are lost when your file overwrites the installed file with the automatic restore.

You may want to wait until after the upgrade, then compare your customized file with the newly installed file. You can then decide whether you need to modify your file before restoring it.

9 Review the summary, then click *Install*.

10 View the upgrade log file found in the following location:

Windows 2008: `C:\Program Files (x86)\Novell\log\AccessManagerServer_InstallLog.log`

11 Copy any custom login pages to the `C:\Program Files\Novell\Tomcat\webapps\nidp\jsp` directory.

12 Restore any customized files from the backup taken earlier.

To restore the files, copy the content of the following files to the corresponding file in the new location.

server.xml:

If you have customized the `server.xml` file from the backup taken in 3.1 SP4, ensure that you apply the same to the new 3.2 `server.xml` located at `C:\Program Files (x86)\Novell\Tomcat\conf\` directory.

An example below shows that the IP address is removed and ciphers added.`<Connector NIDP_Name="connector" port="8443" address="" ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, ... ../>`

tomcat5.conf:

Copy any elements or attributes that you have customized in the `tomcat5.conf` file to the `tomcat7.conf` file.

For example, if you have included the environment variable to increase the heap size by using-`Xmx/Xms/Xss` settings in the `C:\Program Files (x86)\Novell\Tomcat\conf` file.

13 Restart tomcat server using the Windows service. Go to *Start* > *Control Panel* > *System and Security* > *Administrative Tools* > *Services*.

IMPORTANT: If NetIQ Access Manager is federated with other service providers or if the users are redirected to Access Gateway protected resources from the Identity Server using the target_url, you may see errors regardless of successful authentication. The ConfigUpgrade script enables 'Allow any target' for the 'Intersite Transfer Service' configuration service for all the service providers.

3.2.4 Upgrading the Windows Access Gateway Service

You can upgrade using the same installer you used to install the product. The program detects that the Access Gateway Service is already installed and prompts you to upgrade.

1 Manually back up any customized tomcat files. If you have customized the `tomcat5.conf` file or the `server.xml(C:\Program Files\Novell\Tomcat\conf`)file, back up these files before upgrading. These files are overwritten during the upgrade process.

2 Download and run `AM_32_AccessGatewayService_Win64.exe`.

3 Run the installation program. When the installation program detects an installed version of the Access Gateway, it automatically prompts you to upgrade.

4 Answer `Yes` to the prompt to upgrade.

5 Read the Introduction, then click *Next.*

6 Review the Readme information, then click *Next*.

7 Accept the License Agreement, then click *Next.*

8 Specify the following information:

User ID: Specify the name of the administration user for the Administration Console.

Password and Re-enter Password: Specify the password and re-enter the password for the administration user account.

9 Review the installation summary, then click Install.

The Access Gateway Service is upgraded.

10 View the log files. The install logs are located in the `C:\Program Files\Novell\log` and `C:\agsinstall.log` directories.

11 Restore any customized files from the backup taken earlier.

To restore the files, copy the content of the following files to the corresponding file in the new location.

server.xml:

If you have customized the `server.xml` file from the backup taken in 3.1 SP4, ensure that you apply the same to the new 3.2 `server.xml` located at `C:\Program Files (x86)\Novell\Tomcat\conf\` directory.

An example below shows that the IP address is removed and ciphers added.

```
<Connector NIDP_Name="connector" port="8443" address=""
ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, ...   ../>
```

tomcat5.conf:

Copy any elements or attributes that you have customized in the `tomcat5.conf` file to the `tomcat7.conf` file.

For example, if you have included the environment variable to increase the heap size by using `-Xmx/Xms/Xss` settings in the `C:\Program Files (x86)\Novell\Tomcat\conf` file.

12 Restart tomcat server using the Windows service. Go to *Start* > *Control Panel* > *System and Security* > *Administrative Tools* > *Services*.

3.3 Verifying the Upgrade

After upgrading your Access Manager components, verify that they have all been upgraded to the latest version.

1 In the Administration Console, click *Access Manager* > *Dashboard.*

All components should be in a healthy state. If any have problems, fix those problems before continuing.

2 Click *Auditing* > *Troubleshooting* > *Version.*

Most of the components should display the same version number. If the version numbers vary, click the Readme link and verify what versions are required in the current update.

3 If any component is displaying an incorrect version number, update that component.For smooth performance, make sure that all clustered devices are running the same version.

4 TroubleShooting

4.1 During Primary Administration Console Migration, ndsconfig rm Exits with "Error /opt/novell/eDirectory/bin/ndsconfig return value = 79"

To workaround this issue:

1. Open the terminal in the 3.2 Novell Administration Console.
   - **1a** Run the `/opt/novell/eDirectory/bin/ndsrepair -N` command.
   - **1b** Enter the server number.
   - **1c** Enter the replica option 1 that is `Repair all network addresses`.
2. Open the terminal in the 3.1 SP4 Novell Administration Console.
   - **2a** Run the following command and provide user name in the "admin.novell" format and password:

     ```
     /opt/novell/eDirectory/bin/ndsconfig rm /etc/opt/novell/eDirectory/conf/nds.conf
     ```
   - **2b** Provide the admin credentials and proceed with deletion.
3. Proceed with the migration steps.

4.2 When Migration to 3.2 Access Manager Terminates Abruptly

The 3.2 migration may terminate due to any reason such as network issue. In such cases, re-run the migration after cleaning up partly installed components as in the following procedure:

To workaround this issue, perform the following steps to cleanup before re-running the `install_and_migrate` script:

1. Ensure that the 3.1 SP4 machine remains as master replica
   - **1a** In the 3.1 SP4 machine, run the `ndsrepair -P -Ad` command.
   - **1b** Enter 1 and press Enter.
   - **1c** Enter 5 and press Enter.
2. Restore certificates back to 3.1 SP4.
   - **2a** In the 3.1 SP4 machine, go to `/opt/novell/devman/bin`, then run the `aminst-certs.sh` script.
   - **2b** Enter the credentials and path for the backup file that was originally taken.
3. Remove the failed server.
   - **3a** In the new 3.2 machine, run the following command:

     ```
     /opt/novell/eDirectory/bin/ndsconfig rm /etc/opt/novell/eDirectory/conf/nds.conf
     ```
   - **3b** Enter the admin credentials in the admin.novell format and proceed with deletion.
4. In the new 3.2 machine, uninstall the Novell Access Manager binaries.
   - **4a** From the `novell-access-manager` folder, run the `./uninstall.sh` script.
   - **4b** Select the option *5* and proceed.
   - **4c** Delete the `migrate_inputs.sh` script under `scripts` folder.
5. Delete objects from the eDirectory Configuration Store.
   - **5a** Log in to the 3.1 SP4 Administration Console, then click *Auditing* > *Troubleshooting*.
   - **5b** In the *Other Known Device Manager Servers* section, select the failed primary Administration Console.
   - **5c** Click *Remove*.

     Few objects in eDirectory require to be deleted. Sometime manual deletion could lead to errors. It is recommended to take a backup of entire eDirectory before you delete the objects.

     Run the following command to back up the eDirectory objects:

     ```
     ndsbackup cvf ndsbackupfile -a <user id like admin.novell> -p <password>
     ```

     In case of any issue due to manual delete, you can restore the same by running the following command:

     ```
     ndsbackup xvf ndsbackupfile
     ```
   - **5d** To delete the objects in eDirectory, select *View Objects* from the *iManager* menu bar.
   - **5e** In the Tree view, select *novell* and view the objects.
   - **5f** Delete all objects that refer to the failed primary console. You should find the following types of objects:
     - SAS Service object with the host name of the failed primary console

- An object that starts with the last octet of the IP address of the failed primary console
- DNS AG object with the host name of the failed primary console
- DNS IP object with the host name of the failed primary console
- SSL CertificateDNS with the host name of the failed primary console
- SSL CertificateIP with the host name of the failed primary console

NOTE: You must follow the procedure irrespective of where the migration terminated to ensure that the machine is clean.

6. On the 3.1 SP4 machine, run the `/opt/novell/eDirectory/bin ndsstat -r` command to verify if there are any replicas in eDirectory caused due to failure while migrating. Ensure that you remove them.
7. In the 3.2 machine, run the install_and_migate_3.2.sh script the `novell-access-manager` folder and proceed with the installation steps.

4.3 Migration Exits Stating That the Server's DIB Does Not Contain Replicas

Some of the objects in the eDirectory store have invalid timestamps and the timestamps must be fixed before migrating.

To workaround this issue perform the following procedure:

1. Configure NTP server using YaST and synchronize the time.
2. Run the `ndsrepair -P -Ad` command, select option 1 and then option 12 which repairs the timestamps and declares a new epoch.
3. Run `ndsrepair -R`
4. Run the `ndsd restart` command at `/etc/init.d`.

4.4 Exception During the Access Gateway Migration

Exporting and importing policies from containers other than master containers will not automatically correct the existing policy references from the devices.You will have to re-reference to the imported policies.

To workaround this issue, perform the following steps:

1. In the Administration Console, click *Auditing* > *Troubleshooting* > *Policies*.
2. Click *Remove* under *Access Gateways with Protected Resources Referencing Nonexistent Policies*.

4.5 Device Is Not Reachable After Migrating From the 3.1 SP4 Access Gateway Appliance to Access Gateway Appliance

After migrating, Yast adds the default route through second interface if both the NIC interfaces are on the same subnet.

To workaround this issue, perform the following steps:

1. Go to *YaST* > *Network Devices* > *Network Settings* > *Routing* and remove the default gateway.
2. Select *Add* in the Routing Table and enter the following details:

   Destination: Enter the destination IP address 0.0.0.0.

   Device: Enter the device id eth0.

   Gateway: Enter the default gateway IP address.

   Netmask: Enter the netmask address 0.0.0.0.
3. Click *OK* and *Quit*. If the service provider does not start successfully perform the workaround provided in Section 4.6, "Service Provider Does Not Start," on page 64.

4.6 Service Provider Does Not Start

After migrating and performing the workaround mentioned in Device Is Not Reachable After Migrating From the 3.1 SP4 Access Gateway Appliance to Access Gateway Appliance, you may receive the following error message:

```
Start unsuccessful. Reason: Unable to read Truststore: /opt/novell/devman/jcc/
certs/esp/6E781CF4892AB22D/truststore.keystore.
```

To workaround this issue, re-push the certificates from the *Administration Console* > *Troubleshooting* > *Certificates* and update the device. The service provider starts successfully.

4.7 The Access Gateway Throws a 403 Forbidden Page Error for a Resource Protected by a Form Fill Policy

This issue can happen if a Web server returns a form with a http 403 error code. The Access Gateway, by default, returns its own custom error pages. Hence, this prevents the Form Fill feature to work. To workaround, go to *Access Gateway* > *Advanced Options*, enter ProxyErrorOverride off > click *OK*.

4.8 While Migrating 3.1 SP4 Access Gateway with SSL VPN, ESP is in a Halted State After Rip and Replace

Keep the hostname and IP address same while migrating the 3.1 SP4 Access Gateway Appliance to 3.2 Access Gateway Appliance.

4.9 Datastore Authentication Error, Bad Password or Certificate

After migrating to 3.2 SP1, when you log in to the Administration Console, the following alert is displayed:

```
Datastore authentication error, bad password or certificate.
```

This alert can be ignored because it does not have any impact on the functionality.

A Utility Scripts

Table A-1 *Utility Scripts*

Script Name	Description
ambkup.sh	Backs up the Access Manager configuration. This script is located in `/opt/novell/devman/bin/`.
install_and_migrate-3.2.sh	Migrates the Access Manager Administration Console from 3.1 SP4 to 3.2. This script is located in the `novell-access-manager` folder in the `AM_32_AccessManagerService_Linux64.tar.gz` file.
install.sh	Installs the fresh 3.2 Access Manager components. This script is located in the `novell-access-manager` folder in the `AM_32_AccessManagerService_Linux64.tar.gz` file.
migrate_backup.sh	Backs up any customized files of Identity Server, 3.1 SP4 Access Gateway and SSL VPN. This script is located in the `novell-access-manager` folder in the `AM_32_AccessManagerService_Linux64.tar.gz` file.
lag2mag_files.csv and migrate_files.sh	These files when copied and run on the 3.1 SP4 Access Gateway Appliance help in finding the equivalent Access Gateway advanced option. This file and script are located in the `novell-access-manager/utils` folder in the `AM_32_AccessManager_Service_Linux64.tar.gz` file and also in `/opt/novell/ag/doc/` directory on the 3.2 Access Gateway Appliance.