# Contents

## About this Book and the Library

### 1 Planning Your Access Manager Environment

1.1 Deployment Models ............................................. 11
1.2 Access Manager Versus Access Manager Appliance ................. 13
1.3 Network Requirements ........................................... 19
1.4 System Requirements ........................................... 20
1.5 Recommended Installation Scenarios ................................ 20
  1.5.1 Basic Setup .................................................. 21
  1.5.2 High Availability Configuration with Load Balancing .......... 22
1.6 Deploying Access Manager on Public Cloud ........................ 22
  1.6.1 Deploying on AWS EC2 .................................... 23
  1.6.2 Deploying on Microsoft Azure ............................. 24
1.7 Installing Access Manager Components in NAT Environments ........ 25
  1.7.1 Network Prerequisites ....................................... 26
  1.7.2 Network Setup Flow Chart .................................. 27
  1.7.3 Installing Access Manager Components in NAT Environments . 27
  1.7.4 Configuring Network Address Translation .................... 29
1.8 Setting Up Firewalls ............................................. 30
  1.8.1 Required Ports ............................................... 31
  1.8.2 Restricted Ports ............................................. 38
  1.8.3 Sample Configurations ....................................... 38
1.9 Using Certificates for Secure Communication ........................ 40
1.10 Protecting an Identity Server Through Access Gateway .............. 41

## Part I Installing Access Manager

### 2 Installing Administration Console

2.1 Installing Administration Console on Linux ........................... 45
  2.1.1 System Requirements on Linux ................................ 45
  2.1.2 Installation Procedure ....................................... 48
2.2 Installing Administration Console on Windows ......................... 52
  2.2.1 System Requirements on Windows ............................. 52
  2.2.2 Installation Procedure ....................................... 52
2.3 Logging In to Administration Console ................................ 54
2.4 Enabling Administration Console for Multiple Network Interface Cards . 55

### 3 Installing Identity Server

3.1 Prerequisites for Installing Identity Server .......................... 57
3.2 Installing Identity Server on Linux ................................ 58
  3.2.1 System Requirements on Linux ............................... 58
  3.2.2 Installation Procedure ....................................... 60
3.3 Installing Identity Server on Windows ............................... 61
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.1 System Requirements on Windows</td>
<td>61</td>
</tr>
<tr>
<td>3.3.2 Installation Procedure</td>
<td>62</td>
</tr>
<tr>
<td>3.4 Verifying Identity Server Installation</td>
<td>63</td>
</tr>
<tr>
<td>3.5 Translating Identity Server Configuration Port</td>
<td>63</td>
</tr>
<tr>
<td>3.5.1 Changing the Port on Windows Identity Server</td>
<td>63</td>
</tr>
<tr>
<td>3.5.2 Changing the Port on Linux Identity Server</td>
<td>64</td>
</tr>
<tr>
<td>4 Installing Access Gateway</td>
<td>69</td>
</tr>
<tr>
<td>4.1 Feature Comparison of Different Types of Access Gateways</td>
<td>69</td>
</tr>
<tr>
<td>4.2 Installing Access Gateway Appliance</td>
<td>70</td>
</tr>
<tr>
<td>4.2.1 System Requirements</td>
<td>70</td>
</tr>
<tr>
<td>4.2.2 Installing Access Gateway Appliance</td>
<td>71</td>
</tr>
<tr>
<td>4.2.3 Configuring Access Gateway Appliance</td>
<td>73</td>
</tr>
<tr>
<td>4.3 Installing Access Gateway Service</td>
<td>79</td>
</tr>
<tr>
<td>4.3.1 Installing Access Gateway Service on Linux</td>
<td>79</td>
</tr>
<tr>
<td>4.3.2 Installing Access Gateway Service on Windows</td>
<td>82</td>
</tr>
<tr>
<td>4.4 Verifying Access Gateway Installation</td>
<td>84</td>
</tr>
<tr>
<td>5 Installing Analytics Server</td>
<td>85</td>
</tr>
<tr>
<td>5.1 System Requirements</td>
<td>85</td>
</tr>
<tr>
<td>5.1.1 System Requirements for Storing 500 Events Per Second (EPS)</td>
<td>85</td>
</tr>
<tr>
<td>5.2 Procedure to Install Analytics Server</td>
<td>86</td>
</tr>
<tr>
<td>5.3 Modifying Password After Installation</td>
<td>88</td>
</tr>
<tr>
<td>5.4 Adding and Configuring Multiple NIC to Analytics Server</td>
<td>88</td>
</tr>
<tr>
<td>5.5 Post-Installation Configuration for Analytics Server</td>
<td>88</td>
</tr>
<tr>
<td>5.6 Deploying Analytics Server for High Availability</td>
<td>88</td>
</tr>
<tr>
<td>5.6.1 Prerequisite</td>
<td>89</td>
</tr>
<tr>
<td>5.6.2 Installing Analytics Server in High Availability Environment</td>
<td>89</td>
</tr>
<tr>
<td>5.6.3 Post-Installation Cluster Configuration for Analytics Server</td>
<td>99</td>
</tr>
<tr>
<td>6 Deploying Access Manager on Amazon Web Services EC2</td>
<td>101</td>
</tr>
<tr>
<td>6.1 Prerequisites or Deploying Access Manager on AWS</td>
<td>101</td>
</tr>
<tr>
<td>6.2 Deployment Procedure</td>
<td>102</td>
</tr>
<tr>
<td>6.2.1 Creating AWS EC2 Services</td>
<td>102</td>
</tr>
<tr>
<td>6.2.2 Creating and Deploying Instances</td>
<td>103</td>
</tr>
<tr>
<td>6.2.3 Installing Access Manager</td>
<td>104</td>
</tr>
<tr>
<td>6.2.4 (Optional) Creating an AWS EC2 Load Balancer</td>
<td>106</td>
</tr>
<tr>
<td>6.3 Auto Scaling Access Manager on AWS</td>
<td>111</td>
</tr>
<tr>
<td>6.3.1 Configuring Auto Scaling</td>
<td>112</td>
</tr>
<tr>
<td>6.3.2 Limitations</td>
<td>120</td>
</tr>
<tr>
<td>6.4 Monitoring Access Manager in AWS Using CloudWatch</td>
<td>121</td>
</tr>
<tr>
<td>7 Deploying Access Manager on Microsoft Azure</td>
<td>123</td>
</tr>
<tr>
<td>7.1 Prerequisites for Deploying Access Manager on Microsoft Azure</td>
<td>123</td>
</tr>
<tr>
<td>7.2 Deployment Procedure</td>
<td>124</td>
</tr>
<tr>
<td>7.2.1 Creating Azure Services</td>
<td>124</td>
</tr>
<tr>
<td>7.2.2 Creating and Deploying Virtual Machines</td>
<td>125</td>
</tr>
<tr>
<td>7.2.3 Configuring Network Security Groups</td>
<td>128</td>
</tr>
<tr>
<td>7.2.4 Changing the Private IP Address from Dynamic to Static</td>
<td>129</td>
</tr>
</tbody>
</table>
7.2.5 Installing Access Manager ................................................................. 129
7.3 (Optional) Azure Load Balancer ............................................................ 130
7.3.1 Creating a Load Balancer ................................................................. 131
7.3.2 Configuring a Load Balancer ............................................................. 131

8 Installing Packages and Dependent RPMs on RHEL for Access Manager 137

9 Uninstalling Components ................................................................. 141
  9.1 Uninstalling Identity Server ................................................................. 141
    9.1.1 Deleting Identity Server References .............................................. 141
    9.1.2 Uninstalling the Linux Identity Server ........................................... 141
    9.1.3 Uninstalling the Windows Identity Server ..................................... 142
  9.2 Reinstalling an Identity Server to a New Hard Drive ............................ 142
  9.3 Uninstalling Access Gateway ............................................................. 143
    9.3.1 Uninstalling Windows Access Gateway Service ............................... 143
    9.3.2 Uninstalling Linux Access Gateway Service ................................... 143
  9.4 Uninstalling Administration Console ................................................ 144
    9.4.1 Uninstalling Linux Administration Console .................................. 144
    9.4.2 Uninstalling Windows Administration Console ............................... 145

Part II Upgrading Access Manager ....................................................... 147

10 Prerequisites for Upgrading Access Manager ........................................ 149
  10.1 Maintaining Customized JSP Files for Identity Server ......................... 150
    10.1.1 Using Customized JSP Pages from Access Manager 4.1 or Prior .......... 150
    10.1.2 Using Customized JSP Pages from Access Manager 4.1 or Prior and Enabling the New Access Manager Portal ........................................... 151
  10.2 Maintaining Customized JSP Files for Access Gateway ......................... 152

11 Upgrading Administration Console ...................................................... 153
  11.1 Upgrading Administration Console on Linux ...................................... 153
    11.1.1 Upgrading the Evaluation Version to the Purchased Version ............ 153
    11.1.2 Upgrading Administration Console ........................................... 154
  11.2 Upgrading Administration Console on Windows ................................... 156
    11.2.1 Upgrading the Evaluation Version to the Purchased Version ............ 156
    11.2.2 Upgrading Administration Console ........................................... 156

12 Upgrading Identity Server ................................................................. 159
  12.1 Upgrading Identity Server on Linux ................................................ 159
    12.1.1 Upgrading the Evaluation Version to the Purchased Version ............ 159
    12.1.2 Upgrading Identity Server .................................................... 160
  12.2 Upgrading Identity Server on Windows ............................................. 162
    12.2.1 Upgrading the Evaluation Version to the Purchased Version ............ 162
    12.2.2 Upgrading Identity Server .................................................... 162

13 Upgrading Access Gateway ............................................................... 165
  13.1 Upgrading Access Gateway on Linux .............................................. 165
Part IV  Appendix  

A  Configuring Administration Console Ports 9000 and 9001 to Listen on the Specified Address

B  Recommendations for Scaling Access Manager Components in Public Cloud

Scaling Up the Access Manager Nodes
Scaling Down the Access Manager Nodes
About this Book and the Library

The *Installation Guide* provides an introduction to NetIQ Access Manager and describes the installation and upgrade procedures.

**Intended Audience**

This book is intended for Access Manager administrators. It is assumed that you have knowledge of evolving Internet protocols, such as:

- Extensible Markup Language (XML)
- Simple Object Access Protocol (SOAP)
- Security Assertion Markup Language (SAML)
- Public Key Infrastructure (PKI) digital signature concepts and Internet security
- Secure Socket Layer/Transport Layer Security (SSL/TLS)
- Hypertext Transfer Protocol (HTTP and HTTPS)
- Uniform Resource Identifiers (URIs)
- Domain Name System (DNS)
- Web Services Description Language (WSDL)

**Other Information in the Library**

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

- [Access Manager Product Documentation](https://www.netiq.com/documentation/access-manager/index.html)
- [Access Manager Developer Resources](https://www.netiq.com/documentation/access-manager-45-developer-documentation/)

**NOTE:** Contact namsdk@microfocus.com for any query related to Access Manager SDK.
Planning Your Access Manager Environment

This section includes the following topics:

- Section 1.1, “Deployment Models,” on page 11
- Section 1.2, “Access Manager Versus Access Manager Appliance,” on page 13
- Section 1.3, “Network Requirements,” on page 19
- Section 1.4, “System Requirements,” on page 20
- Section 1.5, “Recommended Installation Scenarios,” on page 20
- Section 1.6, “Deploying Access Manager on Public Cloud,” on page 22
- Section 1.7, “Installing Access Manager Components in NAT Environments,” on page 25
- Section 1.8, “Setting Up Firewalls,” on page 30
- Section 1.9, “Using Certificates for Secure Communication,” on page 40
- Section 1.10, “Protecting an Identity Server Through Access Gateway,” on page 41

1.1 Deployment Models

Access Manager Appliance is a deployment model introduced from NetIQ Access Manager 3.2 onwards. It includes all major components such as Administration Console, Identity Server, and Access Gateway in a single soft appliance. This solution differs from the other Access Manager model where all components can be installed on separate systems. Access Manager Appliance enables organizations to rapidly deploy and secure web and enterprise applications. This simplifies access to any application. The reduced deployment and configuration time gives quick time to value and helps to lower the total cost of ownership.

Some of the key differentiators that Access Manager Appliance offers over Access Manager are:

- Quick installation and automatic configuration
- Single port configuration and common location to manage certificates
- Sample portal for administrator reference
- Fewer DNS names, SSL certificates, and IP addresses
- Reduced hardware requirements

For details about these differentiators and other features of Access Manager Appliance, see Section 1.2, “Access Manager Versus Access Manager Appliance,” on page 13.
The following diagrams describe differences between Access Manager and Access Manager Appliance:

**Figure 1-1  Typical Deployment of Access Manager**

![Diagram of typical Access Manager deployment](image)

**Figure 1-2  Typical Deployment of Access Manager Appliance**

![Diagram of typical Access Manager Appliance deployment](image)
1.2 **Access Manager Versus Access Manager Appliance**

Both Access Manager and Access Manager Appliance deployment models use a common code base. However, a few differences exist between both models.

The following table provides details to help you determine which solution fits your business:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Access Manager Appliance</th>
<th>Access Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtualization Support</td>
<td>Supported on the virtual servers based on SUSE Linux Enterprise Server (SLES) 11 SP4 with 64-bit operating system x86-64 hardware.</td>
<td>Supported on the virtual servers based on SLES 12 SP3 or SLES 12 SP4 with 64-bit operating system x86-64 hardware.</td>
</tr>
<tr>
<td>Host Operating System</td>
<td>A soft appliance that includes a pre-installed and configured SUSE Linux operating system. NetIQ maintains both the operating system and Access Manager patches through the patch update channel.</td>
<td>Operating System choice is more flexible. Install Administration Console, Identity Server, and Access Gateway on a supported operating system (SUSE, Red Hat, or Windows). The patch update channel maintains the patches for Access Manager. You must purchase, install, and maintain the underlying operating system.</td>
</tr>
<tr>
<td>Component Installation Flexibility</td>
<td>Access Manager components such as Administration Console, Identity Server, and Access Gateway cannot be selectively installed or uninstalled.</td>
<td>Each Access Manager component such as Administration Console, Identity Server, and Access Gateway are installed on independent host servers. Although the ability to install multiple components on a single host server exists, it is very limited and generally not recommended. A typical highly available deployment requires 6-8 or more virtual or physical servers (2 Administration Consoles, 2 Identity Servers, 2 Access Gateways).</td>
</tr>
<tr>
<td>Administration Console Access</td>
<td>Administration Console is installed on Access Manager Appliance along with all other components. If you use two network interfaces, access to Administration Console can be limited to the private IP network bound to the internal network. The public interface is bound to an externally accessible network.</td>
<td>Administration Console can be installed on an independent host inside your private network but can still securely manage Access Manager components that reside in your DMZ or external network.</td>
</tr>
<tr>
<td>Feature</td>
<td>Access Manager Appliance</td>
<td>Access Manager</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Scalability and Performance</td>
<td>Scales vertically on adding CPU and memory resources to each node. For more information, see NetIQ Access Manager Performance and Sizing Guidelines</td>
<td>Scales both vertically and horizontally on adding nodes. For more information, see NetIQ Access Manager Performance and Sizing Guidelines.</td>
</tr>
<tr>
<td>High Availability</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Upgrade</td>
<td>You can upgrade from one version of Access Manager Appliance to another version. However, upgrading from Access Manager to Access Manager Appliance is not supported.</td>
<td>You can upgrade from one version of Access Manager to another version. However, upgrading from Access Manager Appliance to Access Manager is not supported.</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>You can use the backup and restore process to save your Access Manager Appliance configuration.</td>
<td>You can use the backup and restore process to save your Access Manager configuration.</td>
</tr>
<tr>
<td>Time to Value</td>
<td>Automates several configuration steps to quickly set up the system.</td>
<td>Requires more time to install and configure as the components are on different servers.</td>
</tr>
<tr>
<td>User Input required during installation</td>
<td>Access Manager Appliance is a software appliance that takes only a few basic parameters as input. Several options assume default values.</td>
<td>More flexibility during installation in terms of selectable parameters.</td>
</tr>
<tr>
<td>Installation and Configuration Phases</td>
<td>The installer takes care of configuration for each component. The system is ready for use after it is installed.</td>
<td>Separate installation and configuration phases for each component. After installation, each Access Manager component is separately configured.</td>
</tr>
<tr>
<td>Mode of release</td>
<td>Access Manager Appliance is released as a software appliance.</td>
<td>Access Manager is delivered in the form of multiple operating system-specific binaries.</td>
</tr>
<tr>
<td>NIC Bonding</td>
<td>IP address configuration is done through Administration Console. So, NIC bonding is not supported.</td>
<td>NIC bonding can be done through the operating system and Access Manager in turn uses this configuration.</td>
</tr>
<tr>
<td>Networking: Port Details</td>
<td>Administration Console and Identity Server are accelerated and protected by Access Gateways. Only HTTPS port 443 is required to access Access Manager Appliance through a firewall.</td>
<td>Multiple ports need to be opened for deployment.</td>
</tr>
<tr>
<td>Networking: General</td>
<td>Administration Console must be in DMZ, but access can be restricted through the private interface.</td>
<td>As Administration Console is a separate device, access can be restricted or Administration Console can be placed in an internal network.</td>
</tr>
<tr>
<td>Feature</td>
<td>Access Manager Appliance</td>
<td>Access Manager</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Certificate Management</td>
<td>Certificate management is simplified. All certificates and key stores are stored at one place making replacing or renewing certificates easier.</td>
<td>Changes are required at multiple places to replace or renew certificates.</td>
</tr>
<tr>
<td>SAML Assertion Signing</td>
<td>Same certificate is used for all communication. (signing, encryption, and transport).</td>
<td>As there are multiple key stores, you can configure different certificates for the communication.</td>
</tr>
<tr>
<td>Associating different signing certificates for each service provider</td>
<td>Not supported</td>
<td>A unique signing certificate can be assigned to each service provider. In environments with a large number of trust relationships, this feature eases the process of replacing expiring certificates.</td>
</tr>
<tr>
<td>Associating different certificates to Identity Server</td>
<td>Not applicable because Identity Server is accelerated by Access Gateway.</td>
<td>Supported. Identity Server can be behind Access Gateway or can be placed separately in the DMZ.</td>
</tr>
<tr>
<td>Sample Portal</td>
<td>After a successful installation, a sample web portal is deployed for the administrator’s reference. The administrator can access the sample portal by using the <a href="http://hostname">http://hostname</a> URL. This portal provides detailed example of Access Manager Appliance usage and policy configuration.</td>
<td>Not available.</td>
</tr>
</tbody>
</table>
| Ready-made Access Manager | The following configuration is automatically done after Access Manager Appliance installation:  
- Importing Identity Server and Access Gateway.  
- Cluster creation of Identity Server and Access Gateway.  
- Configuration of Identity Server to bring it to green state.  
- Configuration of Access Gateways and Identity Server association.  
- Service creation to accelerate or protect Identity Server, Administration Console, and sample portal. As the inter-component configuration is automated, the administrator only needs to add the existing user store and accelerate, protect, sso-enable existing web applications. | Each component requires manual configuration and setup before web applications can be federation enabled, accelerated, and protected. |
### Planning Your Access Manager Environment

#### Updating Kernel with Security Patches

- **Access Manager Appliance**: Supports installation of latest SLES operating system security patches.
- **Access Manager**: You are fully responsible for all operating system maintenance including patching.

#### Clustering

- **Access Manager Appliance**: For additional capacity and for failover, cluster a group of NetIQ Access Manager Appliances and configure them to act as a single server. You can cluster any number of Identity Servers and Access Gateways, and up to three of Administration Consoles. The first three nodes of Access Manager Appliance contain Administration Console, Identity Server, and Access Gateway. Fourth installation onwards, the node has all components except for Administration Console. A typical Access Manager Appliance deployment in a cluster is described in Figure 1-3 on page 17.
- **Access Manager**: For additional capacity and for failover, cluster a group of Identity Servers and configure them to act as a single server. You can create a cluster of Access Gateways and configure them to act as a single server. Fault tolerance can be achieved by installing up to two secondary consoles. To deploy the existing solution in a cluster mode, at least 6 systems are required. A typical Access Manager deployment in a cluster is described in Figure 1-4 on page 18.
Figure 1-3  Access Manager Appliance Cluster

- Can be clustered.
- Cannot be clustered
General Guidelines

- It is not possible to add an Access Gateway Service or Access Gateway Appliance to an Access Manager Appliance cluster.
- Deploying Administration Console in a DMZ network limits access from a private interface or network.
- It is recommended to not change the primary IP Address of Access Manager. This may result in corruption of the configuration store. However, you can modify the listening IP address of reverse proxy or the outbound IP address used to communicate with the web server. For more information, see Changing the IP Address of Access Manager Devices in the Access Manager 4.5 Administration Guide.
- You cannot have different certificates for signing and encryption in a federation setup.
When to Choose Access Manager Appliance

The following are common usage patterns when you can deploy Access Manager Appliance:

- You are interested in deploying Access Manager, but need fewer servers.
- You are still on iChain because you prefer a single-server solution.
- You are new to Access Manager and are interested in providing secure access, but want to avoid the long process of designing, installing, and configuring a full-fledged web access management solution.
- You do not have a web access management or federation solution and you are considering moving to a web access management solution.
- You represent a division of a large organization (for example, the Marketing division) that wants secure single sign-on access to a SaaS application such as Salesforce.
- You want to reduce server hardware and management cost by consolidating Access Manager services on fewer servers.
- You want to quickly set up a test environment to verify changes.
- You want to quickly setup and evaluate Access Manager.

1.3 Network Requirements

In addition to the servers on which Access Manager software is installed, your network environment must meet the following requirements:

- An LDAP directory (eDirectory, Sun ONE, Active Directory, or Azure Active Directory) that contains your system users. Identity Server uses the LDAP directory to authenticate users to the system.

**NOTE:** Azure Active Directory is supported when Access Manager is deployed on Microsoft Azure.

- Web servers with content or applications that need protection and single-sign on.
- Static IP addresses for each machine used for Access Manager components. If the IP address of the machine changes, Access Manager components installed on that machine will not start.
- A domain name server, which resolves DNS names to IP addresses and which has reverse lookups enabled.

Access Manager devices know each other by their IP addresses, and some requests require them to match an IP address with the device’s DNS name. Without reverse lookups enabled, these requests fail. In particular, Identity Servers perform reverse lookups to their user stores. If reverse lookups are not available, host table entries can be used.

- Time must be synchronized to within one minute among all components of the configuration using NTP or similar solution.

**IMPORTANT:** If time is not synchronized, users cannot authenticate and access resources.
• (OPTIONAL) An L4 switch or similar solution if you are planning to configure load balancing.
• Clients with an Internet browser.

1.4 System Requirements

The component-specific installation sections contain the system requirements of respective components. The following table lists links to the system requirement section of each component:

<table>
<thead>
<tr>
<th>Component</th>
<th>Linux</th>
<th>Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration Console</td>
<td><a href="#">System Requirements on Linux</a></td>
<td><a href="#">System Requirements on Windows</a></td>
</tr>
<tr>
<td>Identity Server</td>
<td><a href="#">System Requirements on Linux</a></td>
<td><a href="#">System Requirements on Windows</a></td>
</tr>
<tr>
<td>Access Gateway Service</td>
<td><a href="#">System Requirements on Linux</a></td>
<td><a href="#">System Requirements on Windows</a></td>
</tr>
<tr>
<td>Access Gateway Appliance</td>
<td><a href="#">System Requirements</a></td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Analytics Server</td>
<td><a href="#">System Requirements for Storing 500 Events Per Second (EPS)</a></td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

**Client Browser Support**

You can access the Access Gateway Server from any latest version of the browser.

For accessing User Portal and Administration Console, users can log in using the following browsers:

• Firefox 66.0.2
• Chrome 73.0.3683.86
• Microsoft Edge 42.17134.1.0/ EdgeHTML 17.17134
• Internet Explorer 11.648.17134.0 Update Versions 11.0.115 (KB4489873)

1.5 Recommended Installation Scenarios

The following scenarios provide an overview of the flexibility built into Access Manager. Use them to design a deployment strategy that fits the needs of your company.

• Section 1.5.1, “Basic Setup,” on page 21
• Section 1.5.2, “High Availability Configuration with Load Balancing,” on page 22
1.5.1 Basic Setup

You need to protect Administration Console from Internet attacks. It should be installed behind your firewall. For a basic Access Manager installation, you can install Identity Server and Access Gateway outside your firewall. Figure 1-5 illustrates this scenario:

*Figure 1-5  Basic Installation Configuration*

1. Install Administration Console.
   Administration Console and Identity Server are bundled in the same download file or ISO image.

2. If your firewall is set up, open the ports required for Identity Server and Access Gateway to communicate with Administration Console: TCP 1443, TCP 8444, TCP 1289, TCP 1290, TCP 524, TCP 636.

   For more information about these ports, see Section 1.8, “Setting Up Firewalls,” on page 30.

3. Run the installation again and install Identity Server on a separate server.

   Log in to Administration Console and verify that Identity Server installation was successful.

4. Install Access Gateway.

   Log in to Administration Console and verify that Access Gateway imported successfully.

5. Install Analytics Server.

   Log in to Administration Console to verify that Analytics Server is imported successfully.


   In this configuration, the LDAP server is separated from Identity Server by the firewall. Make sure you open the required ports. See Section 1.8, “Setting Up Firewalls,” on page 30.

For information about setting up configurations for fault tolerance and clustering, see High Availability and Fault Tolerance in the Access Manager 4.5 Administration Guide.
Firewall protects the LDAP server and Administration Console, both of which contain a permanent store of sensitive data. Web servers are also installed behind the firewall for added protection. Identity Server is not much of a security risk, because it does not permanently store any user data. NetIQ has tested and recommends this configuration. We have also tested this configuration with an L4 switch in place of the router so that the configuration can support clusters of Identity Servers and Access Gateways.

1.5.2 High Availability Configuration with Load Balancing

Figure 1-6 illustrates a deployment scenario where web resources are securely accessible from the Internet. The scenario also provides high availability because both Identity Servers and Access Gateways are clustered and have been configured to use an L4 switch for load balancing and fault tolerance.

![Figure 1-6 Clustering Configuration for High Availability](image)

You can configure end users to communicate with Identity Servers and Access Gateways through HTTP or HTTPS. You can configure Access Gateways to communicate with web servers through HTTP or HTTPS. Multiple Administration Consoles provide administration and configuration redundancy.

This configuration is scalable. As the number of users increase and the demands for web resources increase, you can easily add another Identity Server or Access Gateway to handle the load, then add the new servers to the L4 switch. When the new servers are added to the cluster, they are automatically sent the cluster configuration.

1.6 Deploying Access Manager on Public Cloud

The following list provides the recommended configuration details for deploying Access Manager on Amazon Web Services (AWS) EC2 and Microsoft Azure:

- Install the LDAP server and Administration Console in the private subnet. Both of these contain a permanent store of sensitive data. Install web servers also in the private subnet for added protection.

  In the private subnet, servers do not have any public IP address. This prevents the servers from security vulnerabilities. However, the servers on the public subnet can have public IP addresses.
You cannot access Administration Console directly in the private subnet. Therefore, it is recommended to configure a dedicated server called as jump server in the public subnet. You can then use the jump server to access Administration Console. You can use a Windows server as a jump server and Remote Desktop Protocol to access the jump server.

For more information about jump servers, see Linux Bastion Host Quick Start (https://docs.aws.amazon.com/quickstart/latest/linux-bastion/architecture.html).

The cloud-based service provider routes communications among servers on the public subnet and servers on the private subnet.

Install Identity Server in the public subnet because it does not permanently store any sensitive user data.

This configuration has been tested with a load balancer to support clusters of Identity Servers and Access Gateways. As the number of users and demands for web resources increase, you can easily add another Identity Server or Access Gateway to handle the load. You can then add the new servers to the load balancer. When the new servers are added to the cluster, they are automatically sent the cluster configuration. See Appendix B, “Recommendations for Scaling Access Manager Components in Public Cloud,” on page 209.

The following sections provide information specific to AWS EC2 and Microsoft Azure:

- Section 1.6.1, “Deploying on AWS EC2,” on page 23
- Section 1.6.2, “Deploying on Microsoft Azure,” on page 24

1.6.1 Deploying on AWS EC2

You need to configure a VPC NAT gateway. Servers in the private subnet use VPC NAT gateway to access the Internet. Similarly, you need to configure an Internet gateway for enabling servers in the public subnet to access Internet and vice versa. For more information, see the Amazon Virtual Private Cloud Documentation (https://aws.amazon.com/documentation/vpc/).

For more information about AWS EC2 VPC, see Amazon Virtual Private Cloud Documentation (https://aws.amazon.com/documentation/vpc/).

For information about how to deploy Access Manager on AWS EC2, see Chapter 6, “Deploying Access Manager on Amazon Web Services EC2,” on page 101.
1.6.2 Deploying on Microsoft Azure

In Microsoft Azure, you do not need to configure a VPC NAT gateway and Internet gateway. Azure takes care of this configuration.

For more information about the Azure virtual network, see Virtual Network Documentation (https://docs.microsoft.com/en-in/azure/virtual-network/).

For information about how to deploy Access Manager on Azure, see “Deploying Access Manager on Microsoft Azure” on page 123.
1.7 Installing Access Manager Components in NAT Environments

You can deploy Access Manager components in a multi-tenant or service provider environment, where Network Address Translation (NAT) protocol is used as one of the network configuration.

This section includes the following topics:

- Section 1.7.1, “Network Prerequisites,” on page 26
- Section 1.7.2, “Network Setup Flow Chart,” on page 27
- Section 1.7.3, “Installing Access Manager Components in NAT Environments,” on page 27
- Section 1.7.4, “Configuring Network Address Translation,” on page 29
1.7.1 Network Prerequisites

Service Provider Network Setup

- Obtain Static IP addresses for Administration Console, Identity Server, and Analytics Server or Sentinel. If the IP address of the machine changes, Access Manager components on that machine cannot start.
- Install operating system, configure Network Time Protocol (NTP) server, and check connectivity.
- NTP server, which provides accurate time to the machines on your network. Time must be synchronized within one minute among the components, or the security features of the product disrupt the communication processes. You can install your own or use a publicly available server such as pool.ntp.org.

**IMPORTANT:** If time is not synchronized, users cannot authenticate and access resources and data corruption can also happen in user stores.

- An L4 switch if you need to configure load balancing. This can be hardware or software (for example, a Linux machine running Linux Virtual Services).
- IP connectivity is established between different Access Manager components. Because the components can be in different private networks, you can use NAT, VPNs, or combination of both to achieve connectivity.

Customer Network Setup

- A server configured with an LDAP directory (eDirectory 8.8.8.8 or later, Sun ONE, or Active Directory) that contains your system users. Identity Server uses the LDAP directory to authenticate users to the system.
- Domain name server, which resolves DNS names to IP addresses and which has reverse lookups enabled.
  Access Manager devices communicate to each other by their IP addresses, and some requests require them to match an IP address with the device's DNS name. Without reverse lookups enabled, these requests fail. In particular, Identity Servers perform reverse lookups to their user stores. If reverse lookups are not available, host table entries can be used.
- Obtain Static IP addresses for Administration Console, Identity Server, and Analytics Server or Sentinel. If the IP address of the machine changes, Access Manager components on that machine cannot start.
- IP connectivity is established between different Access Manager components. Because the components can be in different private networks, you can use NAT, VPNs, or combination of both to achieve connectivity.
1.7.2 Network Setup Flow Chart

Figure 1-9 provides the setup information about installing Access Manager components and configuring NAT in a multi-tenant or service provider network.

Figure 1-9 Network Setup Flow Chart

1.7.3 Installing Access Manager Components in NAT Environments

Installing Access Manager in the NAT environment consists of the following steps:

1. “Installing Administration Console” on page 27.
2. “Configuring Global Settings” on page 28
3. “Installing Identity Server” on page 57
4. “Installing Access Gateway” on page 69

1.7.3.1 Installing Administration Console

For installation requirements, see “Installing Administration Console” on page 45.

1 Before installing Access Manager components, check the network connectivity across these machines.
2 Verify the link latency and ensure that it is less than 100 milliseconds.
If the link latency is greater than 100ms, it might lead to performance degradation.

3 Synchronize time across all Access Manager components.

The primary Administration Console should be configured to synchronize time with the corporate Network Time Protocol (NTP) server. The remaining machines should be configured to synchronize time with the primary Administration Console.

3a Configure the NTP server in the `/etc/ntp.conf` file.
   
   For information about how to configure the NTP server, see Configuring NTP (https://support.ntp.org/bin/view/Support/ConfiguringNTP).

3b Run the following commands on the primary Administration Console to start the NTP server:
   
   ```
   systemctl start ntpd
   systemctl enable ntpd
   ```

3c Run the `ntpd pool.ntp.org` command on the primary Administration Console to synchronize devices.

   **NOTE:** The ntpd process must be running to keep the time in sync among devices.

4 Install the primary Administration Consoles by providing the listening IP address for the primary Administration Console.

   For more information about installing Administration Console, see the “Installing Administration Console on Windows” on page 52.

5 Install the secondary Administration Console and repeat the above procedures for secondary Administration Console IP address.

6 Continue with Section 1.7.3.2, “Configuring Global Settings,” on page 28 to add both the primary and secondary Administration Consoles to the Global Settings configuration.

1.7.3.2 Configuring Global Settings

You need to map the private IP address of Administration Console and to the public NAT IP address. You need to specify the NAT IP addresses before importing Identity Server and Access Gateway. You need to specify the NAT IP Addresses prior to importing devices. The devices that cannot reach the Private Administration Console IP address will use the NAT IP address.

1 Log in to Administration Console.

2 Select Access Manager > Global Settings.

3 Click New.

4 Select Administration Console Listening IP address from the drop-down list.

5 Specify the corresponding Public NAT IP address.

   If you do not specify a Public NAT IP address or if a mapping already exists for the selected Administration Console IP address, the following message is displayed:

   IP Address is not valid

6 Click OK to continue and apply the configuration changes.
1.7.3.3 Installing and Configuring Identity Server

For information about how to install Identity Server, see “Installing Identity Server” on page 57.

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

For information about how to configure Identity Server, see Configuring Identity Servers Clusters in the Access Manager 4.5 Administration Guide.

1.7.3.4 Installing and Configuring Access Gateway

For information about how to install Access Gateway, see “Installing Access Gateway” on page 69.

When you are setting up Access Gateway to protect web resources, you create and configure reverse proxies, proxy services, and protected resources. The authentication contract, authentication procedure, Authorization policy, Identity Injection policy, and Form Fill policy are configured at the resource level so that you can enable exactly what the resource requires.

For information about configuring Access Gateway, see Configuring Access Gateway in the Access Manager 4.5 Administration Guide.

1.7.4 Configuring Network Address Translation

You can configure Access Manager by using Network Address Translation (NAT). NAT enables the communication between Administration Console from local network to other Access Manager devices such as Identity Server and Access Gateway. The devices can be in the external network or in another private network. You must configure the NAT address in the router.

See your router documentation for more information.

- Section 1.7.4.1, “Configuring Administration Console Behind NAT,” on page 29
- Section 1.7.4.2, “Configuring Identity Server and Access Gateway Behind NAT,” on page 30

1.7.4.1 Configuring Administration Console Behind NAT

1 Log in to Administration Console.
2 Go to Access Manager > Global Settings, then click New.
3 Select an IP address from the Administration Console Public IP Address list.
   This list contains primary and secondary Administration Console IP addresses.
4 Enter the respective NAT IP address for primary and secondary Administration Console in Public NAT IP Address.

**NOTE:** If the NAT IP address is not provided or if a mapping exists for the selected Administration Console IP, a message **IP Address is not valid** is displayed.

5 Click OK.
   Administration Console NAT IP is shared to other Access Manager devices.
For more information about configuring NAT, see Mapping the Private IP Address to Public IP Address in the Access Manager 4.5 Administration Guide.

### 1.7.4.2 Configuring Identity Server and Access Gateway Behind NAT

During installation, the system prompts the following message to specify the NAT address for the component:

**Is local NAT available for the <device name> y/n? [n]:**

Enter **Y** and specify the NAT address. This enables Administration Console to use this NAT address when communicating to this device.

Alternatively, if the device is already installed, then run the `reimport_nidp.sh` or `reimport_ags.sh` script to specify the NAT address.

### 1.8 Setting Up Firewalls

It is recommended to use Access Manager with firewalls. Figure 1-10 illustrates a simple firewall setup for a basic Access Manager configuration of an Identity Server, an Access Gateway, and an Administration Console. This is one of many possible configurations.

**Figure 1-10 Access Manager Components between Firewalls**

The first firewall separates Access Manager from the Internet, allowing browsers to access the resources through specific ports. The second firewall separates Access Manager components from web servers they are protecting and from Administration Console.

This section describes the following topics:

- Section 1.8.1, “Required Ports,” on page 31
- Section 1.8.3, “Sample Configurations,” on page 38
### 1.8.1 Required Ports

**List of Tables**

- Table 1-2, “When a Firewall Separates an Access Manager Component from a Global Service,” on page 31
- Table 1-3, “When a Firewall Separates Administration Console from a Component,” on page 32
- Table 1-4, “When a Firewall Separates Identity Server from a Component,” on page 33
- Table 1-5, “When a Firewall Separates Access Gateway from a Component,” on page 34
- Table 1-6, “When a Firewall Separates Analytics Server from Administration Console or any Services,” on page 36
- Table 1-7, “Administration Console on Cloud,” on page 36
- Table 1-8, “Identity Server on Cloud,” on page 37
- Table 1-9, “Access Gateway on Cloud,” on page 37

**Table 1-2 When a Firewall Separates an Access Manager Component from a Global Service**

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP Server</td>
<td>UDP 123</td>
<td>Access Manager components must have time synchronized else the authentication fails. It is recommended to configure all components to use an network time protocol (NTP) server. Depending upon where your NTP server is located, you might need to open UDP 123, so that Access Manager components can use the NTP server.</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>UDP 53</td>
<td>Access Manager components must be able to resolve DNS names. Depending upon where your DNS servers are located, you might need to open UDP 53, so that Access Manager components can resolve DNS names.</td>
</tr>
<tr>
<td>Remote Linux Administration Workstation</td>
<td>TCP 22</td>
<td>If you want to use SSH for remote administration of Access Manager components, open TCP 22 to allow.</td>
</tr>
<tr>
<td>Remote Windows Administration Workstation</td>
<td>Configurable</td>
<td>If you want to use RDP or VNC for remote administration of Access Manager components, open the ports required by your application from the remote administration workstation to your Access Manager components. You need to open ports for console access and for file sharing. For console access, VNC usually uses TCP 5901 and RDP uses TCP 3389. For file sharing, UDP 135-139 are the default ports.</td>
</tr>
</tbody>
</table>
### Table 1-3 When a Firewall Separates Administration Console from a Component

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Gateway, Identity Server</td>
<td>TCP 1443</td>
<td>For communication from Administration Console to devices.</td>
</tr>
<tr>
<td></td>
<td>TCP 8444</td>
<td>For communication from devices to Administration Console.</td>
</tr>
<tr>
<td></td>
<td>TCP 1290</td>
<td>For communication from devices to the Syslog server on Administration Console.</td>
</tr>
<tr>
<td></td>
<td>TCP 524</td>
<td>For NCP certificate management with NPKI. Open this port so that both the device and Administration Console can use the port.</td>
</tr>
<tr>
<td></td>
<td>TCP 636</td>
<td>For secure LDAP communication from devices to Administration Console.</td>
</tr>
<tr>
<td></td>
<td>HTTP 2443</td>
<td>For the installer to communicate with Administration Console. You can close these port after installation is complete.</td>
</tr>
<tr>
<td></td>
<td>HTTP 8443</td>
<td></td>
</tr>
<tr>
<td>Importing an Access Gateway Appliance</td>
<td>ICMP</td>
<td>During an import, Access Gateway Appliance sends two pings through ICMP to Administration Console. When the import has finished, you can disable the ICMP echo requests and echo replies.</td>
</tr>
<tr>
<td>LDAP User Store</td>
<td>TCP 524</td>
<td>Required only if the user store is eDirectory. When configuring a new eDirectory user store, NCP is used to enable Novell SecretStore by adding a SAML authentication method and storing a public key for Administration Console. It is not used in day-to-day operations.</td>
</tr>
<tr>
<td></td>
<td>TCP 636</td>
<td>For secure LDAP communication from Administration Console to user store.</td>
</tr>
<tr>
<td>Administration Console</td>
<td>TCP 524</td>
<td>Required to synchronize the configuration data store.</td>
</tr>
<tr>
<td></td>
<td>TCP 636</td>
<td>Required for the secure LDAP communication.</td>
</tr>
<tr>
<td></td>
<td>TCP 8080, 8443</td>
<td>Used for the Tomcat communication.</td>
</tr>
<tr>
<td></td>
<td>TCP 705</td>
<td>Used by Sub Agent-Master Agent communication inside Administration Console.</td>
</tr>
<tr>
<td></td>
<td>UDP 161</td>
<td>Used for communication by an external Network Monitoring System with Administration Console by using SNMP.</td>
</tr>
<tr>
<td>Component</td>
<td>Port</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Browsers</td>
<td>TCP 8080</td>
<td>For HTTP communication from browsers to Administration Console.</td>
</tr>
<tr>
<td></td>
<td>TCP 8443, 2443, 2080</td>
<td>For HTTPS communication from browsers to Administration Console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> 2443 and 2080 are optional ports required when Administration Console and Identity Server are collocated.</td>
</tr>
<tr>
<td></td>
<td>TCP 8028, 8030</td>
<td>To use iMonitor or DSTrace from a client to view information about the configuration store on Administration Console.</td>
</tr>
<tr>
<td>Access Gateway</td>
<td>TCP 8080 or 8443</td>
<td>For authentication communication from Access Gateway to Identity Server. The default ports for Identity Server are TCP 8080 and 8443. They are configurable. You need to open the port that you configured for the base URL of Identity Server.</td>
</tr>
<tr>
<td></td>
<td>TCP 80 or 443</td>
<td>For communication from Identity Server to ESP of Access Gateway. This is the reverse proxy port that is assigned to be ESP (see the Reverse Proxy / Authentication page). This is usually port 80 or 443.</td>
</tr>
<tr>
<td>Administration Console</td>
<td>TCP 1443</td>
<td>For communication from Administration Console to devices. This is configurable.</td>
</tr>
<tr>
<td></td>
<td>TCP 8444</td>
<td>For communication from Identity Server to Administration Console.</td>
</tr>
<tr>
<td></td>
<td>TCP 1290</td>
<td>For communication from devices to the Syslog server on Administration Console.</td>
</tr>
<tr>
<td></td>
<td>TCP 524</td>
<td>For NCP certificate management with NPKI from Identity Server to Administration Console.</td>
</tr>
<tr>
<td></td>
<td>TCP 636</td>
<td>For the secure LDAP communication from Identity Server to Administration Console.</td>
</tr>
<tr>
<td>Identity Server</td>
<td>TCP 8443 or 443</td>
<td>For HTTPS communication. You can use iptables to configure this for TCP 443. See Section 3.5, “Translating Identity Server Configuration Port,” on page 63.</td>
</tr>
<tr>
<td></td>
<td>TCP 7801</td>
<td>For back-channel communication with cluster members.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This port is configurable.</td>
</tr>
<tr>
<td>LDAP User Stores</td>
<td>TCP 636</td>
<td>For secure LDAP communication from Identity Server to the LDAP user store.</td>
</tr>
</tbody>
</table>

*Table 1-4  When a Firewall Separates Identity Server from a Component*
<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Providers</td>
<td>TCP 8445</td>
<td>If you have enabled identity provider introductions, open a port to allow HTTPS communication from the user’s browser to the service provider.</td>
</tr>
<tr>
<td></td>
<td>TCP 8446</td>
<td>If you have enabled identity provider introductions, open a port to allow HTTPS communication from the user’s browser to the service consumer.</td>
</tr>
<tr>
<td>Browsers</td>
<td>TCP 8080</td>
<td>For HTTP communication from a browser to Identity Server. You can use iptables to configure this for TCP 80. See Section 3.5, “Translating Identity Server Configuration Port,” on page 63.</td>
</tr>
<tr>
<td></td>
<td>TCP 8443</td>
<td>For HTTPS communication from a browser to Identity Server. You can use iptables to configure this for TCP 443. See Section 3.5, “Translating Identity Server Configuration Port,” on page 63.</td>
</tr>
<tr>
<td>CRL and OCSP Servers</td>
<td>Configurable</td>
<td>If you are using x.509 certificates that include an AIA or CRL Distribution Point attribute, you need to open the port required to talk to that server. Ports 80/443 are the most common ports, but the LDAP ports 389/636 can also be used.</td>
</tr>
<tr>
<td>Active Directory Server with Kerberos</td>
<td>TCP 88, UDP 88</td>
<td>For communication with KDC on the Active Directory Server for Kerberos authentication.</td>
</tr>
</tbody>
</table>

Table 1-5  When a Firewall Separates Access Gateway from a Component

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Server</td>
<td>TCP 8080 or 8443</td>
<td>For authentication communication from Access Gateway to Identity Server. The default ports are TCP 8080 and 8443, which are configurable. You need to open the port of the base URL of Identity Server.</td>
</tr>
<tr>
<td></td>
<td>TCP 80 or 443</td>
<td>For communication from Identity Server to ESP of Access Gateway. This is the reverse proxy port that is assigned to be ESP (see the Reverse Proxy / Authentication page). This is usually port 80 or 443.</td>
</tr>
<tr>
<td>Administration Console</td>
<td>TCP 1443</td>
<td>For communication from Administration Console to Access Gateway. This is configurable.</td>
</tr>
<tr>
<td></td>
<td>TCP 8444</td>
<td>For communication from Access Gateway to Administration Console.</td>
</tr>
<tr>
<td></td>
<td>TCP 1290</td>
<td>For communication from devices to the Syslog server on Administration Console.</td>
</tr>
<tr>
<td></td>
<td>TCP 524</td>
<td>For NCP certificate management with NPKI from Access Gateway to Administration Console.</td>
</tr>
<tr>
<td></td>
<td>TCP 636</td>
<td>For secure LDAP communication from Access Gateway to Administration Console.</td>
</tr>
<tr>
<td>Component</td>
<td>Port</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Access Gateway</td>
<td>TCP 7801</td>
<td>For back-channel communication with cluster members.</td>
</tr>
<tr>
<td></td>
<td>TCP 80 or 443</td>
<td>For communication among Embedded Service Providers (ESP) of the Access Gateway cluster members. This is the reverse proxy port that is assigned to be ESP (see the Reverse Proxy / Authentication page). This is usually port 80 or 443. This port is configurable.</td>
</tr>
<tr>
<td>Access Gateway Appliance Configuration console</td>
<td>TCP 9090 or 9443</td>
<td>For using the Jetty service on the appliance Configuration console. For more information about the Configuration console, see Section 4.2.3, “Configuring Access Gateway Appliance,” on page 73.</td>
</tr>
<tr>
<td></td>
<td>TCP 1099</td>
<td>For the Java RMI communication.</td>
</tr>
<tr>
<td>Browsers/Clients</td>
<td>TCP 80</td>
<td>For HTTP communication from the client to Access Gateway. This is configurable.</td>
</tr>
<tr>
<td></td>
<td>TCP 443</td>
<td>For HTTPS communication from the client to Access Gateway. This is configurable.</td>
</tr>
<tr>
<td>Web Servers</td>
<td>TCP 80</td>
<td>For HTTP communication from Access Gateway to web servers. This is configurable.</td>
</tr>
<tr>
<td></td>
<td>TCP 443</td>
<td>For HTTPS communication from Access Gateway to web servers. This is configurable.</td>
</tr>
</tbody>
</table>
### Table 1-6  When a Firewall Separates Analytics Server from Administration Console or any Services

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration Console</td>
<td>TCP 1444</td>
<td>For communication between Administration Console and Analytics Server.</td>
</tr>
<tr>
<td>Browsers</td>
<td>TCP 8445</td>
<td>For HTTPS communication with Analytics Server for Analytics Dashboard.</td>
</tr>
<tr>
<td>Browsers</td>
<td>TCP 8443</td>
<td>For HTTPS communication with Analytics Server for Reports console.</td>
</tr>
<tr>
<td>Syslog</td>
<td>TCP 1468</td>
<td>For sending Syslog messages from Access Manager components to Analytics Server.</td>
</tr>
<tr>
<td>Control Center</td>
<td>TCP 10013</td>
<td>For communicating from a computer to the control center on Analytics Server.</td>
</tr>
<tr>
<td>Remote Linux Administration</td>
<td>TCP 22</td>
<td>For communication from your remote administration workstation to Analytics Server.</td>
</tr>
<tr>
<td>Workstation</td>
<td>TCP 22</td>
<td>For communication from your remote administration workstation to Analytics Server.</td>
</tr>
<tr>
<td>High availability configuration</td>
<td>TCP 7360</td>
<td>For communication between the servers in an Analytics Server cluster.</td>
</tr>
</tbody>
</table>

**NOTE:** On SLES, you can use YaST to configure UDP ports and internal networks.

Table 1-7, Table 1-8, and Table 1-9 are intended for use in configuring the security groups in cloud deployments. The security groups by default do not restrict the outbound ports. Therefore, these tables include only the inbound ports.

### Table 1-7  Administration Console on Cloud

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Traffic Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Gateway, Identity Server</td>
<td>TCP 1290</td>
<td>Inbound</td>
<td>For communication from devices to the Syslog server on Administration Console.</td>
</tr>
<tr>
<td></td>
<td>TCP 8443</td>
<td>Inbound</td>
<td>For the installer to communicate with Administration Console.</td>
</tr>
<tr>
<td></td>
<td>TCP 8444</td>
<td>Inbound</td>
<td>For communication from devices to Administration Console.</td>
</tr>
<tr>
<td></td>
<td>TCP 524</td>
<td>Inbound</td>
<td>For NCP certificate management with NPKI. Open this port so that both the device and Administration Console can use the port.</td>
</tr>
<tr>
<td></td>
<td>TCP 636</td>
<td>Inbound</td>
<td>For secure LDAP communication from devices to Administration Console.</td>
</tr>
<tr>
<td>Access Gateway</td>
<td>TCP 1289</td>
<td>Inbound</td>
<td>For importing Access Gateway into Administration Console.</td>
</tr>
<tr>
<td>SSH</td>
<td>TCP 22</td>
<td>Inbound</td>
<td>For accessing Administration Console using SSH.</td>
</tr>
<tr>
<td>Access Gateway</td>
<td>ICMP</td>
<td>Inbound</td>
<td>For importing Access Gateway.</td>
</tr>
</tbody>
</table>
### Table 1-8  Identity Server on Cloud

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Traffic Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration Console</td>
<td>TCP 1443</td>
<td>Inbound</td>
<td>For communication from Administration Console to devices. This is configurable.</td>
</tr>
<tr>
<td></td>
<td>TCP 524</td>
<td>Inbound</td>
<td>For NCP certificate management with NPKI from Identity Server to Administration Console.</td>
</tr>
<tr>
<td>Identity Server</td>
<td>TCP 7801</td>
<td>Inbound</td>
<td>For the back-channel communication with cluster members. This port is configurable.</td>
</tr>
<tr>
<td>SSH</td>
<td>TCP 22</td>
<td>Inbound</td>
<td>For accessing Identity Server using SSH.</td>
</tr>
<tr>
<td>Access Gateway, Browsers</td>
<td>TCP 8443</td>
<td>Inbound</td>
<td>For authentication communication from Access Gateway to Identity Server. For HTTPS communication from a browser to Identity Server's base URL when the default ports are used.</td>
</tr>
</tbody>
</table>

### Table 1-9  Access Gateway on Cloud

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Traffic Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Providers</td>
<td>TCP 8445</td>
<td>Inbound</td>
<td>If you have enabled identity provider introductions, open a port to allow HTTPS communication from the user’s browser to the service provider.</td>
</tr>
<tr>
<td></td>
<td>TCP 8446</td>
<td>Inbound</td>
<td>If you have enabled identity provider introductions, open a port to allow HTTPS communication from the user’s browser to the service consumer.</td>
</tr>
<tr>
<td>Access Gateway</td>
<td>TCP 7801</td>
<td>Inbound</td>
<td>For back-channel communication with cluster members.</td>
</tr>
<tr>
<td>Administration Console</td>
<td>TCP 1443</td>
<td>Inbound</td>
<td>For communication from Administration Console to Access Gateway. This is configurable.</td>
</tr>
<tr>
<td>SSH</td>
<td>TCP 22</td>
<td>Inbound</td>
<td>For accessing Administration Console using SSH.</td>
</tr>
<tr>
<td>Identity Server</td>
<td>TCP 80 or 443</td>
<td>Inbound</td>
<td>For communication from Identity Server to Access Gateway ESP. This is the reverse proxy port that is assigned to be ESP.</td>
</tr>
<tr>
<td>Browsers/Clients</td>
<td>TCP 443</td>
<td>Inbound</td>
<td>For HTTPS communication from workstation browsers to Access Gateway.</td>
</tr>
<tr>
<td></td>
<td>TCP 80</td>
<td>Inbound</td>
<td>For HTTP communication from workstation browsers to Access Gateway.</td>
</tr>
</tbody>
</table>
1.8.2 Restricted Ports

The following ports are reserved for internal use only and other applications should not use these ports:

22
111
524
1443
2443
3443
8028
8030
8080
8443
8444
9000
9001
55982
61222
61613
61616
61617
9443
9090

If required, use port redirection by using IP tables.

1.8.3 Sample Configurations

- Section 1.8.3.1, “Access Gateway and Identity Server in DMZ,” on page 38
- Section 1.8.3.2, “A Firewall Separating Access Manager Components from the LDAP Servers,” on page 40

1.8.3.1 Access Gateway and Identity Server in DMZ

- “First Firewall” on page 38
- “Second Firewall” on page 39

First Firewall

If you place a firewall between browsers and Access Gateway and Identity Server, you need to open ports so that browsers can communicate with Access Gateway and Identity Server and Identity Server can communicate with other identity providers.

See, Figure 1-10 on page 30
### Table 1-10  Ports to Open in the First Firewall

<table>
<thead>
<tr>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 80</td>
<td>For HTTP communication.</td>
</tr>
<tr>
<td>TCP 443</td>
<td>For HTTPS communication.</td>
</tr>
<tr>
<td>TCP 8080</td>
<td>For HTTP communication with Identity Server.</td>
</tr>
<tr>
<td></td>
<td>For information about redirecting Identity Server to use port 80, see Section 3.5, “Translating Identity Server Configuration Port,” on page 63.</td>
</tr>
<tr>
<td>TCP 8443</td>
<td>For HTTPS communication with Identity Server.</td>
</tr>
<tr>
<td></td>
<td>For information about redirecting Identity Server to use port 443, see Section 3.5, “Translating Identity Server Configuration Port,” on page 63.</td>
</tr>
<tr>
<td>TCP 8445</td>
<td>For HTTP Identity Provider introductions. If you do not enable Identity Provider introductions, you do not need to open this port.</td>
</tr>
<tr>
<td>TCP 8446</td>
<td>For HTTPS Identity Provider introductions. If you do not enable Identity Provider introductions, you do not need to open this port.</td>
</tr>
</tbody>
</table>

### Second Firewall

The second firewall separates web servers, LDAP servers, and Administration Console from Identity Server and Access Gateway. You need the following ports opened in the second firewall:

### Table 1-11  Ports to Open in the Second Firewall

<table>
<thead>
<tr>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 80</td>
<td>For HTTP communication with web servers.</td>
</tr>
<tr>
<td>TCP 443</td>
<td>For HTTPS communication with web servers.</td>
</tr>
<tr>
<td>TCP 1443</td>
<td>For communication from Administration Console to the devices.</td>
</tr>
<tr>
<td>TCP 8444</td>
<td>For communication from the devices to Administration Console.</td>
</tr>
<tr>
<td>TCP 1290</td>
<td>For communication from the devices to the Syslog server installed on Administration Console. If you do not enable auditing, you do not need to open this port.</td>
</tr>
<tr>
<td>TCP 524</td>
<td>For NCP certificate management in NPKI. The port needs to be opened so that both the device and Administration Console can use the port.</td>
</tr>
<tr>
<td>TCP 636</td>
<td>For secure LDAP communication of configuration information.</td>
</tr>
</tbody>
</table>
1.8.3.2 A Firewall Separating Access Manager Components from the LDAP Servers

You can configure Access Manager components so that your Administration Console is on the same side of the firewall as your Access Manager components and have a firewall between them and the LDAP servers.

Figure 1-11 A Firewall Separating Administration Console and the LDAP Server

In this configuration, you need to open the following ports in the second firewall for Administration Console and Identity Server:

<table>
<thead>
<tr>
<th>Ports</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 636</td>
<td>For secure LDAP communication. This is used by Identity Server and Administration Console.</td>
</tr>
<tr>
<td>TCP 524</td>
<td>For configuring eDirectory as a new User Store. NCP is used to enable SecretStore by adding a SAML authentication method and storing a public key for Administration Console. During day-to-day operations, this port is not used. If your LDAP server is Active Directory or Sun ONE, this port does not need to be opened.</td>
</tr>
</tbody>
</table>

1.9 Using Certificates for Secure Communication

When you install Administration Console, the following test certificates are automatically generated:

test-signing

test-encryption

test-connector

test-provider

test-consumer

test-stunnel
For strong security, it is recommended that you replace these certificates, except the test-stunnel certificate, with certificates from a well-known certificate authority.

For more information, see “Strengthening Certificates” in the NetIQ Access Manager 4.5 Security Guide.

### 1.10 Protecting an Identity Server Through Access Gateway

For security reasons, you might want to set up your Access Manager configuration so that Identity Server is a resource protected by an Access Gateway. This configuration reduces the number of ports you need to open between the outside world and your network. Figure 1-12 illustrates such a configuration.

*Figure 1-12  Identity Servers behind an Access Gateway*

With this configuration, you need an L4 switch to cluster Access Gateways. However, you do not need an L4 switch to cluster Identity Servers. When Identity Server is configured to be a protected resource of Access Gateway, Access Gateway uses its web server communication channel. Each Identity Server in the cluster must be added to the web server list, and Access Gateway uses its web server load balancing and failover policies for the clustered Identity Servers.

**Limitations:** The following features are not supported with this configuration:

- Identity Server cannot respond to Identity Provider introductions.
- Federation to an external service provider that requires the artifact profile with SOAP/Mutual SSL binding cannot be supported with this configuration.
- The proxy service that is protecting Identity Server cannot be configured to use mutual SSL. For example with this configuration, X.509 authentication cannot be used for any proxy service. To perform X.509 authentication (which is a form of mutual SSL), a user's browser must have direct access to Identity Server.
- The proxy service that is protecting Identity Server cannot be configured to use NMAS.

For configuration details, see Configuring a Protected Identity Server Through Access Gateways in the Access Manager 4.5 Administration Guide.
Installing Access Manager

Before you start installation, evaluate how you want to implement Access Manager. You can install components on a single server (excluding Analytics Server) or on separate servers. For more information about installing other components, see Chapter 1, “Planning Your Access Manager Environment,” on page 11.

The following is the sequence of installing Access Manager components:

1. Administration Console
2. Identity Server
3. Access Gateway
4. Analytics Server

This section includes the following topics:

- Chapter 2, “Installing Administration Console,” on page 45
- Chapter 3, “Installing Identity Server,” on page 57
- Chapter 4, “Installing Access Gateway,” on page 69
- Chapter 5, “Installing Analytics Server,” on page 85
- Chapter 6, “Deploying Access Manager on Amazon Web Services EC2,” on page 101
- Chapter 7, “Deploying Access Manager on Microsoft Azure,” on page 123
- Chapter 8, “Installing Packages and Dependent RPMs on RHEL for Access Manager,” on page 137
- Chapter 9, “Uninstalling Components,” on page 141

This section includes the following topics:

- Chapter 2, “Installing Administration Console,” on page 45
- Chapter 3, “Installing Identity Server,” on page 57
- Chapter 4, “Installing Access Gateway,” on page 69
- Chapter 5, “Installing Analytics Server,” on page 85
- Chapter 6, “Deploying Access Manager on Amazon Web Services EC2,” on page 101
- Chapter 7, “Deploying Access Manager on Microsoft Azure,” on page 123
- Chapter 8, “Installing Packages and Dependent RPMs on RHEL for Access Manager,” on page 137
- Chapter 9, “Uninstalling Components,” on page 141
2 Installing Administration Console

Administration Console must be installed before you install any other Access Manager devices. If iManager is installed for other products, you still need to install this version on a separate server. Administration Console is installed with an embedded version of eDirectory, which is used as the configuration store for Access Manager.

For a functioning system, you need Administration Console for configuration and management, Identity Server for authentication, and Access Gateway for protecting resources.

After you install Administration Console, the installation scripts for other components (Identity Server and Access Gateway) auto-import their configurations into Administration Console.

This chapter includes the following topics:

- Section 2.1, “Installing Administration Console on Linux,” on page 45
- Section 2.2, “Installing Administration Console on Windows,” on page 52
- Section 2.3, “Logging In to Administration Console,” on page 54
- Section 2.4, “Enabling Administration Console for Multiple Network Interface Cards,” on page 55

For information about installing a secondary Administration Console and fault tolerance, see Installing Secondary Administration Console in the Access Manager 4.5 Administration Guide.

2.1 Installing Administration Console on Linux

**IMPORTANT:** The eDirectory DIB within the Administration Console installation is not supported in a B-tree file system (BTRFS). If your Administration Console system uses BTRFS, create a separate mount point using XFS or ext4 that mounts automatically at /var/opt/novell/eDirectory to meet this requirement. For more information, see eDirectory documentation (https://www.netiq.com/documentation/edirectory-9/edir_install/data/a79kg0t.html).

- Section 2.1.1, “System Requirements on Linux,” on page 45
- Section 2.1.2, “Installation Procedure,” on page 48

2.1.1 System Requirements on Linux

- 4 GB RAM
- Dual CPU or Core (3.0 GHz or comparable chip)
- 100 GB hard disk

The hard disk must have ample space for logging in a production environment. This disk space must be in the local server not in the remote server.
If you have custom partitioned your hard disk as follows, ensure that you have allocated the minimum space for each partition as mentioned in the following table:

<table>
<thead>
<tr>
<th>Partition</th>
<th>Minimum Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/novell</td>
<td>1 GB</td>
</tr>
<tr>
<td>/opt/volera</td>
<td>5 MB</td>
</tr>
<tr>
<td>/var/opt/novell</td>
<td>1 GB</td>
</tr>
<tr>
<td>/var</td>
<td>512 MB</td>
</tr>
<tr>
<td>/usr</td>
<td>25 MB</td>
</tr>
<tr>
<td>/etc</td>
<td>1 MB</td>
</tr>
<tr>
<td>/tmp/novell_access_manager</td>
<td>10 MB</td>
</tr>
<tr>
<td>/tmp</td>
<td>10 MB</td>
</tr>
<tr>
<td>/</td>
<td>512 MB</td>
</tr>
</tbody>
</table>

You can perform the disk partitioning based on your requirement. For example, consider a scenario where an administrator is installing Access Manager with 100 GB disk space. The administrator wants to allocate enough space for the logs from the available space. Therefore, the administrator can partition the hard disk as follows:

<table>
<thead>
<tr>
<th>Partition</th>
<th>Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt</td>
<td>5 GB</td>
</tr>
<tr>
<td>/var</td>
<td>30 GB</td>
</tr>
<tr>
<td>/tmp</td>
<td>2 GB</td>
</tr>
<tr>
<td>/</td>
<td>63 GB</td>
</tr>
</tbody>
</table>

One of the following operating systems:
- SUSE Linux Enterprise Server (SLES) 12 SP3 or SLES 12 SP4 with 64-bit operating system x86-64 hardware (physical or virtual).

Ensure that the following packages are installed:

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>perl-gettext, gettext-runtime</td>
<td>The required library and tools to create and maintain message catalogs.</td>
</tr>
<tr>
<td>python</td>
<td>The basic Python library.</td>
</tr>
</tbody>
</table>
Installing Administration Console

- Red Hat Enterprise Linux (RHEL) 6.10 or RHEL 7.6 (64-bit) (physical or virtual). RHEL 7.7 (Applicable for Access Manager 4.5 SP1 and later).

For installing the RHEL packages, see Appendix 8, “Installing Packages and Dependent RPMs on RHEL for Access Manager,” on page 137.

**NOTE:** You can select to install these RPMs automatically along with Access Manager installation. While installing Access Manager, specify N when you get the following prompt:

```
Enter the local mount directory if you have the OS ISO mounted locally. This will be used as the local catalog for the additional rpms.
Do you have a locally mounted ISO (y/n)?
```

The Access Manager installer checks the online catalog and then installs the required RPMs automatically.

- The latest `net-snmp` package from the SLES or RedHat update channel is installed.
- Zip and unzip utilities is available for the backup and restore procedure.
- Ports 389 and 636 are open.
- Static IP addresses.
  - If the IP address changes after devices have been imported, these devices can no longer communicate with Administration Console.
- The tree for the configuration store is named after the server on which you install Administration Console. Check the hostname and rename the machine if the name is not appropriate for a configuration tree name.

**Browser Support**

- Mozilla Firefox 66.0.2
- Google Chrome 73.0.3683.86

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>compat</td>
<td>Libraries to address compatibility issues. For information about enabling this repository, see TID 7004701 (<a href="http://www.novell.com/support/php/search.do?cmd=displayKC&amp;docType=kc&amp;externalId=7004701&amp;sliceId=1&amp;docTypeID=DT_TID_1_1&amp;dialogID=68926420&amp;stateId=0%2020130264119">http://www.novell.com/support/php/search.do?cmd=displayKC&amp;docType=kc&amp;externalId=7004701&amp;sliceId=1&amp;docTypeID=DT_TID_1_1&amp;dialogID=68926420&amp;stateId=0%2020130264119</a>)</td>
</tr>
</tbody>
</table>

Use the following command to verify:
```
rpm -qa | grep <package name>
```

Use YaST to install the packages.

- The latest `net-snmp` package from the SLES or RedHat update channel is installed.
- Zip and unzip utilities is available for the backup and restore procedure.
- Ports 389 and 636 are open.
- Static IP addresses.
  - If the IP address changes after devices have been imported, these devices can no longer communicate with Administration Console.
- The tree for the configuration store is named after the server on which you install Administration Console. Check the hostname and rename the machine if the name is not appropriate for a configuration tree name.

**Browser Support**

- Mozilla Firefox 66.0.2
- Google Chrome 73.0.3683.86
• Microsoft Edge 42.17134.1.0/ EdgeHTML 17.17134
• Internet Explorer 11.648.17134.0 Update Versions 11.0.115 (KB4489873)

Browser pop-ups must be enabled to use Administration Console.

**Network Requirements**


**IMPORTANT:** You cannot install the following software with Administration Console:

• OpenLDAP server. If it is installed, uninstall it. If you do not want to uninstall it, ensure that it does not use the port 636 or does not bind the port 389 to localhost.

• The LDAP software such as eDirectory.

• Other version of iManager.

  In addition, you cannot add other iManager product plug-ins to this Administration Console.

• You cannot install Access Manager on a Linux User Management (LUM) machine because of library update conflicts.

• JRE. If it is installed, uninstall it.

2.1.2 **Installation Procedure**

Installation time: about 20 minutes.

<table>
<thead>
<tr>
<th>What you need to create during installation</th>
<th>A username and password for the Administrator.</th>
</tr>
</thead>
</table>

**IMPORTANT:** If Administration Console and Identity Server are installed on different servers, both use 8080 and 8443 ports. If Administration Console and Identity Server are installed on the same server, Identity Server uses 8080 and 8443 ports and Administration Console uses 2080 and 2443 ports.

1. If you have Red Carpet or auto update running, stop these programs before you install Administration Console.

2. Verify that the machine meets the minimum requirements. See Section 2.1.1, “System Requirements on Linux,” on page 45.

3. Open a terminal window.

4. Access the install script as a **root** user:

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

      For software download instructions, see the release-specific Release Notes.

   4b. Do one of the following:

      • Insert the CD into the drive, then navigate to the device. Specify the following:

        ```
        cd /media
        ```

        Change to your CD-ROM drive, which is usually `cdrom` but can be something else such as `cdrecorder` or `dvdrecorder`, depending on your hardware.
If you downloaded the tar.gz file, unzip it by using the following command:

tar -xzvf <filename>

4c Change to the novell-access-manager directory.

5 At the command prompt, specify the following:

./install.sh

Ensure that you have adequate space in the system before you proceed with installation.

6 When you are prompted to install a product, select 1. Install Administration Console and then press Enter.

The system displays an error message if /var uses BTRFS filesystem and the installation is terminated. You can change the filesystem from BTRFS to any other available filesystem, and then try installing.

7 Review and accept the License Agreement.

Novell Base and JDK for NetIQ are installed.

8 (Optional) The installer displays a warning if the host name of the system is mapped to the IP address 127.0.0.2 in the /etc/hosts file:

An entry of 127.0.0.2 in the /etc/hosts file affects the Access Manager functionality. Do you want to proceed with removing it (y/n) [y]

Specify Y to proceed.

The host name mapping to 127.0.0.2 may cause certain Access Manager processes to encounter errors when they attempt to resolve the host name of the machine. To avoid these problems, remove the 127.0.0.2 entry from the /etc/hosts file.

9 Verify that the required rpms are of the latest versions. Specify Y to proceed.

10 Specify the IP address of the local Administrator server.

11 Specify whether this is a primary Administration Console in a failover group. The first Administration Console installed becomes the primary console:

You can install up to three Administration Consoles for replication and failover purposes. If this is not the primary console, you must provide the IP address of the primary Administration Console.

12 Specify the administration username.

Press Enter to use admin as the default admin username, or change this to a username of your choice.

NOTE

- Administration Console username does not accept special characters # (hash), & (ampersand), and () (round brackets).
- If you are installing secondary Administration Console, the username must be from the o=novell container. If the username is from any other container, the Administration Console installation fails.

13 Specify the administration password.

Use alphanumeric characters only.
NOTE: Administration Console password does not accept the : (colon) and " (double quotes) special characters.

14 Confirm the password, then wait for the system to install components. This may take several minutes depending on the speed of your hardware. The following components are installed:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog</td>
<td>Responsible for packaging and forwarding the audit log entries to the configured Syslog Server. For more information, see Auditing in the Access Manager 4.5 Administration Guide.</td>
</tr>
<tr>
<td>Tomcat for NetIQ</td>
<td>NetIQ packaging of the Java-based Tomcat web server used to run servlets and JavaServer Pages (JSP) associated with NetIQ Access Manager web applications.</td>
</tr>
<tr>
<td>Access Manager Configuration Store</td>
<td>An embedded version of eDirectory used to store user-defined server configurations, LDAP attributes, Certificate Authority keys, certificates, and other Access Manager attributes that must be securely stored.</td>
</tr>
<tr>
<td>iManager</td>
<td>The web-based Administration Console that provides customized and secure access to server administration utilities. It is a modified version and cannot be used to manage other eDirectory trees.</td>
</tr>
<tr>
<td>Device Manager</td>
<td></td>
</tr>
<tr>
<td>Administration Console</td>
<td>A modification of iManager that enables management of all aspects of Access Manager. This component is not a standard iManager plug-in. It significantly modifies the tasks that iManager can perform.</td>
</tr>
<tr>
<td>Identity Server Administration Plug-In</td>
<td>Works in conjunction with Administration Console for managing Identity Server.</td>
</tr>
<tr>
<td>REST API Service (AMService)</td>
<td></td>
</tr>
<tr>
<td>Patch Management Tool</td>
<td></td>
</tr>
</tbody>
</table>

15 Record the login URL.

When installation completes, the login URL is displayed. It looks similar to the following:

http://10.10.10.50:8080/nps

Use this to configure Access Manager components.

16 Continue with “Configuring the Linux Administration Console Firewall” on page 51.
2.1.2.1 Configuring the Linux Administration Console Firewall

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

1 Click Computer > YaST > Security and Users > Firewall.
   This launches the Firewall Configuration screen.

2 Click Allowed Services > Advanced.

3 In TCP Ports, specify the ports to open.
   (Conditional) If you are installing Administration Console and Identity Server on different machine, list the following additional ports in TCP Ports:
   - 8080
   - 8443
   - 3080
   - 3443

   (Conditional) If you are installing Administration Console and Identity Server on the same machine, list the following additional ports in TCP Ports:
   - 2080
   - 2443

4 (Conditional) To import an Access Gateway into Administration Console, list the following additional ports in TCP Ports:
   - 1443
   - 8444
   - 1289
   - 1290
   - 524
   - 636

   If you are importing an Access Gateway Appliance, specify icmp in IP Protocols.

   For specific information about the ports listed in Step 3 and Step 4, see Table 1-3 on page 32.

   NOTE: Administration Console is accessible on ports 2080 (HTTP) and 2443 (HTTPs) when Identity Server is installed on the same machine.

5 Restart Tomcat by running the following commands from the Administration Console command line.

   /etc/init.d/novell-ac stop
   /etc/init.d/novell-ac start

6 Continue with Section 2.3, “Logging In to Administration Console,” on page 54.
2.2 Installing Administration Console on Windows

- Section 2.2.1, “System Requirements on Windows,” on page 52
- Section 2.2.2, “Installation Procedure,” on page 52

2.2.1 System Requirements on Windows

- 4 GB RAM
- Dual CPU or Core (3.0 GHz or comparable chip)
- 100 GB hard disk
  The hard disk should have ample space for logging in a production environment. This disk space must be in the local server and not in the remote server.
- Windows Server 2016, 64-bit operating system (physical or virtual), in either Standard or Enterprise Edition, with the latest patches applied.
- Static IP address
- Ports 389 and 636 are open

For information about browser support, see “Browser Support” on page 47.

For information about network requirements, see Section 1.3, “Network Requirements,” on page 19.

2.2.2 Installation Procedure

**IMPORTANT:** Before you start the installation, ensure that Powershell is installed and enabled.

Installation time: about 20 minutes.

<table>
<thead>
<tr>
<th>What you need to create during installation</th>
<th>A username and password for the Administrator.</th>
</tr>
</thead>
</table>

**NOTE:** If Administration Console and Identity Server are installed on different servers, both use 8080 and 8443 ports. If Administration Console and Identity Server are installed on the same server, Identity Server uses 8080 and 8443 ports and Administration Console uses 2080 and 2443 ports.

1. Verify that the machine meets the minimum requirements. See Section 2.2.1, “System Requirements on Windows,” on page 52.
2. Close any running applications and disable any virus scanning programs.
3. (Conditional) To use a remote desktop for installation, use any one of the following:
   - Current version of VNC viewer
   - Microsoft Remote Desktop with the /console switch for Windows XP SP2
   - Microsoft Remote Desktop with the /admin switch for Windows XP SP3
4. Download the ZIP file and extract it.
   For software download instructions and the filename, see the release-specific Release Notes.
5. Double-click the `<ZIP filename>.exe` file from the extracted folder.
6 Read the introduction, then click Next.
7 Accept the license agreement, then click Next.
8 Select Access Manager Administration Console, then click Next.
   If you are installing Identity Server on the same machine, select Access Manager Identity Server.
9 Specify whether this is a primary Administration Console in a failover group, then click Next.
   The first Administration Console installed becomes the primary console.
   You can install up to three Administration Consoles for replication and failover purposes. If this is not the primary console, you must provide the IP address for the primary Administration Console.
10 Specify an administration user ID and password.

   **NOTE:** If you are installing secondary Administration Console, the user ID must be from the o=novell container. If you specify a user from other container, the installer fails to install Administration Console.

11 Specify the static IP address of the machine.
12 Click Install.
   The configuration database takes awhile to install and configure.
13 (Optional) After the installation completes, view the install log file found in the following location:
   \\Program Files\Novell\log\AccessManagerServer_ InstallLog.log
14 Restart the server.

   **IMPORTANT:** You must restart the server before installing any other Access Manager components.

15 Continue with “Configuring the Windows Administration Console Firewall” on page 53.

### 2.2.2.1 Configuring the Windows Administration Console Firewall

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

1 Click Control Panel > Windows Firewall.
2 Click Advanced, then for the Local Area Connection, click Settings.
3 For each port that needs to be opened, click Add, then Specify the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description of service</td>
<td>Specify a name. For example, Admin Console Access for port 8080 or Secure Admin Console Access for port 8443.</td>
</tr>
<tr>
<td>Name or IP address</td>
<td>Specify the IP address of Administration Console.</td>
</tr>
</tbody>
</table>
(Conditional) If you are importing Access Gateway into Administration Console, add the following ports:

- 1443
- 8444
- 1289
- 1290
- 524
- 636

For specific information about the ports listed in Step 3 and Step 4, see Table 1-3 on page 32.

(Conditional) If you are importing an Access Gateway Appliance, click ICMP, select all options, then click OK > OK.

6 Run the following commands to restart Tomcat:

```bash
net stop Tomcat8
net start Tomcat8
```

7 Continue with Section 2.3, “Logging In to Administration Console,” on page 54:

## 2.3 Logging In to Administration Console

Administration Console is a combination of iManager and a device manager. It has been customized for Access Manager so that it can manage the Access Manager components.

**Important points that you must know:**

- You cannot use Administration Console to log in to other eDirectory trees and manage them.
- Do not download and add iManager plug-ins to this customized version. It may result in destroying the Access Manager schema, which can prevent you from managing Access Manager components. This can also prevent communication among the modules.
- Do not start multiple sessions of Administration Console on the same machine through the same browser. Browsers share session information and this can cause unpredictable issues in Administration Console. However, you can start different sessions with different brands of browsers.

Perform the following steps to log in to Administration Console:

1 Enable browser pop-ups.

2 On Administration Console, ensure that ports 8080 and 8443 are open.

   For information, see “Configuring the Linux Administration Console Firewall” on page 51 and “Configuring the Windows Administration Console Firewall” on page 53.
3 From a client machine external to your Administration Console server, launch a browser and specify the Administration Console URL.

Use the IP address established when you installed Administration Console. It includes the application /nps and the following ports:

- 8080 (HTTP) or 8443 (HTTPs): When only Administration Console is installed on the machine.
- 2080 (HTTP) and 2443 (HTTPs): When Identity Server is installed on the same machine.

For example, if the IP address of your Administration Console is 10.10.10.50, specify the following as URL:

http://10.10.10.50:8080/nps

4 Click OK to accept the certificate.

You can select either the permanent or temporary session certificate option.

5 On the Login page, specify the administrator name and password that you defined during Administration Console installation.

6 Click Login. Access Manager Dashboard opens.

For more information about this view or about configuring Administration Console, see Configuring the Default View in the Access Manager 4.5 Administration Guide.

**IMPORTANT:** All configuration and management tasks in the Access Manager documentation assume that you know how to log in to Administration Console.

7 Continue with one of the following:

- Before configuring the system, you need to install other Access Manager components. You need to install at least one Identity Server and one Access Gateway. It is recommended to next install Identity Server. See Chapter 3, “Installing Identity Server,” on page 57.

- If your Administration Console server has multiple interface cards, see “Enabling Administration Console for Multiple Network Interface Cards” on page 55.

**NOTE:** You can provide fault tolerance for the configuration store on Administration Console by installing secondary versions of the console. See “High Availability and Fault Tolerance” in the Access Manager 4.5 Administration Guide.

### 2.4 Enabling Administration Console for Multiple Network Interface Cards

Making Administration Console available for all network interface cards (NICs) is a security risk. However, you might want to allow this situation when, for example, Identity Server has multiple NICs and is also available on all ports.

Perform the following steps to enable Administration Console for Multiple NICs:

1 Open the server.xml file, which is found in the following directory.

   **Linux:** /opt/novell/nam/adminconsole/conf
   
   **Windows Server 2016 R2:** \Program Files\Novell\Tomcat\conf
2 Locate the connector with the `NIDP_Name="connector"` set.

3 Delete the `address` attribute and save the file.
3 Installing Identity Server

Identity Server is the second component you install. You can install it on Linux or Windows.

This chapter includes the following topics:

- Section 3.1, “Prerequisites for Installing Identity Server,” on page 57
- Section 3.2, “Installing Identity Server on Linux,” on page 58
- Section 3.3, “Installing Identity Server on Windows,” on page 61
- Section 3.4, “Verifying Identity Server Installation,” on page 63
- Section 3.5, “Translating Identity Server Configuration Port,” on page 63

3.1 Prerequisites for Installing Identity Server

- If you are installing Access Manager components on multiple machines, ensure that the time and date are synchronized on all machines.
- Ensure that Administration Console is running. See Chapter 2, “Installing Administration Console,” on page 45.
- Do not perform any configuration tasks in Administration Console during an Identity Server installation.
- If you installed Administration Console on a separate machine, ensure that the DNS names resolve between Identity Server and Administration Console.
- When you are installing Identity Server on a separate machine (recommended for production environments), ensure that the following ports are open on both Administration Console and Identity Server:
  
  8444
  1443
  1289
  1290
  524
  636

  For information about how to open ports, see “Configuring the Linux Administration Console Firewall” on page 51 and “Configuring the Windows Administration Console Firewall” on page 53.

  IMPORTANT: When you are installing Identity Server on a machine with Administration Console (not recommended for production environments), do not run simultaneous external installations of Identity Server and Access Gateway. These installations communicate with Administration Console. During installation, Tomcat is restarted, which can disrupt the component import process.
• Verify that the machine meets the minimum requirements. See Section 3.2.1, “System Requirements on Linux,” on page 58.
• You must establish a static IP address for your Identity Server to reliably connect with other Access Manager components. If the IP address changes, Identity Server can no longer communicate with Administration Console.

3.2 Installing Identity Server on Linux

• Section 3.2.1, “System Requirements on Linux,” on page 58
• Section 3.2.2, “Installation Procedure,” on page 60

3.2.1 System Requirements on Linux

• 4 GB RAM
• Dual CPU or Core (3.0 GHz or comparable chip)
• 100 GB hard disk
  This size is recommended to ensure ample space for logging in a production environment. This disk space must be local and not remote.
• If you have custom partitioned your hard disk as follows, ensure that the free disk space mentioned against each partition is available:

<table>
<thead>
<tr>
<th>Partition</th>
<th>Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/novell</td>
<td>1 GB</td>
</tr>
<tr>
<td>/opt/volera</td>
<td>5 MB</td>
</tr>
<tr>
<td>/var/opt/novell</td>
<td>1 GB</td>
</tr>
<tr>
<td>/var</td>
<td>512 MB</td>
</tr>
<tr>
<td>/usr</td>
<td>25 MB</td>
</tr>
<tr>
<td>/etc</td>
<td>1 MB</td>
</tr>
<tr>
<td>/tmp/novell_access_manager</td>
<td>10 MB</td>
</tr>
<tr>
<td>/tmp</td>
<td>10 MB</td>
</tr>
<tr>
<td>/</td>
<td>512 MB</td>
</tr>
</tbody>
</table>

• One of the following operating systems:
  • SUSE Linux Enterprise Server (SLES) 12 SP3 or SLES 12 SP4 with 64-bit operating system x86-64 hardware. (physical or virtual).
  Ensure that the following packages are installed:
  • rsyslog-module-gtls
  • rsyslog
  • binutils
  • glibc-32bit
• Red Hat Enterprise Linux (RHEL) 6.10 or RHEL 7.6 (64-bit) (physical or virtual). RHEL 7.7 (Applicable for Access Manager 4.5 SP1 and later).

For installing the RHEL packages, see Appendix B, “Installing Packages and Dependent RPMs on RHEL for Access Manager,” on page 137.

**NOTE:** You can select to install these RPMs automatically along with Access Manager installation. While installing Access Manager, specify N when you get the following prompt:

Enter the local mount directory if you have the OS ISO mounted locally. This will be used as the local catalog for the additional rpms.

Do you have a locally mounted ISO (y/n)?

The Access Manager installer checks the online catalog and then installs the required RPMs automatically.

• gettext
• python (interpreter)
• Static IP address.

**IMPORTANT:**

• No LDAP software, such as eDirectory or OpenLDAP, can be installed.
• If the OpenLDAP server is installed, uninstall it. If you do not want to uninstall it, ensure that it does not use the port 636 or does not bind the port 389 to localhost.
• Because of library update conflicts, you cannot install Access Manager on a Linux User Management (LUM) machine.

**Browser Support**

To authenticate to Identity Server through User Portal, use one of the following web browsers:

• Firefox 66.0.2
• Chrome 73.0.3683.86
• Microsoft Edge 42.17134.1.0/ EdgeHTML 17.17134
• Internet Explorer 11.648.17134.0 Update Versions 11.0.115 (KB4489873)

For information about network requirements, see Section 1.3, “Network Requirements,” on page 19.
3.2.2 Installation Procedure

Installation time: about 10 minutes.

| What you need to know to install Identity Server | • Username and password of the administrator.  
| | • (Conditional) IP address of Administration Console if it is installed on a separate machine. |

1. Open a terminal window.
2. Log in as a root user.
3. Access the install script.
   3a. Ensure that you have downloaded the software or you have the CD available. 
   For software download instructions, see the release-specific Readme.
   3b. Do one of the following:
      • If you are installing from CD or DVD, insert the disc into the drive, then navigate to the device. The location might be /media/cdrom, /media/cdrecorder, or /media/dvddisc, depending on your hardware.
      • If you downloaded the tar.gz file, unzip the file by using the following command:

```
tar -xzvf <filename>
```
   3c. Change to the novell-access-manager directory.
4. At the command prompt, run the following install script:

```
./install.sh
```
5. When you are prompted to install a product, specify 2, Install Identity Server, then press Enter. This selection is also used for installing additional Identity Servers for clustering behind an L4 switch. You need to run this install for each Identity Server you add to the cluster.

**NOTE:** Administration Console is accessible on ports 2080 (HTTP) and 2443 (HTTPS) if Identity Server is installed on the same machine.

The following warning is displayed:

**Warning:** If NAT is present between this machine and Administration Console, configure NAT in Administration Console.
Exit this installation if NAT is not configured in Administration Console.
Would you like to continue (y/n)?

For more information about how to configure NAT, see “Configuring Administration Console Behind NAT” on page 29.
6. Specify Y to proceed.
7. Review and accept the License Agreement.
8. Verify that the required rpms are of the latest versions. Specify Y to proceed.
9. Specify the IP address, user ID, and password for of the primary Administration Console.
10. Specify the IP address of the Novell Access Manager Server Communications Local Listener. Specify the local NAT IP address if local NAT is available for Identity Server.
If the installation program rejects the credentials and IP address, ensure that the correct ports are open on both Administration Console and Identity Server, as described in Section 3.1, “Prerequisites for Installing Identity Server,” on page 57.

The following components are installed:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Manager Server Communication</td>
<td>Enables network communications, including identifying devices, finding services, moving data packets, and maintaining data integrity.</td>
</tr>
<tr>
<td>Identity Server</td>
<td>Provides authentication and identity services for the other Access Manager components and third-party service providers.</td>
</tr>
<tr>
<td>Identity Server Configuration</td>
<td>Allows Identity Server to be securely configured by Administration Console. If the installation process terminates at this step, the probable cause is a failure to communicate with Administration Console. Ensure that you specified the correct IP address.</td>
</tr>
<tr>
<td>Access Manager Server Communications Configuration</td>
<td>Enables Identity Server to auto-import itself into Administration Console.</td>
</tr>
</tbody>
</table>

Continue with one of the following actions:

- Verify the installation. See “Verifying Identity Server Installation” on page 63
- Configure Identity Server. See Setting Up a Basic Access Manager Configuration in the Access Manager 4.5 Administration Guide.

**NOTE:** After installing Identity Server, you must create a cluster configuration. See Configuring Identity Servers Clusters in the Access Manager 4.5 Administration Guide.

### 3.3 Installing Identity Server on Windows

- Section 3.3.1, “System Requirements on Windows,” on page 61
- Section 3.3.2, “Installation Procedure,” on page 62

#### 3.3.1 System Requirements on Windows

- 4 GB RAM
- Dual CPU or Core (3.0 Ghz or comparable chip)
- 100 GB hard disk

This size is recommended to ensure ample space for logging in a production environment. This disk space must be local and not remote.
• Windows Server 2016, 64-bit operating system (physical or virtual), in either Standard or Enterprise Edition, with the latest patches applied.
• Static IP address

**IMPORTANT:** No LDAP software, such as eDirectory or OpenLDAP, can be installed. (A default installation of SLES installs and enables OpenLDAP)

For information about network requirements, see Section 1.3, “Network Requirements,” on page 19.

For information about browser requirements, see “Browser Support” on page 59.

### 3.3.2 Installation Procedure

Installation time: about 10 minutes.

| What you need to know to install Identity Server | • Username and password of the administrator.  
• (Conditional) IP address of Administration Console if it is installed on a separate machine. |
|---|---|

1. Verify that the machine meets the minimum requirements. See Section 3.3.1, “System Requirements on Windows,” on page 61.
   
   Ensure that you have read and implemented prerequisites specified in Section 3.1, “Prerequisites for Installing Identity Server,” on page 57.

2. Close any running applications and disable any virus scanning programs.

3. (Conditional) If you have installed Administration Console on this server, ensure that you have restarted the server before installing Identity Server.

4. Download the ZIP file and extract it.
   
   For software download instructions and the filename, see the release-specific Release Notes.

5. Double-click the `<ZIP filename>.exe` file from the extracted folder.

6. Read the introduction, then click Next.

7. Accept the license agreement, then click Next.

8. Select Access Manager Identity Provider, then click Next.
   
   **A warning is displayed:** If NAT is present between this machine and Administration Console, the NAT configuration needs to be done in Administration Console.

9. Specify the IP address, user ID, and password for the primary Administration Console.

10. (Optional) Specify Identity Server Local NAT IP address, if the device is behind NAT.

11. Click Next, review the summary, and click Install.

12. (Conditional) If you are installing Identity Server on a machine that contains a previous installation of Administration Console, you are asked whether the program should overwrite an existing file in the \Program Files\Novell directory. Specify yes.

13. Continue with one of the following actions:
   
   • Verify the installation. See “Verifying Identity Server Installation” on page 63
3.4 Verifying Identity Server Installation

1 Log in to Administration Console.
   See Section 2.3, “Logging In to Administration Console,” on page 54.
2 Click Devices > Identity Servers.

3.5 Translating Identity Server Configuration Port

To enable Identity Server to communicate through a firewall, you can perform one of the following actions:

- Open TCP ports 8080 or 8443. These are default ports used respectively for non-secure and secure communication with Identity Server.
- Configure the Identity Server service to use the TCP port 80 or 443.

This section includes the following topics:

- “Changing the Port on Windows Identity Server” on page 63
- “Changing the Port on Linux Identity Server” on page 64

3.5.1 Changing the Port on Windows Identity Server

Set the port in Base URL in Identity Server and save the changes. Then, modify the server.xml file located in the Tomcat configuration directory.

Perform the following steps:

1 In Administration Console, click Devices > Identity Server > Edit, and configure Base URL with the HTTPS protocol and TCP port 443.
2 Click OK.
3 Update Identity Server.
4 In a terminal window, open the \Program Files\Novell\Tomcat\conf\server.xml file.
5 Change the ports from 8080 and 8443 to 80 and 443.
6 Restart the Tomcat service by running the following command:
   - net stop Tomcat8
   - net start Tomcat8
3.5.2 Changing the Port on Linux Identity Server

The Identity Server service (hosted on Tomcat) runs as a non-privileged user on Linux and cannot bind to ports below 1024. To allow requests to port 80/443 while Tomcat is listening on 8080/8443, the preferred approach is to use the iptables to perform a port translation. Port translation allows the base URL of Identity Server to be configured for port 443 and to listen on this port. The iptables translates it to port 8443 when communicating with Tomcat.

The following are two solutions out of many possibilities:

- If you have disabled the SUSE Linux Enterprise Server (SLES) firewall and do not have any other Access Manager components installed on the same server along with Identity Server, use a simple iptables script to translate the ports. See “Configuring a Simple Redirect Script” on page 64.

- If you have configured the SLES firewall or have installed other Access Manager components on the same server along with Identity Server, use a custom rule script that allows for multiple port translations. See “Configuring iptables for Multiple Components” on page 67.

For more information about iptables, see “Iptable Tutorial 1.2.2” (https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html) and “NAM Filters for iptables Commands” (http://www.novell.com/communities/node/4029/nam-filters-iptables-commands).

Port Forwarding

For both of these configurations (Configuring a Simple Redirect Script and Configuring iptables for Multiple Components) to work, you must enable port forwarding. To verify whether port forwarding is enabled, run the following command:

```
- cat /proc/sys/net/ipv4/ip_forward
```

If the value is 0, then port forwarding is not enabled.

To enable port forwarding, perform the following steps:

1. Run the following command:

   ```
   echo 1 > /proc/sys/net/ipv4/ip_forward
   ```

2. Verify the status.

For more information, see How To Forward Ports through a Linux Gateway with Iptables (https://www.digitalocean.com/community/tutorials/how-to-forward-ports-through-a-linux-gateway-with-iptables).

3.5.2.1 Configuring a Simple Redirect Script

This simple solution works only if you are not using iptables to translate ports of other applications or other Access Manager components. For a solution that works with multiple components, see “Configuring iptables for Multiple Components” on page 67.

Ensure that you have enabled port forwarding. See “Port Forwarding” on page 64.

Perform the following steps to configure a simple redirect script:
On SLES 12 SP4 or RHEL server

1 In Administration Console, click Devices > Identity Server > Edit., and configure Base URL with the HTTPS protocol and the TCP Port 443.

2 Click OK.

3 Update Identity Server.

4 At a terminal window, log in as the root user.

5 Create a unit configuration file to hold the iptables rule and place it in any directory. For example, /usr/bin/redirect-idp.

   Ensure that it has execute rights. You can use CHMOD as appropriate.


6 Copy the following example script and paste it in the file that you created in Step 5 on page 65.

   The following is an example of a redirect startup file:

   ```sh
   #!/bin/sh
   # Copyright (c) 2010 Novell, Inc.
   # All rights reserved.
   #
   #!/bin/sh
   #!/etc/init.d/idp_8443_redirect
   ### BEGIN INIT INFO
   # Provides: idp_8443_redirect
   # Required-Start: 
   # Required-Stop: 
   # Default-Start: 2 3 5
   # Default-Stop: 0 1 6
   # Description: Redirect 8443 to 443 for Novell IDP
   ### END INIT INFO

   # Environment-specific variables.
   IPT_BIN=/usr/sbin/iptables
   INTF=eth0
   ADDR=10.10.0.1

   . /etc/rc.status
   ```
# First reset status of this service
rc_reset

case "\$1" in
  start)
    echo -n "Starting IP Port redirection"
    $IPT_BIN -t nat --flush
    $IPT_BIN -t nat -A PREROUTING -i $INTF -p tcp --dport 80 -j DNAT
    --to ${ADDR}:8080
    $IPT_BIN -t nat -A PREROUTING -i $INTF -p tcp --dport 443 -j
    DNAT --to ${ADDR}:8443
    $IPT_BIN -t nat -A OUTPUT -p tcp -d $ADDR --dport 443 -j DNAT
    --to ${ADDR}:8443
    $IPT_BIN -t nat -A OUTPUT -p tcp -d $ADDR --dport 80 -j DNAT
    --to ${ADDR}:8080
    rc_status -v
  ;;
  stop)
    echo -n "Flushing all IP Port redirection rules"
    $IPT_BIN -t nat --flush
    rc_status -v
  ;;
  restart)
    $0 stop
    $0 start
    rc_status
  ;;
  *)
    echo "Usage: \$0 {start|stop|restart}"
    exit 1
  ;;
esac
rc_exit


7 Create a systemd service unit at /etc/systemd/system/<unit-name>.service. In this example unit-name is redirect-idp therefore, the service unit is /etc/systemd/system/redirect-idp.service.

8 Copy the following code and paste it in the service unit:
[Unit]
Description=Novell AM-IDP-Redirection
After=local-fs.target network.target

[Service]
Type=oneshot
ExecStart=/usr/bin/redirect-idp start
ExecStop=/usr/bin/redirect-idp stop
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target

9 Modify the service unit content as per requirement but ensure that ExecStart and ExecStop script points to the script that you created in the unit configuration file. In this example, the scripts must include /usr/bin/redirect-idp.

10 Execute the following commands:
   1. systemctl daemon-reload
   2. systemctl enable <unit-name>.service
      For example, systemctl enable redirect-idp.service

11 Reboot the Identity Server machine.

12 Verify that port 443 is being routed to Identity Server by running the following command:

   iptables -t nat -nvL

   The following is a sample entry:

   pkts bytes target prot opt in     out     source destination
   17   748    DNAT       tcp  --  eth0   *       0.0.0.0/0
       0.0.0.0/0           tcp dpt:443 to:10.10.0.1:8443

   This entry states that eth0 is routing TCP port 443 to IP address 10.10.0.1.

13 (Conditional) If your Identity Server cluster configuration contains more than one Identity Server, repeat these steps on each server in the cluster.

3.5.2.2 Configuring iptables for Multiple Components

If you need to use iptables for multiple components (the host machine, Identity Server), centralize the commands into one manageable location. The following sections explain how to use the SuSEFirewall2 option in YaST to centralize the commands.

Identity Server requires pre-routing commands.

NOTE: Port forwarding must be enabled for this configuration to work. See “Port Forwarding” on page 64.
Adding Identity Server Commands

1. In Administration Console, click Devices > Identity Server > Edit, and configure Base URL with the HTTPS protocol and the TCP port 443.
2. Click OK.
   4a. Change the FW_CUSTOMRULES="" line to the following:

   ```
   FW_CUSTOMRULES="/etc/sysconfig/scripts/SuSEfirewall2-custom"
   ```
   4b. Save the changes and exit.
5. Open the /etc/sysconfig/scripts/SuSEfirewall2-custom file in an editor.
   This is the custom rules file you specified in Step 4.
6. Add the following lines under the `fw_custom_before_port_handling()` section:

   ```
   iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to 10.10.0.1:8443
   iptables -t nat -A OUTPUT -p tcp -o eth0 --dport 443 -j DNAT --to 10.10.0.1:8443
   ```
   true

   The first command rewrites all incoming requests with a destination TCP port of 443 to TCP port 8443 on the 10.10.0.1 IP address for eth0. Modify the IP address to match the IP address of your Identity Server.
   The second command rewrites the health checks.
7. Save the file.
8. At the system console, restart the firewall by running the following command:

   ```
   /etc/init.d/SuSEfirewall2_setup restart
   ```
9. Verify that port 443 is being routed to Identity Server by running the following command:

   ```
   iptables -t nat -nvL
   ```

   The following is a sample entry:

   ```
   pkts bytes target     prot opt in     out     source           destination
   17   748 DNAT       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443 to:10.10.0.1:8443
   ```

   This entry states that eth0 is routing TCP port 443 to IP address 10.10.0.1:8443.
10. (Conditional) If your Identity Server cluster configuration contains more than one Identity Server, repeat these steps on each server in the cluster.
4 Installing Access Gateway

You can install Access Gateway in one of the following two modes:

- Appliance: Operating system is installed with Access Gateway software.
- Service: Access Gateway installed on a machine with an existing operating system.

This chapter explains the difference between Access Gateway Appliance and Access Gateway Service and how to install Access Gateway. Topics include:

- Section 4.1, “Feature Comparison of Different Types of Access Gateways,” on page 69
- Section 4.2, “Installing Access Gateway Appliance,” on page 70
- Section 4.3, “Installing Access Gateway Service,” on page 79
- Section 4.4, “Verifying Access Gateway Installation,” on page 84

4.1 Feature Comparison of Different Types of Access Gateways

Access Manager includes Access Gateway Appliance and Access Gateway Service. Access Gateway Appliance installs its own embedded Linux operating system. Whereas, Access Gateway Service runs on top of an existing installation of a Linux or Windows operating system. Both types of gateways support similar functionalities, but they differ slightly in the way some of these features are supported. For example, both can be configured for the following features:

- Protecting web resources with contracts, Authorization, Form Fill, and Identity Injection policies.
- Providing fault tolerance by clustering multiple gateways of the same type.
- Providing fault tolerance by grouping multiple web servers, so that if one web server goes down, the content can be retrieved from another server in the group.
- Rewriting URLs so that the names and IP addresses of web servers are hidden from the users making requests.
- Generating alert, audit, and logging events with notify options.

Most differences between Access Gateway Appliance and Access Gateway Service result from the differences required for an appliance and for a service. An appliance can know, control, and configure many features of the operating system. A service that runs on top of an operating system can query the operating system for some information, but it cannot configure or control the operating system. For the service, operating system utilities must be used to configure system parameters and hardware. For the appliance, the operating system features that are important to the appliance, such as time, DNS servers, gateways, and network interface cards, can be configured in Administration Console.

This table describes the differences between Access Gateway Appliance and Access Gateway Service. Only your network and web server configurations can determine whether the differences are significant.
Table 4-1 Differences between Access Gateway Appliance and Access Gateway Service

<table>
<thead>
<tr>
<th>Feature</th>
<th>Access Gateway Appliance</th>
<th>Access Gateway Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform support</td>
<td>SLES 12 SP3</td>
<td>• SLES 12 SP4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Red Hat Enterprise Linux 6.10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Red Hat Enterprise Linux 7.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Windows Server 2016</td>
</tr>
<tr>
<td>Network configuration</td>
<td>Configurable from Administration Console. After the installation, by default only one network interface card is displayed in Administration Console. To detect other network interface card, perform the following steps: 1. Configure a primary IP Address in YaST for the remaining interfaces. 2. Click Devices &gt; Access Gateways &gt; Select the device &gt; New IP &gt; click OK.</td>
<td>Configurable with standard operating system utilities.</td>
</tr>
<tr>
<td>DNS servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gateways</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network interface cards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host names</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date and time</td>
<td>Configurable from Administration Console.</td>
<td>Configurable with standard operating system utilities.</td>
</tr>
<tr>
<td>Cache directory</td>
<td>Uses Apache-caching. The cached files are stored in clear text. The operating system must be configured to protect this directory. For more information about the Apache model, see “Caching Guide”.</td>
<td>Uses filesystem provided by the Apache mod_cache module. For more information about the Apache model, see “Caching Guide”.</td>
</tr>
</tbody>
</table>

4.2 Installing Access Gateway Appliance

- Section 4.2.1, “System Requirements,” on page 70
- Section 4.2.2, “Installing Access Gateway Appliance,” on page 71
- Section 4.2.3, “Configuring Access Gateway Appliance,” on page 73

4.2.1 System Requirements

Access Gateway Appliance is a virtual appliance that is packaged in an OVF format. This makes the deployment of Access Gateway easy and fast.

The following list contains the minimum requirement to deploy the OVF template of Access Gateway Appliance:

- VMware ESXi 5.5 or later
- Dual CPU (3 GHz or comparable chip)

The OVF is preconfigured with the following hardware:

- 4 GB RAM
• Dual CPU or Core
• A static IP address for your Access Gateway server and an assigned DNS name (host name and domain name).
• 100 GB hard disk
  8 GB is reserved for swap.
You can modify the RAM and CPU based on your requirement.

Linux allows four primary partitions per hard disk. Access Gateway Appliance uses the following partitions:

<table>
<thead>
<tr>
<th>Partition Type</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>This partition is 40% of available disk space. It contains the boot files, system files, and log files. This space should be more than 40 GB.</td>
</tr>
<tr>
<td>swap</td>
<td>This partition is twice the size of RAM installed on the machine.</td>
</tr>
<tr>
<td>var</td>
<td>The remaining space is allocated for this partition, which should be more than 50 GB. This partition is used for log files and caching objects of Access Gateway.</td>
</tr>
</tbody>
</table>

**NOTE:** If the production environment requires more space for logging the data, you must provide additional disk space before configuring Access Gateway Appliance. You cannot add the hard disk space after configuring Access Gateway Appliance. For information about using the additional hard disk, see “Using Additional Hard Disk” on page 78.

For information about network requirements, see Section 1.3, “Network Requirements,” on page 19.

### 4.2.2 Installing Access Gateway Appliance

Installation time: 15 to 30 minutes, depending upon the hardware.

<table>
<thead>
<tr>
<th>What you need to know</th>
<th>• Username and password of the administrator.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• IP address of Administration Console.</td>
</tr>
<tr>
<td></td>
<td>• Static IP address for Access Gateway.</td>
</tr>
<tr>
<td></td>
<td>• DNS name (host and domain name) for Access Gateway that resolves to the IP address.</td>
</tr>
<tr>
<td></td>
<td>• Subnet mask that corresponds to the IP address for Access Gateway.</td>
</tr>
<tr>
<td></td>
<td>• IP address of your network’s default gateway.</td>
</tr>
<tr>
<td></td>
<td>• IP addresses of the DNS servers on your network.</td>
</tr>
<tr>
<td></td>
<td>• IP address or DNS name of an NTP server.</td>
</tr>
</tbody>
</table>

**IMPORTANT:** After Access Gateway Appliance installation, upgrade the Linux kernel to the latest security patch to avoid any security vulnerabilities. For more information, see “Performing an Online Update” on page 77.
This section provides the following information about how to install Access Gateway Appliance:

- Section 4.2.2.1, “Prerequisites,” on page 72
- Section 4.2.2.2, “Installing Access Gateway Appliance,” on page 72

### 4.2.2.1 Prerequisites

- Ensure that the server meets the minimum hardware requirements. See Section 4.2.1, “System Requirements,” on page 70.
- If you want to try any advanced installation options such as driver installation or network installation, see the SUSE Linux Enterprise Server 12 Installation Guide (https://www.suse.com/documentation/sles-12/book_sle_deployment/data/book_sle_deployment.html).

### 4.2.2.2 Installing Access Gateway Appliance


2. Select your desired language, review the agreement on the Appliance License Agreement page, then click Accept.

3. Specify the following details on the Appliance Passwords and Time Zone page:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>root Password</td>
<td>Specify the password for root.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>Specify the name of the primary and secondary NTP server.</td>
</tr>
<tr>
<td>Region and Time Zone</td>
<td>Select a region and time zone.</td>
</tr>
</tbody>
</table>

4. Specify the hostname for the Access Gateway Appliance server.

5. Click Next.

6. Specify the following network setting details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of Access Gateway.</td>
</tr>
<tr>
<td>Network Mask</td>
<td>The subnet mask of Access Gateway Appliance network.</td>
</tr>
<tr>
<td>Gateway</td>
<td>The IP address of the default gateway.</td>
</tr>
<tr>
<td>DNS Server</td>
<td>The IP address of your DNS server. You must configure at least one DNS server.</td>
</tr>
<tr>
<td></td>
<td>Specify the IP address of your additional DNS server, if you have configured. This is an optional configuration.</td>
</tr>
<tr>
<td>Domain Search</td>
<td>Specify the domain name.</td>
</tr>
</tbody>
</table>
7 Click Next.

8 Continue with configuring Access Gateway Appliance. See “Configuring Access Gateway Appliance” on page 73.


4.2.3 Configuring Access Gateway Appliance

Access Gateway Appliance is bundled with Configuration console (https://<access_gateway_appliance-IP address>:9443), Common Appliance Framework (CAF). You can use this console for modifying the Access Gateway Appliance configuration.

After installing Access Gateway Appliance, you must configure Access Gateway Appliance using the Configuration console to make it available in Administration Console.

Perform the following steps to configure Access Gateway Appliance:

NOTE: If you are using an existing IP address of Access Gateway Appliance and it uses a multiple NIC card in your cluster set up, ensure to configure the primary IP addresses for all the interfaces before configuring Access Gateway Appliance.

Also, ensure that you provide the IP address in the same order to the interfaces as it is in the existing Access Gateway Appliance.

1 Access the https://<access_gateway_appliance-IP address>:9443 URL to launch the Configuration console.

2 Log in as a root user.

3 Click Access Gateway Configuration under Access Gateway Tools.

4 Specify the Administration Console URL, username, and password.

5 Click Save.

You can use the following configuration options in the console based on your requirement:

- Section 4.2.3.1, “Managing Digital Certificates,” on page 73
- Section 4.2.3.2, “Setting Administrative Passwords,” on page 76
- Section 4.2.3.3, “Performing an Online Update,’’ on page 77
- Section 4.2.3.4, “Using Additional Hard Disk,” on page 78
- Section 4.2.3.5, “Performing a Product Upgrade,” on page 78
- Section 4.2.3.6, “Rebooting or Shutting Down the Appliance,” on page 79

4.2.3.1 Managing Digital Certificates

You can perform the following actions using the Digital Certificates tab:

- Add and activate certificates for Access Gateway Appliance.
- Create your own certificate and then get it signed by a CA.
- Use an existing certificate and key pair.

**IMPORTANT:** You can manage the certificates only for the Access Gateway Appliance (port 9443).

Access Gateway Appliance is shipped with a self-signed digital certificate. Instead of this self-signed certificate, it is recommended to use a trusted server certificate signed by a trusted CA, such as Digicert or Equifax.

To use and activate the digital certificate, perform the following tasks:

- “Using the Digital Certificate Tool” on page 74
- “Using an Existing Certificate and Key Pair” on page 75
- “Activating the Certificate” on page 76

**Using the Digital Certificate Tool**

- “Creating a New Self-Signed Certificate” on page 74
- “Getting Your Certificate Officially Signed” on page 75

**Creating a New Self-Signed Certificate**

1. Log in to the Configuration console (https://<access_gateway_appliance-IP address>:9443) as the root user.
2. Click Digital Certificates.
3. In the Key Store list, select Web Application Certificates.
4. Click File > New Certificate (Key Pair) and specify the following information:
   4a. **General**
      - **Alias:** Specify a name that you want to use to identify and manage this certificate.
      - **Validity (days):** Specify for how long you want the certificate to remain valid.
   4b. **Algorithm Details**
      - **Key Algorithm:** Select either RSA or DSA.
      - **Key Size:** Select the preferred key size.
      - **Signature Algorithm:** Select the preferred signature algorithm.
   4c. **Owner Information**
      - **Common Name (CN):** Specify the name that exactly matches the server name in the URL for browsers to accept the certificate for SSL communication.
      - **Organization (O):** (Optional) Specify the organization. For example, My Company.
      - **Organizational Unit (OU):** (Optional) Specify the organizational unit as mentioned in the directory, such as a department or division. For example, Purchasing.
      - **Two-letter Country Code (C):** (Optional) Specify the two-letter country code. For example, US.
      - **State or Province (ST):** (Optional) Specify the state or the province name. For example, Utah.
City or Locality (L): (Optional) Specify the city name. For example, Provo.

5 Click OK.

After the certificate is created, it is self-signed.

6 Make the certificate official. See “Getting Your Certificate Officially Signed” on page 75.

Getting Your Certificate Officially Signed

1 On the Digital Certificates page, select the certificate that you just created.

2 Click File > Certificate Requests > Generate CSR.

3 Complete the process of emailing your digital certificate to a certificate authority (CA), such as Digicert.

   The CA takes your Certificate Signing Request (CSR) and generates an official certificate based on the information in the CSR. The CA then emails the new certificate and certificate chain to you.

4 After you have received the official certificate and certificate chain from the CA, perform the following actions:
   4a Revisit the Digital Certificates page.
   4b Click File > Import > Trusted Certificate.
   4c Click Browse and select the trusted certificate chain that you received from the CA.
   4d Click OK.
   4e Select the self-signed certificate.
   4f Click File > Certification Request > Import CA Reply.
   4g Click Browse and select the official certificate to be used to update the certificate information.

      On the Digital Certificates page, the name in the Issuer column for your certificate changes to the name of the CA that stamped your certificate.

5 Continue with activating the certificate, as described in “Activating the Certificate” on page 76.

Using an Existing Certificate and Key Pair

When you use an existing certificate and key pair, use the .P12 key pair format.

1 Log in to the Configuration console (https://<access_gateway_appliance-IP address>:9443) as the root user.

2 Click Digital Certificates.

3 In the Key Store menu, select JVM Certificates.

4 Click File > Import > Trusted Certificate.

5 Click Browse and select your existing certificate.

6 Click OK.

7 Click File > Import > Trusted Certificate.

8 Click Browse and select your existing certificate chain for the certificate that you selected in Step 4.

9 Click OK.
10 Click File > Import > Key Pair.

11 Click Browse and select your .P12 key pair file and specify your password if required.

12 Click OK.

13 Continue with “Activating the Certificate” on page 76.

Activating the Certificate

1 On the Digital Certificates page, in the Key Store list, select Web Application Certificates.

2 Select the certificate that you want to make active and click Set as Active, then click Yes.

3 Select the certificate and click View Info to verify that the certificate and certificate chains are created appropriately.

4 Click Close, when you have activated the certificate successfully.

5 Restart the Jetty service by using the systemctl restart vabase-jetty.service command.

4.2.3.2 Setting Administrative Passwords

You can modify passwords and SSH access permissions for an Access Gateway Appliance root administrator in the Administrative Passwords tab. Depending on your password policy requirements, modify passwords periodically or reassign responsibility of the Access Gateway Appliance administration to another person.

NOTE: vaadmin helps in managing virtual-machine-level settings and service configurations that affect an entire service and its interactions with other services.

On the Administrative Passwords page, the vaadmin user can change the vaadmin user password and root user can change the root password. Perform the following steps to change the password:

Managing the administrative access as the vaadmin user:

1 Log in to the Configuration console (https://<access_gateway_appliance-IP address>:9443) as the vaadmin user.

2 Click Administrative Passwords.

3 Specify a new password for the vaadmin administrator. You must also specify the current vaadmin password.

4 Click OK.

Managing the administrative access as the root user:

1 Log in to the Configuration console (https://<access_gateway_appliance-IP address>:9443) as the root user.

2 Click Administrative Passwords.

3 Specify a new password for the root administrator. You must also specify the current root password.

4 (Optional) Select or deselect Allow root access to SSH.

5 Click OK.
4.2.3.3 Performing an Online Update

Use the Online Update option to register to the online update service from the Customer Center (https://www.netiq.com/customercenter). You can select to install updates automatically or manually.


To activate the Update Channel, you must obtain the key from the Customer Center. If the key is not available, contact the Customer Center through an email.

**WARNING:** Before performing the online update, ensure to add rules in the firewall to allow https traffic to the URLs such as nu.novell.com and secure-www.novell.com.

For more information about configuring the firewall and ports, see Section 1.8, “Setting Up Firewalls,” on page 30.

To register for the Online Update Service:

1. Log in to the Configuration console (https://<access_gateway_appliance-IP address>:9443) as the root user.
2. Click Online Update.
3. If the Registration dialog does not open automatically, click the Register tab.
4. Select the Service Type:
   - Local SMT (Proceed with Step 5.)
   - Micro Focus Customer Center (Proceed with Step 6.)
5. (Local SMT) Specify the following information for the SMT server, then continue with Step 7.
   - Hostname such as smt.example.com
   - (Optional) SSL certificate URL that communicates with the SMT server
   - (Optional) Namespace path of the file or directory
6. (Customer Center) Specify the following information about the Customer Center (https://www.netiq.com/customercenter) account for Access Gateway Appliance:
   - Email address of the account in Customer Center
   - Activation key (the same Full License key that you used to activate the product)
   - Allow data send (select any of the following) to share information with the Customer Center:
     - Hardware Profile
     - Optional information
7 Click Register.
   Wait while Access Gateway Appliance registers with the service.
8 Click OK.

After completing the registration, you can view the list of the needed updates and the list of installed updates.

Performing post-registration actions:

- **Update Now:** Click *Update Now* to activate the downloaded updates.

**NOTE:** Some of the updates might require rebooting Access Gateway Appliance. It is recommended to reboot Access Gateway Appliance in the following scenarios:

- When Configuration console displays the *Reboot Needed* option in the upper right corner of the Appliance Configuration pane.
- When Configuration console displays a message or a warning to reboot.

- **Schedule:** Configure the type of updates to download and whether to automatically agree to the licenses.

  **To schedule online update:**
  1. Click the *Schedule* tab.
  2. Select a schedule for download updates (*Manual, Daily, Weekly, Monthly*).

- **View Info:** Click *View Info* to display a list of installed and downloaded software updates.

- **Refresh:** Click *Refresh* to reload the status of updates on Access Gateway Appliance.

### 4.2.3.4 Using Additional Hard Disk

By default, the var directory is in the boot partition. If the logs fill the space of the var directory, Access Gateway Appliance can stop working. Therefore, you can add hard disk for the var directory.

You can use the additional hard disk that you added before configuring Access Gateway. To use additional hard disk, perform the following steps:

1. Log in to Configuration console ([https://<access_gateway_appliance-IP address>:9443](https://<access_gateway_appliance-IP address>:9443)). then click `/var Mount Configuration`.
2. Select the appropriate hard disk and the file system type.
3. Click *Save*.
4. Reboot the Access Gateway Appliance.

### 4.2.3.5 Performing a Product Upgrade

In this release, you need to migrate Access Gateway Appliance to the latest version.

For information about how to migrate to Access Gateway Appliance 4.5, see “Upgrading Access Gateway Appliance” on page 165.
4.2.3.6 Rebooting or Shutting Down the Appliance

You might require to shutdown or to restart Access Gateway Appliance for maintenance. It is recommended to use the console options instead of using Power Off/On option in the hypervisor’s VM management tool.

1. Log in to the Configuration console (https://<access_gateway_appliance-IP address>:9443) as the root user.
2. In the upper right corner of the Appliance Configuration pane, click Reboot or click Shutdown.

4.3 Installing Access Gateway Service

- Section 4.3.1, “Installing Access Gateway Service on Linux,” on page 79
- Section 4.3.2, “Installing Access Gateway Service on Windows,” on page 82

4.3.1 Installing Access Gateway Service on Linux

**IMPORTANT:** Because of library update conflicts, you cannot install Access Manager on a Linux User Management machine.

- Section 4.3.1.1, “System Requirements on Linux,” on page 79
- Section 4.3.1.2, “Prerequisites,” on page 80
- Section 4.3.1.3, “Installation Procedure,” on page 81

4.3.1.1 System Requirements on Linux

- One of the following operating systems:
  - SUSE Linux Enterprise Server (SLES) 12 SP3 or SLES 12 SP4 (64-bit) (physical or virtual).
  - Ensure that the following rpms or higher versions are installed:
    - rsyslog-module-gtls-5.10.1-0.7.49
    - rsyslog-5.10.1-0.7.49
    - binutils 2.23.1-0.17.18
    - glibc-32bit

**IMPORTANT**

- SLES installation libraries may be distributed across multiple CDs or DVDs. In YaST > Software > Software Repositories select the required CD or DVD to install the rpm files. If the rpm files are not available on the SLES server, the Access Manager installation process takes care of installing these rpm files from the SLES repository.
- To search if an rpm is installed, use `rpm -qa | grep <rpm name>`. For example, `rpm - qa | grep libapr-util`.

- Red Hat Enterprise Linux (RHEL) 6.10 RHEL 7.6 (64-bit) (physical or virtual). RHEL 7.7 (Applicable for Access Manager 4.5 SP1 and later).
For installing the RHEL packages, see Appendix 8, “Installing Packages and Dependent RPMs on RHEL for Access Manager,” on page 137.

**NOTE:** You can select to install these RPMs automatically along with Access Manager installation. While installing Access Manager, specify \( \text{N} \) when you get the following prompt:

Enter the local mount directory if you have the OS ISO mounted locally. This will be used as the local catalog for the additional rpms.

Do you have a locally mounted ISO (y/n)?

The Access Manager installer checks the online catalog and then installs the required RPMs automatically.

- 4 GB RAM.
- Dual CPU or Core (3.0 GHz or comparable chip).
- 2 to 10 GB hard disk space per reverse proxy that requires caching and for log files. The amount varies with rollover options and logging level that you configure.
- If you have custom partitioned your hard disk as follows, ensure that the free disk space mentioned against each partition is available:

<table>
<thead>
<tr>
<th>Partition</th>
<th>Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/novell</td>
<td>1 GB</td>
</tr>
<tr>
<td>/opt/volera</td>
<td>5 MB</td>
</tr>
<tr>
<td>/var/opt/novell</td>
<td>1 GB</td>
</tr>
<tr>
<td>/var</td>
<td>512 MB</td>
</tr>
<tr>
<td>/usr</td>
<td>25 MB</td>
</tr>
<tr>
<td>/etc</td>
<td>1 MB</td>
</tr>
<tr>
<td>/tmp/novell_access_manager</td>
<td>10 MB</td>
</tr>
<tr>
<td>/tmp</td>
<td>10 MB</td>
</tr>
<tr>
<td>/</td>
<td>512 MB</td>
</tr>
</tbody>
</table>

- A static IP address and a DNS name. The ActiveMQ module of Access Gateway Service must be able to resolve the machine’s IP address to a DNS name. If the module can’t resolve the IP address, the module does not start.
- Other Access Manager components should not be installed on the same machine.

For information about network requirements, see Section 1.3, “Network Requirements,” on page 19.

### 4.3.1.2 Prerequisites

- An Administration Console is installed.

  See Section 2, “Installing Administration Console,” on page 45.
- An Identity Server is installed and configured.

- Verify that the server meets the minimum requirements.

See Section 4.3.1, “Installing Access Gateway Service on Linux,” on page 79.

- Verify that the time on the machine is synchronized with the time on Administration Console. If the times differ, Access Gateway Service does not import into Administration Console.

- If a firewall separates the machine and Administration Console, ensure that the required ports are opened. See Table 1-3 on page 32.

- Because Access Gateway Service runs as a service, the default ports (80 and 443) that Access Gateway Service uses might conflict with the ports of other services running on the machine. If there is a conflict, you need to decide which ports each service can use.

- (Windows Server 2012) If the web server (IIS) has been installed by default during the Windows Server 2012 install, the Access Gateway Service installation program detects its presence from the registry and issues a shutdown command. Even if you have never activated the web server and if even it is not running, the shutdown command is issued. Because Access Gateway Service cannot be installed while the IIS server is running, the installation program needs to ensure that it is not running.

NOTE: Access Gateway Service clustering is supported for devices that are on the same operating system.

### 4.3.1.3 Installation Procedure

You must install Access Gateway Service on a separate machine.

Installation time: about 10 minutes.

<table>
<thead>
<tr>
<th>What you need to know</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Username and password of the administrator.</td>
</tr>
<tr>
<td></td>
<td>• IP address of Administration Console.</td>
</tr>
</tbody>
</table>

1. Log in to the NetIQ Customer Center and follow the link that allows you to download software. For an evaluation version, download the media kit from NetIQ Downloads.

2. Copy the file to your machine.

   For the filename, see the release-specific Release Notes.

3. Prepare your machine for installation:

   Make your operating system installation media available.

   The installation program checks for Apache dependencies and installs any missing packages.

4. Start installation by running the following script:

   ./ag_install.sh

5. Review and accept the License Agreement.

6. (Optional) Specify the local NAT IP address if the local NAT is available for Access Gateway.

7. Specify the IP address, user ID, and password of the primary Administration Console.

8. Specify the IP address of Access Gateway.
Continue with one of the following sections:

- Verify the installation. See “Verifying Access Gateway Installation” on page 84

**IMPORTANT:** (Applicable for RHEL) When you configure more than 60 proxy services, Apache fails to start. RHEL has 128 semaphore arrays by default which is inadequate for more than 60 proxy services. Apache 2.4 requires a semaphore array for each proxy service.

You must increase the number of semaphore arrays depending on the number of proxy services you are going to use. Perform the following steps to increase the number of semaphore arrays to the recommended value:

1. Open `/etc/sysctl.conf`
2. Add `kernel.sem = 250 256000 100 1024`  
   This creates the following:
   - Maximum number of arrays = 1024 (number of proxy services x 2)
   - Maximum semaphores per array = 250
   - Maximum semaphores system wide = 256000 (Maximum number of arrays x Maximum semaphores per array)
   - Maximum ops per semop call = 100
3. Use command `sysctl -p` to update the changes.
4. Start Apache.

### 4.3.2 Installing Access Gateway Service on Windows

- Section 4.3.2.1, “System Requirements on Windows,” on page 82
- Section 4.3.2.2, “Installation Procedure,” on page 83

#### 4.3.2.1 System Requirements on Windows

- Windows Server 2016, 64-bit operating system (physical or virtual), in either Standard or Enterprise Edition, with the latest patches applied
- 4 GB RAM
- Dual CPU or Core (3.0 GHz or comparable chip)
- 2 to10 GB per reverse proxy that requires caching and for log files. The amount varies with rollover options and logging level that you configure
- A static IP address and a DNS name. The ActiveMQ module of Access Gateway Service must be able to resolve the machine’s IP address to a DNS name. If the module can’t resolve the IP address, the module does not start.

You can verify this by using the `nslookup` command. Enter this command with hostname in the command prompt and it should return the IP address of the host.
• Windows packages KB2919442 and KB2919355 must be installed before installing Access Gateway Service. These packages must be installed in the same sequence. You can verify if these packages are installed by using the following commands:
  • `dism /online /get-packages | findstr KB2919442`
  • `dism /online /get-packages | findstr KB2919355`

If these packages are installed, you will get a confirmation message. If the packages are not installed, you will not receive any response.

• Other Access Manager components should not be installed on the same machine

For information about network requirements, see Section 1.3, “Network Requirements,” on page 19.

For prerequisites, see “Prerequisites” on page 72.

### 4.3.2.2 Installation Procedure

You must install Access Gateway Service on a separate server.

Installation time: about 10 minutes.

<table>
<thead>
<tr>
<th>What you need to know</th>
<th>Username and password of the administrator.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP address of Administration Console.</td>
</tr>
</tbody>
</table>

1. Log in to the NetIQ Customer Center (https://www.netiq.com/customercenter) and follow the link that allows you to download software. For an evaluation version, download the media kit from NetIQ Downloads (https://dl.netiq.com/index.jsp).
2. Download the ZIP file and extract it.
   For the filename, see the release-specific Access Manager Release Notes.
3. Disable any virus scanning programs.
4. To use a remote desktop for installation, use one of the following:
   • Current version of VNC viewer
   • Microsoft Remote Desktop with the `/console` switch for Windows XP SP2
   • Microsoft Remote Desktop with the `/admin` switch for Windows XP SP3
5. Double-click the executable file in the `<ZIP filename>` folder.

A warning is displayed stating If NAT is present between console, the NAT configuration needs to be done in Administration Console.

If NAT is configured then ensure that you configure the same in Administration Console. Else, click **Continue >Next**.
6. Review the readme, and click **Next**.
7. Review and accept the License Agreement, then click **Next**.
8. Specify the IP address, user ID, and password of the primary Administration Console.
9. (Conditional) Specify the local IP address, if your machine has more than one IP address, which Access Gateway Service will use for communication with Administration Console.
10. (Optional) Specify Access Gateway Local NAT IP address, if the device is behind NAT.
11. Click **Next**.
12 Configure disk cache. This holds the caching objects of Access Gateway.

**NOTE:** Access Gateway Appliance uses the mod_cache module filesystem provided by Apache for storing the caching objects. If you want to change the size of this cache after installation, see [TID on Changing the Cache Size of an Access Gateway Appliance after Installation](#).

13 Click Next, then review the installation summary.

14 Click Install.

15 Review the log information at the following location:

   C:\Program Files\Novell\log

16 Click Next > Done.

17 To verify that Access Gateway Service imported into Administration Console, wait for few minutes, log in to Administration Console, then click Devices > Access Gateways.

At this point, Access Gateway Service is not configured.

18 Continue with one of the following:

   - “Verifying Access Gateway Installation” on page 84
   - Configure Access Gateway. See Configuring Access Gateway in the **Access Manager 4.5 Administration Guide**.
   - Install another Access Manager component.

### 4.4 Verifying Access Gateway Installation

1 Log in to Administration Console.

   See Section 2.3, “Logging In to Administration Console,” on page 54.

2 Click Devices > Access Gateways.

   If the installation was successful, the IP address of your Access Gateway appears in the Server list.

   The Health status indicates the health state after Access Gateway is imported and registers with Administration Console.

**NOTE:** Access Gateway Appliance health is displayed as green instead of yellow, even before a trust relationship is established between an Embedded Service Provider and Access Gateway. You must establish a trust relationship with Administration before you proceed with any other configuration.

If an Access Gateway starts to import into Administration Console but fails to complete the process, the following message appears:

   Server gateway-<name> is currently importing. If it has been several minutes after installation, click repair import to fix it.

   If you have waited at least ten minutes, but the message doesn’t disappear and Access Gateway does not appear in the list, click the repair import link.
5 Installing Analytics Server

You can install Analytics Server after installing Administration Console. You can install it on any server without the requirement for any base operating system because Analytics Server is packaged with SLES operating system. Analytics Server runs 64-bit operating system on x86-64 hardware supported by SLES 11 SP4. Install it on a separate server because it clears the hard drive and sets up a soft appliance environment.

Before you install Analytics Server, review the new functionality and known issues in the supported SLES Release Notes.

Analytics Server is packaged in the ISO format, which can be deployed to the virtual environments.

The image format allows you to generate a full disk image format that can be deployed directly to hardware, either physical (bare metal) or virtual (uninstalled virtual machine in a hypervisor) by using a bootable ISO DVD image.

This chapter includes the following topics:

- Section 5.1, “System Requirements,” on page 85
- Section 5.2, “Procedure to Install Analytics Server,” on page 86
- Section 5.3, “Modifying Password After Installation,” on page 88
- Section 5.4, “Adding and Configuring Multiple NIC to Analytics Server,” on page 88
- Section 5.5, “Post-Installation Configuration for Analytics Server,” on page 88
- Section 5.6, “Deploying Analytics Server for High Availability,” on page 88

5.1 System Requirements

- 24 GB RAM for production environment. However, the minimum memory of 8 GB can be used for demonstration purpose.
- 50 GB hard disk space for the installer to make the automatic partition proposal.
- (4 core) CPUs (8 cores total).

If you are installing the ISO on bare metal hardware, download the ISO disk image from the support site, unpack the file, and make a DVD.

5.1.1 System Requirements for Storing 500 Events Per Second (EPS)

- **CPU:** Two Intel(R) Xeon(R) CPU ES-2650 @ 2.00GHz (4 core) CPUs (8 cores total), no hyper-threading.
- **Primary storage:** 10 x 300 GB SAS 15k RPM (Hardware RAID 10)
- **Memory:** 24 GB RAM
5.2 Procedure to Install Analytics Server

If you plan to include multiple Network Interface Card (NIC), then you must install Analytics Server with one NIC and then proceed with configuring other network interfaces. For more information, see Section 5.4, “Adding and Configuring Multiple NIC to Analytics Server,” on page 88.

Ensure that you have completed the following tasks before you start the installation:

- Verify that your hardware and software meet the system requirements listed in Section 5.1.1, “System Requirements for Storing 500 Events Per Second (EPS),” on page 85.
- No files or system settings from a previous Analytics Server installation, if any, are available on the machine.
- Ports listed in Section 1.8, “Setting Up Firewalls,” on page 30 are opened.
- The password used for Administration Console does not include the “&” symbol. If the password includes “&”, the Analytics Server installation fails. If you have used “&” in the password for Administration Console, change Administration Console password, then start the Analytics Server installation.

To install Analytics Server, perform the following steps:

2. (Conditional) If you are using a hypervisor, do one of the following actions:
   - Set up the virtual machine using the ISO virtual appliance image, and power it on.
   - Copy the ISO image into a DVD, set up the virtual machine using the DVD, and power it on.
3. (Conditional) If you are installing Analytics Server on bare metal hardware, perform the following actions:
   3a. Boot the physical machine from the DVD drive with the DVD.
   3b. Follow the installation wizard on-screen instructions.
   3c. Run the Live DVD appliance image by selecting the top entry in the boot menu.
      The installation checks for the available memory. If the available memory is less than 6.5 GB, the installation will not proceed further. Enter y if you want to continue with the installation, or enter n if you do not want to proceed.
4. Select the language of your choice and keyboard Configuration, then click Next.
5. Read and accept the Access Manager Analytics Server End User License Agreement.
6. Click Next.
7. On the Hostname and Domain Name page, specify the hostname and domain name. De-select Assign Hostname to Loopback IP, then click Next.
8. Choose one of the following connection settings options:
   - To use the current network connection settings, select Use the following configuration on the Network Configuration II page.
   - To change the network connection settings, click Change, then make the desired changes.
9. Click Next.
10. Set the Time and Date, then click Next.

   To change the NTP configuration after installation, use YaST from the appliance command line.
If the time appears out of sync immediately after the install, run the following command to restart NTP:

```
rcntp restart
```

11 Set the root password, then click Next.

12 In the Analytics Server Configuration page, set the Analytics Server admin password, select Use IP address for event routing, then click Next.

**NOTE:** The Analytics Server admin password must not contain “$”, “_”, “!”, “<”, “>”, “,”, “|”, “("”, “&” or “)”. Also, the password must not begin with “#”.

13 In the Administration console server Information page, specify the following details to import Analytics server to the specified Administration Console:

- **IP Address:** IP address of Administration Console.
- **Admin User:** The name of the user accessing Administration Console.
- **Password:** Password of Administration Console user.

Confirm the password, then click Next.

**NOTE:** If the password includes the “&” symbol, the installation fails. You must change the admin password in Administration Console (without “&”) to continue with Analytics server installation.

14 The Live Installation Settings page displays the selected installation settings. Review the settings, configure the settings (if necessary), and then select Install.

15 Select Install to confirm the Installation.

Wait until the installation finishes. It might take few minutes for all services to start up after installation because the system performs a one-time initialization.

16 The Suggested Partitioning screen displays the recommended partition setup. Review the partition setup, configure the setup (if necessary), and then select Next. Modify these settings only if you are familiar with configuring partitions in SLES.

You can configure the partition setup by using the various partitioning options on the screen. For more information about configuring partitions, see Using the YaST Partitioner in the *SLES* documentation.

17 Select OK to reboot the system.

18 (Conditional) If you are using a physical machine, eject the DVD.

19 (Conditional) If you are using a hypervisor click Enter.

20 Enter the root username and password at the console to log in to the appliance.

   The default value for the username is root and the password is the password you set in Step 11.

21 Proceed with Section 5.5, “Post-Installation Configuration for Analytics Server,” on page 88.

**NOTE:** For installing Analytics Server in high-availability mode, see Section 5.6.2, “Installing Analytics Server in High Availability Environment,” on page 89.
5.3 **Modifying Password After Installation**

After installing Analytics server if you want to change the password of the Analytics Server administrator, you can run the `configure.sh` script. The script is available in the `/opt/novell/sentinel/setup` folder.

1. Specify the following command at the command line to run the `configure.sh` script:
   
   ```bash
   ./configure.sh
   ```

2. Specify 1 to perform a standard configuration.
3. To change the existing password, enter 2, specify the new password, confirm the password.

5.4 **Adding and Configuring Multiple NIC to Analytics Server**

If you want to install multiple NIC and configure multiple IP addresses for Analytics Server, then perform the following steps:

1. Install Analytics Server with one NIC that is configured with the IP address that must be used for communicating with Administration Console. For installation steps, see Section 5.2, “Procedure to Install Analytics Server,” on page 86.

2. After the installation completes, configure the other required network interfaces by using YaST.

5.5 **Post-Installation Configuration for Analytics Server**

You must register Analytics Server with the server update channel to receive patch updates. For more information about registering the server, see Section 15.1.1, “Registering to Novell Customer Center,” on page 184.

5.6 **Deploying Analytics Server for High Availability**

This section provides information about how to install Analytics Server in an Active-Passive High Availability mode, which allows the server to fail over to a redundant cluster node in case of hardware or software failure.

For more information about implementing high availability and disaster recovery in the Analytics Server environment, contact NetIQ Technical Support.

High availability refers to a design methodology that is intended to keep a system available for use as much as is practicable. The intent is to minimize the causes of downtime such as system failures and maintenance, and to minimize the time it will take to detect and recover from downtime events that do occur. In practice, automated means of detecting and recovering from downtime events quickly become necessary as higher levels of availability must be achieved.
For more information about high availability, see the SUSE High Availability Guide.

- Section 5.6.1, “Prerequisite,” on page 89
- Section 5.6.2, “Installing Analytics Server in High Availability Environment,” on page 89
- Section 5.6.3, “Post-Installation Cluster Configuration for Analytics Server,” on page 99

5.6.1 Prerequisite

When allocating cluster resources to support a high availability (HA) installation, consider the following requirements:

- Ensure that each cluster node that hosts the Analytics Server services meet the requirements specified in Section 5.1.1, “System Requirements for Storing 500 Events Per Second (EPS),” on page 85.
- Ensure that sufficient shared storage is available for the Analytics Server data and application.
- Ensure that you use a virtual IP address for the services that can be migrated from node to node on failover.
- Ensure that your shared storage device meets the performance and size characteristics requirements. It is recommended to use a standard SUSE Linux VM configured with iSCSI Targets as shared storage.
- Ensure that you have only two cluster nodes that meet the resource requirements for running Analytics Server in the cluster environment.
- Ensure you have a virtual IP that can be migrated from one node to another node in a cluster to serve as the external IP address for Analytics Server.
- Ensure you create a method for the cluster nodes to communicate with the shared storage, such as FibreChannel for a SAN. NetIQ recommends a dedicated IP address to connect to the iSCSI Target.
- Ensure you have at least one IP address per cluster node for internal cluster communications. NetIQ recommends a simple unicast IP address, but multicast is preferred for production environments.

5.6.2 Installing Analytics Server in High Availability Environment

To install Analytics Server in High Availability mode, perform the following:

- Section 5.6.2.1, “Initial Setup,” on page 90
- Section 5.6.2.2, “Shared Storage Setup,” on page 91
- Section 5.6.2.3, “Configuring Analytics Server for High Availability on the Nodes,” on page 93
- Section 5.6.2.4, “Cluster Installation and Configuration,” on page 94
- Section 5.6.2.5, “Resource Configuration,” on page 96
5.6.2.1 Initial Setup

Configure the computer hardware, network hardware, storage hardware, operating systems, user accounts, and other basic system resources per the documented requirements for Analytics Server and local customer requirements. Test the systems to ensure proper function and stability.

Use the following checklist to guide you through initial setup and configuration:

- The CPU, RAM, and disk space characteristics for each cluster node must meet the system requirements defined in Section 5.1.1, “System Requirements for Storing 500 Events Per Second (EPS),” on page 85 based on the expected event rate.
- If you want to configure the operating system firewalls to restrict access to Analytics Server and the cluster, refer to Table 1-6 on page 36, for details of which ports must be available depending on your local configuration and the sources that will be sending event data.
- Ensure that all cluster nodes are time-synchronized. You can use NTP or a similar technology for this purpose.
- The cluster requires reliable host name resolution. Enter all internal cluster host names into the /etc/hosts file to ensure cluster continuity in case of DNS failure.
- Ensure that you do not assign a host name to a loopback IP address.
- When configuring host name and domain name while installing the operating system, deselect Assign Hostname to Loopback IP.
- The nodes will have one NIC for external access and one for iSCSI communications.
- Configure the external NICs with IP addresses that allow for remote access through SSH or similar. For this example, we will use 172.16.0.1 (node01) and 172.16.0.2 (node02).
- Each node should have sufficient disk for the operating system, and Analytics Server. For system requirements, see Section 5.1.1, “System Requirements for Storing 500 Events Per Second (EPS),” on page 85.
- One SUSE Linux 11 SP3 VM configured with iSCSI Targets for shared storage
  - (Conditional) You can install X Windows if you require GUI configuration. Set the boot scripts to start without X (runlevel 3), so you can start them only when needed.
  - The system will have two NICs: one for external access and one for iSCSI communications.
  - Configure the external NIC with an IP address that allows for remote access using SSH or similar. For example, 172.16.0.3 (storage03).
  - The system should have sufficient space for the operating system, temp space, a large volume for shared storage to hold Sentinel data, and a small amount of space for an SBD partition. See the SUSE Linux system requirements, and Sentinel event data storage requirements.
  - Perform the steps mentioned in the following sections.

**NOTE:** In a production cluster, you can use internal, non-routable IPs on separate NICs (possibly a couple, for redundancy) for internal cluster communications.
5.6.2.2 Shared Storage Setup

Set up your shared storage and make sure that you can mount it on each cluster node. If you are using FibreChannel and a SAN, you might need to provide physical connections as well as additional configuration. Analytics Server uses this shared storage to store the databases and event data. Ensure that the shared storage is appropriately sized accordingly based on the expected event rate and data retention policies.

A typical implementation might use a fast SAN attached using FibreChannel to all the cluster nodes, with a large RAID array to store the local event data. As long as the cluster node can mount the shared storage as a normal block device, it can be used by the solution.

**NOTE:** NetIQ recommends that you configure your shared storage and test mounting it on each cluster node. However, the cluster configuration will handle the actual mount of the storage.

NetIQ recommends using the following procedure to create iSCSI Targets hosted by a SLES VM:

1. Connect to *storage03*, the VM you created during *Initial Setup*, and start a console session.
2. Use the `dd` command to create a blank file of any desired size for Analytics Server shared storage. For creating a 20 GB file filled with zeros copied from the `/dev/zero` pseudo-device file, run the following command:
   ```
   dd if=/dev/zero of=/localdata count=20480000 bs=1024
   ```
3. Configure iSCSI targets

   Configure the files *localdata* as iSCSI Targets:
   1. Run YaST from the command line (or use the Graphical User Interface, if preferred): `/sbin/yast`
   2. Select *Network Devices* > *Network Settings*.
   3. Ensure that the *Overview* tab is selected.
   4. Select the secondary NIC from the displayed list, then tab forward to *Edit* and press *Enter*.
   5. On the *Address* tab, assign a static IP address of 10.0.0.3. This will be the internal iSCSI communications IP.
   6. Click *Next*, then click *OK*.
   7. On the main screen, select *Network Services* > *iSCSI Target*.
   8. If prompted, install the required software (*iscsitarget* RPM) from the SUSE Linux 11 SP3 media.
   9. Click *Service*, select the *When Booting* option to ensure that the service starts when the operating system boots.
   10. Click *Global*, and then select *No Authentication* because the current OCF Resource Agent for iSCSI does not support authentication.
   11. Click *Targets* and then click *Add* to add a new target.
       - The iSCSI Target will auto-generate an ID and then present an empty list of LUNs (drives) that are available.
   12. Click *Add* to add a new LUN.
Leave the LUN number as 0, then browse in the Path dialog (under Type=fileio) and select the /localdata file that you created. If you have a dedicated disk for storage, specify a block device, such as /dev/sdc.

Leave the other options at their defaults. Click OK and then click Next.

Click Next again to select the default authentication options, then Finish to exit the configuration. Accept if asked to restart iSCSI.

Exit YaST.

**NOTE:** This procedure exposes two iSCSI Targets on the server at IP address 10.0.0.3. At each cluster node, ensure that it can mount the local data shared storage device.

### Configuring iSCSI initiators

Use the following procedure to format the devices:

1. Connect to one of the cluster nodes (node01) and start YaST.
2. Select Network Devices > Network Settings.
3. Ensure that the Overview tab is selected.
4. Select the secondary NIC from the displayed list, then tab forward to Edit and press Enter.
5. Click Address, assign a static IP address of 10.0.0.1. This will be the internal iSCSI communications IP.
6. Select Next, then click OK.
7. Click Network Services > iSCSI Initiator.
8. If prompted, install the required software (open-iscsi RPM) from the SUSE Linux 11 SP3 media.
9. Click Service, select When Booting to ensure the iSCSI service is started on boot.
10. Click Discovered Targets, and select Discovery.
11. Specify the iSCSI Target IP address (10.0.0.3), select No Authentication, and then click Next.
12. Select the discovered iSCSI Target with the IP address 10.0.0.3 and then select Log In.
13. Switch to automatic in the Startup drop-down and select No Authentication, then click Next.
14. Switch to the Connected Targets tab to ensure that we are connected to the target.
15. Exit the configuration. This should have mounted the iSCSI Targets as block devices on the cluster node.
16. In the YaST main menu, select System > Partitioner.
17. In the System View, you should see new hard disk (such as /dev/sdb) in the list - they will have a type of IET-VIRTUAL-DISK. Tab over to this hard disk, select it, then press Enter.
18. Select Add to add a new partition to the empty disk. Format the disk as a primary ext3 partition, but do not mount it. Ensure that the option Do not mount partition is selected.
19. Select Next, then Finish after reviewing the changes that will be made. Assuming you create a single large partition on this shared iSCSI LUN, you should end up with a /dev/sdb1 or similar formatted disk (referred to as /dev/<SHARED1> below).
20. Exit YaST.
21. Repeat steps 1-15 to ensure that each cluster node can mount the local shared storage. Replace the node IP in step 5 with a different IP for each cluster node.
5.6.2.3 Configuring Analytics Server for High Availability on the Nodes

Install Analytics Server to each cluster node that can host it. After you install Analytics Server the first time, you must perform a complete installation including the application binaries, configuration, and all the data stores. For subsequent installations on the other cluster nodes, you will only install the application. The Analytics Server data will be available after you have mounted the shared storage.

First node

To configure Analytics Server for HA, perform the following steps:

1. Connect to one of the cluster nodes (node01) and open a console window.
2. Navigate to the following directory:
   
   cd /opt/novell/sentinel/setup

3. Record the configuration:
   3a. Execute the following command:

   ./configure.sh --record-unattended=/tmp/install.props --no-start

   This step records the configuration in the file install.props, which is required to configure the cluster resources using the install-resources.sh script.

   3b. Specify the Standard configuration option for Analytics Server Configuration method.

   3c. Specify 2 to enter a new password.

   Even if you require to use the existing password, choose 2 so that the password is stored and synchronized with the other node.

   If you specify 1, the install.props file does not store the password.

4. Shut down Analytics Server services by using the following commands:

   /etc/init.d/novell-offline stop
   /etc/init.d/novell-realtime stop
   /etc/init.d/novell-jcc stop
   rcssentinel stop
   inserv -r sentinel

5. Move the Analytics Server data folder to the shared storage using the following commands. This movement allows the nodes to utilize the Analytics Server data folder through shared storage.

   mkdir -p /tmp/new
   mount /dev/<SHARED1> /tmp/new
   mv /var/opt/novell/sentinel /tmp/new
   umount /tmp/new/

6. Verify the movement of the Analytics Server data folder to the shared storage using the following commands:

   mount /dev/<SHARED1> /var/opt/novell/
   umount /var/opt/novell/
Subsequent node

1. Connect to second cluster node (node02) and open a console window.
2. Execute the following command:
   
   ```bash
   insserv -r sentinel
   ```
3. Stop Analytics Server services.
   
   ```bash
   rcsentinel stop
   ```
4. Remove Analytics Server directory.
   
   ```bash
   rm -rf /var/opt/novell/sentinel
   ```

At the end of this process, Analytics Server should be installed on all nodes, but it will likely not work correctly on any but the first node until various keys are synchronized, which will happen when we configure the cluster resources.

5.6.2.4 Cluster Installation and Configuration

Analytics Server includes the cluster software and does not require manual installation.

As part of this configuration, you can also set up fencing and Shoot The Other Node In The Head (STONITH) resources to ensure cluster consistency.

For this solution you must use private IP addresses for internal cluster communications, and use unicast to minimize the need to request a multicast address from a network administrator. You must also use an iSCSI Target configured on the same SUSE Linux VM that hosts the shared storage to serve as a Split Brain Detection (SBD) device for fencing purposes.

NetIQ Recommends the following procedure for cluster configuration:

SBD Setup

1. Connect to storage03 and start a console session. Use the `dd` command to create a blank file of any desired size:

   ```bash
   dd if=/dev/zero of=/sbd count=1024 bs=1024
   ```

2. Create a 1MB file filled with zeros copied from the `/dev/zero` pseudo-device.
3. Run YaST from the command line or the Graphical User Interface: `/sbin/yast`
4. Select **Network Services** > **iSCSI Target**.
5. Click **Targets** and select the existing target.
6. Select **Edit**. The UI will present a list of LUNs (drives) that are available.
7. Select **Add** to add a new LUN.
8. Leave the LUN number as 1. Browse in the **Path** dialog and select the `/sbd` file that you created.
9. Leave the other options at their defaults, then select **OK** then **Next**, then click **Next** again to select the default authentication options.
10. Click **Finish** to exit the configuration. Restart the services if needed. Exit YaST.
NOTE: The following steps require that each cluster node be able to resolve the hostname of all other cluster nodes (the file sync service csync2 will fail if this is not the case). If DNS is not set up or available, add entries for each host to the /etc/hosts file that list each IP and its hostname (as reported by the hostname command). Also, ensure that you do not assign a hostname to a loopback IP address.

Perform the following steps to expose an iSCSI Target for the SBD device on the server at IP address 10.0.0.3 (storage03).

Node Configuration

Connect to a cluster node (node01) and open a console:

1. Run YaST.
2. Open Network Services > iSCSI Initiator.
3. Select Connected Targets, then the iSCSI Target you configured above.
4. Select the Log Out option and log out of the Target.
5. Switch to the Discovered Targets tab, select the Target, and log back in to refresh the list of devices (leave the automatic startup option and No Authentication).
6. Select OK to exit the iSCSI Initiator tool.
7. Open System > Partitioner and identify the SBD device as the 1MB IET-VIRTUAL-DISK. It will be listed as /dev/sdc or similar - note which one.
8. Exit YaST.
9. Execute the command ls -l /dev/disk/by-id/ and note the device ID that is linked to the device name you located above.
10. Execute the command sleha-init.
11. When prompted for the network address to bind to, specify the external NIC IP (172.16.0.1).
12. Accept the default multicast address and port. We will override this later.
13. Enter 'y' to enable SBD, then specify /dev/disk/by-id/<device id>, where <device id> is the ID you located above (you can use Tab to auto-complete the path).
14. Complete the wizard and make sure no errors are reported.
15. Start YaST.
16. Select High Availability > Cluster (or just Cluster on some systems).
17. In the box at left, ensure Communication Channels is selected.
18. Tab over to the top line of the configuration, and change the udp selection to udpu (this disables multicast and selects unicast).
19. Select to Add a Member Address and specify this node (172.16.0.1), then repeat and add the other cluster node(s): 172.16.0.2.
20. Select Finish to complete the configuration.
21. Exit YaST.
22. Run the command /etc/rc.d/openais restart to restart the cluster services with the new sync protocol.
Connect to other cluster node (node02) and open a console:

1. Run YaST.
2. Open Network Services > iSCSI Initiator.
3. Select Connected Targets, then the iSCSI Target you configured above.
4. Select the Log Out option and log out of the Target.
5. Switch to the Discovered Targets tab, select the Target, and log back in to refresh the list of devices (leave the automatic startup option and No Authentication).
6. Select OK to exit the iSCSI Initiator tool.
7. Run the following command: `sleha-join`
   Enter the IP address of the first cluster node.
8. Run `crm_mon` on each cluster node to verify that the cluster is running properly.

(Conditional) If the cluster does not start correctly, perform the following steps:

1. Manually copy `/etc/corosync/corosync.conf` from node01 to node02, or run `csync2 -x -v` on node01, or manually set the cluster up on node02 through YaST.
   If the `csync2` command fails, perform the steps mentioned in Step 3 on page 97.
2. Run `/etc/rc.d/openais start` on node02
   (Conditional) If the `xinetd` service does not properly add the new `csync2` service, the script will not function properly. The `xinetd` service is required so that the other node can sync the cluster configuration files down to this node. If you see errors like `csync2 run failed`, you may have this problem.
   To resolve this issue, execute the `kill -HUP `cat /var/run/xinetd.init.pid` command and then re-run the `sleha-join` script.
3. Run `crm_mon` on each cluster node to verify that the cluster is running properly. You can also use 'hawk', the web console, to verify the cluster. The default login name is `hacluster` and the password is `linux`.

Perform the following tasks to modify additional parameters:

1. To ensure that in a single node failure in your two-node cluster does not unexpectedly stop the entire cluster, set the global cluster option `no-quorum-policy` to `ignore`:
   ```bash
   crm configure property no-quorum-policy=ignore
   ```
2. To ensure that the resource manager allows resources to run in place and move, set the global cluster option `default-resource-stickiness` to `1`:
   ```bash
   crm configure property default-resource-stickiness=1
   ```

### 5.6.2.5 Resource Configuration

Resource Agents are provided by default with SLE HAE. If you do not want to use SLE HAE, you need to monitor these additional resources using an alternate technology:

- A filesystem resource corresponding to the shared storage that the software uses.
- An IP address resource corresponding to the virtual IP by which the services will be accessed.
- The PostgreSQL database software that stores configuration and event metadata.
NetIQ recommends the following for resource configuration:

NetIQ provides a crm script to aid in cluster configuration. The script pulls relevant configuration variables from the unattended setup file generated as part of the Analytics Server installation. If you did not generate the setup file, or you wish to change the configuration of the resources, you can use the following procedure to edit the script accordingly.

The proceeding steps must be performed on the nodes on which Analytics Server is installed.

1. Run the following commands on both nodes:
   - `mkdir -p /var/log/agg-analytics-var`
   - `mkdir -p /var/log/agg-analytics-var/nam/logs/dashboard/tomcat`
   - `chown -R novell.novell /var/log/agg-analytics-var/`

2. On the primary node, run the following commands in the same sequence, where `<SHARED1>` is the shared volume you created previously:
   ```
   mount /dev/<SHARED1> /var/opt/novell
   ln -s /var/log/agg-analytics-var/nam /var/opt/novell/nam
   cd /usr/lib/ocf/resource.d/novell
   ./install-resources.sh
   ```
   The `install-resources.sh` script will prompt you for a couple values, namely the virtual IP that you would like people to use to access Analytics Server and the device name of the shared storage, and then will auto-create the required cluster resources. Note that the script requires the shared volume to already be mounted, and also requires the unattended installation file which was created during Analytics Server install to be present (`/tmp/install.props`). You do not need to run this script on any but the first installed node; all relevant config files will be automatically synced to the other nodes.

   After running the `install-resources` script, if you get the error for the file synchronization, then run `csync2 -x -v`. If you get the message that file is up to date and is with no errors, then you can continue the deployment.

3. (Conditional) If the `csync2 -x -v` command fails to synchronize all files, perform the following steps:
   3a. Clear the csync2 database in the `/var/lib/csync2` directory on all the nodes.
   3b. Run the following command on all the nodes to update the csync2 database that will match the filesystem without marking anything as needing to be synchronized to other servers:
   ```
   csync2 -cIr /
   ```
   3c. On the active node, perform the following:
      3c1. Run the following command to find all the differences between active and passive nodes, then mark those differences for synchronization:
      ```
      csync2 -TUXI
      ```
      3c2. Run the following command to reset the database to force the active node to override any conflicts:
      ```
      csync2 -fr /
      ```
3c  Run the following command to start synchronization with all other nodes:
   csync2 -xr /

3d  On all the nodes, run the following command to verify that all the files are synchronized:
   csync2 -T
   This command will list only the files that are not synchronized.

4  Run the following commands on the primary node:
   ✷ /etc/init.d/novell-offline start
   ✷ /etc/init.d/novell-realtime start
   ✷ /etc/init.d/novell-jcc start

5  Run /etc/rc.d/openais restart on node02.

6  If your environment varies from this NetIQ recommended solution, you can edit the
   resources.cli file (in the same directory) and modify the primitives definitions from there.
   For example, the recommended solution uses a simple Filesystem resource; you may wish to
   use a more cluster-aware cLVM resource.

7  After running the shell script, you can issue a crm status command and the output should
   look like this:

   crm status

   Last updated: Thu Jul 26 16:34:34 2012
   Last change: Thu Jul 26 16:28:52 2012 by hacluster via crmd on node01
   Stack: openais
   Current DC: node01 - partition with quorum
   Version: 1.1.6-b988976485d15cb702c9307df55512d323831a5e
   2 Nodes configured, 2 expected votes
   5 Resources configured.

   Online: [ node01, node02 ]
   stonith-sbd   (stonith:external/sbd):    Started node01
   Resource Group: sentinelgrp
   sentinelp    (ocf::heartbeat:IPaddr2):    Started node01
   sentinelfs   (ocf::heartbeat:Filesystem):    Started node01
   sentineldb   (ocf::novell:pgsql):    Started node01
   sentinelserver    (ocf::novell:sentinel):    Started node01

8  Add the following entry to /etc/csync2/csync2.cfg ensuring that the last entry is auto
    first.

    include /etc/opt/novell/sentinel/config/auth.login;
    include /etc/opt/novell/nam/sentinelReportAdminConfig;
    auto first;

9  Run csync2 -x -v.
    Run the command again if you get any error.

NOTE: The preceding steps are used for installing and configuring the cluster for high availability.
However, to use this cluster configuration, you must enable clustering from Administration Console.
For more information, refer Section 5.6.3, “Post-Installation Cluster Configuration for Analytics
Server,” on page 99.
5.6.3 Post-Installation Cluster Configuration for Analytics Server

After performing the cluster installation steps, you can view the active and standby nodes in Administration Console. But to use Analytics Server in high availability mode you must perform the following in Administration Console in the same sequence:

- Section 5.6.3.1, “Enable Clustering,” on page 99
- Section 5.6.3.2, “Configure the settings for auditing,” on page 99

5.6.3.1 Enable Clustering

1. Click Devices > Analytics Server.
2. In the cluster row, click Edit.
3. In the Cluster Configuration section, set the Clustering is Configured: field to Yes and specify the same virtual IP address in the Cluster’s Virtual IP: field that you had specified during resource configuration. For more information, see Step 2 on page 97.

5.6.3.2 Configure the settings for auditing

Analytics Server will be functional only when it is set as the audit server in Administration Console. To set it as the audit server perform the following:

1. Perform the steps mentioned in “Enable Clustering” on page 99.
2. In the Admin Tasks pane, click Auditing.
3. In the Audit Messages Using: field, Select Syslog: > Send to Analytics Server

The Server Listening Address gets auto-populated with the virtual IP address that you had specified when performing step 1.
Chapter 6: Deploying Access Manager on Amazon Web Services EC2

You can deploy the following Access Manager components as services on Amazon Web Services (AWS) EC2:

- Administration Console
- Identity Server
- Access Gateway

**NOTE:** Deployment of Access Gateway Appliance and Analytics Server is not supported on AWS EC2.

Access Manager supports the following operating systems on AWS EC2:

- SUSE Linux Enterprise Server (SLES) 12 SP4
- Red Hat Enterprise Linux (RHEL) 7.6
- RHEL 7.7 (Applicable for Access Manager 4.5 SP1 and later)

This section includes the following topics:

- Section 6.1, “Prerequisites or Deploying Access Manager on AWS,” on page 101
- Section 6.2, “Deployment Procedure,” on page 102
- Section 6.3, “Auto Scaling Access Manager on AWS,” on page 111
- Section 6.4, “Monitoring Access Manager in AWS Using CloudWatch,” on page 121

### 6.1 Prerequisites or Deploying Access Manager on AWS

In addition to the system requirements of Access Manager components, ensure that you meet the following prerequisites:

- An administrative account on AWS EC2.
- The Access Manager installer (tarball) has been downloaded, extracted, and available for copying to the instances.
- An SSH client to connect to the AWS EC2 instances from your local client machine.

By default, Linux and Mac provide access to OpenSSH through the terminal. On Windows, use PuTTY or install the Windows Subsystem for Linux feature (Windows 10 only) to install a Linux distribution environment.
6.2 Deployment Procedure

The deployment procedure consists of the following steps:

1. **Creating AWS EC2 Services**
2. **Creating and Deploying Instances**
3. **Installing Access Manager**
4. **(Optional) Creating an AWS EC2 Load Balancer**

*Figure 1-7 in Section 1.6, “Deploying Access Manager on Public Cloud,” on page 22 illustrates the recommended way for deploying Access Manager on AWS EC2.*

**IMPORTANT:** The LDAP server and web services must be deployed in the public clouds along with Identity Server and Access Gateway.

A VPN connection from Identity Server and Access Gateway in the public cloud to the LDAP user store and web servers in the on-premises deployments is not supported.

### 6.2.1 Creating AWS EC2 Services

This section outlines steps for creating AWS EC2 services to use with Access Manager. For more information, see the Amazon Elastic Compute Cloud Documentation (https://aws.amazon.com/documentation/ec2/).

Perform the following steps to create AWS EC2 services:

1. **Log in to AWS Management Console (https://signin.aws.amazon.com/).**
2. **Click Services and create the following services:**

<table>
<thead>
<tr>
<th>Service</th>
<th>Steps</th>
</tr>
</thead>
</table>
| **VPC**  | 1. Click Services > VPC under Networking & Content Delivery.  
2. Click Start VPC Wizard.  
3. Select a VPC configuration type and click Select.  
4. Specify the details in the form, and then click Create VPC.  
   This creates a private network of the specified size. VPC and subnet creation use the CIDR notation for address ranges. The largest VPC size is a /16 network.  
   For more information, see the Amazon Virtual Private Cloud Documentation (https://aws.amazon.com/documentation/vpc/). |

**IMPORTANT:** Creating a VPC using Start VPC Wizard creates Subnets, Internet gateways, and Route table for the VPC. You can view or edit these items as follows:

| Subnets   | 1. In the left menu, click Subnets.  
2. Locate the subnet associated with this VPC.  
3. Select the subnet, verify the details, and edit if required. |
6.2.2 Creating and Deploying Instances

This section outlines steps to create and deploy instances for a basic setup of Access Manager, which includes an Administration Console, an Identity Server, an Access Gateway, and a user store.

Perform the following steps to create four instances: One for Administration Console, one for Identity Server, one for Access Gateway, and one for the Active Directory user store.

1. Click Services > EC2.
2. Click Launch Instance.
3. Select the SLES 12 SP4 or RHEL 7.6 image if you are creating this instance for an Access Manager component (Administration Console, Identity Server, or Access Gateway).

   When creating an instance for the Active Directory user store, select a Windows 2012 R2 image instead of SLES or RHEL.

   All instances that you create for deploying Access Manager components (Administration Console, Identity Server, or Access Gateway) must have the same operating system type (either SLES or RHEL).

4. Select the instance type that meets requirements of the base operating system and deployment of Access Manager components. See Section 1.4, “System Requirements,” on page 20.

   Each type has its own instance configuration settings, optimizations, and costs associated with it.

5. Click Next: Configure Instance Details.

   Ensure that the instance is using the correct VPC and subnet.

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-assign Public IP</td>
<td>Set to Enable.</td>
</tr>
<tr>
<td>Network Interfaces</td>
<td>Specify a static IP address in Primary IP.</td>
</tr>
</tbody>
</table>
6 Click Next: Add Storage.
   The default storage size is 10 GB. Change it as per your requirement.

7 Click Next: Add Tags.
   Add tags as desired. Tags enable you to organize instances. For example, you can add the following two tags to each instance:
   - A tag indicating what the instance is being used for
   - A tag indicating who is the owner of this machine

8 Click Next: Configure Security Group.
   Security groups are virtual firewall rules for groups of instances. It is recommended to create a separate security group for each group of instances with the same firewall requirements.
   For example, you can configure a security group for all nodes of Administration Console, one security group for all nodes of Identity Server, and one security group for all nodes of Access Gateway. By default, a new security group only allows incoming traffic on port 22, so that you can only connect to the instance by using SSH.

9 Create a new security group; specify a name and description for it.
   Add additional port rules before installing the Access Manager components. For information about required ports, see Table 1-7, Table 1-8, “Identity Server on Cloud,” on page 37, and Table 1-9, “Access Gateway on Cloud,” on page 37.

10 Click Review and Launch.
11 After reviewing the details, click Launch.
12 Select an existing key pair or create a new one.
   This key pair is used for SSH access to the instance. You can use the same key pair with multiple machines.
13 Click Download Key Pair.

   **IMPORTANT:** You can connect to and manage your instances only using the private key. Therefore, do not lose the private key after downloading it.

14 Repeat Step 1 to Step 13 and create other instances.
15 Continue with “Installing Access Manager” on page 104.

### 6.2.3 Installing Access Manager

**Prerequisites**

- Ensure that you meet the requirements listed in Section 1.3, “Network Requirements,” on page 19.
- Edit the `/etc/hosts` files on each instance and add an entry to resolve its hostname to its private IP address.
- Create port rules in the various security groups.

   See Step 8 and Step 9 in Section 6.2.2, “Creating and Deploying Instances,” on page 103. For the list of ports, see Table 1-7 on page 36, Table 1-8 on page 37, and Table 1-9 on page 37.
Before starting Access Manager installation, ensure that the additional packages listed in the system requirement sections of each Access Manager component are added.

Verify the SSH connectivity to the instances. The following is a sample syntax for verifying the connectivity:

```
ssh -i <key_name> ec2-user@<instance_public_ip>
```

To view the public IP address of an instance, click **Instances > [instance] > Description**.

**Important Points to Consider before Installation**

You must know the following points before you start the installation:

- Re-importing Identity Server and Access Gateway is not supported.
- Auto scaling of nodes is not supported. You can add or remove nodes manually. See Appendix B, “Recommendations for Scaling Access Manager Components in Public Cloud,” on page 209.

**Installation Procedure**

Perform the following steps to install Access Manager components on the respective instances:

**IMPORTANT:** In the following steps, run the Access Manager installation scripts as a root user using `sudo`. For example, `sudo sh <script-name>`.

1. Copy the `novell-access-manager-<version>.tar.gz` file using Secure Copy (scp) to the instances on which you will install Administration Console and Identity Server.
   
   The following is a sample scp command that shows how to copy the installer using the SSH key and username specified while creating the instance:
   
   ```
   scp -i <keyname> <path&name_of_file_to_copy> ec2-user@<instance_ip>:/<directory>
   ```
   
   2. Copy the `novell-access-gateway-<version>.tar.gz` file to the instance on which you will install Access Gateway.
   
   3. Install Administration Console, Identity Server, and Access Gateway on the respective instances.
      
      For information about how to install these components, see **Section 2.1, “Installing Administration Console on Linux,” on page 45, Section 3.2, ”Installing Identity Server on Linux,” on page 58, and Section 4.3.1, “Installing Access Gateway Service on Linux,” on page 79.**
      
      **IMPORTANT:** While installing Identity Server and Access Gateway, specify the internal IP address of the Administration Console machine.
      
      This ensures that communications among machines happen inside the firewall.
      
      
      For information about how to configure, see “Setting Up a Basic Access Manager Configuration” in the **Access Manager 4.5 Administration Guide**.
### 6.2.4 (Optional) Creating an AWS EC2 Load Balancer

If multiple Access Gateway and Identity Server instances have been created and configured for clustering, you can configure an AWS EC2 load balancer for each cluster to balance the load of incoming requests across the clustered instances. A separate load balancer is used for an Identity Server cluster and an Access Gateway cluster.

The following procedures provide differences in the configuration details for Identity Server load balancer and Access Gateway load balancer wherever required.


- Section 6.2.4.1, “Creating Target Groups,” on page 106
- Section 6.2.4.2, “Creating an Elastic IP Address,” on page 108
- Section 6.2.4.3, “Creating a Load Balancer,” on page 108

#### 6.2.4.1 Creating Target Groups

A target group provides a way to associate the load balancer to the IP addresses of instances (targets) among which the load will be distributed.

**IMPORTANT:** For each load balancer, you need to create two target groups: one for HTTP and one for HTTPS.

For more information about target groups, see Target group (http://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html).

Perform the following steps to create a target group:

1. In the EC2 Dashboard, click Target Groups under LOAD BALANCING.
2. Click Create target group.
3. Specify the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target group name</td>
<td>Specify a name for the target group.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select TCP.</td>
</tr>
</tbody>
</table>
4 Click Create.

5 Enable session stickiness.
   5a Select the target group you have created.
   5b In the Description tab, click Edit attributes.
   5c Select Enable for Stickiness.

6 Add the IP addresses of instances (targets) among which load will be distributed.
   6a In the edit mode, select the Targets tab, and then click Edit.
   6b Click the + (Register targets) icon.
Specify the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Populated with the VPC that you have selected under VPC in Step 3.</td>
</tr>
<tr>
<td>IP</td>
<td>Specify the private IP address of Identity Server or Access Gateway instances (targets) to register as targets that you want to add in the load balancer.</td>
</tr>
<tr>
<td>Port</td>
<td>Populated with the port value that you have specified for Port in Step 3.</td>
</tr>
</tbody>
</table>

Click Add to list.
Click Register.
Repeat Step 6b to Step 6e and add other instances of the same component type that you want to add in the load balancer.

### 6.2.4.2 Creating an Elastic IP Address

An elastic IP address is a public IPv4 address, which is reachable from the Internet. Elastic IP addresses are used as the listeners for the load balancers.

1. Click Services > EC2.
2. Click Elastic IPs.
3. Click Allocate new address.
4. Click Allocate.
   A static IPv4 address is allocated that is not used by any other resource.
5. Click Close.

### 6.2.4.3 Creating a Load Balancer

Perform the following steps to create a load balancer:

1. In the left menu, click Load Balancers.
2. Click Create Load Balancers.
3. Click Create under Network Load Balancer.
4. Specify the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify a name for the load balancer.</td>
</tr>
<tr>
<td>Scheme</td>
<td>Select internet-facing.</td>
</tr>
</tbody>
</table>
Deploying Access Manager on Amazon Web Services EC2

1. Specify the listener ports as follows:

   **For Identity Server:**
   - Load Balancer Protocol: TCP
   - Load Balancer Port: 8080

   Click **Add listener** and specify the following:
   - Load Balancer Protocol: TCP
   - Load Balancer Port: 8443

   **For Access Gateway:**
   - Load Balancer Protocol: TCP
   - Load Balancer Port: 80

   Click **Add listener** and specify the following:
   - Load Balancer Protocol: TCP
   - Load Balancer Port: 443

2. Select the same **VPC** that you have created earlier for Access Manager components.
3. Select the **Availability Zone** in which Access Manager instances are available. The load balancer routes traffic to the targets in the specified Availability Zones only.
4. Select the **Subnet** where the Access Manager component, for which you are configuring this load balancer, is available.
5. In **Elastic IP**, select the elastic IP address you created for this load balancer in “Creating an Elastic IP Address” on page 108.

6. Do not make any change.

**Field** | **Description**
---|---
Listeners | Specify the listener ports as follows:

   **For Identity Server:**
   - Load Balancer Protocol: TCP
   - Load Balancer Port: 8080

   Click **Add listener** and specify the following:
   - Load Balancer Protocol: TCP
   - Load Balancer Port: 8443

   **For Access Gateway:**
   - Load Balancer Protocol: TCP
   - Load Balancer Port: 80

   Click **Add listener** and specify the following:
   - Load Balancer Protocol: TCP
   - Load Balancer Port: 443

Availability Zones | 1. Select the same **VPC** that you have created earlier for Access Manager components.
2. Select the **Availability Zone** in which Access Manager instances are available. The load balancer routes traffic to the targets in the specified Availability Zones only.
3. Select the **Subnet** where the Access Manager component, for which you are configuring this load balancer, is available.
4. In **Elastic IP**, select the elastic IP address you created for this load balancer in “Creating an Elastic IP Address” on page 108.

Tags | Do not make any change.

5. Click **Next: Configure Routing**.
6 Under Target group, specify the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target group</td>
<td>Select Existing target group.</td>
</tr>
<tr>
<td>Name</td>
<td>Select a target group from the list. You can select only one target group here. For example, select the target group that you have created for the HTTP protocol. After creating the load balancer, you will need to modify the listener port 8443 to use the target group that is configured for the HTTPS protocol. See Step 12 on page 110 of this section.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Populated with the value that you have configured in the specified target group. Review to ensure that the value is listed correctly.</td>
</tr>
<tr>
<td>Port</td>
<td>Populated with the value that you have configured in the specified target group. Review to ensure that the value is listed correctly.</td>
</tr>
<tr>
<td>Target type</td>
<td>Populated with the value that you have configured in the specified target group. Review to ensure that the correct value is listed.</td>
</tr>
</tbody>
</table>

7 Under Health Checks, review the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Populated with HTTPS or HTTP based on the configuration of the target group you have selected in Step 6. See “Creating Target Groups” on page 106.</td>
</tr>
<tr>
<td>Path</td>
<td>Populated with the health URL that you have configured in the target group selected in Step 6. See “Creating Target Groups” on page 106.</td>
</tr>
<tr>
<td>Advanced health check settings</td>
<td>Keep the default values.</td>
</tr>
</tbody>
</table>

8 Click Next: Register Targets.

The list of all targets registered with the target group that you selected is displayed. You can modify this list only after creating the load balancer.

9 Click Next: Review.

10 Verify that the load balancer details are correct.

11 Click Create and then click Close.

12 Update the listener ports to use the appropriate target groups.

12a Select the load balancer you have created.

12b Select the Listeners tab.

By default, both listeners (HTTP and HTTPS) are configured to forward to the same target group that you have created in Step 6 > Name.
12c Select the HTTPS listener (8443 for Identity Server or 443 for Access Gateway).

12d Click Actions > Edit to change the target group of the HTTPS listener.

12e In Default target group, select the HTTPS target group for that component type (Identity Server or Access Gateway).

12f Click Save.

NOTE: For scaling recommendations, see Appendix B, “Recommendations for Scaling Access Manager Components in Public Cloud,” on page 209.

6.3 Auto Scaling Access Manager on AWS

Amazon Elastic Compute Cloud (EC2) Auto Scaling helps you maintain the application availability and allows you to automatically add or remove EC2 instances according to the conditions you define.

Based on the auto scaling configuration, new instances of Identity Server and Access Gateway are created automatically using custom AMIs. These instances are automatically imported into Administration Console and assigned to the respective clusters. These instances are also assigned automatically to AWS Load Balancer. Similarly, when not in use, the instances are removed from Administration Console and then get terminated automatically.

To automate these steps, Access Manager credentials are stored in the AWS EC2 Parameter Store as a secure string encrypted by KMS. All instances of Access Manager are assigned an IAM role to read the encrypted credentials and perform the auto scaling configuration automatically.

You require the CloudFormation template (https://www.netiq.com/documentation/access-manager-45/resources/AccessManagerAutoscale_45.zip) to deploy the auto scaling configuration.

Scaling Options

You can configure Access Manager auto scaling in the following ways:

- **Target Tracking Scaling**: The Target Tracking scaling responds to the changing demand. It reduces the need for manual provisioning Amazon EC2 capacity and enables you to meet the demand of Access Manager closely. For example, if you use target tracking scaling policies to select a load metric for Access Manager, such as CPU utilization. Auto Scaling automatically adjusts the number of EC2 instances required to maintain your target metric.

- **Scheduled Scaling**: The Scheduled scaling automatically schedules the appropriate number of EC2 instances based on the predicted demand. It enables you to scale your application before the predicted load changes. For example, every week the traffic to Access Manager starts to increase on Monday, remains high on Thursday, and starts to decrease on Friday. You can plan your scaling activities based on the known traffic patterns.

IMPORTANT: The auto scaling configuration explained in this section is supported only for Identity Server and Access Gateway components of Access Manager. To auto scale LDAP user stores and web servers, refer to Amazon EC2 Auto Scaling (https://aws.amazon.com/ec2/autoscaling/).
**Benefits**

The following are benefits of using Amazon EC2 auto scaling:

- Detects when an instance is not working, terminate it, and replace it with a new one.
- Adds instances only when needed, and can scale across purchase options to optimize performance and cost.
- Ensures that the application always has the appropriate amount of compute and provisions it with predictive scaling.

For more information, see Amazon EC2 Auto Scaling (https://aws.amazon.com/ec2/autoscaling/).

Watch the following video to understand how the auto scaling of Access Manager works in AWS.

http://www.youtube.com/watch?v=IJYx3qbA1gQ

This section discusses the following topics:

- Section 6.3.1, “Configuring Auto Scaling,” on page 112
- Section 6.3.2, “Limitations,” on page 120

### 6.3.1 Configuring Auto Scaling

This section includes the prerequisites and configuration steps to deploy the auto scaling configuration of Access Manager on AWS using the CloudFormation template.

Watch the following video to understand the configuration of Access Manager auto scaling in AWS.

http://www.youtube.com/watch?v=X7OwBHuQFmU

- Section 6.3.1.1, “Prerequisites,” on page 112
- Section 6.3.1.2, “AWS Services,” on page 113
- Section 6.3.1.3, “Deploying the Auto Scaling Configuration,” on page 114
- Section 6.3.1.4, “Post-Deployment Tasks,” on page 117
- Section 6.3.1.5, “Customizing the Scaled Instances,” on page 118
- Section 6.3.1.6, “Troubleshooting Auto Scaling,” on page 118
- Section 6.3.1.7, “Auditing Auto Scaling,” on page 119
- Section 6.3.1.8, “Monitoring Auto Scaling,” on page 119
- Section 6.3.1.9, “Deleting a CloudFormation Stack,” on page 120

### 6.3.1.1 Prerequisites

- Access Manager 4.5 is deployed on AWS and contains working Administration Console, Access Gateway cluster and Identity Server cluster.

  For more information about how to deploy Access Manager on AWS, see Section 6.2, “Deployment Procedure,” on page 102.

- An administrative Access Manager account is available.
Load balancer is configured and the load balancer target type is specified as `instance`.

For more information about how to configure the target group, see Target Groups for Your Network Load Balancers (https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-target-groups.html).

The following details are available to be specified during the auto scaling configuration:
- Amazon Virtual Private Cloud (VPC) ID of the existing Access Manager deployment.
- The subnet ID of the existing Identity Server and Access Gateway deployments.
  The new instances of Identity Servers and Access Gateway servers will be deployed in the respective subnets.
- A unique ARN of Identity Server and Access Gateway load balancer target group. The newly created Identity Servers and Access Gateway servers will be registered to these targets group automatically.

If you are configuring auto scaling for Access Gateway then identify and terminate the existing Access Gateway instances before you deploy the auto scaling configuration.

### 6.3.1.2 AWS Services

This following AWS services are deployed in the auto scaling configuration:

<table>
<thead>
<tr>
<th>AWS Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Amazon Machine Image (AMIs)</td>
<td>AMI of Identity Server and Access Gateway servers are created that are used in the auto scaling process.</td>
</tr>
<tr>
<td>AWS Auto Scaling</td>
<td>EC2 auto scaling launch configuration and auto scaling groups are created.</td>
</tr>
<tr>
<td>Key Management Service (KMS)</td>
<td>The AWS KMS key is created. This key is used for encrypting and decrypting Access Manager credentials to be stored in the AWS EC2 Parameter store.</td>
</tr>
<tr>
<td>EC2 Parameter Store</td>
<td>Access Manager credentials are stored in the EC2 Parameter store as a secure string.</td>
</tr>
<tr>
<td>Auto Scaling Life Cycle Hooks</td>
<td>Necessary Auto scaling life cycle hooks are created that helps in performing customized actions whenever auto scaling launches or terminates an instance.</td>
</tr>
<tr>
<td>Identity and Access Management (IAM) Roles</td>
<td>Necessary AWS IAM roles are created to automate the tasks involved in auto scaling.</td>
</tr>
<tr>
<td>AWS Lambda Functions</td>
<td>AWS Lambda functions are created that create AMI of Identity Servers and Access Gateway servers automatically.</td>
</tr>
<tr>
<td>AWS Simple Notification Service (SNS)</td>
<td>An AWS SNS topic is created. You can subscribe to this to receive notifications whenever an instance is launched and terminated during auto scaling.</td>
</tr>
</tbody>
</table>
Deploying Access Manager on Amazon Web Services EC2

### 6.3.1.3 Deploying the Auto Scaling Configuration

Perform the following steps to deploy the Access Manager auto scaling on AWS using the CloudFormation templates:

1. Download the CloudFormation templates package (https://www.netiq.com/documentation/access-manager-45/resources/AccessManagerAutoscale_45.zip) and extract the AccessManagerAutoscale.zip file.

2. Log in to AWS Console.

3. Click S3 > Create bucket.

4. Specify a bucket name.

5. Select a region and click Next.

6. Click the bucket name that you created.

7. Click Upload.

8. Drag and drop the following folders from the extracted content to the bucket:
   - logs
   - source

9. Upload the Access Manager installers (AM_45_AccessGatewayService_Linux64.tar.gz and AM_45_AccessManagerService_Linux64.tar.gz) to the S3 bucket.

10. Browse to the S3 bucket > source folder.

    The CloudFormation package contains the following six templates:

    | Filename | Description |
    |----------|-------------|
    | Schedule_Scaling_Identity_Server_Access_Gateway.yml | Use this template to deploy scheduled auto scaling of Identity Server and Access Gateway. |
    | Target_Tracking_Scaling_Identity_Server_Access_Gateway.yml | Use this template to deploy target tracking auto scaling of Identity Server and Access Gateway. |
    | Schedule_Scaling_Identity_Server.yml | Use this template to deploy scheduled auto scaling of Identity Server. |
    | Target_Tracking_Scaling_Identity_Server.yml | Use this template to deploy target tracking auto scaling of Identity Server. |
    | Schedule_Scaling_Access_Gateway.yml | Use this template to deploy scheduled auto scaling of Access Gateway. |
    | Target_Tracking_Scaling_Access_Gateway.yml | Use this template to deploy target tracking auto scaling of Access Gateway. |

11. Click the required CloudFormation template and copy Object URL.

12. Navigate to Services > CloudFormation and click Create Stack.

13. Select Specify an Amazon S3 template URL.

14. Specify the Object URL that you copied in Step 11 and click Next.

15. In Stack name, specify a name for the auto scaling configuration.
### Specify the following details in **Access Manager Configuration:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Name</td>
<td>The Access Manager administrator’s name of the existing Access Manager deployment.</td>
</tr>
<tr>
<td>Administrator Password</td>
<td>The password of the Access Manager administrator.</td>
</tr>
<tr>
<td>Administration Console IP Address</td>
<td>The IP address of Administration Console.</td>
</tr>
<tr>
<td>Identity Server Cluster Name</td>
<td>The name of the Identity Server cluster for which auto scaling needs to be configured.</td>
</tr>
<tr>
<td>Access Gateway Cluster Name</td>
<td>The name of the Access Gateway cluster for which auto scaling needs to be configured.</td>
</tr>
<tr>
<td>Platform</td>
<td>The name of the required operating system.</td>
</tr>
</tbody>
</table>

**IMPORTANT:** After specifying cluster details, ensure that you do not change the cluster name and cluster ID in the AWS Parameter Store. If you change the cluster ID, the auto scaling configuration will not work. If you change the cluster name, the cluster logs will display incorrect cluster name. This is applicable for both Identity Server cluster and Access Gateway cluster.

### Specify the following details in **Access Manager Installer Location:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3 Bucket Name</td>
<td>The name of the S3 bucket that contains auto scaling files and Access Manager installer.</td>
</tr>
<tr>
<td>S3 Bucket Region</td>
<td>The AWS region where the S3 bucket is created.</td>
</tr>
</tbody>
</table>

### Specify the following details in **EC2 Configuration:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Type</td>
<td>The AWS EC2 instance type for Access Manager components. To understand the instance types, see <a href="https://aws.amazon.com/ec2-instance-types/">Amazon EC2 Instance Types</a> and to understand the pricing for each instances, see <a href="https://aws.amazon.com/ec2/pricing/on-demand/">Amazon EC2 Pricing</a>.</td>
</tr>
<tr>
<td>SSH KeyPair Name</td>
<td>The existing EC2 key pair to enable SSH access to deployed servers.</td>
</tr>
<tr>
<td>VPC</td>
<td>ID of the Virtual Private Cloud (VPC) where Access Manager is deployed.</td>
</tr>
<tr>
<td>Identity Server Subnet</td>
<td>The existing subnets for Identity Servers deployment in the Access Manager VPC. Ensure that you select the subnets which are part of the selected VPC.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Access Gateway Server Subnet</td>
<td>The existing subnets for the Access Gateway deployment in the Access Manager VPC. Ensure that you select the subnets which are part of the selected VPC.</td>
</tr>
<tr>
<td>AWS Administrator</td>
<td>The AWS Administrator username with required rights to deploy auto scaling. <strong>NOTE</strong>: This field is case-sensitive.</td>
</tr>
</tbody>
</table>

19 Specify the following details in **Auto Scaling Configuration**:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Size</td>
<td>The initial size of the auto scaling group.</td>
</tr>
<tr>
<td>Minimum Size</td>
<td>The minimum required size for the auto scaling group. Access Manager will not scale in after this limit. It must be a numerical value.</td>
</tr>
<tr>
<td>Maximum Size</td>
<td>The maximum required size for the auto scaling group. Access Manager will not scale out beyond this limit. It must be a numerical value.</td>
</tr>
<tr>
<td>Scale Up Time</td>
<td>Access Manager nodes scale out to the maximum size at this time. <strong>Specify the time in the UNIX cron format.</strong></td>
</tr>
<tr>
<td>Scale Down Time</td>
<td>Access Manager nodes scale in to the minimum size at this time. <strong>Specify the time in the UNIX cron format.</strong></td>
</tr>
<tr>
<td>Metric Threshold Value</td>
<td>The minimum required size for the auto scaling group. Access Manager does not scale in after this limit. It must be a numerical value. This option is available only when you use a CloudFormation template for target tracking auto scaling.</td>
</tr>
<tr>
<td>Metric Value</td>
<td>The maximum required size for the auto scaling group. Access Manager does not scale out beyond this limit. It must be a numerical value. This option is available only when you use a CloudFormation template for target tracking auto scaling.</td>
</tr>
</tbody>
</table>

20 Click Next.
(optional) In **Tags**, specify the Key and Value for the resources available in the stack. This value will be applied to all resources created by the CloudFormation template.

In **Advanced**, specify additional details based on your requirements.

Click **Next** and review the stack details that you specified.

Select the acknowledgment check boxes and click **Create**.

### 6.3.1.4 Post-Deployment Tasks

When the auto scaling configuration is deployed, new instances of Identity Server and Access Gateway are created. Auto scaling works seamlessly with new instances that are created as part of the auto scaling group. The existing Identity Server and Access Gateway instances must be deleted.

Perform the following steps after the auto scaling configuration is deployed:

**For Identity Servers**

1. Log in to AWS EC2 Console.
2. Identify and terminate the AWS EC2 Identity Server instances that are created manually before deploying the auto scaling group.
3. Log in to Administration Console.
4. Go to the Identity Server cluster, identify, and delete Identity Server nodes that are added manually before deploying the auto scaling configuration.

**IMPORTANT:** If the initial size of the Identity Server auto scaling is two or more than two then all the scaled-up nodes might not appear with a green health status immediately. However, if the nodes do not appear with a green health status even after one hour, perform the following steps.

1. Log in to Administration Console.
2. Go to the Identity Server cluster and stop all the nodes.
3. Identify, and delete Identity Server nodes that are added manually before deploying the auto scaling configuration.
4. Restart all the nodes.

**For Access Gateway**

1. Log in to AWS EC2 Console.
2. Go to the Access Gateway auto scaling group.
3. Ensure that the primary Access Gateway instance is protected against scale-in. To verify, select the primary instance and right-click **Instance Protection**. Ensure that the **Enable Set Scale In Protection** option is enabled.
4. Log in to Administration Console.
5. Go to the Access Gateway cluster.
6. Ensure that the Access Gateway nodes that are created as part of the auto scaling group are listed in the Access Gateway cluster.
7. Ensure that the primary Access Gateway node IP is the same IP that is listed in the auto scaling group in AWS EC2 Console.
6.3.1.5 Customizing the Scaled Instances

In Administration Console, a cache of Identity Server and Access Gateway customization files is created when Identity Server and Access Gateways are imported into Administration Console and assigned to respective clusters. The auto scaling configuration creates new instances with the customization stored in the cache of Administration console.

When you make a change in customization files, Administration Console cache must be updated to updated the customization files. For example, you add a new option in the login page. Use the following APIs to update the Administration Console cache.

- `/customizations/cache/{clusterID}`: It refreshes the Administration Console cache with customized files from a device.
- `/customizations/{clusterID}/devices/{deviceID}`: It sends the customized files from Administration Console cache to the specified device.

For more information about how to invoke the APIs, see “Accessing Administration APIs” in the NetIQ Access Manager 4.5 Administration API Guide.

6.3.1.6 Troubleshooting Auto Scaling

The auto scaling configuration automatically creates log files and uploads the log files to the S3 bucket in the following scenarios:

- During AMI creation of Identity Server and Access Gateway
- Before terminating instances of Identity Server and Access Gateway

You can analyze these logs to identify the problem areas and troubleshoot. The following table lists the log files that are created and uploaded automatically to the S3 bucket > Logs location:

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/logs/idp_amis_&lt;log creation date&gt;_&lt;xxxxxx&gt;.tar.gz</td>
<td>The log file created while creating AMI for Identity Server</td>
</tr>
<tr>
<td>/logs/ag_amis_&lt;log creation date&gt;_&lt;xxxxxx&gt;.tar.gz</td>
<td>The log file created while creating AMI for Access Gateway</td>
</tr>
<tr>
<td>/logs/idp_i-_instance ID&gt;_instance IP address&gt;.tar.gz</td>
<td>The log file created while terminating an Identity Server instance</td>
</tr>
<tr>
<td>/logs/ag_i-_instance ID&gt;_instance IP address&gt;.tar.gz</td>
<td>The log file created while terminating an Access Gateway instance</td>
</tr>
</tbody>
</table>
6.3.1.7 Auditing Auto Scaling

You can configure Administrator Console to generate audit events whenever a new server is imported or deleted as part of the auto scaling process.

Perform the following steps:

1. In Administration Console Dashboard, click Auditing.
2. Under Management Console Audit Events, select the following options:
   - Server Imports: An event is generated whenever a server is imported into Administration Console.
   - Server Deletes: An event is generated whenever a server is deleted from Administration Console.
3. Click OK.

6.3.1.8 Monitoring Auto Scaling

This section provides the following options to monitor the auto scaling deployment:

- “Monitoring the Activity History” on page 119
- “Subscribing to Auto Scaling Notifications” on page 119

Monitoring the Activity History

1. Log in to AWS Console.
2. Click Services > Auto Scaling > Auto Scaling Groups.
3. Select an auto scaling group.
4. Click Activity History.
5. On the Activity History page, you can see various activity details of the automatically scaled instances. These details include start time, end time, reason of scaling, and so forth.

Subscribing to Auto Scaling Notifications

The auto scaling configuration creates two Simple Notification Service (SNS) topics automatically after a successful deployment. These SNS topics are created for Identity Server and Access Gateway. You can subscribe to these topics to receive notifications whenever a change occurs in the auto scaling deployment.

Perform the following steps to configure SNS:

1. Log in to AWS Console.
2. Click Services.
3. In Find Services, search for Simple Notification Service.
4. Select the SNS topic for which you want to receive notifications.
5. Click Create subscription.
6. In Protocol, select a protocol of your choice. For example, Email.
7. In Endpoint, specify your email address.
8 Click Create Subscription.

9 To confirm the subscription, Amazon SNS sends you an email. Click the link in the email to confirm your subscription.

### 6.3.1.9 Deleting a CloudFormation Stack

You can delete the CloudFormation stacks if required. Beware that deleting a CloudFormation stack deletes all configuration that you created as part of the deployment.

You can do it in the AWS CloudFormation console by selecting the main stack > Actions > Delete Stack. This action deletes all nested CloudFormation stack along with the main stack. However, some nested stacks may fail to be deleted and that prevents deleting the main stack. In such cases, you need to delete the failed nested CloudFormation stack first and then the main stack.

In some scenarios, the nested stacks fail to delete. In such scenarios, you must delete the resources created by these nested stacks. Perform the following steps to delete the resources.

1 Log in to AWS Console.

2 Navigate to Service > System manager > Parameter store.

3 Delete the parameters that nested stacks created.

4 Log in to Administration Console and delete the nodes that nested stacks created.


### 6.3.2 Limitations

The following list includes the limitations of the auto scaling process:

- The auto scaling configuration can be used only for scheduled scaling or target tracking policy for CPU utilization of the auto scaling group.

- During scale in, the auto scaling process terminates an Identity Server instance immediately if this instance does not have any active session. If Identity Server has an active session, it waits for a maximum of 60 minutes for session timeout before performing a periodical check for active sessions. After this duration, auto scaling forcibly terminates the instances.

  However, for an Access Gateway instance, auto scaling does not wait for even session timeout and terminates the instances immediately during scale in. In this scenario, Identity Server keeps a copy of the session to prevent the user to re-authenticate.

- If you delete an Identity Server stack and do not remove all the nodes that the stack created then the new stacks to be created might not work properly. It causes a number of non-responsive IPs to appear in the Identity Server cluster. These IPs do not belong to old or new stack and prevent the new nodes to have a green health status.

  To avoid this issue, you must delete all the old nodes before you create a new stack.
6.4 Monitoring Access Manager in AWS Using CloudWatch

Amazon CloudWatch provides real-time monitoring of the AWS resources.

It tracks various metrics and allows you to create alarms or send notifications when a metric reaches the threshold value. You can configure CloudWatch with CloudWatch Agent to collect system-level metrics and logs from the Access Manager instances and AWS resources. It includes AWS servers as well as on-premises servers.

For example, you can use CloudWatch to monitor the CPU usage and then determine whether you should create or delete instances to meet the dynamic load.

For more information on CloudWatch, see What Is Amazon CloudWatch? (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html)

For more information on CloudWatch Agent, see Collecting Metrics and Logs from Amazon EC2 Instances and On-Premises Servers with the CloudWatch Agent (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html).

Perform the following tasks to configure CloudWatch with on-premises servers.

1. Install AWS Command Line Interface (CLI) on the on-premises servers. Access Manager uses AWS CLI to access CloudWatch. The primary distribution method for AWS CLI is Python pip.
   Open a terminal window on the on-premises server run the following commands:
   1a Run the curl -O https://bootstrap.pypa.io/get-pip.py command to download the get-pip.py installer package.
   1b Run the pip install --upgrade awscli command to install AWS CLI.
   For more information about installing AWS CLI, see Installing the AWS CLI (https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-install.html).

2. Create IAM Users for CloudWatch Agent. IAM Users are required to access the AWS resources. For more information about creating IAM Users, see Create IAM Roles and Users for Use with the CloudWatch Agent (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create-iam-roles-for-cloudwatch-agent.html#create-iam-roles-for-cloudwatch-agent-users).

3. Install the CloudWatch Agent package on the Access Manager servers. For more information about installing the CloudWatch Agent package on servers see, Installing and Running the CloudWatch Agent on Your Servers (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/install-CloudWatch-Agent-commandline-fleet.html).

4. Specify the AWS IAM credentials and AWS Region using the aws configure command. When you run this command, AWS CLI prompts you to specify access key, secret access key, AWS Region, and output format.
   For more information about using the aws configure command, see Quickly Configuring the AWS CLI (https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-configure.html#cli-quick-configuration).

5. Create the CloudWatch Agent configuration file with configuration file wizard. The wizard prompts you to specify various details, for example monitoring metrics and log files location. Specify these details based on your requirements.
   For example, to monitor the Identity Server node logs, you must specify the following log file location in the configuration file.

   /opt/novell/nam/idp/logs/catalina.out
For more information about creating the configuration file using wizard, see Create the CloudWatch Agent Configuration File with the Wizard (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create-cloudwatch-agent-configuration-file-wizard.html).

6 Start CloudWatch Agent using the CloudWatch Agent configuration file that you created in the previous step. For example, if the configuration file is saved in the Systems Manager Parameter Store, run the following command:

```bash
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m onPremise -c ssm:configuration-parameter-store-name -s
```

In the above example command, `-a fetch-config` loads the latest version of the CloudWatch Agent configuration file and `-s` starts the CloudWatch Agent.

For more information about installing the CloudWatch Agent on servers and creating the configuration file, see Installing the CloudWatch Agent on On-Premises Servers (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/install-CloudWatch-Agent-on-premise.html).

7 Log in to AWS Console.

8 Click Services and search for the CloudWatch service.

9 In the CloudWatch dashboard, you can find log files under Logs and monitoring parameters like CPU and RAM under Metrics.

You can install CloudWatch Agent for EC2 instances. For more information see, Installing the CloudWatch Agent on EC2 Instances Using Your Agent Configuration (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/install-CloudWatch-Agent-on-EC2-Instance-fleet.html).
7 Deploying Access Manager on Microsoft Azure

You can deploy the following Access Manager components as services on Azure:

- Administration Console
- Identity Server
- Access Gateway

**NOTE:** Deployment of Access Gateway Appliance and Analytics Server is not supported on Azure.

Access Manager supports the following operating systems on Azure:

- SUSE Linux Enterprise Server (SLES) 12 SP4
- Red Hat Enterprise Linux (RHEL) 7.6
- RHEL 7.7 (Applicable for Access Manager 4.5 SP1 and later)

This section includes the following topics:

- Section 7.1, “Prerequisites for Deploying Access Manager on Microsoft Azure,” on page 123
- Section 7.2, “Deployment Procedure,” on page 124
- Section 7.3, “(Optional) Azure Load Balancer,” on page 130

7.1 Prerequisites for Deploying Access Manager on Microsoft Azure

In addition to system requirements of Access Manager components, ensure that you meet the following prerequisites:

- An administrative account on Azure.
- A resource group exists in Azure for the administrator.
- The Access Manager installer (tarball) has been downloaded, extracted, and available for copying to the virtual machines.
- An SSH key pair.
  This key pair is used for administrative access to the virtual machines over SSH. You can create the key pair by using ssh-keygen or a similar utility.

  For example, `ssh-keygen -t <type> -b <keysize>`

  Supported types include RSA, DSA, ECDSA, and Ed25519. The default algorithm is RSA. However, the ECDSA algorithm is recommended.

  When using ECDSA, supported key sizes are 256, 384, and 521.
By default, the resulting files are named as id <type> and id_<type>.pub. These files are available in your user accounts’ home folder. For example, /home/devuser/.ssh/

Remember to check the appropriate permissions on the certificate file by using chmod. For example, chmod 400 <filename>.

### 7.2 Deployment Procedure

The deployment procedure consists of the following steps:

1. Creating Azure Services
2. Creating and Deploying Virtual Machines
3. Configuring Network Security Groups
4. Changing the Private IP Address from Dynamic to Static
5. Installing Access Manager
6. (Optional) Azure Load Balancer

Figure 1-8 in Section 1.6, “Deploying Access Manager on Public Cloud,” on page 22 illustrates the recommended way for deploying Access Manager on Azure.

#### 7.2.1 Creating Azure Services

This section outlines general steps for creating Azure services for use with Access Manager.

For more information, see the Azure documentation.

**IMPORTANT:** While creating services, (such as availability set, virtual network, security groups, instances, and load balancers), ensure to specify the same value for Location.

Perform the following steps to create Azure services:

1. Log in to Azure (https://portal.azure.com/).
2. Create or determine an existing Resource group for use with Access Manager.
   2a. In the Azure portal, click New.
   2b. Search for resource group and select Resource group.
   2c. Click Create.


   **NOTE:** Not all administrators may have rights to create a new resource group.

3. Create or determine an existing Availability Set for use with Access Manager.
NOTE: If you plan to configure load balancing for Identity Server and Access Gateway, create a separate availability set for each cluster type.

3a In the Azure portal, click New.
3b Search for availability set and select Availability Set.
3c Click Create.
3d Specify values for Name, Subscription, Resource group, and Location.
3e Set Fault domains and Update domains to 2.
3f Click Create.

4 Create or determine a Virtual Network for use with Access Manager.
For this example configuration, all Access Manager components use the same virtual network.

4a In the Azure portal, click New.
4b Search for virtual network and select Virtual Network.
4c Click Create.
4d Configure the required network settings, such as Name, Subscription, Resource group, Location, Address Space, Subnet name, and Subnet address range.
The following is an example configuration:

Name: NAM-subnet1
Address space: 10.10.10.0/24
Subnet name: default
Subnet address range: 10.10.10.0/24
4e Click Create.

5 Continue with Section 7.2.2, “Creating and Deploying Virtual Machines,” on page 125.

7.2.2 Creating and Deploying Virtual Machines

This section outlines steps to create and deploy virtual machines for a basic setup of Access Manager, which includes an Administration Console, an Identity Server, an Access Gateway, and a user store.

Perform the following steps to create four virtual machines: one for Administration Console, one for Identity Server, one for Access Gateway, and one for the user store.

NOTE: If you are using Azure Active Directory as the user store, deploy virtual machines only for Access Manager components. Azure hosts and manages Azure Active Directory as a service on the cloud.

Perform the following steps to create and deploy a virtual machine:

1 Log in to Azure (https://portal.azure.com/).
2 Click New in the upper left pane of the dashboard.
3 In the search bar, search for SLES 12 SP4 or Red Hat Enterprise Linux 7.6 based on the operating system you want to use.
When creating a virtual machine for Active Directory, select a Windows 2016 R2 image instead of SLES or RHEL.

Each of these operating systems has their own licensing and costs associated with them. With the exception of the BYOS (Bring Your Own Subscription) option, each option includes a valid support license for the operating system.

**NOTE:** SLES 12 SP4 has been selected here as an example configuration.

4 Select SLES 12 SP4.

5 Click Create.

6 Configure the following settings in step 1 Basics:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify a name for the virtual machine.</td>
</tr>
<tr>
<td>VM disk type</td>
<td>Select SSD or HDD based on your requirements. This selection affects the list of templates displayed for selection in Step 8.</td>
</tr>
<tr>
<td>User name</td>
<td>Specify the name of the account that you want to use for administering the virtual machine. This username is used for ssh access to the virtual machine after deployment.</td>
</tr>
<tr>
<td>Authentication type</td>
<td>Select SSH public key.</td>
</tr>
<tr>
<td>SSH public key</td>
<td>Copy the content of your <code>id_rsa.pub</code> file that you have generated earlier, and paste it.</td>
</tr>
<tr>
<td>Subscription</td>
<td>Select the Azure subscription that should be used for the virtual machine.</td>
</tr>
<tr>
<td>Resource group</td>
<td>Select the resource group that you have created or determined in Step 2.</td>
</tr>
<tr>
<td>Location</td>
<td>Select from the list of the supported Azure location where you want to create the virtual machine.</td>
</tr>
</tbody>
</table>

7 Click OK.

8 In 2 Size, click View all to see all available templates.

You can filter this list based on disk type, vCPU, and memory.

Each template has its own intended use cases, optimizations, and costs per hour of usage.

Click a template that matches your requirements and the requirements of the Access Manager component that will later be installed on this virtual machine.

**NOTE:** You must select a virtual machine size of the **Standard** type if you require to configure an Azure load balancer later.

9 Click Select.

10 In 3 Settings, review networking, high availability, storage, and monitoring options by clicking the > icon.
Click OK.

In 4 Summary, review the summary of settings, terms of use, privacy policies, and cost of use.

Click Create.

Azure begins provisioning the virtual machine as you have configured it. This process may take a few minutes.

Verify SSH access to the virtual machine after deployment completes by running the following command:

```
ssh -i <keyfile> <username>@<publicIP>
```

Where,

- `<keyfile>`: The name of the certificate file created with ssh-keygen.
- `<username>`: The User name specified in Step 6 on page 126 while deploying the virtual machine.
<publicIP>: The public IP address assigned to the virtual machine. You can view this in the dashboard by clicking the virtual machine.

15 Repeat Step 1 to Step 14 to create additional virtual machines.


### 7.2.3 Configuring Network Security Groups

In the previous section Creating and Deploying Virtual Machines, a separate network security group is created for each virtual machine. You must modify these security groups to open the required incoming ports, depending on the Access Manager component type that will be installed on the virtual machine.

Edit the network security groups for Administration Console, Identity Server, and Access Gateway to configure the ports based on requirements of that component.

For information about the required ports, see Table 1-7, “Administration Console on Cloud,” on page 36, Table 1-8, “Identity Server on Cloud,” on page 37, and Table 1-9, “Access Gateway on Cloud,” on page 37.

1 In the Azure portal, click All resources.
2 You can filter the list can using the fields at the top of the page.
3 Find and click the desired network security group created in Step 10 on page 126.
4 Click Inbound security rules > Add.
5 Specify details in fields.

The following is an example configuration:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Any</td>
</tr>
<tr>
<td>Source port range</td>
<td>*</td>
</tr>
<tr>
<td>Destination</td>
<td>Any</td>
</tr>
<tr>
<td>Destination port range</td>
<td>8443</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Action</td>
<td>Allow</td>
</tr>
<tr>
<td>Priority</td>
<td>100</td>
</tr>
<tr>
<td>Name</td>
<td>Administration Console HTTPS</td>
</tr>
<tr>
<td>Description</td>
<td>HTTPS port for Access Manager Administration Console.</td>
</tr>
</tbody>
</table>

5 Repeat Step 3 and Step 4 for each inbound port rule to be added as listed in Table 1-7, “Administration Console on Cloud,” on page 36, Table 1-8, “Identity Server on Cloud,” on page 37, and Table 1-9, “Access Gateway on Cloud,” on page 37, depending on the component type that will use this network security group.

6 Continue with Section 7.2.4, “Changing the Private IP Address from Dynamic to Static,” on page 129.
7.2.4 Changing the Private IP Address from Dynamic to Static

The private IP addresses of Access Manager virtual machines must be static for proper communications between these devices.

Perform the following steps for each virtual machine:

1. In the Azure portal, click Virtual machines > name of the virtual machine.
2. Under Settings, click Networking.
3. Click the Network Interface.
4. In the left menu, click IP configurations under Settings.
5. Click the IP configuration line.
6. Under Assignment, click Static.
7. In IP address, specify the desired IP address.
8. Click Save.

7.2.5 Installing Access Manager

Prerequisites
- Ensure that you meet the network requirements listed in Network Requirements.
- Edit the /etc/hosts files on each virtual machine and add an entry to resolve its hostname to its private IP address.
- Ensure that the virtual machines do not have a default firewall configuration that could prevent proper installation and use of the Access Manager components.
- Ensure that the required port rules in the network security groups have been created.

Important Points to Consider before Installation

You must know the following points before you start the installation:

- Re-importing Identity Server and Access Gateway is not supported.
- Auto scaling of nodes is not supported. You can add or remove nodes manually. See “Recommendations for Scaling Access Manager Components in Public Cloud” on page 209.

Installation Procedure

Perform the following steps to install Access Manager components on virtual machines:

---

**IMPORTANT**: In the following steps, run the Access Manager installation scripts as a root user using sudo. For example, sudo sh <script-name>.

1. Copy the novell-access-manager-<version>.tar.gz file using Secure Copy (scp) to the virtual machines on which you will install Administration Console and Identity Server.

   The following is a sample scp command that shows how to copy the installer using the SSH key and username specified while creating the virtual machine:

   ```
   scp -i <key> <path/filename_of_tarball> <username>@<vm_ip>:/<path>
   ```
2 Copy the `novell-access-gateway-<version>.tar.gz` file to the virtual machine on which you will install Access Gateway.

3 Install Administration Console, Identity Server, and Access Gateway on respective virtual machines.

   For information about how to install these components, see Section 2.1, “Installing Administration Console on Linux,” on page 45, Section 3.2, “Installing Identity Server on Linux,” on page 58, and Section 4.3.1, “Installing Access Gateway Service on Linux,” on page 79.

   **IMPORTANT:** While installing Identity Server and Access Gateway, specify the internal IP address of the Administration Console machine. This ensures that communications among machines happen inside the firewall.

4 Configure Identity Server and Access Gateway.

   For information about how to configure, see “Setting Up a Basic Access Manager Configuration” in the *Access Manager 4.5 Administration Guide*.

### 7.3 (Optional) Azure Load Balancer

If multiple Access Gateway and Identity Server virtual machines have been created and configured for clustering, you can configure an Azure load balancer for each cluster to balance the load of incoming requests across the clustered machines. A separate load balancer is used for an Identity Server cluster and an Access Gateway cluster.

The following procedures provide the differences in configuration details for Identity Server and Access Gateway load balancer wherever required. Repeat the steps and create separate load balancers for Identity Server and Access Gateway clusters.

**Important points to consider before configuring an Azure load balancer for Access Manager:**

- All nodes of a cluster must be deployed in the same availability set. For example, all Identity Server nodes in a cluster are deployed in the same availability set, and all Access Gateway nodes in a cluster are deployed in a different availability set.
- Separate load balancers are required for Identity Server and Access Gateway.
- The Configuring a Load Balancer section includes examples assuming that the default ports are used (8080/8443 for Identity Server and 80/443 for Access Gateway). You can use iptables to configure the listeners on Identity Server to use other ports. See Translating Identity Server Configuration Port.
- Azure load balancer supports HTTP and TCP health check probe. It does not support the HTTPS probe.
  
  As such, using the Access Gateway heartbeat URL requires additional steps that are covered in the section “To Create a Reverse Proxy for Health Probe” on page 134.

**NOTE:** For scaling recommendations, see Appendix B, “Recommendations for Scaling Access Manager Components in Public Cloud,” on page 209.

- Section 7.3.1, “Creating a Load Balancer,” on page 131
- Section 7.3.2, “Configuring a Load Balancer,” on page 131
7.3.1 Creating a Load Balancer

You must create separate load balancers and configure separate settings, such as IP configuration, backend pool, probes, and rules settings for an Identity Server cluster and for an Access Gateway cluster.

IMPORTANT: Before creating a load balancer for an Access Gateway cluster, complete the steps available in To Create a Reverse Proxy for Health Probe.

Perform the following steps to create a load balancer:

1. In the Azure portal, click Load balancers.
2. Click Add.
3. Specify the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify a name for the load balancer.</td>
</tr>
<tr>
<td>Type</td>
<td>Select Public.</td>
</tr>
<tr>
<td>Public IP address</td>
<td>Create a new public IP address for this load balancer.</td>
</tr>
<tr>
<td></td>
<td>1. Click &gt;.</td>
</tr>
<tr>
<td></td>
<td>2. Click Create new.</td>
</tr>
<tr>
<td></td>
<td>3. Specify a name.</td>
</tr>
<tr>
<td></td>
<td>4. Select Static.</td>
</tr>
<tr>
<td></td>
<td>5. Click OK.</td>
</tr>
<tr>
<td>Subscription</td>
<td>Select the same Azure subscription that you have selected for virtual machines on which Access Manager is installed.</td>
</tr>
<tr>
<td>Resource group</td>
<td>Select the same resource group that you have selected for virtual machines on which Access Manager is installed.</td>
</tr>
<tr>
<td>Location</td>
<td>Select the same location that you have used for virtual machines.</td>
</tr>
</tbody>
</table>

4. Click Create.

7.3.2 Configuring a Load Balancer

1. In the Azure portal, click Load balancers.
2. Click the load balancer that you created in the previous procedure.
3. Configure the following settings:
   - Frontend IP configuration
   - Backend pools
   - Health Probes
   - Load balancing rules
Frontend IP configuration

By default, this setting takes the IP address you have configured in Public IP address while creating the load balancer.

You can create and select another IP address if you need to change this frontend IP address.

Backend pools

This setting provides a way to associate the load balancer to the IP addresses of virtual machines among which you want to distribute the load.

Perform the following steps to configure backend pools:

1. Click Backend pools.
2. Click Add.
3. Specify a name.
4. In Associated to, select Availability set.
5. Select the availability set for which you want to use this load balancer.
   This enables the load balancer to distribute the load among virtual machines available in the selected availability set.
6. Under Target network IP configuration, click Add a target network IP configuration.
7. In Target virtual machine, select the virtual machine that you want to add in the load balancer.
   You can select virtual machines available only in the specified availability set.
8. In Network IP configuration, select the related virtual machine.
9. Click Add a target network IP configuration to select other virtual machines from the same availability set to be added to the pool.
10. Click OK.

Health Probes

The load balancer uses probes to keep track of the health of virtual machines. If a probe fails, the related virtual machine is excluded from the load balancing automatically.

Perform the following steps to configure a health probe:

1. Click Health probes.
2. Click Add.
3. Specify a name.
4 Specify the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select HTTP.</td>
</tr>
</tbody>
</table>
| Port              | • For Identity Server listening on the default ports of 8080/8443, specify 8080.  
                  | • For Access Gateway, specify the port that you have configured in the reverse proxy for health probe. See “To Create a Reverse Proxy for Health Probe” on page 134.  
                  | IMPORTANT: You must configure these ports in network security groups associated with the respective Access Manager component’s cluster. |
| Path              | • For Identity Server, specify /nidp/app/heartbeat.  
                  | • For Access Gateway, specify /nesp/app/heartbeat.  
                  | IMPORTANT: An external communication to Access Gateway is typically configured to use HTTPS. Azure load balancer does not support the HTTPS probe. Therefore, when creating a health probe for an Access Gateway cluster, first create a reverse proxy that opens a non-SSL port for the probe URL. See “To Create a Reverse Proxy for Health Probe” on page 134. |
| Interval          | Specify the time after which the load balancer verifies the health of the virtual machine. |
| Unhealthy threshold | Specify the number. If the health probe fails for the specified number consecutively for a virtual machine, then the load balancer removes it automatically from the load distribution. |

5 Click OK.

Load balancing rules

This setting maps the frontend IP address and port combination to the backend IP addresses and port combination associated with virtual machines. You can configure multiple load balancing rules for a load balancer.

Perform the following steps to configure a load balancing rule:

1 Click Load balancing rules.
2 Click Add.
3 Specify the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify a name for the rule.</td>
</tr>
<tr>
<td>Frontend IP address</td>
<td>Select the frontend IP address for this rule.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select TCP.</td>
</tr>
</tbody>
</table>

**IMPORTANT:** If you want the load balancer to handle both HTTP and HTTPS traffic, create a separate rule for both by specifying appropriate ports in Port and Backend port.

The port configured in Port and Backend port must match the listening port configured in Identity Server or Access Gateway.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>For Access Gateway, specify the following values:</td>
</tr>
<tr>
<td></td>
<td>- For HTTPS traffic, specify 443.</td>
</tr>
<tr>
<td></td>
<td>- For HTTP traffic, specify 80.</td>
</tr>
<tr>
<td></td>
<td>For an Identity Server listening on the default ports of 8080/8443,</td>
</tr>
<tr>
<td></td>
<td>specify the following values:</td>
</tr>
<tr>
<td></td>
<td>- For HTTPS traffic, specify 8443.</td>
</tr>
<tr>
<td></td>
<td>- For HTTP traffic, specify 8080.</td>
</tr>
<tr>
<td>Backend port</td>
<td>For Access Gateway, specify the following values:</td>
</tr>
<tr>
<td></td>
<td>- For HTTPS traffic, specify 443.</td>
</tr>
<tr>
<td></td>
<td>- For HTTP traffic, specify 80.</td>
</tr>
<tr>
<td></td>
<td>For an Identity Server listening on the default ports of 8080/8443,</td>
</tr>
<tr>
<td></td>
<td>specify the following values:</td>
</tr>
<tr>
<td></td>
<td>- For HTTPS traffic, specify 8443.</td>
</tr>
<tr>
<td></td>
<td>- For HTTP traffic, specify 8080.</td>
</tr>
<tr>
<td>Backend pool</td>
<td>Select the backend pool for this rule.</td>
</tr>
<tr>
<td>Health probe</td>
<td>Select the health probe for this rule.</td>
</tr>
<tr>
<td>Session persistence</td>
<td>Keep the default value.</td>
</tr>
<tr>
<td>Idle timeout</td>
<td>Keep the default value.</td>
</tr>
<tr>
<td>Floating IP (direct server return)</td>
<td>Keep the default value.</td>
</tr>
</tbody>
</table>

4 Click OK.

**To Create a Reverse Proxy for Health Probe**

The port 80 on Access Gateway is reserved for redirects to the SSL port. Configure this reverse proxy to use any other free port.
Perform the following steps to create a reverse proxy for the health probe:

2. Under Reverse Proxy List, click New, and then specify a name.
3. Change the Non-Secure Port to a port that is not already in use by another reverse proxy.
4. Click New to create the proxy service.
5. Specify the following details:
   - **Field**: Proxy Service Name
     - **Description**: Specify a name that identifies the purpose of this proxy service.
   - **Field**: Published DNS Name
     - **Description**: Specify a value, such as HealthProbe. A value is required, however it is not used for connection purposes.
   - **Field**: Web Server IP Address
     - **Description**: Specify 127.0.0.1.
   - **Field**: Host Header
     - **Description**: Select Forward Received Host Name.

6. Click OK.
7. On the Reverse Proxy page, click the new proxy service under Proxy Service List, and then click Web Servers.
8. Change the Connect Port value to 9009.
   - The service provider (ESP) in Access Gateway that provides the heartbeat service listens on 127.0.0.1:9009.
9. Click Protected Resources.
10. Click New, specify a name and click OK.
11. In URL Path List, click /*, and modify the path to contain the following value:
    - `/nesp/app/heartbeat`
      - This is the path to the heartbeat application.
12. Click OK > OK.
13. Click OK and apply the changes to the configuration.
Installing Packages and Dependent RPMs on RHEL for Access Manager

**IMPORTANT:** You do not need to manually install the RPMs listed in Table 8-1 if the RHEL subscription is available. The install script takes care of installing required RPMs from the RHEL subscription.

**Important Points to Consider before Installing RHEL Packages and Dependent RPMs**

If you require to manually install the RPMs before the installation, you must consider the following points:

- You must install the RHEL Enterprise Server-with-GUI. Run the `sudo yum groupinstall "Server with GUI"` command to obtain the required RPMs.
- To avoid RPM dependency issues, NetIQ Corporation recommends installing the package along with its respective dependent RPMs. You can also install all packages together in the same sequence as these appear in Table 8-1.
- The version of RPMs varies based on the base operating system version of RHEL. Table 8-1 lists RPMs for RHEL 7.6.
- You must install these RPMs in the same sequence as they appear in Table 8-1.

**Table 8-1   RHEL Packages and Dependent RPMs**

<table>
<thead>
<tr>
<th>Package</th>
<th>Dependent RPM</th>
</tr>
</thead>
<tbody>
<tr>
<td>glibc-2.17-260.el7.i686.rpm</td>
<td>• nss-softokn-freebl-3.36.0-5.el7_5.i686</td>
</tr>
<tr>
<td></td>
<td>This must be installed along with glibc-2.17-260.el7.i686.rpm. To install these rpm files together, run the following:</td>
</tr>
<tr>
<td></td>
<td>rpm -ivh glibc-2.17-260.el7.i686.rpm nss-softokn-freebl-3.36.0-5.el7_5.i686.rpm</td>
</tr>
<tr>
<td>libstdc++-4.8.5-36.el7.i686.rpm</td>
<td>• glibc-2.17-260.el7.i686.rpm</td>
</tr>
<tr>
<td></td>
<td>• libgcc-4.8.5-36.el7.i686.rpm</td>
</tr>
<tr>
<td>libstdc++-4.8.5-36.el7.x86_64.rpm</td>
<td>• glibc-2.17-260.el7.x86_64.rpm</td>
</tr>
<tr>
<td></td>
<td>• libgcc-4.8.5-36.el7.x86_64.rpm</td>
</tr>
<tr>
<td>libstdc++-4.8.5-36.el7.i686</td>
<td>• glibc-2.17-260.el7.i686</td>
</tr>
<tr>
<td></td>
<td>• libgcc-4.8.5-36.el7.i686</td>
</tr>
<tr>
<td>libstdc++-4.8.5-36.el7.x86_64</td>
<td>• glibc-2.17-260.el7.x86_64</td>
</tr>
<tr>
<td></td>
<td>• libgcc-4.8.5-36.el7.x86_64</td>
</tr>
<tr>
<td>Package</td>
<td>Dependent RPM</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>libstdc++-4.8.5-36.el7.x86_64</td>
<td>• libgcc-4.8.5-36.el7.x86_64</td>
</tr>
<tr>
<td>libXau-1.0.8-2.1.el7.x86_64.rpm</td>
<td>• glibc-2.17-260.el7.i686.rpm</td>
</tr>
<tr>
<td>xcb-1.13-1.el7.x86_64.rpm</td>
<td>• glibc-2.17-260.el7.i686.rpm</td>
</tr>
<tr>
<td>libxcb-1.13-1.el7.x86_64.rpm</td>
<td>• libXau-1.0.8-2.1.el7.x86_64.rpm</td>
</tr>
<tr>
<td>libX11-1.6.5-2.el7.x86_64.rpm</td>
<td>• glibc-2.17-260.el7.i686.rpm</td>
</tr>
<tr>
<td>libxext-1.3.3-3.el7.x86_64.rpm</td>
<td>• libXau-1.0.8-2.1.el7.x86_64.rpm</td>
</tr>
<tr>
<td>libxi-1.7.9-1.el7.x86_64.rpm</td>
<td>• glibc-2.17-260.el7.i686.rpm</td>
</tr>
<tr>
<td>libxtst-1.2.3-1.el7.x86_64.rpm</td>
<td>• libX11-1.6.5-2.el7.x86_64.rpm</td>
</tr>
<tr>
<td>libxcb-1.13-1.el7.x86_64.rpm</td>
<td>• libX11-1.6.5-2.el7.x86_64.rpm</td>
</tr>
<tr>
<td>libX11-1.6.5-2.el7.x86_64.rpm</td>
<td>• libXext-1.3.3-3.el7.x86_64.rpm</td>
</tr>
<tr>
<td>libxtst-1.2.3-1.el7.x86_64.rpm</td>
<td>• glibc-2.17-260.el7.i686.rpm</td>
</tr>
<tr>
<td>libXrender-0.9.10-1.el7.x86_64.rpm</td>
<td>• No dependency</td>
</tr>
<tr>
<td>Administration Console</td>
<td></td>
</tr>
<tr>
<td>gettext-0.19.8.1-2.el7.x86_64</td>
<td>• No dependency</td>
</tr>
<tr>
<td>glibc-2.17-260.el7.i686.rpm</td>
<td>• nss-softokn-3.36.0-5.el7_5.x86_64.rpm</td>
</tr>
<tr>
<td>libstdc++-4.8.5-36.el7.i686.rpm</td>
<td>• glibc-2.17-260.el7.i686.rpm</td>
</tr>
<tr>
<td>libgcc-4.8.5-36.el7.i686.rpm</td>
<td>• libgcc-4.8.5-36.el7.i686.rpm</td>
</tr>
<tr>
<td>ncurses-libs-5.9-14.20130511.el7_4.i686.rpm</td>
<td>• glibc-2.17-260.el7.i686.rpm</td>
</tr>
<tr>
<td>libgcc-4.8.5-36.el7.i686.rpm</td>
<td>• No dependency</td>
</tr>
<tr>
<td>rsyslog-8.24.0-34.el7.x86_64</td>
<td>• No dependency</td>
</tr>
<tr>
<td>rsyslog-gnutls-8.24.0-34.el7.x86_64</td>
<td>• No dependency</td>
</tr>
<tr>
<td>binutils-2.27-34.base.el7.x86_64</td>
<td>• No dependency</td>
</tr>
<tr>
<td>gperftools-libs-2.4-8.el7.x86_64</td>
<td>• No dependency</td>
</tr>
<tr>
<td>ntp-4.2.6p5-28.el7.x86_64</td>
<td>• No dependency</td>
</tr>
<tr>
<td>Package</td>
<td>Dependent RPM</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td><strong>Identity Server</strong></td>
<td></td>
</tr>
<tr>
<td>glibc-2.17-260.el7.i686.rpm</td>
<td>• nss-softokn-3.36.0-5.el7_5.x86_64</td>
</tr>
<tr>
<td>libstdc++-4.8.5-36.el7.i686</td>
<td>• glibc-2.17-260.el7.i686.rpm</td>
</tr>
<tr>
<td>ncurses-libs-5.9-14.20130511.el7_4.i686.rpm</td>
<td>• glibc-2.17-260.el7.i686.rpm</td>
</tr>
<tr>
<td>libgcc-4.8.5-36.el7.i686.rpm</td>
<td>• No dependency</td>
</tr>
<tr>
<td>rsyslog-8.24.0-34.el7.x86_64</td>
<td>• No dependency</td>
</tr>
<tr>
<td>rsyslog-gnutls-8.24.0-34.el7.x86_64</td>
<td>• No dependency</td>
</tr>
<tr>
<td>binutils-2.27-34.base.el7.x86_64</td>
<td>• No dependency</td>
</tr>
<tr>
<td>ntp-4.2.6p5-28.el7.x86_64</td>
<td>• No dependency</td>
</tr>
<tr>
<td><strong>Access Gateway</strong></td>
<td></td>
</tr>
<tr>
<td>glibc-2.17-260.el7.i686.rpm</td>
<td>• nss-softokn-freebl-3.16.2.3-14.4.el7.i686</td>
</tr>
<tr>
<td>apr-1.4.8-3.el7_4.1.x86_64</td>
<td>• glibc-2.17-260.el7.i686.x86_64.rpm</td>
</tr>
<tr>
<td>apr-util-1.5.2-6.el7.x86_64</td>
<td>• apr-1.4.8-3.el7_4.1.x86_64.rpm</td>
</tr>
<tr>
<td>libtool-ltdl-2.4.2-22.el7_3.x86_64</td>
<td>• glibc-2.17-260.el7.x86_64.rpm</td>
</tr>
<tr>
<td>unixODBC-2.3.1-11.el7.x86_64</td>
<td>• libtool-ltdl-2.4.2-22.el7_3.x86_64.rpm</td>
</tr>
<tr>
<td>libesmtp-1.0.6-7.el7.x86_64</td>
<td>• glibc-2.17-260.el7.x86_64.rpm</td>
</tr>
<tr>
<td>rsyslog-8.24.0-34.el7.x86_64</td>
<td>• No dependency</td>
</tr>
<tr>
<td>rsyslog-gnutls-8.24.0-34.el7.x86_64</td>
<td>• No dependency</td>
</tr>
<tr>
<td>binutils-2.27-34.base.el7.x86_64</td>
<td>• No dependency</td>
</tr>
<tr>
<td>patch-2.7.1-10.el7_5.x86_64</td>
<td>• No dependency</td>
</tr>
<tr>
<td>ntp-4.2.6p5-28.el7.x86_64</td>
<td>• No dependency</td>
</tr>
</tbody>
</table>

Use the following command to verify whether a package is installed on RHEL:

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

Use the following command to install a RPM:

```
rpm -ivh <rpm name>
```

Use the following command to install all RPMs together:

```
rpm -ivh <rpm name> <rpm name> <rpm name> ...
```

Perform the following steps to install packages and their dependent RPMs while installing RHEL:

1. Mount the RHEL CD-ROM by running the following command and go to the Packages folder:
mount /dev/cdrom /mnt

**NOTE:** If the RHEL CD-ROM is auto mounted, the mount path will be /media/RHEL_x.x\ x86_64 Disc 1. (The x in RHEL_x.x represents the version number) Unmount the default mount path by using the unmount /media/RHEL_x.x\ x86_64\ Disc\ 1/command and then mount the RHEL CD-ROM by using mount /dev/cdrom /mnt.

2. If you have a locally mounted ISO image, you can install RPMs for Access Manager by providing the mount path to the installer. The install.sh scripts prompts for the mounted disc if it identifies that the required RPMs are not installed. Provide the mount path to the installer with an ending /. For example, /mnt/.

**NOTE:** Installer will install only RPMs required for Access Manager components. You need to install iManager RPMs separately.

Install RPMs for SNMP after installing RPMs for Administration Console. See “RHEL Packages and Their Dependent RPMs for SNMP” on page 140.

**RHEL Packages and Their Dependent RPMs for SNMP**

The RHEL base installation does not install the net-snmp package by default. Install the following packages manually to make the net-snmp service (Master Agent) functional:

- net-snmp-libs-5.7.2-37.el7.x86_64.rpm
- net-snmp-5.7.2-37.el7.x86_64.rpm

Use the following procedure to install these packages to avoid any dependency issue:

1. Mount the RHEL CD-ROM by running the following command:
   ```
   mount /dev/cdrom /mnt
   ```

2. Run the following commands:
   ```
   yum install --nogpgcheck net-snmp-libs-5.7.2-37.el7.x86_64.rpm
   yum install --nogpgcheck net-snmp-5.7.2-37.el7.x86_64
   ```

3. After installation, run `/etc/init.d/novell-snmpd start`. **This will succeed for a successful installation.**

140  Installing Packages and Dependent RPMs on RHEL for Access Manager
9 Uninstalling Components

This section provides the required uninstallation steps:

- Section 9.1, “Uninstalling Identity Server,” on page 141
- Section 9.2, “Reinstalling an Identity Server to a New Hard Drive,” on page 142
- Section 9.3, “Uninstalling Access Gateway,” on page 143
- Section 9.4, “Uninstalling Administration Console,” on page 144

9.1 Uninstalling Identity Server

Uninstalling Identity Server is a two-step process:


9.1.1 Deleting Identity Server References

As part of the full Identity Server uninstall process, you must delete Identity Server from Administration Console. Identity Server must first be removed from the cluster configuration, then it can be deleted from Administration Console. You must do this before removing the software from the machine.

1 In Administration Console, click Devices > Identity Servers.
2 Select Identity Server that you want uninstalled, then click Stop.
3 Wait for its health to turn red, then select the server and click Actions > Remove from Cluster.
4 Update the cluster configuration.
5 Select Identity Server that you are going to uninstall, then click Actions > Delete.
6 Continue with Section 9.1.2, “Uninstalling the Linux Identity Server,” on page 141 or Section 9.1.3, “Uninstalling the Windows Identity Server,” on page 142.

9.1.2 Uninstalling the Linux Identity Server

If you have installed Identity Server with Administration Console, you can select to uninstall only Identity Server or to uninstall both.

1 On your Linux Identity Server, insert the Access Manager installation CD.
2 Navigate to the novell-access-manager directory.
3 Enter ./uninstall.sh to initiate the uninstallation script.
4 Select 2 to uninstall Identity Server.
5 Enter the name and password of the admin user. (When Administration Console and Identity Server are installed on the same server)
   Uninstall removes Identity Server. A log file is created at /tmp/novell_access_manager/uninstall.log.

9.1.3 Uninstalling the Windows Identity Server

If you have installed Identity Server with Administration Console, you can select to uninstall only Identity Server or to uninstall both.

1 Exit any applications and disable any virus scanning programs.
2 Access the Control Panel, click Add or Remove Programs, then select to remove the AccessManagerServer program.
3 Read the introduction, then click Next.
4 Specify the credentials for the admin user, then click Next.
5 Select one of the following, then click Next.
   - Complete Uninstall: Select this option if you have installed both Identity Server and Administration Console on the same machine and you want to uninstall both.
   - Uninstall Specific Features: Select this option to uninstall only Identity Server.
6 (Conditional) If you selected to uninstall specific features, select one of the following, then click Uninstall.
   - Administration Console: Select this option to uninstall Administration Console. You cannot uninstall Administration Console without uninstalling Identity Server.
   - Identity Server: Select this option to uninstall only Identity Server.
   If the uninstall fails because the primary Administration Console is not available to validate the credentials, see “Uninstalling the Windows Identity Server” on page 142.
7 (Conditional) If Administration Console was installed with Identity Server and you selected only to uninstall Identity Server, reboot the machine.

9.2 Reinstalling an Identity Server to a New Hard Drive

If your Identity Server hard drive fails, you must reinstall Identity Server (see Chapter 3, “Installing Identity Server,” on page 57) and leave Identity Server configuration intact in Administration Console. To preserve the existing keystores, perform the following steps before installing Identity Server on the new hard drive.

1 Stop the server.
   In Administration Console, click Access Manager > Identity Servers. Select the server and click Stop. Allow a few seconds for the server to stop.
2 Select the server, then click Actions > Remove from Cluster.
3 Select the server, then click Actions > Delete.
4 Reinstall Identity Server. (See Chapter 3, “Installing Identity Server,” on page 57.)
5 On Identity Server page, select the server, then click Actions > Assign to Cluster.
6 Select the Identity Server cluster configuration, then click Assign.
7 Click OK.

9.3 Uninstalling Access Gateway

1 In Administration Console, click Access Gateways.
2 If Access Gateway belongs to a cluster, you need to remove it from the cluster.
   2a Select Access Gateway, then click Actions > Remove from Cluster:
   2b Confirm the action, then click OK.
3 On Access Gateways Servers page, select the name of the server, then click Actions > Delete > OK.
This removes the configuration object for Access Gateway from Administration Console.
4 On the Identity Server page, update the Identity Server status for the Identity Server cluster configuration that was using this Access Gateway.
See Updating Identity Server Configuration in the Access Manager 4.5 Administration Guide.
5 Complete one of the following:
   - If you are uninstalling Access Gateway Appliance machine, re-image the machine by booting to a CD containing the desired operating system software.
   - If you are uninstalling the Windows Access Gateway Service, continue with Section 9.3.1, “Uninstalling Windows Access Gateway Service,” on page 143.
   - If you are uninstalling the Linux Access Gateway Service, continue with Section 9.3.2, “Uninstalling Linux Access Gateway Service,” on page 143.

9.3.1 Uninstalling Windows Access Gateway Service

1 Exit any applications and disable any virus scanning programs.
2 Access the Control Panel, click Add or Remove Programs and select to remove the AccessGateway program.
3 Click Next.
4 Specify the credentials for the admin user, then click Uninstall.

9.3.2 Uninstalling Linux Access Gateway Service

1 On your Linux Access Gateway Service, insert the Access Manager installation CD.
2 Navigate to the novell-access-gateway directory.
3 Enter ./uninstall.sh to initiate the uninstallation script.
4 Enter the name of the admin user.
5 Enter the password of the admin user.
   Uninstall removes Access Gateway Service. A log file is created at /tmp/novell_access_manager/uninstall.log.
9.4 Uninstalling Administration Console

Only the primary version of Administration Console contains the certificate authority. If you uninstall this version, you can no longer use Access Manager for certificate management. You need to promote a secondary console to be the primary console. See Installing Secondary Administration Console in the Access Manager 4.5 Administration Guide.

**IMPORTANT:** If you are uninstalling all Access Manager devices, the primary Administration Console must be the last device you uninstall. The uninstall programs for the other devices contact the primary Administration Console and validate the admin’s credentials before allowing the device to be removed.

Select the process that corresponds to your platform:

- Section 9.4.1, “Uninstalling Linux Administration Console,” on page 144
- Section 9.4.2, “Uninstalling Windows Administration Console,” on page 145

9.4.1 Uninstalling Linux Administration Console

1. Insert CD 1 into the drive.
2. Log in as the root user or equivalent.
3. At the command prompt of the Access Manager directory, enter the following:
   
   ```
   ./uninstall.sh
   ```

   **IMPORTANT:** If SLES 12 SP4 has the latest patches from SUSE update channel, run the `systemctl enable ndsd.service` command and then choose option 6.

4. Specify option 6 to uninstall all products or specify Q to quit without uninstalling.
   You must use option 6 instead of option 1.
5. After running the `./uninstall.sh` script, go to Auditing > Troubleshooting > Other Known Device Manager Servers, then remove the entry for this secondary Administration Console from the servers list.
   A log file is created at `/tmp/novell_access_manager_uninstall.log`.

9.4.1.1 Removing Administration Console Replicas

Remove any traces of the Administration Console replicas from the configuration datastore:

1. In Administration Console Dashboard, click `<user name>` at the top right of the page and then click Configure Console.
2. Click Objects.
3. In the tree view, click novell.
4. Delete all objects that reference the failed primary Administration Console. You should find the following types of objects:
   - SAS Service object with the hostname 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 hostname of the failed primary console
DNS IP object with the hostname of the failed primary console
SSL CertificateDNS with the hostname of the failed primary console
SSL CertificateIP with the hostname of the failed primary console
NCP server object

5 Run the /opt/novell/eDirectory/bin/ndsstat -r command to view the list of available replicas.

6 If you can still see the replica that you deleted from Other Known Device Manager Servers, then perform the following steps:
   6a Log in to Administration Console as a root user.
   6b Change to the /opt/novell/eDirectory/bin directory.
   6c Run the ndsrepair -P -Ad command.
   6d Select the replica and click View replica ring.
       Select the name of the replica that is visible and click Remove this server from replica ring.
   6e Specify the DN of the admin user in leading dot notation. For example, .admin.novell.
   6f Specify the password and select I Agree.

9.4.2 Uninstalling Windows Administration Console

When you uninstall Administration Console, any other Access Manager components on the machine must also be uninstalled.

1 Exit any applications and stop any virus scanning programs.
2 Access the Control Panel, click Add or Remove Programs, then select to remove the AccessManagerServer program.
3 Read the introduction, then click Next.
4 Specify the credentials for the admin user, then click Next.
5 Click Complete Uninstall, then click Next.
6 Restart the machine.

NOTE: Some services are not completely removed. To remove it completely, you must remove few registry settings after restarting the server. For information about removing required registry settings, see “Deleting Services from Registry” on page 146.
9.4.2.1 Deleting Services from Registry

When you uninstall Administration Console by using the steps mentioned in Section 9.4.2, “Uninstalling Windows Administration Console,” on page 145, some service are not deleted. To delete the required services to uninstall Administration Console completely from the machine, perform the following steps:

1. Stop SLP service
2. Back up the registry settings
3. Remove HKLM>SOFTWARE>Wow6432Node>Apache Software Foundation
4. Remove HKLM>SOFTWARE>Novell
5. Remove HKLM>SOFTWARE>Wow6432Node>Microsoft>Windows>CurrentVersion\Uninstall>NetsIQ iManager
6. Remove HKLM>SOFTWARE>Microsoft>Windows>CurrentVersion>App Paths>java.exe
7. Remove HKLM>SOFTWARE>Microsoft>Windows>CurrentVersion>Uninstall>NDSonNT
8. Remove HKLM>SOFTWARE>Wow6432Node>JavaSoft
9. Remove HKLM>SYSTEM>ControlSet001>Services>EventLog>Application>NDS Server
10. Remove HKLM>SYSTEM>ControlSet001>Services>NDS Server
11. Remove HKLM>SYSTEM>ControlSet001>Services>slpd
12. Remove HKLM>SYSTEM>ControlSet001>Services>SNMP>Parameters>ExtensionAgents>Novell.eDir-Snmp.1
13. Remove HKLM>SYSTEM>ControlSet001>Services>Tomcat8
14. Remove HKLM>SYSTEM>ControlSet002>Services>EventLog>Application>NDS Server
15. Remove HKLM>SYSTEM>ControlSet002>Services>NDS Server
16. Remove HKLM>SYSTEM>ControlSet002>Services>slpd
17. Remove HKLM>SYSTEM>ControlSet002>Services>SNMP>Parameters>ExtensionAgents>Novell.eDir-Snmp.1
18. Remove HKLM>SYSTEM>ControlSet002>Services>Tomcat8
19. Remove all files from the following location:
   * C:\Program Files (x86)\Novell
   * C:\Program Files\Common Files\Novell
   * C:\Novell\NDS
20. Restart the machine.
Upgrading Access Manager

This section discusses how to upgrade Access Manager to the newer version. You must take a backup of the existing configurations before upgrading Access Manager components.

For more information, see “Back Up and Restore” in the Access Manager 4.5 Administration Guide.

**NOTE:** By default, the Access Manager configuration uses stronger TLS protocols, ciphers, and other security settings. If you want to revert these settings after upgrading, see “Restoring Previous Security Level After Upgrading Access Manager” in the NetIQ Access Manager 4.5 Security Guide.

When you upgrade Access Manager components, first back up your configuration and then move Administration Console. You can then upgrade other devices that you have imported into Administration Console.

You must upgrade the Access Manager components in the following sequence:

1. Administration Console
2. Identity Server
3. Access Gateway
4. (Optional) Analytics Server

**Supported Upgrade Paths**

To upgrade to Access Manager 4.5, you need to be on one of the following versions of Access Manager:

- 4.4 Service Pack 2
- 4.4 Service Pack 3
- 4.4 Service Pack 4

For information about the latest supported upgrade paths, see the specific Release Notes on the Access Manager Documentation Website (https://www.netiq.com/documentation/access-manager-45/).

**Important Points to Consider**

- If you have installed additional nodes of Administration Console on other servers for fault tolerance, ensure to first upgrade the primary Administration Console. Else, the directory schema does not get updated.
- Upgrade all nodes of a cluster before you start upgrading another type of device.
- When nodes in a cluster are running on different release versions, you must not change any configuration through Administration Console.
This section includes the following topics:

- Chapter 10, “Prerequisites for Upgrading Access Manager,” on page 149
- Chapter 11, “Upgrading Administration Console,” on page 153
- Chapter 12, “Upgrading Identity Server,” on page 159
- Chapter 13, “Upgrading Access Gateway,” on page 165
- Chapter 14, “Upgrading Analytics Server,” on page 179
- Chapter 15, “Getting the Latest OpenSSL Updates for Access Manager,” on page 183
Prerequisites for Upgrading Access Manager

Watch the following video for important considerations that you must know before starting the Access Manager upgrade:

http://www.youtube.com/watch?v=u6l2815jhDM

Before performing an upgrade, ensure that the following prerequisites are met:

- Any option that is configured through the \texttt{nidpconfig.properties} file will be overwritten after upgrade. Therefore, back up the \texttt{nidpconfig.properties} file before upgrading to Access Manager 4.5. After the upgrade, replace the new \texttt{nidpconfig.properties} file with the backed up file.

**Identity Server:**

\textbf{Linux:} /opt/novell/nids/lib/webapp/WEB-INF/classes/nidpconfig.properties

\textbf{Windows:} C:\Program Files\Novell\Tomcat\webapps\nidp\WEB-INF\classes\nidpconfig.properties

**Access Gateway:**

\textbf{Linux:} /opt/novell/nesp/lib/webapp/WEB-INF/classes/nidpconfig.properties

\textbf{Windows:} C:\Program Files\Novell\Tomcat\webapps\nesp\WEB-INF\classes\nidpconfig.properties

- Some of the options are supported only through Administration Console. After the upgrade, configure those options through Administration Console. For the list of options that must be configured through Administration Console, see Configuring Identity Server Global Options, Configuring ESP Global Options, Defining Options for SAML 2.0 in the Access Manager 4.5 Administration Guide.

- Access Manager 4.2 and later versions do not support Platform Agent and Novell Audit. If you are upgrading from an older version of Access Manager where you have configured Platform Agent, ensure to remove this configuration before upgrading to the latest version. Otherwise, auditing will fail because the Platform Agent service is not available post upgrade.

- The upgrade process overwrites all customized JSP files. If you have customized JSP files for Identity Server or Access Gateway, you must perform manual steps to maintain the customized JSP files. For more information, see Section 10.1, “Maintaining Customized JSP Files for Identity Server,” on page 150 or Section 10.2, “Maintaining Customized JSP Files for Access Gateway,” on page 152.

- If you have customized any changes to \texttt{tomcat.conf} or \texttt{server.xml}, back up the files. After the upgrade, restore the files.

- If you have installed the unlimited strength java crypto extensions before upgrade, re-install it after the upgrade because a new Java version will be used.
If you are using Kerberos, back up the /opt/novell/nids/lib/webapp/WEB-INF/classes/kerb.properties file. After the upgrade, restore the files.

Similarly, if you are using any customized files, ensure to back it up and copy the customized content from the backed up file to the upgraded file after the upgrade is successful.

If you have made any customization in the /opt/novell/nam/idp/webapps/nidp/META-INF/context.xml file, back up the file.

After the upgrade, add the customized content to the upgraded context.xml file and uncomment the following lines in the context.xml file:

```xml
<!-- Force use the old Cookie processor (because this new tomcat version uses RFC6265 Cookie Specification) -->
<!-- <CookieProcessor className="org.apache.tomcat.util.http.LegacyCookieProcessor" /> -->
</Context>
```

(Linux) Ensure to perform the following procedure for both SLES and Red Hat:

1. Open the nds.conf file available under /etc/opt/novell/eDirectory/conf/.
2. Delete all the duplicate lines from the file. For example the file may contain two lines of n4u.server.vardir=/var/opt/novell/eDirectory/data. Delete one of them.

If you have enabled history for risk-based authentication in a prior version of Access Manager, you must upgrade the database for risk-based authentication after upgrading to 4.5. You can find the upgrade script here: /opt/novell/nids/lib/webapp/WEB-INF/RiskDBScript.zip.

- **MySQL**: Run netiq_risk_mysql_upgrade.sql
- **Oracle**: Run netiq_risk_oracle_upgrade.sql
- **Microsoft SQL Server**: Run netiq_risk_sql_server_upgrade.sql

In addition to these prerequisites, ensure that you also meet the hardware requirements. For more information about hardware requirements, see the component-specific requirements in Part I, “Installing Access Manager,” on page 43.

### 10.1 Maintaining Customized JSP Files for Identity Server

Access Manager contains a default user portal and a set of default login pages from Access Manager 4.2 onwards. The new login pages have a different look and feel compared to the default login pages of Access Manager 4.1 or prior. If you have customized the legacy user portal, you can maintain the customized JSP pages in the following two ways:

- **Using Customized JSP Pages from Access Manager 4.1 or Prior**
- **Using Customized JSP Pages from Access Manager 4.1 or Prior and Enabling the New Access Manager Portal**

#### 10.1.1 Using Customized JSP Pages from Access Manager 4.1 or Prior

1. Before upgrade, create a copy of all JSP files inside the jsp directory and place the copy somewhere else.
**Prerequisites for Upgrading Access Manager**

1. **Linux:** `/opt/novell/nids/lib/webapp/jsp`
   
   **Windows:** `\Program Files\Novell\Tomcat\webapps\nidp\jsp`

   **WARNING:** The upgrade overwrites all existing JSP files.

2. Upgrade Identity Server.

3. Create an empty folder `legacy` in Identity Server
   
   **Linux:** `/opt/novell/nids/lib/webapp/WEB-INF/legacy`
   
   **Windows:** `\Program Files\Novell\Tomcat\webapps\nidp\WEB-INF\legacy`

   **NOTE:** If you do not create the `legacy` folder, Access Manager uses the logic of the default new login pages.

4. Copy your all backed up JSP files into the `jsp` directory.
   
   **Linux:** `/opt/novell/nids/lib/webapp/jsp`
   
   **Windows:** `\Program Files\Novell\Tomcat\webapps\nidp\jsp`

5. Refresh the browser to see the changes.

### 10.1.2 Using Customized JSP Pages from Access Manager 4.1 or Prior and Enabling the New Access Manager Portal

1. Before upgrade, create a copy of all JSP files inside the `jsp` directory and place the copy somewhere else.
   
   **Linux:** `/opt/novell/nids/lib/webapp/jsp`
   
   **Windows:** `\Program Files\Novell\Tomcat\webapps\nidp\jsp`

   **WARNING:** The upgrade overwrites all existing JSP files.

2. Upgrade Identity Server.

3. Create an empty folder `legacy` in Identity Server
   
   **Linux:** `/opt/novell/nids/lib/webapp/WEB-INF/legacy`
   
   **Windows:** `\Program Files\Novell\Tomcat\webapps\nidp\WEB-INF\legacy`

   **NOTE:** If you do not create the `legacy` folder, Access Manager uses the logic of the default new login pages.

4. Copy your all backed up JSP files into the `jsp` directory.
   
   **Linux:** `/opt/novell/nids/lib/webapp/jsp`
   
   **Windows:** `\Program Files\Novell\Tomcat\webapps\nidp\jsp`

5. Find the customized `nidp.jsp` and `content.jsp` files and make the following changes in both files:

   5a. In the top Java section of the JSP file, find the `ContentHandler` object that looks similar to the following:

       ```java
       ContentHandler handler = new ContentHandler(request,response);
       ```
5b In the code, add the following Java line under `ContentHandler`:

```java
boolean bGotoAlternateLandingPageUrl = handler.gotoAlternateLandingPageUrl();
```

5c Find the first instance of `<script></script>` in the JSP file that is not `<script src></script>`, then insert the following line in to the JavaScript section between the `<script></script>` tags:

```jsp
<% if (bGotoAlternateLandingPageUrl) { %>
  document.location = 
  "<%=handler.getAlternateLandingPageUrl()%>";
<%  } %>
```

This redirects control to the default portal page that contains appmarks.

5d Save the file.

5e Repeat the steps for the second JSP file.

6 Refresh the browser to see the changes.

### 10.2 Maintaining Customized JSP Files for Access Gateway

If you have customized the JSP files for Access Gateway, you must perform the following steps to maintain the customized files:

1. Before upgrade, create a copy of all JSP files inside the `jsp` directory and place the copy somewhere else.
   - **Linux**: `/opt/novell/nesp/lib/webapp/jsp`
   - **Windows**: `\Program Files\Novell\Tomcat\webapps\nesp\jsp`

   **WARNING:** The upgrade overwrites all existing JSP files.

2. Upgrade Access Gateway.

3. Create an empty folder `legacy` in Access Gateway:
   - **Linux**: `/opt/novell/nesp/lib/webapp/WEB-INF/legacy`
   - **Windows**: `\Program Files\Novell\Tomcat\webapps\nesp\WEBINF\legacy`

   **NOTE:** If you do not create the `legacy` folder, Access Manager uses the logic of the default new login pages.

4. Copy your all backed up JSP files into the `jsp` directory.
   - **Linux**: `/opt/novell/nesp/lib/webapp/jsp`
   - **Windows**: `\Program Files\Novell\Tomcat\webapps\nesp\jsp`

5. Refresh the browser to see the changes.
11 Upgrading Administration Console

- Section 11.1, “Upgrading Administration Console on Linux,” on page 153
- Section 11.2, “Upgrading Administration Console on Windows,” on page 156

11.1 Upgrading Administration Console on Linux

- Section 11.1.1, “Upgrading the Evaluation Version to the Purchased Version,” on page 153
- Section 11.1.2, “Upgrading Administration Console,” on page 154

IMPORTANT: If the base operating system is RHEL 7.5, you must first upgrade to Access Manager 4.5, then upgrade to RHEL 7.6.

11.1.1 Upgrading the Evaluation Version to the Purchased Version

If you have downloaded the evaluation version and want to keep your configuration after purchasing the product, you need to upgrade each of your components with the purchased version. The upgrade to the purchased version automatically changes your installation to a licensed version.

After you have purchased the product, log in to the NetIQ Customer Center and follow the link that allows you to download the product. Then use the following sections for instructions on upgrading the components:

If Identity Server is installed on the same machine as Administration Console, Identity Server is automatically upgraded with Administration Console.

Perform the following steps to upgrade the evaluation version to the purchased version:

1. Open a terminal window.
2. Log in as the root user.
3. Download the upgrade file from Customer Center and extract the tar.gz file using the following command: `tar -xzf <filename>`.

   NOTE: For information about the name of the upgrade file, see the specific Release Notes on the Access Manager Documentation Website (https://www.netiq.com/documentation/access-manager-45/).

4. Change to the directory where you unpacked the file, then enter the following command in a terminal window:

   ```
   ./upgrade.sh
   ```

5. The system displays the confirmation message along with the list of installed components. For example, if Administration Console and Identity Server are installed on the same machine, the following message is displayed:
The following components were installed on this machine

1. Access Manager Administration Console
2. Identity Server

Do you want to upgrade the above components (y/n)?

6 Type Y and press Enter.
7 Type Y to continue with the upgrade, then press Enter.
8 Enter the Access Manager Administration Console user ID.
9 Enter the Access Manager Administration Console password.
10 Re-enter the password for verification.
11 The system displays the following message when the upgrade is complete:

   Upgrade completed successfully.

   The upgrade logs are located in the /tmp/novell_access_manager/ directory. The logs have time stamping.

If you encounter an error, see “Troubleshooting Linux Administration Console Upgrade” on page 199.

11.2 Upgrading Administration Console

Access Manager by default supports Tomcat 8.5.32 and OpenSSL 1.0.2r. Due to this, Identity Server and Access Gateway disable requests from clients that are on versions lower than TLS1. However, Access Gateway can continue communication with web servers that are on versions lower than TLS1.

If Identity Server is installed on the same machine as Administration Console, Identity Server is automatically upgraded with Administration Console. If you are upgrading this configuration and you have custom JSP pages, you can backup these files or allow the upgrade program to back them up for you.

Perform the following steps to upgrade Administration Console:

**NOTE:** To prevent security vulnerability, Access Manager uses the jQuery version that is higher than the version used in the earlier release of Access Manager. The higher version of jQuery is not compatible with the Skype for Business 2016 application. Hence, after the upgrade, you cannot log in to Skype for Business 2016 using the Identity Server login page.

If you want to continue using an old version of jQuery, which is less secure, see “Single Sign-on Fails in Skype for Business 2016” in the Access Manager 4.5 Administration Guide.

1 Back up any customized JSP pages and related files.
   Even though the upgrade program backs up the JSP directory and its related files in the /root/nambkup folder, it is a good practice to backup these files.
   /var/opt/novell/tomcat/webapps/nidp/jsp
2 Open a terminal window.
3 Log in as the root user.
4 Download the upgrade file from Customer Center and extract the tar.gz file using the following command: tar -xzvf <filename>.
**NOTE:** For information about the name of the upgrade file, see the specific Release Notes on the Access Manager Documentation website (https://www.netiq.com/documentation/access-manager-45/).

5 Change to the directory where you unpacked the file, then enter the following command in a terminal window:

```
./upgrade.sh
```

6 The system displays the confirmation message along with the list of installed components. For example, if Administration Console and Identity Server are installed on the same machine, the following message is displayed:

```
The following components were installed on this machine

1. Access Manager Administration Console
2. Identity Server
Do you want to upgrade the above components (y/n)?
```

7 Type Y and press Enter.

The system displays a warning message because the latest version of Access Manager uses stronger TLS protocols, ciphers, and other security settings.

If you are using a BTRFS filesystem, the system displays a warning message that the BTRFS filesystem might cause performance issues with the eDirectory database. It is recommended to change the filesystem from BTRFS to any other available filesystem.

For information about moving the existing database from BTRFS filesystem to any other available filesystem, see TID 7022755 (https://www.novell.com/support/kb/doc.php?id=7022755).

8 Type Y to continue with the upgrade, then press Enter.

If you do not want to include the security configurations, then type n. This stops the upgrade.

9 Enter the Access Manager Administration Console user ID.

10 Enter the Access Manager Administration Console password.

11 Re-enter the password for verification.

12 The system displays the following message when the upgrade is complete:

```
Upgrade completed successfully.
```

13 (Optional) To view the upgrade files:

- To view the upgrade log files, see the files in the `/tmp/novell_access_manager` directory.

- If you selected to back up your configuration and used the default directory, see the zip file in the `./root/nambkup` directory. The log file for this backup is located in the `./var/log` directory.

- If Identity Server is installed on the same machine, the JSP directory was backed up to the `./root/nambkup` directory. The file is prefixed with `nidp_jps` and contains the date and time of the backup.
NOTE: If you have customized the Java settings in the /opt/novell/nam/idp/conf/tomcat.conf file, then after the upgrade, you must copy the customized setting to the new file.

If you encounter an error, see Section 17.2, “Troubleshooting Linux Administration Console Upgrade,” on page 199.

11.2 Upgrading Administration Console on Windows

- Section 11.2.1, “Upgrading the Evaluation Version to the Purchased Version,” on page 156
- Section 11.2.2, “Upgrading Administration Console,” on page 156

11.2.1 Upgrading the Evaluation Version to the Purchased Version

If you have downloaded the evaluation version and want to keep your configuration after purchasing the product, you need to upgrade each of your components with the purchased version. The upgrade to the purchased version automatically changes your installation to a licensed version.

After you have purchased the product, log in to the NetIQ Customer Center (https://www.netiq.com/customercenter) and follow the link that allows you to download the product. Then follow the instructions in Section 11.2.2, “Upgrading Administration Console,” on page 156.

11.2.2 Upgrading Administration Console

Log in to the NetIQ Downloads page and follow the link that allows you to download the product.

NOTE: If you have enabled history for risk-based authentication in a prior version of Access Manager, you must upgrade the database for risk-based authentication after upgrading to 4.5. You can find the upgrade script here: C:\Program Files\Novell\Tomcat\webapps\nidp\WEB-INF\RiskDBScript.zip.

MySQL: Run netiq_risk_mysql_upgrade.sql
Oracle: Run netiq_risk_oracle_upgrade.sql
Microsoft SQL Server: Run netiq_risk_sql_server_upgrade.sql

If you have installed Administration Console and Identity Server on the same server, you must upgrade both of them at the same time.

Perform the following steps to upgrade Administration Console on Windows:

NOTE: To prevent security vulnerability, Access Manager uses the jQuery version that is higher than the version used in the earlier release of Access Manager. The higher version of jQuery is not compatible with the Skype for Business 2016 application. Hence, after the upgrade, you cannot log in to Skype for Business 2016 using the Identity Server login page.
If you want to continue using an old version of jQuery, which is less secure, see “Single Sign-on Fails in Skype for Business 2016” in the Access Manager 4.5 Administration Guide.

1. Manually back up your current Access Manager configuration using ambkup.bat file. For instructions, see Back Up and Restore in the Access Manager 4.5 Administration Guide.

2. If Administration 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 tomcat.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. Run the installation program. When the installation program detects an installed version of Administration Console, it automatically prompts you to upgrade.

5. Read the Introduction, then click Next.

6. Accept the License Agreement, then click Next.

7. Select the component to upgrade that is currently installed, then click Next.

8. Type Y and press Enter.
   
   The system displays an information message to enable Syslog on the Auditing user interface of Administration Console after the upgrade.

9. Type Y to continue with the upgrade, then press Enter.

10. At the upgrade prompt, click Continue.

11. Specify the following information for the administrator account on Administration Console:

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

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

12. 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.

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\Novell\log\AccessManagerServer_InstallLog.log

17. If Identity Server is 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 4.4.x, ensure that you apply the same to the new server.xml located at C:\Program Files\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, ...
../>

Tomcat properties:

Go to C:\Program Files\Novell\Tomcat\bin. Click the tomcat8w file, and make a note of any elements or attributes customized in 4.4.x.

On the 4.5 server, go to C:\Program Files\Tomcat\bin\tomcat8w. Change the values and attributes as required.
12 Upgrading Identity Server

- Section 12.1, “Upgrading Identity Server on Linux,” on page 159
- Section 12.2, “Upgrading Identity Server on Windows,” on page 162

12.1 Upgrading Identity Server on Linux

- Section 12.1.1, “Upgrading the Evaluation Version to the Purchased Version,” on page 159
- Section 12.1.2, “Upgrading Identity Server,” on page 160

IMPORTANT: If the base operating system is RHEL 7.5, you must first upgrade to Access Manager 4.5, then upgrade to RHEL 7.6.

12.1.1 Upgrading the Evaluation Version to the Purchased Version

If you have downloaded the evaluation version and want to keep your configuration after purchasing the product, you need to upgrade each of your components with the purchased version. The upgrade to the purchased version automatically changes your installation to a licensed version.

After you have purchased the product, log in to the NetIQ Customer Center and follow the link that allows you to download the product.

Use the following procedure to upgrade stand-alone Identity Server. If you have installed both Identity Server and Administration Console on the same machine, see “Upgrading the Evaluation Version to the Purchased Version” on page 153.

NOTE: If you have modified the JSP file to customize the login page, logout page, and error messages, you can restore the JSP file after installation. You should sanitize the restored JSP file to prevent XSS attacks. For more information, see Preventing Cross-site Scripting Attacks in the Access Manager 4.5 Administration Guide.

1. Open a terminal window.
2. Log in as the root user.
3. Download the upgrade file from dl.netiq.com and extract the tar.gz file using the following command: tar -xzf <filename>.

NOTE: For information about the name of the upgrade file, see the specific Release Notes on the Access Manager Documentation website (https://www.netiq.com/documentation/access-manager-45/).

4. Change to the directory where you unpacked the file, then enter the following command in a terminal window:

   ./upgrade.sh
The system displays the following confirmation message:

The following components were installed on this machine
1. Identity Server

Do you want to upgrade the above components (y/n)?

Type Y and press Enter.

Type Y to continue with the upgrade, then press Enter.

Enter the Access Manager Administration Console user ID.

Enter the Access Manager Administration Console password.

Re-enter the password for verification.

The system displays the following message when the upgrade is complete:

Upgrade completed successfully.

The upgrade logs are located in the /tmp/novell_access_manager/ directory. The logs have time stamping.

NOTE: If OAuth and OpenID Connect protocol is enabled, then after upgrading all members of Identity Server cluster, you must update Administration cluster to use the JSON Web Token (JWT token). For more information about JWT token, see Understanding How Access Manager Uses OAuth and OpenID Connect in the Access Manager 4.5 Administration Guide.

12.1.2 Upgrading Identity Server

Use the following procedure to upgrade stand-alone Identity Server. If you have installed both Identity Server and Administration Console on the same machine, see “Upgrading Administration Console” on page 154.

IMPORTANT: Ensure to complete the following actions before you begin:

- If you are upgrading Access Manager components on multiple machines, ensure that the time and date are synchronized among all machines.
- Ensure that Administration Console is running. However, you must not perform any configuration tasks in Administration Console during an Identity Server upgrade.

NOTE: To prevent security vulnerability, Access Manager uses the jQuery version that is higher than the version used in the earlier release of Access Manager. The higher version of jQuery is not compatible with the Skype for Business 2016 application. Hence, after the upgrade, you cannot log in to Skype for Business 2016 using the Identity Server login page.

If you want to continue using an old version of jQuery, which is less secure, see “Single Sign-on Fails in Skype for Business 2016” in the Access Manager 4.5 Administration Guide.

Back up any customized JSP pages and related files.

Even though the upgrade program backs up the JSP directory and its related files in the /root/nambkup folder, it is a good practice to backup these files.
2 Open a terminal window.
3 Log in as the root user.
4 Download the upgrade file from dl.netiq.com and extract the tar.gz file by using the \texttt{tar -xzvf <filename>} command.

\textbf{NOTE:} For information about the name of the upgrade file, see the specific Release Notes on the Access Manager Documentation website (https://www.netiq.com/documentation/access-manager-45/).

5 Change to the directory where you unpacked the file, then enter the following command in a terminal window:

\texttt{./upgrade.sh}

6 The system displays the following confirmation message:

\texttt{The following components were installed on this machine}

1. Identity Server

\texttt{Do you want to upgrade the above components (y/n)?}

7 Type \texttt{Y} and press Enter.

The system displays two warning messages. The first message is for backing up all JSPs before proceeding with the upgrade, and the next is for including security settings.

8 Type \texttt{Y} to continue with the upgrade, then press Enter.

If you do not want to include the security configurations, then type \texttt{n}. This stops the upgrade.

9 Enter the Access Manager Administration Console user ID.

10 Enter the Access Manager Administration Console password.

11 Re-enter the password for verification.

12 The system displays the following message when the upgrade is complete:

\texttt{Upgrade completed successfully.}

13 Restore any customized files from the backup taken earlier. To restore files, copy files to the respective locations:

\begin{itemize}
\item /opt/novell/nam/idp/webapps/nidp/jsp
\item /opt/novell/nam/idp/webapps/nidp/html
\item /opt/novell/nam/idp/webapps/nidp/images
\item /opt/novell/nam/idp/webapps/nidp/config
\item /opt/novell/nam/idp/webapps/nidp WEB-INF/lib
\item /opt/novell/nam/idp/webapps/nidp WEB-INF/web.xml
\item /opt/novell/nam/idp/webapps/nidp WEB-INF/classes
\item /opt/novell/nam/idp/webapps/nidp WEB-INF/conf
\item /opt/novell/java/jre/lib/security/bcslogin.conf
\item /opt/novell/java/jre/lib/security/nidpkey.keytab
\item /opt/novell/nids/lib/webapp/classUtils
\end{itemize}
Also, add the following line to the server.xml file:

```xml
<Connector NIDP_Name="localConnector" URIEncoding="utf-8" acceptCount="100" address="127.0.0.1" connectionTimeout="20000" maxThreads="600" minSpareThreads="5" port="8088" protocol="HTTP/1.1" />
```

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

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

Important Notes:

- If you are using Kerberos and you have renamed `nidpkey.keytab` and `bcsLogin.conf` with any other name, ensure that you modify the `upgrade_utility_functions.sh` script located in the `novell-access-manager-x.x.x-xxx/scripts` folder with these names before upgrading Access Manager.
- If you have customized the Java settings in the `/opt/novell/nam/idp/conf/tomcat.conf` file, then after the upgrade, you must copy the customized setting to the new file.
- If you have modified the JSP file to customize the login page, logout page, and error messages, you can restore the JSP file after installation. You should sanitize the restored JSP file to prevent XSS attacks. For more information, see Preventing Cross-site Scripting Attacks in the Access Manager 4.5 Administration Guide.

### 12.2 Upgrading Identity Server on Windows

- Section 12.2.1, “Upgrading the Evaluation Version to the Purchased Version,” on page 162
- Section 12.2.2, “Upgrading Identity Server,” on page 162

#### 12.2.1 Upgrading the Evaluation Version to the Purchased Version

If you have downloaded the evaluation version and want to keep your configuration after purchasing the product, you need to upgrade each of your components with the purchased version. The upgrade to the purchased version automatically changes your installation to a licensed version.

After you have purchased the product, log in to the NetIQ Customer Center (https://www.netiq.com/customercenter) and follow the link that allows you to download the product. Then follow the instructions in Section 11.2.2, “Upgrading Administration Console,” on page 156.

#### 12.2.2 Upgrading Identity Server

Log in to the NetIQ Downloads page and follow the link that allows you to download the product.

If you have installed only Identity Server on the server, use the following procedure to upgrade Identity Server:
NOTE: To prevent security vulnerability, Access Manager uses the jQuery version that is higher than the version used in the earlier release of Access Manager. The higher version of jQuery is not compatible with the Skype for Business 2016 application. Hence, after the upgrade, you cannot log in to Skype for Business 2016 using the Identity Server login page.

If you want to continue using an old version of jQuery, which is less secure, see “Single Sign-on Fails in Skype for Business 2016” in the Access Manager 4.5 Administration Guide.

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 tomcat.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_45_AccessManagerService_Win64.exe file from NetIQ.
   This file starts the installation program. When the program detects an installed version of 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 Type Y and press Enter.
   The system displays an information message to enable Syslog after the upgrade.

8 Type Y to continue with the upgrade, then press Enter.

9 Specify the following information for Administration Console:
   Administration user ID: Specify the name of the administration user for Administration Console.
   Password and Re-enter Password: Specify and re-enter the password for the administration user account.

10 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.

   NOTE: Ensure that you sanitize the restored customized JSP file to prevent XSS attacks. For more information about how to sanitize the JSP file, see Preventing Cross-site Scripting Attacks in the Access Manager 4.5 Administration Guide.

11 Review the summary, then click Install.
NOTE: If OAuth and OpenID Connect protocol is enabled, then after upgrading all members of Identity Server cluster, you must update the Identity Server cluster to use the JSON Web Token (JWT token). For more information about JWT token, see Understanding How Access Manager Uses OAuth and OpenID Connect in the Access Manager 4.5 Administration Guide.

12 View the upgrade log file found in the following location:
   C:\Program Files\Novell\log\AccessManagerServer_InstallLog.log

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

14 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 4.4.x, ensure that you apply the same to the new server.xml located at C:\Program Files\Novell\Tomcat\conf\ directory.
   Also, add the following line to the server.xml file to use the new features on the user portal:
   <Connector NIDP_Name="localConnector" URIEncoding="utf-8" acceptCount="100" address="127.0.0.1" connectionTimeout="20000" maxThreads="600" minSpareThreads="5" port="8088" protocol="HTTP/1.1" />
   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, ...
   Tomcat properties:
   Go to C:\Program Files\Novell\Tomcat\bin\tomcat7w. Double-click the tomcat7w file and make a note of any elements or attributes customized in 4.4.x.
   On the 4.5 server, go to C:\Program Files\Tomcat\bin\tomcat8w. Change the values and attributes as required.


IMPORTANT: If NetIQ Access Manager is federated with other service providers or if the users are redirected to Access Gateway protected resources from 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.
13 Upgrading Access Gateway

- Section 13.1, “Upgrading Access Gateway on Linux,” on page 165

13.1 Upgrading Access Gateway on Linux

- Section 13.1.1, “Upgrading the Evaluation Version to the Purchased Version,” on page 165
- Section 13.1.2, “Upgrading Access Gateway,” on page 165

**IMPORTANT:** If the base operating system is RHEL 7.5, you must first upgrade to Access Manager 4.5, and then upgrade to RHEL 7.6.

13.1.1 Upgrading the Evaluation Version to the Purchased Version

If you have downloaded the evaluation version and want to keep your configuration after purchasing the product, you need to upgrade each of your components with the purchased version. The upgrade to the purchased version automatically changes your installation to a licensed version.

After you have purchased the product, log in to the NetIQ Customer Center and follow the link that allows you to download the product.

Perform the following procedures to upgrade from the evaluation version to the purchased version:

- Section 13.1.1.1, “Upgrading Access Gateway Appliance,” on page 165
- Section 13.1.1.2, “Upgrading Access Gateway Service,” on page 165

**13.1.1.1 Upgrading Access Gateway Appliance**

From Access Manager 4.5 onwards, the format of the Access Gateway Appliance installer is changed to OVF. Therefore instead of a regular upgrade, you must migrate to the latest Access Gateway Appliance. For information about how to migrate, see Section “Migrating Access Gateway Appliance Setup” on page 167.

**13.1.1.2 Upgrading Access Gateway Service**

Perform the steps provided in Section 13.1.2.3, “Upgrading Access Gateway Service,” on page 173.

13.1.2 Upgrading Access Gateway

- Section 13.1.2.1, “Upgrading Access Gateway Appliance,” on page 166
- Section 13.1.2.2, “Migrating Access Gateway Appliance Setup,” on page 167
- Section 13.1.2.3, “Upgrading Access Gateway Service,” on page 173
13.1.2.1 Upgrading Access Gateway Appliance

Upgrading from Access Gateway Appliance 4.4.x

Access Gateway Appliance is packaged as an OVF installer. Therefore if you are using Access Gateway Appliance 4.4 Service Pack 4 Hotfix 1 or earlier supported versions, you must migrate to latest version of Access Gateway Appliance. For information about how to migrate, see Section “Migrating Access Gateway Appliance Setup” on page 167.

If you are using Access Gateway appliance 4.4, ensure to upgrade to any of the following supported upgrade versions of Access Gateway Appliance before migrating to the latest version:

- 4.4 Service Pack 4 Hotfix 1
- 4.4 Service Pack 4
- 4.4 Service Pack 3
- 4.4 Service Pack 2


**NOTE:** You cannot directly upgrade from Access Gateway Appliance 4.4.x to the latest version.

Upgrading from Access Gateway Appliance 4.5

**NOTE:** You can use the latest upgrade file to upgrade from 4.5 to the latest version of Access Gateway Appliance.

If you are using Access Gateway Appliance 4.4 Service Pack 4 Hotfix 1 or earlier supported versions, see “Upgrading from Access Gateway Appliance 4.4.x” on page 166.

Steps to upgrade from 4.5 to the latest version of Access Gateway Appliance:

1. Back up any customized JSP pages and related files.
   
   Even though the upgrade program backs up the JSP directory and its related files in the /root/nambkup folder, it is a good practice to backup these files.

2. Open a terminal window.

3. Log in as the root user.

4. Download the upgrade file from dl.netiq.com or from your purchased build, and then extract the tar.gz file using the following command:

   ```
   tar -xzvf <filename>
   ```

   **NOTE:** For information about the name of the upgrade file, see the specific Release Notes on the Access Manager Documentation website.

5. Change to the directory where you unpacked the file, then enter the following command in a terminal window:
./ma_upgrade.sh

6 A warning message regarding backup and restore is displayed followed by the message for including security settings.
   If you have customized any files, take a backup and restore them after installation.
7 Would you like to continue this upgrade? Type Y to continue.
   If you do not want to include the security configurations, then type n. This stops the upgrade.
8 Do you want to restore custom login pages? Type Y to confirm.
9 Enter the Access Manager Administration Console user ID.
10 Enter the Access Manager Administration Console password
11 Re-enter the password for verification
12 The system displays the following message when the upgrade is complete:

   Upgrade completed successfully.
13 Restore any customized files from the backup taken earlier. To restore the files, copy the files to the respective locations below:
   • /opt/novell/nam/mag/webapps/nesp/WEB-INF/web.xml
   • /opt/novell/nam/mag/webapps/nesp/jsp
   • /opt/novell/nam/mag/webapps/nesp/html
   • /opt/novell/nam/mag/webapps/nesp/images
   • /opt/novell/nam/mag/webapps/agm/WEB-INF/config/current
   • /opt/novell/nam/mag/webapps/nesp/config
   • /opt/novell/devman/jcc/scripts/presysconfig.sh
   • /opt/novell/devman/jcc/scripts/postsysconfig.sh

13.1.2.2 Migrating Access Gateway Appliance Setup

In migration, you install the latest version of Access Gateway Appliance 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 and host name.
Prerequisites

In addition to the Section 4.2.1, “System Requirements,” on page 70, ensure that the following prerequisites are met before migrating Access Gateway Appliance:

- You have completed upgrading all instances of Administration Console and Identity Server before migrating the Access Gateway Appliance.
- (If the services are managed by an L4 switch) You have removed the device that needs to be migrated from the L4 switch. This prevents the L4 switch from sending the request of the users to that device during migration. Add the device to the L4 switch after the migration is complete.
- The upgrade path mentioned in the Release Notes applies to the migration path of Access Gateway Appliance. Ensure that you are migrating Access Gateway Appliance from 4.4 Service Pack 2 (4.4 SP2) or later to the latest version.


- (For using an existing IP address) You have backed up customized files, if any. It is important to take the backup of the customized files if you are reusing the same IP address. Take a backup of the following files if these are customized:
  - /opt/novell/nam/mag/conf/server.xml
  - /opt/novell/nam/mag/conf/tomcat.conf
  - /opt/novell/nam/mag/conf/web.xml
  - /opt/novell/nesp/lib/webapp/WEB-INF/web.xml
  - /opt/novell/nam/mag/webapps/nesp/jsp/
  - /opt/novell/nam/mag/webapps/nesp/images/
  - /opt/novell/nam/mag/webapps/nesp/web-INF/config/current/ErrorPagesConfig.xml
  - /etc/opt/novell/apache2/conf/extra/httpd-multilang-errordoc.conf
  - /opt/novell/apache2/share/apache2/error/include/top.html
  - /opt/novell/apache2/share/apache2/error/include/bottom.html
  - /opt/novell/apache2/share/apache2/error/images/

- (For using new IP address) Adding the new Access Gateway Appliance in the existing cluster restores the files mentioned in the Settings tab of Code Promotion on Administration Console. If code promotion was performed earlier to get the existing version, a custom file cache is pushed instead of the files mentioned in the Settings tab.

If you have customized the server.xml and the web.xml files, ensure to take a backup of those files because these files are not restored automatically.
• (For using existing IP address) Make a note of the IP address and the host name (with the domain name such as, server.domain.com) of the existing Access Gateway Appliance before migrating to the latest Access Gateway Appliance. The IP address that the existing Access Gateway Appliance uses to communicate with Administration Console will be used for installing the new Access Gateway Appliance.

• (For using existing IP address) The number of network interfaces along with their values are same for both the new Access Gateway Appliance and the existing Access Gateway Appliance.

• You have physical access to the server or server console (in case of VMWare setups) as a root user.

• The required ports are opened in the firewall. For more information about ports, see Section 1.8, “Setting Up Firewalls,” on page 30.

• Determine if you want to reuse your existing IP address or use a new IP address to setup the system.

• Verify if you have configured any Access Gateway advanced option that refers to a non-default folder in the file system. If yes, you must manually create the folders with the same name before migrating a new Access Gateway Appliance.

   For example, if you have configured the CoreDumpDirectory option as CoreDumpDirectory /data/cores, then before migrating Access Gateway Appliance, create the /data/cores folder.

**Migrating Access Gateway Appliance**

Migrating the existing Access Gateway Appliance to new Access Gateway Appliance will not cause any disruption to the existing setup. You can add new Access Gateway Appliance nodes into the existing Access Gateway Appliance cluster. They can co-exist, but it is recommended to replace all the existing nodes to the latest version.

You can select any one of the following approaches to migrate to Access Gateway Appliance 4.5:

• “Using the Existing IP Address” on page 169

• “Using a New IP Address” on page 171

**Using the Existing IP Address**

**Workflow:**

1. Back up any files that you have customized and note down the IP address and host name of the existing Access Gateway Appliance.

2. Shut down the existing Access Gateway Appliance.

3. Install Access Gateway Appliance with the IP address and host name noted in Step 1.

4. Restore any customized files from the backup taken earlier.

**Use case:**

You are upgrading Access Manager 4.4 Service Pack 2 (4.4 SP2) to Access Manager 4.5. After upgrading Administration Console and Identity Server to 4.5 version, you require to migrate Access Gateway Appliance to the 4.5 version using the existing IP address.

This scenario assumes that you have a server with the system requirements as mentioned at Section 4.2.1, “System Requirements,” on page 70 to install the new Access Gateway Appliance.
Consider that the setup includes the following components:

- Access Manager 4.5 Administration Console (primary Administration Console: AC 1)
- Access Manager 4.5 Identity Server cluster (primary Identity Server: IDP 1 and secondary Identity Server: IDP 2)
- Access Manager 4.4 SP2 Access Gateway Appliance cluster (primary Access Gateway: AG 1 and secondary Access Gateway: AG 1, AG 2 and AG 3)

Migration process:

1. If you are first migrating AG 2 using the existing IP address of AG 2, ensure you do the following:
   1a. Shut down AG 2
   1b. Ensure that you have met the “Prerequisites” on page 168.

2. Install the Access Gateway Appliance (newAGA 2) with the same IP address and hostname as of the 4.4 SP2 Access Gateway Appliance (AG 2). For information about installing the new Access Gateway Appliance, see Section 4.2, “Installing Access Gateway Appliance,” on page 70.

   After the installation is complete, the configuration sync up takes some time. Do not modify any configuration during this time.

   When the configuration is synced up, the health of this Access Gateway Appliance and the other members of the cluster turn green.

   **NOTE:** After the installed Access Gateway Appliance turns green, it is recommended to migrate all the other members of Access Gateway Appliance to Access Gateway Appliance 4.5 before applying the changes by using the update option in Administration Console.

3. Restore any customized files that you backed up earlier as part of “Prerequisites” on page 168.

   **server.xml:** If you have modified any elements or attributes in the 4.4 Service Pack 2 environment, the corresponding changes will need to be applied to the /opt/novell/nam/mag/conf/server.xml file of the new Access Gateway Appliance.

   Typical changes done to the server.xml in 4.4 SP2 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, 4.4 SP2 has customized maxThreads value.

   ```xml
   <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 new server.xml file.

4. Test the Access Gateway Appliance functionality by accessing Access Gateway protected resources and ensuring that pages are rendered successfully.

5. Repeat Step 1 through Step 4 until you have completely migrated all the existing 4.4 SP2 Access Gateway Appliance (AG 1 and AG 3) to Access Gateway Appliance 4.5.

6. On the newly added Access Gateway Appliance, restart Tomcat by using the /etc/init.d/novell-mag restart or rcnovell-mag restart command.
Using a New IP Address

Workflow:

1. Back up any files that you have customized.
2. Install the new Access Gateway Appliance.
   For information about installing the new Access Gateway Appliance, see Section 4.2, “Installing Access Gateway Appliance,” on page 70.
3. Restore the customized files from the backup taken earlier.

Use case

You are upgrading Access Manager 4.4 SP2 to Access Manager 4.5. After upgrading Administration Console and Identity Server to 4.5 version, you require to migrate Access Gateway Appliance to the 4.5 version using the new IP address.

This scenario assumes that you have a server with the system requirements as mentioned at Section 4.2.1, “System Requirements,” on page 70 to install the new Access Gateway Appliance.

Consider that the setup includes the following components:

- Access Manager 4.5 Administration Console (primary Administration Console: AC 1)
- Access Manager 4.5 Identity Server cluster (primary Identity Server: IDP 1 and secondary Identity Server: IDP2)

Migration process:

1. Determine the primary server in the 4.4 SP2 Access Gateway cluster.
   In this scenario, AG 1 is the primary server. To verify which is the primary server in your set up, perform the following:
   1a. Log in to Administration Console.
   1b. Click Devices > Access Gateways, and select the cluster.
The primary server is indicated by a red mark beside the IP address.

2 Install the new Access Gateway Appliance (newAGA 1). For more information, see Section 4.2, “Installing Access Gateway Appliance,” on page 70.

After the installation, you must configure Access Gateway Appliance to specify the IP address of Administration Console (AC 1), 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 existing Access Gateway Appliance 4.4 Service Pack 2 cluster.

4 By default, all proxy services of newly added devices to the cluster listen on the same IP address and port. To configure each reverse proxy service to a specific IP address and port, perform the following steps:

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, and select the device.

4c Click New IP > OK.

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

4e Configure the DNS in Network Settings > DNS.

4f Add the Host entries (if any) in Network Settings > Hosts.

4g Set up the routing (if any) in Network Settings > Gateways.

4h Under Services, click 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 > TCP Connect Options. Select the Cluster Member and select the IP address from the list against Make Outbound Connection Using if you want to select the outbound IP address to communicate with the web server.

4i Restore any customized files that you backed up earlier as part of “Prerequisites” on page 168.

The files mentioned in Administration Console at <username> > Code Promotion > Settings get restored automatically:

Copy the content of the server.xml file to the corresponding file in the new location.

Typical changes done to the server.xml in 4.4 SP2 include modifying the 'Address=' attribute to restrict the IP address the application will listen on, or 'maxThreads=' attribute to modify the number of threads.

server.xml: If you have modified any elements or attributes in the 4.4 SP2 environment, the corresponding changes will need to be applied to the /opt/novell/nam/mag/conf/server.xml file of the new Access Gateway Appliance.

In the following example, 4.4 SP2 contains 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 new server.xml file.

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

6 On the Administration Console, specify AGA 1 as the primary server and click Update.

7 Remove 4.4 SP2 Access Gateway Appliance (AG 1) from the cluster.

8 Install new Access Gateway Appliance (AGA 2) as in Step 2 and add it to the 4.4 SP2 Access Gateway Appliance cluster as in Step 3.

9 After you confirm that all the services are running remove 4.4 SP2 Access Gateway Appliance (AG 2) from the cluster.

10 Click OK > Update all.

11 Repeat Step 2 to Step 5 until you migrate all existing Access Gateway Appliance from 4.4 Service Pack 2 to 4.5.

After installing Access Gateway Appliance, delete all 4.4 SP2 Access Gateway Appliances from Administration Console.

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

13.1.2.3 Upgrading Access Gateway Service

- “Prerequisites” on page 174
- “Process” on page 174
Prerequisites

Manually back up the `tomcat.conf` and the `server.xml` files from `/opt/novell/nam/mag/conf`.

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

**IMPORTANT:** (Applicable for RHEL) When more than 60 proxy services are configured, Apache fails to start after upgrade. RHEL has 128 semaphore arrays by default which is inadequate for more than 60 proxy services. Apache 2.4 requires a semaphore array for each proxy service.

You must increase the number of semaphore arrays depending on the number of proxy services you are going to use. Perform the following steps to increase the number of semaphore arrays to the recommended value:

1. Open `/etc/sysctl.conf`
2. Add `kernel.sem = 250 256000 100 1024`
   
   This creates the following:
   
   - Maximum number of arrays = 1024 (number of proxy services x 2)
   - Maximum semaphores per array = 250
   - Maximum semaphores system wide = 256000 (Maximum number of arrays x Maximum semaphores per array)
   - Maximum ops per semop call = 100
3. Use command `sysctl -p` to update the changes
4. Start Apache.

Process

1. Download the `AM_45_AccessGatewayService_Linux_64.tar.gz` file from the NetIQ download site and extract it by using the following command:
   
   ```bash
   tar -xzvf <AM_45_AccessGatewayService_Linux_64.tar.gz>
   ```

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

3. Specify the following information:

   - **User ID**: Specify the name of the administration user for Administration Console.
   - **Password and Re-enter Password**: Specify and re-enter the password for the administration user account.

   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/nambkup. 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” on page 174.

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

<table>
<thead>
<tr>
<th>Old File Locations</th>
<th>New File Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>/root/novell_access_manager/apache2/ (contains apache var files)</td>
<td>/opt/novell/apache2/share/apache2/error</td>
</tr>
<tr>
<td>/root/novell_access_manager/nesp/ (contains modified error pages)</td>
<td>/var/opt/novell/tomcat/webapps/nesp/jsp</td>
</tr>
</tbody>
</table>

**server.xml:**

If you have modified any elements or attributes in the 4.4.x environment the corresponding changes will need to be applied to the 4.5 server.xml file.

Typical changes done to the server.xml 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, 4.4.x 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 4.5 server.xml file.

**tomcat.conf:**

Copy any elements or attributes that you have customized in the tomcat8.conf file to the tomcat.conf file.

For example, if you have included the environment variable to increase the heap size by using -Xmx/Xms/Xss attributes in the tomcat8.conf file, copy this variable to the 4.5 /opt/novell/nam/idp/conf/tomcat.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 4.4.x, ensure that you apply the same to the new 4.5 /opt/novell/nam/mag/webapps/WEB-INF/agm.properties file. An example below shows the how to enable the backend webserver's web page 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/tomcat/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.
**NOTE:** If you have customized the Java settings in the `/opt/novell/nam/idp/conf/tomcat.conf` file, then after the upgrade, you must copy the customized setting to the new file.

### 13.2 Upgrading Access Gateway Service on Windows

- Section 13.2.1, “Upgrading the Evaluation Version to the Purchased Version,” on page 176
- Section 13.2.2, “Upgrading Access Gateway Service,” on page 176

#### 13.2.1 Upgrading the Evaluation Version to the Purchased Version

If you have downloaded the evaluation version and want to keep your configuration after purchasing the product, you need to upgrade each of your components with the purchased version. The upgrade to the purchased version automatically changes your installation to a licensed version.

After you have purchased the product, log in to the NetIQ Customer Center (https://www.netiq.com/customercenter) and follow the link that allows you to download the product. Then follow the instructions in Section 13.2.2, “Upgrading Access Gateway Service,” on page 176.

#### 13.2.2 Upgrading Access Gateway Service

Log in to the NetIQ Downloads page and follow the link that allows you to download the product.

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

**IMPORTANT:** Windows packages KB2919442 and KB2919355 must be installed before upgrading Access Gateway Service. These packages must be installed in the same sequence. You can verify if these packages are installed by using the following commands:

- `dism /online /get-packages | findstr KB2919442`
- `dism /online /get-packages | findstr KB2919355`

If these packages are installed, you will get a confirmation message. If the packages are not installed, you will not receive any response.

1. Download and run `AM_44_AccessGatewayService_Win64.exe` file from NetIQ.
2. Run the installation program. When the installation program detects an installed version of Access Gateway, it automatically prompts you to upgrade.
3. Answer Yes to the prompt to upgrade.
4. Read the Introduction, then click Next.
5. Review the Readme information, then click Next.
6. Accept the License Agreement, then click Next.
7. Specify the following information:
   - **User ID:** Specify the name of the administration user for Administration Console.
   - **Password and Re-enter Password:** Specify the password and re-enter the password for the administration user account.
8  Review the installation summary, then click Install.
    Access Gateway Service is upgraded.
9  View the log files. The install logs are located in the C:\Program Files\Novell\log and C:\agsinstall.log directories.
10 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 4.4.x, ensure that you apply the same to the new server.xml located at C:\Program Files\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, ...

    **Tomcat properties:**
    Go to C:\Program Files\Novell\Tomcat\bin. Click the tomcat8w (for 4.4.x) file and make a note of any elements or attributes that are customized.
    On the 4.4 server, go to C:\Program Files\Novell\Tomcat\bin\tomcat8w. Change the values and attributes as required.
11 Restart the tomcat server by using the Windows service. Go to Start > Control Panel > System and Security > Administrative Tools > Services.
14 Upgrading Analytics Server

For security considerations, see “Securing Analytics Server” in the NetIQ Access Manager 4.5 Security Guide.

- Section 14.1, “Upgrading Analytics Server,” on page 179
- Section 14.2, “Upgrading Analytics Server in a High Availability Setup,” on page 180

14.1 Upgrading Analytics Server

1 Log in to Analytics Server as a root user.

2 Download the upgrade file and extract the tar.gz file by using the following command:

   ```bash
tar -xzvf <filename>
   ```

   **NOTE:** For the name of the upgrade file, see the specific Release Notes on the Access Manager Documentation website.

3 Change to the directory where you extracted the file, then enter the following command in a terminal window:

   ```bash
./ar_upgrade.sh
   ```

4 Specify the following details:

   - Enter the Access Manager Administration Console administrator’s ID. By default, it is admin.
   - Enter the Access Manager Administration Console administrator’s password.
   - Re-enter the Access Manager Administration Console administrator’s password.
   - Enter the Analytics Server administrator’s password. You use this password for logging in to Analytics Server and the Reporting console.
   - Re-enter the Analytics Server administrator’s password.

The upgrade completes with the following options. Choose one of the following options:

   - Delete the existing aggregated data from elasticsearch.
   - Migrate the existing aggregated data to a new data schema. (This may take longer time)

By default, the data is migrated. The migration of data may take longer time. If it fails, you must run the upgrade script again. Even when the data from the elasticsearch is deleted, the audit data is not deleted from the server.

The upgrade logs are saved in the /tmp/novell_access_manager/ directory. The logs include time stamping.
14.2 Upgrading Analytics Server in a High Availability Setup

You must first upgrade the passive node in the cluster, then upgrade the active node. Perform the following steps:

1. Enable the maintenance mode on the cluster.
   
   ```
   crm configure property maintenance-mode=true
   ```
   
   The maintenance mode prevents any disturbance to the running cluster resources when you update Analytics Server. You can run this command from any cluster node.

2. Verify if the maintenance mode is active.
   
   ```
   crm status
   ```
   
   The cluster resources should appear in the unmanaged state.

3. Upgrade the passive cluster node:
   
   3a. Stop the cluster stack.
   
   ```
   rcopenais stop
   ```
   
   Stopping the cluster stack ensures that the cluster resources remain accessible and avoids fencing of nodes.

   3b. Upgrade Analytics Server in the passive node. See “Upgrading Analytics Server” on page 179.

   3c. After the upgrade is complete, start the cluster stack.
   
   ```
   rcopenais start
   ```

4. Upgrade the active cluster node by performing the following steps:
   
   4a. Stop the cluster stack.
   
   ```
   rcopenais stop
   ```
   
   Stopping the cluster stack ensures that the cluster resources remain accessible and avoids fencing of nodes.

   4b. Upgrade Analytics Server on the active node. See “Upgrading Analytics Server” on page 179.

   4c. After the upgrade is complete, start the cluster stack.
   
   ```
   rcopenais start
   ```

   4d. Run the `csync2 -x -v` command to synchronize any changes in the configuration files.

5. Disable the maintenance mode on the cluster.
   
   ```
   crm configure property maintenance-mode=false
   ```
   
   You can run this command from any cluster node.
6 Run the `insserv -r sentinel` command on both the nodes to remove the autostart scripts so that the cluster can manage the product.

7 Verify whether the maintenance mode is inactive.

   `crm status`

The cluster resources should appear in the **Started** state.
Getting the Latest OpenSSL Updates for Access Manager

The OpenSSL open source project team regularly releases updates to known OpenSSL vulnerabilities. Access Gateway and Analytics Server use the OpenSSL library for cryptographic functions. It is recommended that you keep Access Gateway and Analytics Server updated with the latest OpenSSL patch.

Prerequisites

- Before upgrading the kernel, ensure that you have updated the operating system to a supported version.
- Access Gateway Appliance installs a customized version of SLES 12 SP3. If you want to install the latest patches as they become available, you must have a user account to receive the Linux updates.
- Analytics Server installs a customized version of SLES 11 SP4. If you want to install the latest patches as they become available, you must have a user account to receive the Linux updates.
- Ensure that you have obtained the activation code for Access Manager from Novell Customer Center.

WARNING: Installing additional packages other than security updates and VMware tools breaks your support agreement. If you encounter a problem, Technical Support might require you to remove the additional packages and to reproduce the problem before providing any help with your problem.

- Section 15.1, “Installing or Updating Security Patches for Access Gateway Appliance and Analytics Server,” on page 183

15.1 Installing or Updating Security Patches for Access Gateway Appliance and Analytics Server

To get the latest security updates for Access Gateway Appliance, see “Performing an Online Update” on page 77.

To get the latest security updates for Analytics Server, you can follow any of these options:

- Section 15.1.1, “Registering to Novell Customer Center,” on page 184
- Section 15.1.2, “Configuring Subscription Management Tool,” on page 185
15.1.1 Registering to Novell Customer Center

To get the latest security updates for Analytics Server, the user must register with the Novell Customer Center by using the activation code obtained with the product:

**NOTE:** You must perform the proceeding steps to register with Novell Customer Center for Analytics Server.

If you face issues while using the activation code to register, see TID 3303599.

1. Go to YaST > Support > Novell Customer Center Configuration.
2. Select Configure Now (Recommended). In addition to the options that are selected by default, select Registration Code.
3. Click Next.
   The Manual Interaction Required screen appears. It might take a few minutes to connect to the server.
   This screen indicates that to activate the product, you must provide a valid e-mail ID associated with the Novell account and the activation code.
4. Click Continue.
5. To specify the e-mail address, activation code, and system name in the relevant fields:
   5a. Select the relevant option, then press Enter. A text field appears in the bottom left corner of the screen.
   5b. Specify value for the selected option in this text field, then press Enter to return to the screen.
   5c. Repeat these steps for each field.
6. Click Submit after you have specified all the relevant information to complete the registration.
7. Enter Q to close the window.
8. Enter Y at the prompt.
   The Manual Interaction Required screen is displayed. It indicates that the software repositories are created. You will receive a message from the Novell Customer Center Configuration indicating that the configuration was successful.
9. Click OK to return to YaST Control Center.
10. Click Quit to exit YaST.
11. Open a shell prompt and specify the following command to verify if the repository named NAM42-APP-Updates was created:

```
zypper lr
```

An output similar to the following appears:
### Analytics Server

<table>
<thead>
<tr>
<th>#</th>
<th>Alias</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enabled</td>
<td>Refresh</td>
</tr>
<tr>
<td>1</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**NOTE:** In the preceding example, 4.x.x-x represents the Access Manager version that was installed initially. For example, if you had installed Access Manager 4.2.x-x and then upgraded to 4.4.x-x, it will still display 4.2.x-x instead of 4.4.x-x because Access Manager 4.2.x-x, 4.3.x-x, 4.4.x-x, and 4.5.x-x have the same operating system.

12 Run the `zypper up` command to install the patches
13 After the patches are installed, restart the machine.
14 Confirm that all the patches are installed by running `zypper up` command again.

### 15.1.2 Configuring Subscription Management Tool

You can register Analytics Server to local Subscription Management Tool (SMT) server and download software updates from there instead of communicating directly with the Novell Customer Center and the NU servers.

To use an SMT server for client registration and as a local update source, you must configure the SMT server in your network first. The SMT server software is distributed as an add-on for SUSE Linux Enterprise Server. For information about configuring the SMT server, see Subscription Management Tool (SMT) for SUSE Linux Enterprise 11.

The following sections describe the configuration required for Analytics Server:

- Section 15.1.2.1, “SMT Configuration,” on page 185
- Section 15.1.2.2, “Configuring Analytics Server,” on page 186

#### 15.1.2.1 SMT Configuration

You must configure the SMT server and set up subscription for NAM4x-APP-Updates channel to receive the updates for Analytics Server.

1 Install the SMT server in a SLES 11 SP4 server. For more information, see Subscription Management Tool (SMT) for SUSE Linux Enterprise 11.
2 Log in to you Novell Customer Center account.
3 Select My Products > Mirroring Credentials, then click Generate Credentials.
4 Copy the mirroring credentials before logging out of your Novell Customer Center account.
5 Run the SMT Configuration tool from YAST, then specify the mirroring credentials.
6 Run the SMT Management tool.

The NAM4x-APP-Updates, s1e-11-x86_64 repository is displayed in the Repositories tab.
7 Select `sle-11-x86_64`, then click **Toggle Mirroring** to ensure mirroring is selected for this repository.

8 Click **Mirror Now**. This step ensures that the *NAM4x-APP-Updates* channel updates are mirrored from `nu.novell.com` to your local SMT server.

9 When mirroring is complete, click **OK** to close the tool.

### 15.1.2.2 Configuring Analytics Server

1 Copy `/usr/share/doc/packages/smt/clientSetup4SMT.sh` from the SMT server to the client machine.

You can use this script to configure a client machine to use the SMT server or to reconfigure it to use a different SMT server.

2 Specify the following command as **root** to execute the script on the client machine:

```
./clientSetup4SMT.sh --host server_hostname
```

For example,

```
./clientSetup4SMT.sh --host smt.example.com.
```

You can get the SMT server URL by running the SMT Configuration tool at the server. The URL is set by default.

3 Enter **y** to accept the CA certificate of the server.

4 Enter **y** to start the registration.

5 The script performs all necessary modifications on the client.

6 Execute the following command to perform registration:

```
suse_register
```

7 Specify the following command to get online updates from the local SMT server:

```
zypper up
```

8 Reboot the machine if prompted at the end of any patch install.

9 Confirm that all the patches are installed by running `zypper up` command again.

### 15.2 Updating Security Patches for Access Gateway Service

- Updating Linux Access Gateway Service with the Latest OpenSSL Patch
- Updating Windows Access Gateway Service with the Latest OpenSSL Patch

#### 15.2.1 Updating Linux Access Gateway Service with the Latest OpenSSL Patch

1 Download the `openssl-update.sh` script.

2 Change the file permission to executable:

```
chmod +x openssl-update.sh
```

3 Run the following command:
openssl-update.sh username password novell-nacm-apache-extra-4.1.9-1.0.2r'

**NOTE:** This downloads the 1.0.2r version of OpenSSL. Change the version number depending on the version available on the appliance channel.

username and password are the mirror credentials for the Novell Customer Care Portal the product is registered with.

### 15.2.2 Updating Windows Access Gateway Service with the Latest OpenSSL Patch

1. Open the powershell command line with the admin privilege.
   
   `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`

2. Navigate to `C:\Program Files\Novell\bin`, then run `patch_update.ps1` with the following three arguments:
   
   - username
   - password
   - rpmfilename (the RPM file name should not be suffixed with .rpm)

   Here username and password are the mirror credentials for the Novell Customer Care Portal the product is registered with, and the rpmfilename is the version of OpenSSL you are upgrading to. This version includes the OpenSSL version in the string. For example,

   ```
   patch_update.ps1 <myusername> <mypassword> <Openssl_Win_102k>
   ```

   **NOTE:** You must repeat these steps for all the Windows Access Gateway servers.

   This command updates to OpenSSL 1.0.2r.

   The local download location for the OpenSSL update is `C:\Program Files\Novell\apache\novell_patch`. 
Troubleshooting Installation and Upgrade

This section includes the following topics:

- Chapter 16, “Troubleshooting Installation,” on page 191
- Chapter 17, “Troubleshooting Upgrade,” on page 199
16 Troubleshooting Installation

- Section 16.1, “Troubleshooting Windows Administration Console Installation,” on page 191
- Section 16.2, “Secondary Administration Console Installation Fails,” on page 192
- Section 16.3, “Troubleshooting Identity Server Import and Installation,” on page 192
- Section 16.4, “Troubleshooting Windows Access Gateway Service Installation,” on page 194
- Section 16.5, “Access Gateway Appliance Installation Fails Due to an XML Parser Error,” on page 195
- Section 16.6, “Troubleshooting Access Gateway Import,” on page 195
- Section 16.7, “Troubleshooting Windows Identity Server Uninstallation,” on page 197

16.1 Troubleshooting Windows Administration Console Installation

The following instructions explain how to run the installation program in the debug mode and how to clean up after such an installation:

1 Use the following command to start the installation program:

   `<filename>.exe -DAM_INSTALL_DEBUG=true -DAM_INSTALL_DEBUG_JAVA=true`

   Replace `<filename>` with the name of the executable.

2 Press the Ctrl key until the progress bar reaches 100% and goes away.
   A terminal window opens to display standard output.
   Additional verbose information is sent to the \am32setup_debug.txt file.

3 Use the output and the log file to discover the cause of the problem.

4 After you run the installation in the debug mode, you must clean up the results as follows:

   4a Delete the temporary packages in the \pkgdirs directory, then delete the directory.
   4b Delete the \am32setup_debug.txt file.
   4c Delete the installation log files in the following directories:

      Windows 2012 Server: \am32setup.log
      Windows 2012 Server: \Program Files\Novell\log

   **IMPORTANT:** Delete the log files after debugging because they contain sensitive information in clear text.
16.2 Secondary Administration Console Installation Fails

Secondary Administration Console installation fails with a message “Verifying time synchronization”. If you are installing secondary Administration Console, ensure that time is in sync with primary Administration Console prior to installation.

If the time is in sync and secondary Administration Console installation fails or takes a long time, see the eDirectory install logs under /tmp/novell_access_manager. The log file name will be similar to install_edir_xxxxxx. If at the end of the log, you see an entry “Verifying time synchronization” multiple times, perform the following steps:

1. Log in to primary Administration Console and run the ndsrepair -T command.
2. Run the ndsrepair -N command and select the server that has the problem.
3. Log in to secondary Administration Console and you can see that the installation has proceeded.

16.3 Troubleshooting Identity Server Import and Installation

- Section 16.3.1, “Importing Identity Server into Administration Console Fails,” on page 192
- Section 16.3.2, “Reimporting Identity Server,” on page 193
- Section 16.3.3, “Check the Installation Logs,” on page 193

16.3.1 Importing Identity Server into Administration Console Fails

Ensure that the following requirements are met if you have installed Administration Console and Identity Server on different machines:

- The following ports are opened between the machines:
  - 8444
  - 1443
  - 1289
  - 524
  - 636
- Ports 8080 and 8443 must be open between the server and the clients for the clients to log in to Identity Server. For more information about firewalls and ports, see “Setting Up Firewalls” on page 30.
- Time is synchronized between the two machines. Ensure that both machines are configured to use a Network Time Protocol server.

If firewalls and time synchronization do not solve the problem, run the reimport script. See “Reimporting Identity Server” on page 193 for instructions.
16.3.2 Reimporting Identity Server

1. Verify that Administration Console is up by logging in to Administration Console.

2. Verify that you can communicate with Administration Console. From the command line of
   Identity Server machine, enter a ping command with the IP address of Administration Console.
   If the ping command is unsuccessful, fix the network communication problem before
   continuing.

3. In Administration Console, delete Identity Server.
   For more information about how to delete Identity Server in Administration Console, see
   Identity Server Advanced Configuration in the Access Manager 4.5 Administration Guide.

4. On the Identity Server machine, change to the jcc directory:
   Linux: /opt/novell/devman/jcc
   Windows: \Program Files\Novell\devman\jcc

5. Run the following script to configure jcc:
   Linux: ./conf/reimport_nidp.sh jcc
   Windows: conf\reimport_nidp.bat jcc

6. Run the following reimport script:
   Linux: ./conf/reimport_nidp.sh nidp
   Windows: conf\reimport_nidp.bat nidp <admin>
   Replace <admin> with the name of your administrator for Administration Console.

7. If these steps do not work, reinstall the device.

16.3.3 Check the Installation Logs

If Identity Server installation fails, check the installation logs warning and error messages.

- Section 16.3.3.1, “Linux Installation Logs,” on page 193
- Section 16.3.3.2, “Windows Installation Logs,” on page 194

16.3.3.1 Linux Installation Logs

Installation logs are located in the /tmp/novell_access_manager directory.

<table>
<thead>
<tr>
<th>Log File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>install_idp_&lt;date&amp;time&gt;_log</td>
<td>Contains the messages generated for Identity Server module.</td>
</tr>
<tr>
<td>install_main_&lt;date&amp;time&gt;_log</td>
<td>Contains the Tomcat messages generated during the installation.</td>
</tr>
</tbody>
</table>
16.3.3.2 Windows Installation Logs

Installation logs are located in the \Program Files\Novell\Tomcat\webapps\nps\WEB-INF\logs\install directory.

Table 16-2 Installation Log Files for the Windows Identity Server

<table>
<thead>
<tr>
<th>Log File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>install_jcc_&lt;date&amp;time&gt;.log</td>
<td>Contains the messages generated for the communications module.</td>
</tr>
</tbody>
</table>

16.4 Troubleshooting Windows Access Gateway Service Installation

1 Run the following command to start the installation program:

```
<filename>.exe -DAM_INSTALL_DEBUG=true -DAM_INSTALL_DEBUG_JAVA=true
```

Replace `<filename>` with the name of the executable.

2 Press the Ctrl key until the progress bar reaches 100% and goes away.

   Additional verbose information is sent to the \agsinstall_debug.txt file.

3 Use the output and the log file to discover the cause of the problem.

4 After you run the installation in debug mode, you must clean up the results:
   4a Delete the \agsinstall_debug.txt file.
   4b Delete the installation log files in the following directories:
16.5 Access Gateway Appliance Installation Fails Due to an XML Parser Error

This error may happen if Access Gateway Appliance is installed by using a remotely mounted installer. Use a locally mounted installer to avoid this issue.

16.6 Troubleshooting Access Gateway Import

When you install Access Gateway, it is automatically imported into Administration Console you specified during installation. If Access Gateway does not appear in the server list, you need to repair the import.

If the repair option does not resolve the problem, see the following sections:

- Section 16.6.1, “Repairing an Import,” on page 195
- Section 16.6.2, “Troubleshooting the Import Process,” on page 196

16.6.1 Repairing an Import

If Access Gateway does not appear in Administration Console within ten minutes of installing an Access Gateway, perform the following steps:

1. If a firewall separates Administration Console and Access Gateway, ensure that the required ports are opened. See Table 1-3 on page 32.
2. Click Devices > Access Gateways.
3. Wait for a few minutes, then click Refresh.
4. If the device import fails, a message similar to the following appears at the bottom of the table:

   Server gateway-<name> is currently importing. If it has been several minutes after installation, click repair import to fix it.

5. Click repair import.
6. If the device still does not appear or you do not receive a repair import message, continue with “Triggering an Import Retry” on page 197.
7. If triggering an import retry does not solve the problem, reinstall the device.
16.6.2 Troubleshooting the Import Process

If the import process does not complete successfully, the device does not show up in the Access Gateway list. The following sections describe the import process, where to find the log files, and how to use them to determine where the failure occurred:

- Section 16.6.2.1, “Understanding the Import Process,” on page 196
- Section 16.6.2.2, “Locating the Log Files,” on page 196
- Section 16.6.2.3, “Triggering an Import Retry,” on page 197

16.6.2.1 Understanding the Import Process

The following operations are performed during the import process:

1. A user specifies the IP address for Administration Console during installation.
2. A Java process called “JCC” (Java Communication Channel) detects that Administration Console IP address or port has changed between its own configuration and the CLI-updated settings.
3. An import message is sent to Administration Console, notifying it of the IP, port, and ID of Access Gateway.
4. Administration Console then connects to the Access Gateway device to fetch its configuration and version information. The Access Gateway import process is now complete.
5. As a separate asynchronous operation, the Embedded Service Provider (ESP) of Access Gateway connects and registers itself with the JCC.
6. When the ESP connects to the JCC, a similar import message is sent to Administration Console notifying it to import into the system.
7. Administration Console connects to the JCC, asking for the ESP configuration and version information. On Administration Console, an LDIF (Lightweight Directory Interchange Format) file containing the default configuration for the ESP is applied on the local eDirectory configuration store.
8. Administration Console then makes a link between the ESP and its configuration.
9. If the entire process completed properly, Access Gateway appears in the list of Access Gateways in Administration Console.

16.6.2.2 Locating the Log Files

Various Access Manager components produce log files. Use the following logs on Administration Console or Access Gateway:

- Administration Console log:
  - Linux: /opt/novell/devman/share/logs/app_sc.0.log
  - Windows Server 2012: \Program Files\Novell\log\app_sc.0.log
- Tomcat Log on Administration Console:
  - Linux: /opt/novell/nam/device name/logs/catalina.out
  - The device name can be idp, mag, or adminconsole.
Windows Server 2012: \Program Files\Novell\Tomcat\logs\stdout.log and \Program Files\Novell\Tomcat\logs\stderr.log

JCC log on Access Gateway:
- **Linux Appliance or Service:** /opt/novell/devman/jcc/logs/
- **Windows Service:** \Program Files\Novell\devman\jcc\logs

### 16.6.2.3 Triggering an Import Retry

1. Go to the directory:
   - **Linux:** /opt/novell/devman/jcc/
   - **Windows:** \Program Files\Novell\devman\jcc
2. Run the following script:
   - **Linux:** sh conf/reimport_ags.sh jcc
   - **Windows:** conf\reimport_ags.bat jcc
   
   Specify details against the following prompts:
   1. Choose a local listener IP address [x.x.x.x]:
   2. (Optional) Choose a local NAT IP address [optional]:
   3. Choose Administration Console’s IP address []:
   4. Enter Admin User’s DN [cn=admin,o=novell]:
   5. Enter Admin Password: ******
      
      Wait for a few minutes for the configuration to finish.
3. Run the following script:
   - **Linux:** sh conf/reimport_ags.sh agm
   - **Windows:** conf\reimport_ags.bat agm <username>
   
   For example, if the username is *admin*, then run conf\reimport_ags.bat agm admin
   
   Specify details against the following prompts:
   1. (Linux) Do you want to import the device with current configuration or initial configuration after installation (Enter C for current configuration, I for initial configuration).
   2. (Linux) Enter Admin User’s DN [cn=admin,o=novell]:
   3. Enter Admin password:

### 16.7 Troubleshooting Windows Identity Server Uninstallation

When you uninstall Windows Identity Server, the uninstall program prompts you for the credentials of the admin user for Administration Console. If the primary Administration Console is not available for the authentication request, the uninstall fails.

To force the uninstall program to skip the authentication request, run the following command:
\Program Files\Novell\Uninstall_AccessManagerServer\UninstallAccessManagerServer.exe -DAM_INSTALL_AUTH_BYPASS=true
17 Troubleshooting Upgrade

- Section 17.1, “Access Gateway Throws a 403 Forbidden Page Error for a Resource Protected by a Form Fill Policy,” on page 199
- Section 17.2, “Troubleshooting Linux Administration Console Upgrade,” on page 199
- Section 17.3, “Upgrading Secondary Administration Console Fails with an Error,” on page 201
- Section 17.4, “Issue in SSL Communication between Access Gateway and Web Applications,” on page 201
- Section 17.5, “Administration Console Fails to Start When You Upgrade the Operating System After Upgrading Access Manager,” on page 201
- Section 17.6, “Customized Login Pages Are Missing After Upgrading Access Manager,” on page 202
- Section 17.7, “The Email OTP JSP Page Does Not Render Properly on Internet Explorer 11,” on page 202
- Section 17.8, “Access Manager Upgrade Hangs While Upgrading eDirectory,” on page 202
- Section 17.9, “X509 Authentication Does Not Work and Throws HTTP 500 Error After Upgrade,” on page 203

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

This issue happens if a web server returns a form with a HTTP 403 error code. Access Gateway, by default, returns its own custom error pages. Hence, this prevents the Form Fill feature to work.

To workaround, perform the following steps:

2. Specify ProxyErrorOverride off.
3. Click OK.

17.2 Troubleshooting Linux Administration Console Upgrade

- Section 17.2.1, “Upgrade Hangs,” on page 200
- Section 17.2.2, “Multiple IP Addresses,” on page 200
- Section 17.2.3, “Certificate Command Failure,” on page 201
17.2.1 Upgrade Hangs

If the upgrade process encounters an error while installing a component or encounters an unexpected condition that requires a user input, the installation hangs.

Perform the following steps to resolve this issue:

1. View the installation screen and determine which component is being upgraded.
2. Change to the /tmp/novell_access_manager directory.
3. View the log file of the component that is being upgraded.
   Solve the problem described in the log file before continuing with the upgrade.
   For example, if the eDirectory health check fails, the edir log file indicates that the upgrade program is waiting for a response on whether the upgrade should continue. You should abort the upgrade, run ndsrepair to repair the configurations store, then restart with the upgrade process.
4. If the log file of the current component does not contain any errors, use the time stamps of the log files to determine which component just finished its upgrade and check it for errors.
   If you cannot determine which component is causing the problem:
   4a. Stop the upgrade process.
   4b. Run the following command:
      ```
      tail -f /tmp/novell_access_manager/<file-name>
      ```
      This command lists all the files created in the specified directory.
   4c. Restart the upgrade process.

17.2.2 Multiple IP Addresses

If your server has multiple IP addresses, you might see the following message during upgrading Linux Administration Console:

```
Failed to load any MDB driver - Error: Could not load driver /usr/lib/mdb/mdbfile.so, error 9 - /usr/lib/mdb/mdbfile.so: cannot open shared object file: No such file or directory
```

The error occurs when running Novell Audit on servers with more than one IP address. It occurs when the system attempts to upgrade the audit server. Systems with more than one IP address have problems running Novell Audit because the multiple directory database (MDB) driver does not know which IP address to use with eDirectory. You can point Novell Audit to a specific IP address by creating an MDB configuration file.

The required filename and path for the MDB configuration file is as follows:

```
/etc/mdb.conf
```

To point Novell Audit to a specific IP address for eDirectory, the MDB configuration file must store the following parameters:

```
driver=mdbds referral=eDirectory_IP_Address.
```

For example,
You might only have one IP address, but your server might have two network adapters. If you create the `/etc/mdb.conf` file and specify your IP address, you do not encounter this error message when you upgrade.

17.2.3 Certificate Command Failure

Certificate commands are generated when you upgrade Administration Console. Ensure that this process has been completed successfully. In Administration Console Dashboard, click Security > Command Status.

If a certificate command fails, note the store, then click Troubleshooting > Certificates. Select the store, then click Re-push certificates to push the certificates to the store.

17.3 Upgrading Secondary Administration Console Fails with an Error

Upgrading secondary Administration Console fails with the following error:

```
Configuring HTTP service... Failed to configure HTTP service: no referrals
err=-634
```

This issue may occur because of some eDirectory issues. You can run the script again. If you are accessing the console remotely, then run the script from the machine directly.

17.4 Issue in SSL Communication between Access Gateway and Web Applications

After upgrading Access Manager, applications are not accessible. This issue happens when there is any discrepancy between the cipher suites configured for Access Gateway and the applications protected by this Access Gateway.

To workaround this issue, see TID 7016872.

17.5 Administration Console Fails to Start When You Upgrade the Operating System After Upgrading Access Manager

When you upgrade the operating system from SLES 11 SP3 to SLES 12 after upgrading Access Manager, Administration Console does not start. This issue occurs because eDirectory services do not start after the upgrade.

To resolve this issue, perform the following steps:

1. Run `ndsconfig upgrade` at the SLES 12 server, where Administration Console is upgraded.
   
   This generates the necessary template files so that eDirectory starts without any issues.
Run `ndsmanage startall`.
This starts eDirectory services on the SLES 12 server.

### 17.6 Customized Login Pages Are Missing After Upgrading Access Manager

After upgrading Access Manager, you cannot view the customized login JSP pages. This happens when the customized JSP files are not restored or the legacy filesystem directory is not created.

To resolve this issue, see Section 10.1, “Maintaining Customized JSP Files for Identity Server,” on page 150.

### 17.7 The Email OTP JSP Page Does Not Render Properly on Internet Explorer 11

This issue occurs when the Identity Server domain is added to the local intranet or the compatibility mode is enabled.

To workaround this issue, add the following entry to the `nidp_latest.jsp` page:

```java
response.setHeader("X-UA-Compatible","IE=edge");
```

You can locate the `nidp_latest.jsp` file in the following path:

- **Linux**: `/opt/novell/nids/lib/webapp/jsp`
- **Windows**: `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp`

Example, add `response.setHeader("X-UA-Compatible","IE=edge");` after `<%`

```java
final String NIDP_JSP_CONTENT_DIV_ID = "theNidpContent";
```

For more information, see TID 7022722 (https://www.novell.com/support/kb/doc.php?id=7022722).

### 17.8 Access Manager Upgrade Hangs While Upgrading eDirectory

On Windows 2012 R2 Server, the Access Manager upgrade hangs while upgrading eDirectory. This occurs because the `nservmsg.dll` file gets locked. This is a random issue.

To workaround this issue, perform the following steps:

1. Manually stop the Windows Event Log service.
2. On the upgrade pop-up screen, click **Retry**.
3. Restart the Windows Event Log service manually again and proceed with the upgrade.
17.9 X509 Authentication Does Not Work and Throws HTTP 500 Error After Upgrade

This issue occurs in a dual identity server cluster configuration. After upgrading Access Manager, X509 authentication fails because the context.xml file gets overwritten and some configurations get deleted.

To workaround this issue, perform the following steps:

1. Before upgrading Access Manager, back up the `/opt/novell/nam/idp/webapps/nidp/META-INF/context.xml` file, if you have customized the context.xml file.

2. After upgrading Access Manager, add the customized content to the upgraded context.xml file and uncomment the following lines in the context.xml file:

   <!-- Force use the old Cookie processor (because this new tomcat version uses RFC6265 Cookie Specification) -->

   <!-- <CookieProcessor className="org.apache.tomcat.util.http.LegacyCookieProcessor" /> -->

   <!-- -->

   <!-- <Context> -->

   <!-- -->
Appendix

This section includes the following topics:

- Appendix A, “Configuring Administration Console Ports 9000 and 9001 to Listen on the Specified Address,” on page 207
- Appendix B, “Recommendations for Scaling Access Manager Components in Public Cloud,” on page 209
Configuring Administration Console Ports 9000 and 9001 to Listen on the Specified Address

Administration Console ports 9000 and 9001 listen on 127.0.0.1 by default. Administration Console uses these ports for scheduling jobs. If you encounter any issue because of these ports listening on 127.0.0.1, such as issue with IPv6 connectivity, you can specify a different address by using the following Java option in the `tomcat8.conf` (Linux) or `tomcat8w.exe` (Windows) file:

**Linux:** `/opt/novell/nam/adminconsole/conf/tomcat8.conf`

**Windows:** Navigate to `C:\Program Files\Novell\Tomcat\bin` and then double-click `tomcat8w.exe`

"com.microfocus.nam.adminconsole.localhost.ipaddress"

For example:

```java
JAVA_OPTS="${JAVA_OPTS} -Dcom.microfocus.nam.adminconsole.localhost.ipaddress=10.0.0.0"
```
Recommendations for Scaling Access Manager Components in Public Cloud

In the public cloud environment, you can manually add or remove Access Manager components nodes to a cluster depending on the varying scalability requirements.

- “Scaling Up the Access Manager Nodes” on page 209
- “Scaling Down the Access Manager Nodes” on page 210

Scaling Up the Access Manager Nodes

As the number of users and demands for web resources increase, you can easily add another Identity Server or Access Gateway to handle the load. The cluster configuration is sent to the newly added components automatically.

Scaling up a node when the Access Manager component is not deployed in the cloud virtual machine

Perform the following steps to scale up a node:

1. Create new virtual machines. For AWS EC2, see Section 6.2.2, “Creating and Deploying Instances,” on page 103 and for Azure, see Section 7.2.2, “Creating and Deploying Virtual Machines,” on page 125.
2. Install the required Access Manager component and import that component to Administration Console.
3. After importing the component, log in to Administration Console and assign the imported component to the required cluster.
4. Access the cloud console (Azure or AWS EC2) and add the newly imported component to the load balancer group or target group.

Scaling up a node when the Access Manager component is installed in the cloud virtual machines, but not imported into the cluster

Perform the following steps to scale up a node:

1. Switch on the cloud virtual machine on which the required component is installed.
2. Access the terminal of the server and initiate the `ag_import` or `idp_import` script depending on the type of server.
3. Specify the Administration Console IP address while importing the component.
4. After importing, log in to Administration Console and assign the imported component to the required cluster.
5. Access the cloud console (Azure or AWS EC2) and add the newly imported component to the load balancer group or target group.
Scaling Down the Access Manager Nodes

1. Remove the Access Manager component’s IP address from the load balancer rule.
2. Stop the service. (Identity Server or Access Gateway)
3. Stop the virtual machine on which the component is installed. You can also optionally delete the virtual machine.
4. Log in to Administration Console, select the non-reporting node from the cluster, and delete it from the configuration.