Access Manager 5.0
Installation and Upgrade Guide

March 2021

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.microfocus.com/en-us/legal.

Contents

About this Book and the Library

This guide provides an introduction to NetIQ Access Manager and describes the installation and upgrade procedures.

The Install or Upgrade sends the following information to the Telemetry server for checking product version currency:

- Product Name. For example, NAM
- Product Version: For example, 5.0.4.0-43
- Installation Type: For example, Service or Appliance
- Operating System: For example, SLES

This information does not contain any Personal Information (PI) and is collected only while installing or upgrading.

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

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

1 Planning Your Access Manager Environment

1.1 Deployment Models

The product is available in the following two deployment models:

- **Access Manager:** To deploy individual components (Identity Server, Access Gateway, Analytics Server and Administration Console). You can install and manage each component on separate servers. Administration Console, Identity Server, Dashboard, and Access Gateway can also be deployed using Docker and on Cloud as services on AWS EC2 and on Microsoft Azure.

- **Access Manager Appliance:** To deploy all components together as an appliance. It is a soft appliance based on SUSE Linux Enterprise Server. It bundles pre-configured Identity Server, Access Gateway, and Administration Console in one server. You can install and manage Analytics Server on a separate server. This model enables organizations to deploy and secure web and enterprise resources quickly. 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
- 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 15.

The following diagrams describe differences between Access Manager and Access Manager Appliance:

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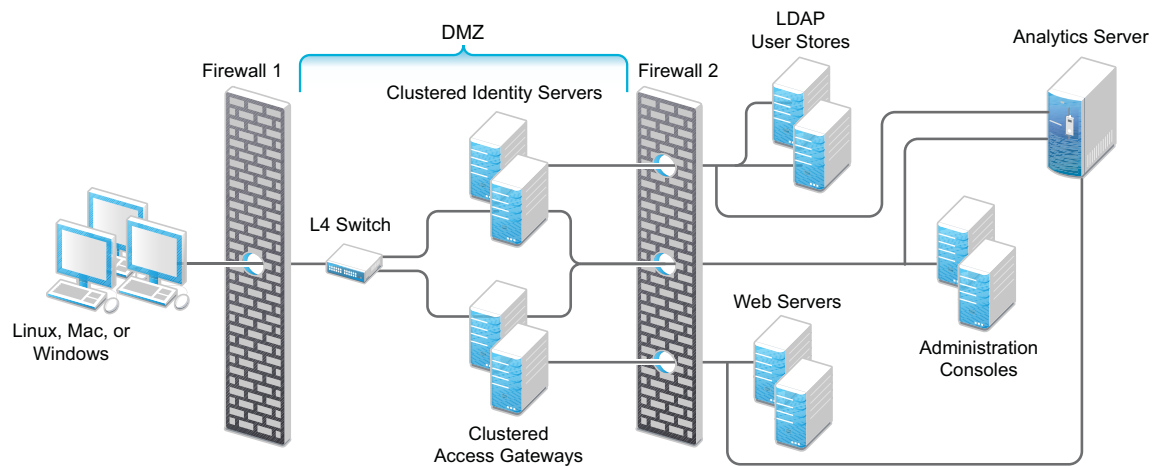
Figure 1-2 *Typical Deployment of Access Manager Appliance*
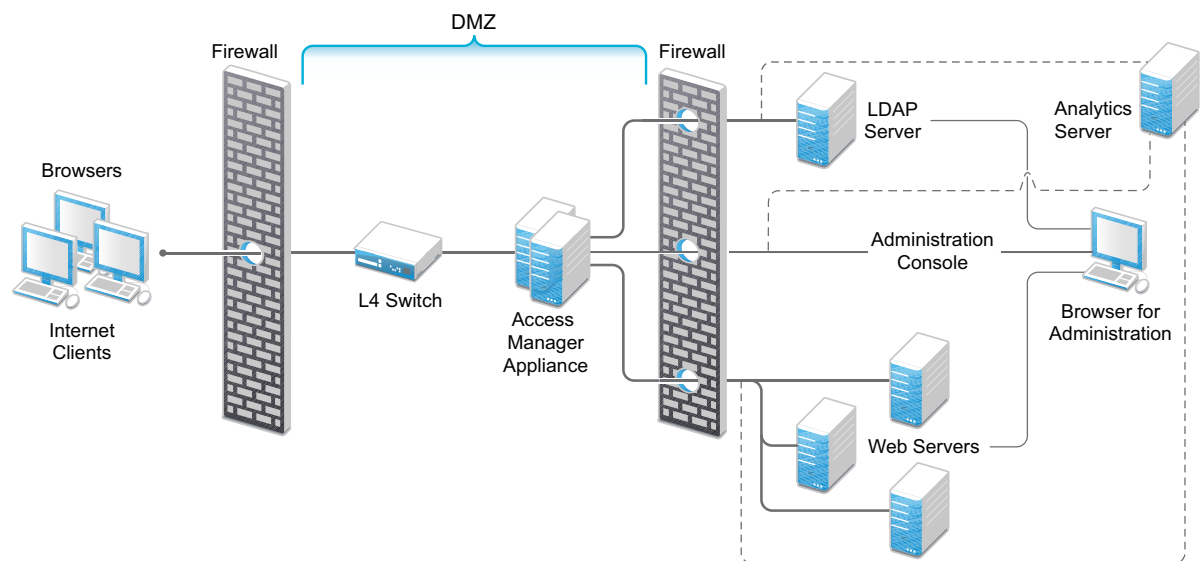
1.2 Access Manager Versus Access Manager Appliance

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 1-1 *Access Manager Versus Access Manager Appliance*

Feature	Access Manager Appliance	Access Manager
Virtualization Support	Supported on the virtual servers based on SUSE Linux Enterprise Server (SLES) 12 SP5 with 64-bit operating system x86-64 hardware.	Supported on the virtual servers based on SLES 12 SP5 or SLES 15 SP2 with 64-bit operating system x86-64 hardware.
Host Operating System	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.	Operating System choice is more flexible. Install Administration Console, Identity Server, and Access Gateway on a supported operating system (SUSE or Red Hat). The patch update channel maintains patches for Access Manager. You must purchase, install, and maintain the underlying operating system.
Component Installation Flexibility	Access Manager components such as Administration Console, Identity Server, and Access Gateway cannot be selectively installed or uninstalled.	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 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).
Administration Console Access	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.	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.
Scalability and Performance	Scales vertically on adding CPU and memory resources to each node. See *NetIQ Access Manager Performance and Sizing Guidelines* .	Scales both vertically and horizontally on adding nodes. See *NetIQ Access Manager Performance and Sizing Guidelines* .

Feature	Access Manager Appliance	Access Manager
High Availability	Supported	Supported
Upgrade	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.	You can upgrade from one version of Access Manager to another version. However, upgrading from Access Manager Appliance to Access Manager is not supported.
Disaster Recovery	You can use the backup and restore process to save your Access Manager Appliance configuration.	You can use the backup and restore process to save your Access Manager configuration.
Time to Value	Automates several configuration steps to quickly set up the system.	Requires more time to install and configure as the components are on different servers.
User Input required during installation	Access Manager Appliance is a software appliance that takes only a few basic parameters as input. Several options assume default values.	More flexibility during installation in terms of selectable parameters.
Installation and Configuration Phases	The installer takes care of configuration for each component. The system is ready for use after it is installed.	Separate installation and configuration phases for each component. After installation, each Access Manager component is separately configured.
Mode of release	Access Manager Appliance is released as a software appliance.	Access Manager is delivered in the form of multiple operating system- specific binaries.
NIC Bonding	IP address configuration is done through Administration Console. So, NIC bonding is not supported.	NIC bonding can be done through the operating system and Access Manager in turn uses this configuration.
Networking: Port Details	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.	Multiple ports need to be opened for deployment.
Networking: General	Administration Console must be in DMZ, but access can be restricted through the private interface.	As Administration Console is a separate device, access can be restricted or Administration Console can be placed in an internal network.
Certificate Management	Certificate management is simplified. All certificates and key stores are stored at one place making replacing or renewing certificates easier.	Changes are required at multiple places to replace or renew certificates.
SAML Assertion Signing	Same certificate is used for all communication. (signing, encryption, and transport).	As there are multiple key stores, you can configure different certificates for the communication.

Feature	Access Manager Appliance	Access Manager
Associating different signing certificates for each service provider	Not supported	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.
Associating different certificates to Identity Server	Not applicable because Identity Server is accelerated by Access Gateway.	Supported. You can place Identity Server behind Access Gateway or place it separately in DMZ.
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, and Administration Console. 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.
Updating Kernel with Security Patches	Supports installation of latest SLES operating system security patches.	You are fully responsible for all operating system maintenance including patching.

Feature	Access Manager Appliance	Access Manager
Clustering	For additional capacity and for failover, cluster a group of 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 does not contain Administration Console. A typical Access Manager Appliance deployment in a cluster is described in Figure 1-3.	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.

Figure 1-3 *Access Manager Appliance Cluster*
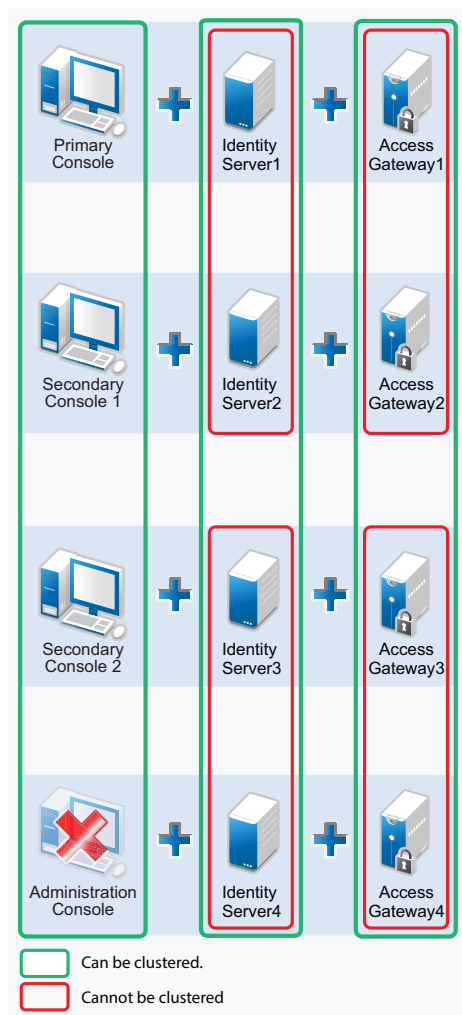
Figure 1-4 *Access Manager Cluster*

Can be clustered.
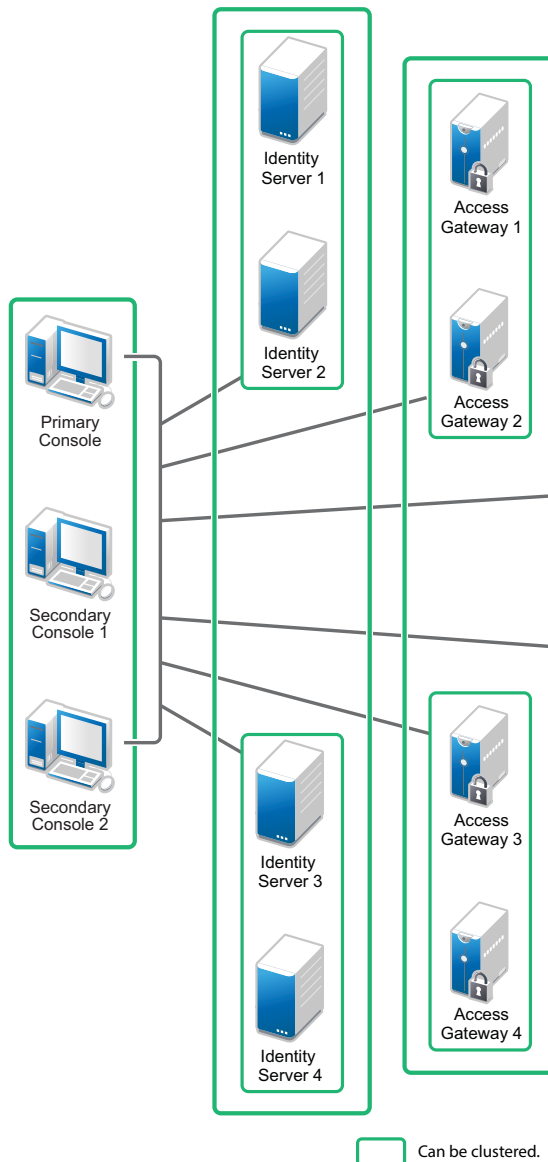
General Guidelines

◆ Adding an Access Gateway Service or Access Gateway Appliance to an Access Manager Appliance cluster is not possible.

◆ 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 might 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 NetIQ Access Manager 5.0 Administration Guide.

◆ You cannot have different certificates for signing and encryption in a federation setup.

- You cannot install any monitoring software to monitor statistics in Access Manager Appliance.
- Clustering between Access Manager and Access Manager Appliance is not supported.

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 costs by consolidating Access Manager services on fewer servers.
- You want to quickly set up a test environment to verify changes.
- You want to quickly set up 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, Active Directory, or Azure Active Directory) that contains your system users. Identity Server uses the LDAP directory to authenticate users.

  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 communicates with 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 with RHEL 7.x. NTP is discontinued in RHEL 8, therefore with RHEL 8.x you must use Chrony. For more information, see Configuring Chrony.

  IMPORTANT: If time is not synchronized, you 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

See the *NetIQ Access Manager System Requirements* guide.

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. Install it behind 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
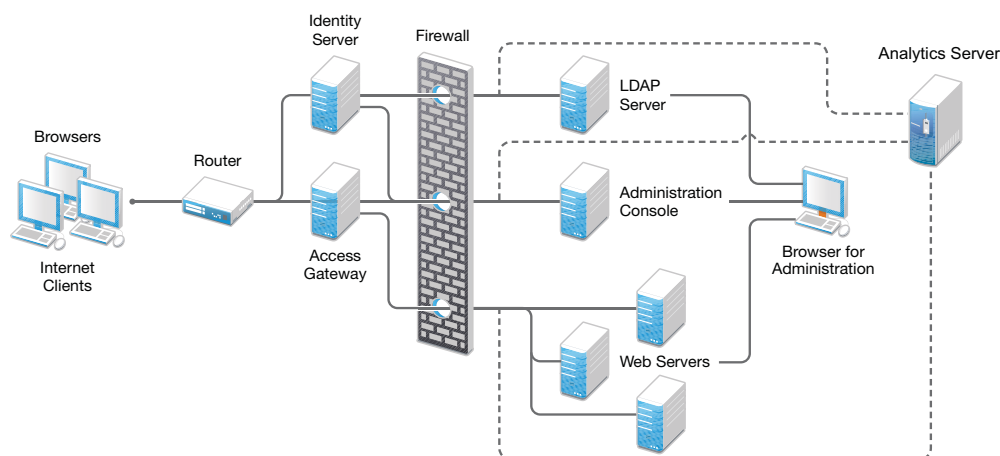
1 Install Administration Console.

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

2 If 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.

6 Configure Identity Server, Analytics Server, and Access Gateway. See Configuring Access Manager in the NetIQ Access Manager 5.0 Administration Guide.

In this configuration, the LDAP server is separated from Identity Server by firewall. Ensure that 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 NetIQ Access Manager 5.0 Administration Guide.

Firewall protects the LDAP server and Administration Console, both of which contain a permanent store of sensitive data. Web servers are installed behind the firewall for added protection. Identity Server does not permanently store any user data. This is the recommended configuration. This configuration also supports an L4 switch in place of a router to 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*
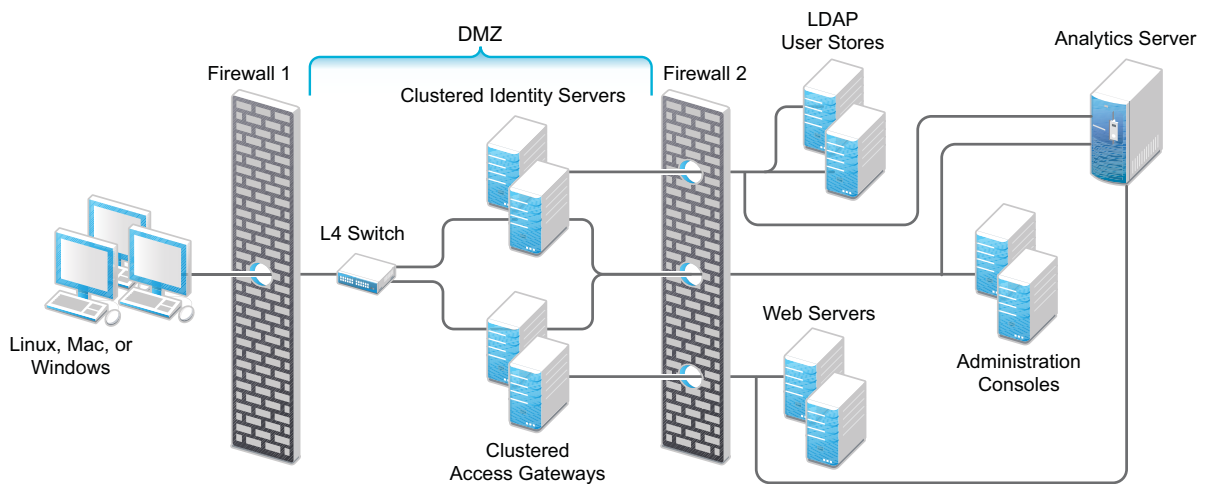
You can configure end users to communicate with Identity Servers and Access Gateways through HTTP or HTTPS. You can configure Access Gateways to communicate with web servers through HTTP or HTTPS. Multiple Administration Consoles provide administration and configuration redundancy.

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.

- 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 Server and Access Gateway. 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 new servers are added to the cluster, they are automatically sent the cluster configuration. See Recommendations for Scaling Access Manager Components in Public Cloud.

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.

For more information about AWS EC2 VPC, see Amazon Virtual Private Cloud Documentation.

For information about how to deploy Access Manager on AWS EC2, see Deploying Access Manager on Amazon Web Services EC2.

Figure 1-7 *Access Manager Deployment on AWS EC2*
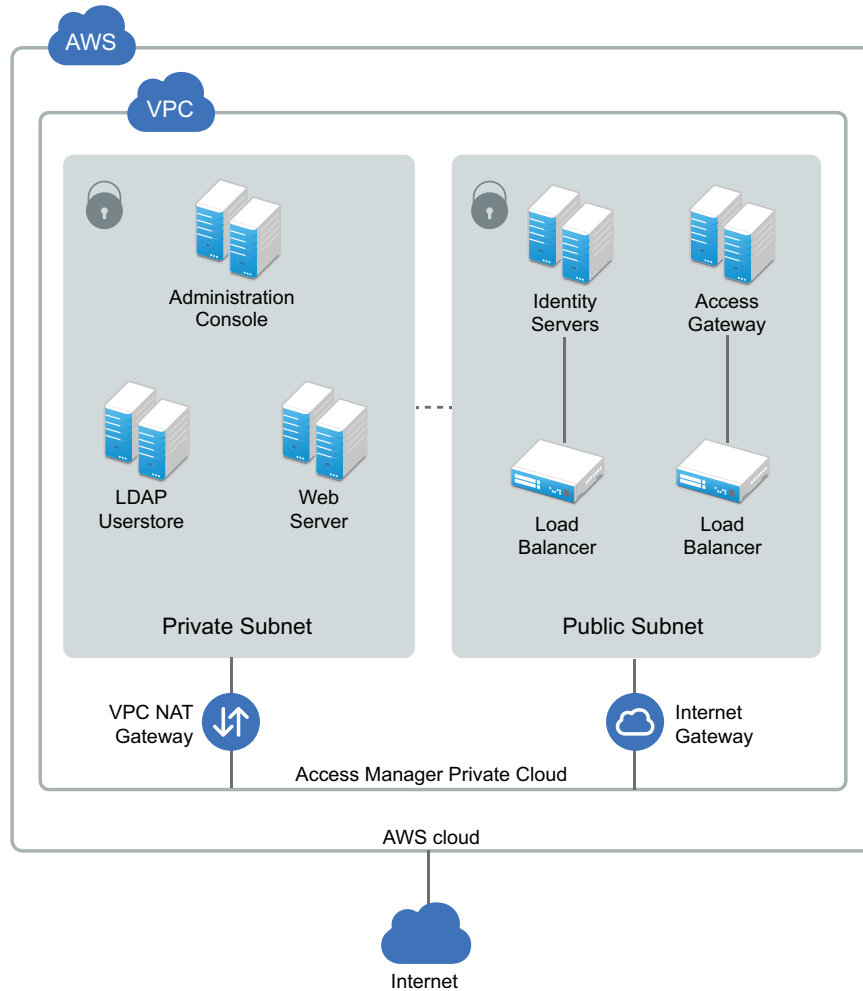
1.6.2 Deploying on Microsoft Azure

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.

For information about how to deploy Access Manager on Azure, see Deploying Access Manager on Microsoft Azure.

Figure 1-8 Access Manager deployment on Microsoft Azure
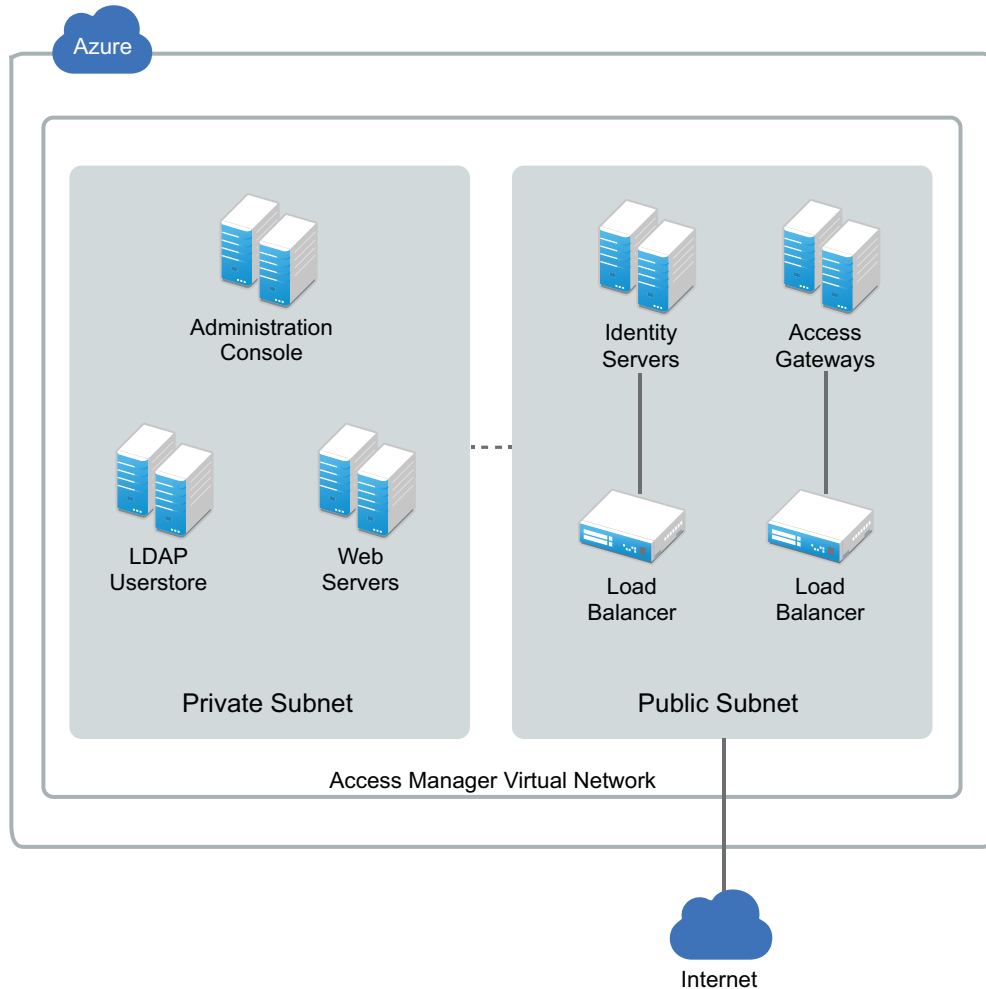
1.7   Installing Access Manager Components in NAT Environments

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:

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.

NOTE: You can use NTP with RHEL 7.x. NTP is discontinued in RHEL 8, therefore with RHEL 8.x you must use chrony.

❑ 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, 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*
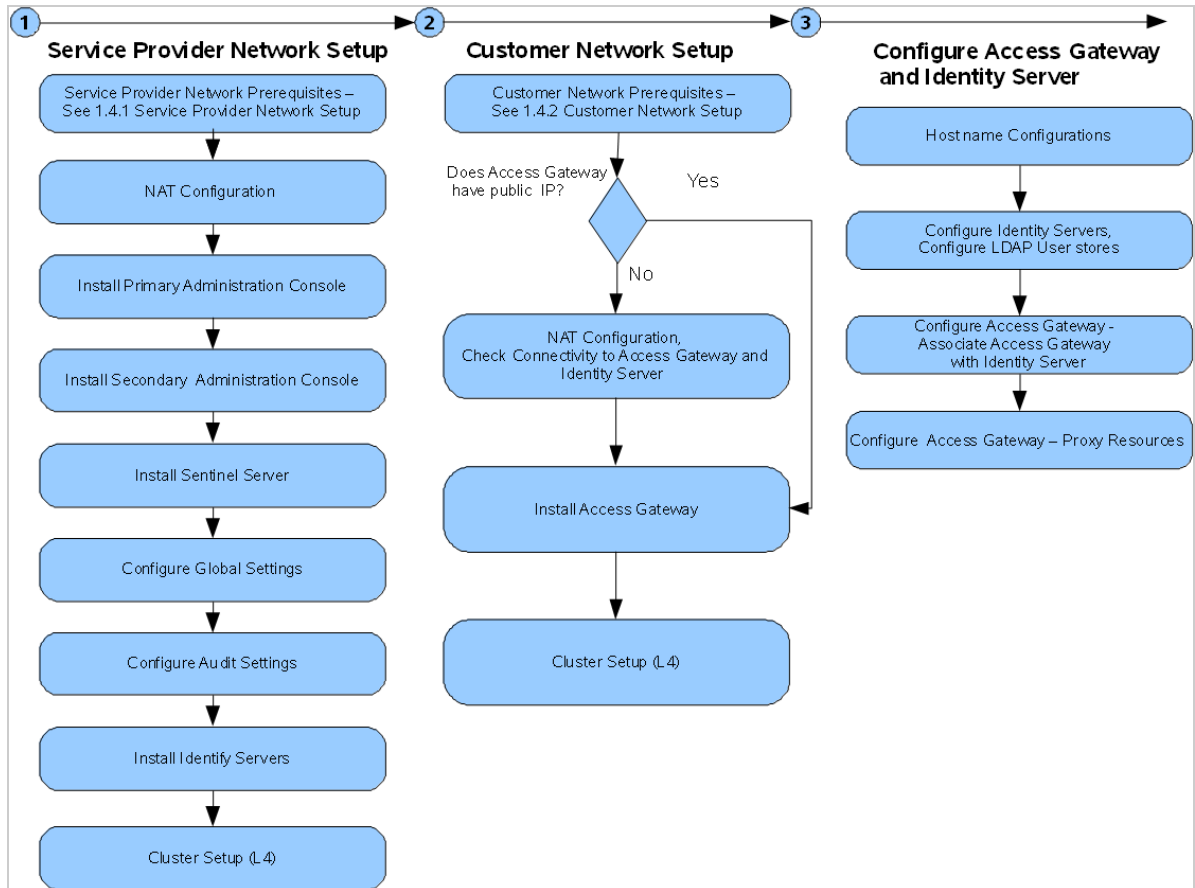
1.7.3   Installing Access Manager Components in NAT Environments

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 53
4. "Installing Access Gateway" on page 63

1.7.3.1   Installing Administration Console

For installation requirements, see *NetIQ Access Manager System Requirements*.

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 if you are using RHEL 7. NTP is discontinued in RHEL 8, therefore with RHEL 8.x you must use chrony. 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.

3b Run the following commands on the primary Administration Console to start the NTP server:

`systemctl start ntpd`

`systemctl enable ntpd`

3c Run the `ntpdate 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 information about installing Administration Console, see Installing Administration Console.

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

6 Continue with Configuring Global Settings to add both 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 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 the Administration Console Listening IP address from the 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 53.

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 NetIQ Access Manager 5.0 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 63.

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 NetIQ Access Manager 5.0 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.

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 address, 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 NetIQ Access Manager 5.0 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*
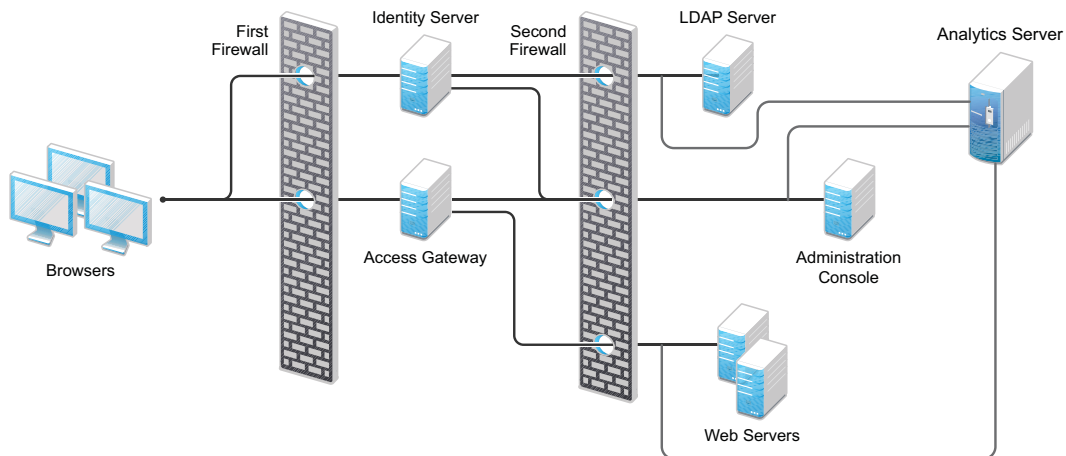
The first firewall separates Access Manager from the Internet, allowing browsers to access the resources through specific ports.The second firewall separates Access Manager components from web servers they are protecting and from Administration Console.

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*

Component	Port	Description
NTP Server	UDP 123	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.
DNS Servers	UDP 53	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.
Remote Administration Workstation	TCP 22	If you want to use SSH for remote administration of Access Manager components, open TCP 22 to allow.

Table 1-3 *When a Firewall Separates Administration Console from a Component*

Component	Port	Description
Access Gateway, Identity Server	TCP 1443	For communication from Administration Console to devices.
	TCP 8444	For communication from devices to Administration Console.
	TCP 1290	For communication from devices to the syslog server on Administration Console.
	TCP 524	For NCP certificate management with NPKI. Open this port so that both the device and Administration Console can use the port.
	TCP 636	For secure LDAP communication from devices to Administration Console.
	HTTP 2443 HTTP 8443	For the installer to communicate with Administration Console. You can close these port after installation is complete.
Importing an Access Gateway Appliance	ICMP	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.
LDAP User Store	TCP 524	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.
	TCP 636	For secure LDAP communication from Administration Console to user store.
Administration Console	TCP 524	Required to synchronize the configuration data store.
	TCP 636	Required for the secure LDAP communication.
	TCP 8080, 8443	Used for the Tomcat communication.
	TCP 705	Used by Sub Agent-Master Agent communication inside Administration Console.
	UDP 161	Used for communication by an external Network Monitoring System with Administration Console by using SNMP.
Browsers	TCP 8080	For HTTP communication from browsers to Administration Console.
	TCP 8443, 2443, 2080	For HTTPS communication from browsers to Administration Console. **NOTE:** 2443 and 2080 are optional ports required when Administration Console and Identity Server are collocated.
	TCP 8028, 8030	To use iMonitor or DSTrace from a client to view information about the configuration store on Administration Console.
Upgrade Assistant Agent	TCP 9968	For HTTPS communication from Upgrade Assistant agent to Administration Console.

Table 1-4 *When a Firewall Separates Identity Server from a Component*

Component	Port	Description
Access Gateway	TCP 8080 or 8443	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.
	TCP 80 or 443	For communication from Identity Server to Access Gateway ESP. 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.
Administration Console	TCP 1443	For communication from Administration Console to devices. This is configurable.
	TCP 8444	For communication from Identity Server to Administration Console.
	TCP 8443	For Docker deployment.
	TCP 1290	For communication from devices to the Syslog server on Administration Console.
	TCP 524	For NCP certificate management with NPKI from Identity Server to Administration Console.
	TCP 636	For the secure LDAP communication from Identity Server to Administration Console.
Identity Server	TCP 8443 or 443	For HTTPS communication. You can use iptables to configure this for TCP 443. See Translating Identity Server Configuration Port.
	TCP 7801	For back-channel communication with cluster members. You must enable the multicast traffic on this port. This port is configurable. **NOTE:** For Docker deployment, use TCP port 7901.
LDAP User Stores	TCP 636	For secure LDAP communication from Identity Server to the LDAP user store.
Service Providers	TCP 8445	If you have enabled identity provider introductions, open a port to allow HTTPS communication from the user's browser to the service provider.
	TCP 8446	If you have enabled identity provider introductions, open a port to allow HTTPS communication from the user's browser to the service consumer.
Browsers	TCP 8080	For HTTP communication from a browser to Identity Server. You can use iptables to configure this for TCP 80. SeeTranslating Identity Server Configuration Port.
	TCP 8443	For HTTPS communication from a browser to Identity Server. You can use iptables to configure this for TCP 443. See Translating Identity Server Configuration Port.

Component	Port	Description
CRL and OCSP Servers	Configurable	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.
Active Directory Server with Kerberos	TCP 88, UDP 88	For communication with KDC on the Active Directory Server for Kerberos authentication.
Upgrade Assistant Agent	TCP 9968	For HTTPS communication from Upgrade Assistant agent to Identity Server.

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

Component	Port	Description
Identity Server	TCP 8080 or 8443	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.
	TCP 80 or 443	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.
Administration Console	TCP 1443	For communication from Administration Console to Access Gateway. This is configurable.
	TCP 8444	For communication from Access Gateway to Administration Console.
	TCP 1290	For communication from devices to the Syslog server on Administration Console.
	TCP 524	For NCP certificate management with NPKI from Access Gateway to Administration Console.
	TCP 636	For secure LDAP communication from Access Gateway to Administration Console.
Access Gateway	TCP 7801	For back-channel communication with cluster members. You must enable the multicast traffic option on this port. This port is configurable. It is set by Identity Server cluster configuration that Access Gateway trusts. See Configuring a Cluster with Multiple Identity Servers in the NetIQ Access Manager 5.0 Administration Guide.
	TCP 80 or 443	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.

Component	Port	Description
Access Gateway Appliance Configuration console (`https://<access_gateway_appliance-IP address>:9443`)	TCP 9090 or 9443	For using the Jetty service on the appliance Configuration console. For information about the Configuration console, see Configuring Access Gateway Appliance.
	TCP 1099	For the Java RMI communication.
Browsers/Clients	TCP 80	For HTTP communication from the client to Access Gateway. This is configurable.
	TCP 443	For HTTPS communication from the client to Access Gateway. This is configurable.
Web Servers	TCP 80	For HTTP communication from Access Gateway to web servers. This is configurable.
	TCP 443	For HTTPS communication from Access Gateway to web servers. This is configurable.
Upgrade Assistant Agent	TCP 9968	For HTTPS communication from Upgrade Assistant agent to Access Gateway.

Table 1-6 *When a Firewall Separates Analytics Server from Administration Console or any Services*

Component	Port	Description
Administration Console	TCP 1444	For communication between Administration Console and Analytics Server.
Browsers	TCP 8445	For HTTPS communication with Analytics Server for Access Manager Dashboard.
Syslog	TCP 1468	For sending Syslog messages from Access Manager components to Analytics Server.
Docker	TCP 2443	For Docker deployment.
Remote Administration Workstation	TCP 22	For communication from your remote administration workstation to Analytics Server.
Upgrade Assistant Agent	TCP 9968	For HTTPS communication from Upgrade Assistant agent to Administration Console or any services.

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*

Component	Port	Traffic Direction	Description
Access Gateway, Identity Server	TCP 1290	Inbound	For communication from devices to the Syslog server on Administration Console.
	TCP 2443	Inbound	For the installer to communicate with Administration Console.
	TCP 8444	Inbound	For communication from devices to Administration Console.
	TCP 524	Inbound	For NCP certificate management with NPKI. Open this port so that both the device and Administration Console can use the port.
	TCP 636	Inbound	For secure LDAP communication from devices to Administration Console.
Access Gateway	TCP 1289	Inbound	For importing Access Gateway into Administration Console.
SSH	TCP 22	Inbound	For accessing Administration Console using SSH.
Access Gateway	ICMP	Inbound	For importing Access Gateway.
Upgrade Assistant Agent	TCP 9968	Inbound	For HTTPS communication from Upgrade Assistant agent to Administration Console on Cloud.

Table 1-8 *Identity Server on Cloud*

Component	Port	Traffic Direction	Description
Administration Console	TCP 1443	Inbound	For communication from Administration Console to devices. This is configurable.
	TCP 524	Inbound	For NCP certificate management with NPKI from Identity Server to Administration Console.
Identity Server	TCP 7801	Inbound	For the back-channel communication with cluster members. You must enable the multicast traffic option on this port. This port is configurable.
SSH	TCP 22	Inbound	For accessing Identity Server using SSH.
Access Gateway, Browsers	TCP 8443	Inbound	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.
Upgrade Assistant Agent	TCP 9968	Inbound	For HTTPS communication from Upgrade Assistant agent to Identity Server on Cloud.

Table 1-9 *Access Gateway on Cloud*

Component	Port	Traffic Direction	Description
Service Providers	TCP 8445	Inbound	If you have enabled identity provider introductions, open a port to allow HTTPS communication from the user's browser to the service provider.
	TCP 8446	Inbound	If you have enabled identity provider introductions, open a port to allow HTTPS communication from the user's browser to the service consumer.
Access Gateway	TCP 7801	Inbound	For back-channel communication with cluster members. You must enable the multicast traffic option on this port.
Administration Console	TCP 1443	Inbound	For communication from Administration Console to Access Gateway. This is configurable.
SSH	TCP 22	Inbound	For accessing Administration Console using SSH.
Identity Server	TCP 80 or 443	Inbound	For communication from Identity Server to Access Gateway ESP. This is the reverse proxy port that is assigned to be ESP.
Browsers/Clients	TCP 443	Inbound	For HTTPS communication from workstation browsers to Access Gateway.
	TCP 80	Inbound	For HTTP communication from workstation browsers to Access Gateway.
Upgrade Assistant Agent	TCP 9968	Inbound	For HTTPS communication from Upgrade Assistant agent to Access Gateway on Cloud.

The following syslog ports for Docker are configured for Access Gateway, Administration Console, and Identity Server so they are unique and do not conflict:

Table 1-10 *Syslog Ports on Docker*

Ports for Administration Console	Ports for Access Gateway	Ports for Identity Server
1290	1490	1390
1291	1491	1391
1292	1492	1392

1.8.2 Restricted Ports

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

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

1.8.3.1 Access Gateway and Identity Server in DMZ

First Firewall

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

See, .

Table 1-11 *Ports to Open in the First Firewall*

Port	Purpose
TCP 80	For HTTP communication.
TCP 443	For HTTPS communication.
Any TCP port assigned to a reverse proxy or tunnel.	
TCP 8080	For HTTP communication with Identity Server. For information about redirecting Identity Server to use port 80, see Translating Identity Server Configuration Port.
TCP 8443	For HTTPS communication with Identity Server. For information about redirecting Identity Server to use port 443, see Translating Identity Server Configuration Port.
TCP 8445	For HTTP Identity Provider introductions. If you do not enable Identity Provider introductions, you do not need to open this port.
TCP 8446	For HTTPS Identity Provider introductions. If you do not enable Identity Provider introductions, you do not need to open this port.

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 1-12 *Ports to Open in the Second Firewall*

Port	Purpose
TCP 80	For HTTP communication with web servers.
TCP 443	For HTTPS communication with web servers.
Any TCP connect port assigned to a web server or to a tunnel.	
TCP 1443	For communication from Administration Console to the devices.
TCP 8444	For communication from the devices to Administration Console.
TCP 1290	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.
TCP 524	For NCP certificate management in NPKI. The port needs to be opened so that both the device and Administration Console can use the port.
TCP 636	For secure LDAP communication of configuration information.

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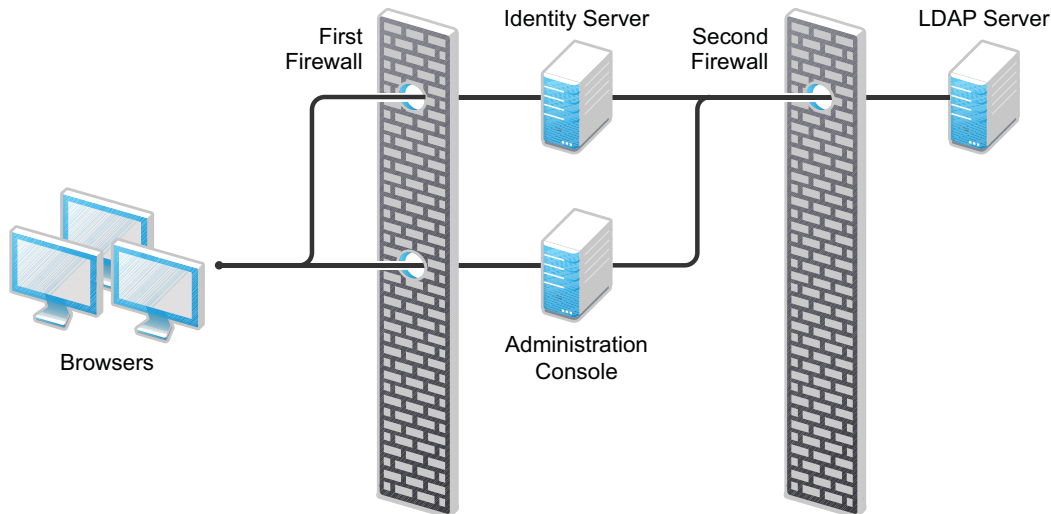
In this configuration, you need to open the following ports in the second firewall for Administration Console and Identity Server:

Table 1-13 *Ports to Open in the Second Firewall*

Ports	Purpose
TCP 636	For secure LDAP communication. This is used by Identity Server and Administration Console.
TCP 524	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, this port does not need to be opened.

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 5.0 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   Identity Servers behind an Access Gateway
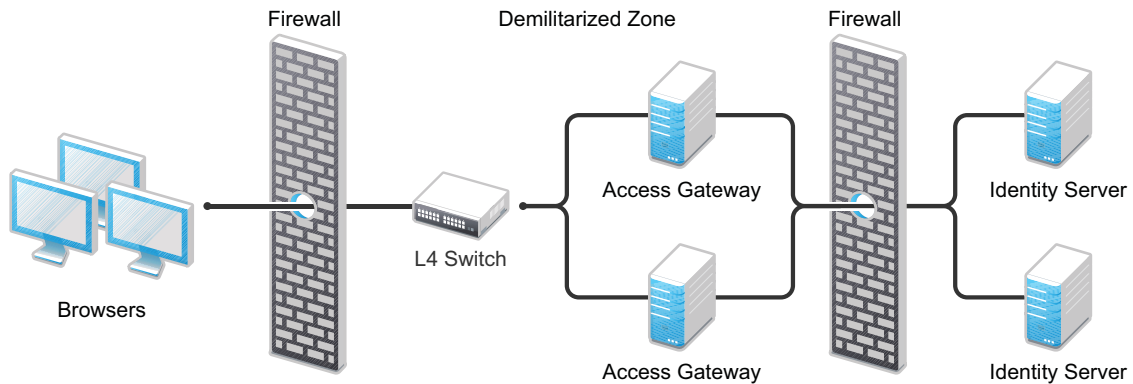
With this configuration, you need an L4 switch to cluster Access Gateways. However, you do not need an L4 switch to cluster Identity Servers. When Identity Server is configured to be a protected resource of Access Gateway, Access Gateway uses its web server communication channel. Each Identity Server 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 NetIQ Access Manager 5.0 Administration Guide.

Installing Access Manager Components on On-Premises Servers

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, see Chapter 1, "Planning Your Access Manager Environment," on page 13.

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:

2 Installing Administration Console

Administration Console must be installed before installing 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.

In this Chapter

- Installing Administration Console
- Logging In to Administration Console
- Enabling Administration Console for Multiple Network Interface Cards

For information about installing a secondary Administration Console and fault tolerance, see Installing Secondary Administration Console in the NetIQ Access Manager 5.0 Administration Guide.

2.1 Installing Administration Console

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.

- Section 2.1.1, "Prerequisites for Installing Administration Console," on page 45
- Section 2.1.2, "Installation Procedure," on page 48
- Section 2.1.3, "Configuring the Administration Console Firewall," on page 49

2.1.1 Prerequisites for Installing Administration Console

❑ Ensure that the system meets the requirements for installing Administration Console.

For information about the requirements, see *NetIQ Access Manager System Requirements*.

❒ If you have custom partitioned your hard disk, ensure to allocate the minimum space for each partition as mentioned in the following table:

Partition	Minimum Disk Space
/opt/novell	1.5 GB
/opt/volera	5 MB
/var/opt/novell	1 GB
/var	512 MB
/usr	25 MB
/etc	10 MB
/tmp/novell_access_manager	50 MB
/tmp	50 MB
/	3 GB

NOTE: These are the minimum free disk spaces that must be available before installation or upgrade. However, it is recommended to maintain more than the specified free disk space based on the requirement of your production environment.

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:

Partition	Disk Space
/opt	5 GB
/var	30 GB
/tmp	2 GB
/	63 GB

❒ (Conditional) For SUSE Linux Enterprise Server (SLES), ensure that the following packages are installed:

Ensure you have installed the following packages a prerequisite:

- `iputils`
- `wget`
- `mozilla-nss-certs`

Package	Description
perl-gettext, gettext-runtime	The required library and tools to create and maintain message catalogs.

Package	Description
python	The basic Python library.
compat	Libraries to address compatibility issues. For information about enabling this repository, see TID 7004701

Use the following command to verify:

`rpm -qa | grep <package name>`

Use YaST to install the packages. |
bind-utils	The package contains utilities (host, dig, and nslookup) used to test and query the Domain Name System (DNS) and also the libraries required for the base 'Bind' package.
rsyslog	The required software for forwarding audit messages.
rsyslog-module-gtls	The required TLS encryption support module for rsyslog.
libXtst6-32bit	Has dependency on iManager

❒ (Conditionally) For manually installing RHEL packages, see Installing Packages and Dependent RPMs on RHEL for Access Manager.

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.

❒ Ensure that 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.

Network Requirements

See Section 1.3, "Network Requirements," on page 20.

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.

What you need to create during installation	A username and password for the Administrator.

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 Prerequisites for Installing Administration Console.

3 Open a terminal window.

4 Access the install script as a `root` user:

    4a Ensure that you have downloaded the software.

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

    4b 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 : (colon) and " (double quotes)
special characters.

---

14 Confirm the password, then wait for the system to install components.

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 Administration Console Firewall" on page 49.

2.1.3   Configuring the 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 For SLES 15 SP3, click **YaST Firewall** > **Trusted** > **Ports** > **Add port** and 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

3 (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 2 and Step 3, 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.

---

4 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
```

5 Continue with Section 2.2, "Logging In to Administration Console," on page 50.

2.2 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 Administration Console Firewall" on page 49.

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**. Analytics Dashboard opens.

   For more information about this view or about configuring Administration Console, see Configuring the Default View in the NetIQ Access Manager 5.0 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 53.
   - If your Administration Console server has multiple interface cards, see "Enabling Administration Console for Multiple Network Interface Cards" on page 52.

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 *NetIQ Access Manager 5.0 Administration Guide*.

2.3 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 Modify Administration Console server.xml.

   For more information about how to modify a file, see "Modifying Configurations" in the *NetIQ Access Manager 5.0 Administration Guide*.

2 Locate the connector with the NIDP_Name="connector" set.

3 Delete the address attribute.

3 Installing Identity Server

Identity Server is the second component you install.

3.1 Prerequisites for Installing Identity Server

- Ensure that the system meets the requirements for installing Identity Server.

  For information about the requirements, see *NetIQ Access Manager System Requirements*.

- When installing Access Manager components on multiple machines, ensure that the time and date are synchronized on all machines.

- Ensure that the hard disk has ample space for logging in a production environment. This disk space must be local and not remote.

- Ensure that Administration Console is running. See Installing Administration Console.

- 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 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 ports, see Configuring the Administration Console Firewall.

NOTE: Install the `insserv-compat` package for SLES installation.

IMPORTANT: When 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.

- 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.

- If you have custom partitioned your hard disk as follows, ensure that the free disk space mentioned against each partition is available:

Partition	Disk Space
/opt/novell	1 GB
/opt/volera	5 MB
/var/opt/novell	1 GB
/var	512 MB
/usr	25 MB
/etc	1 MB
/tmp/novell_access_manager	10 MB
/tmp	10 MB
/	512 MB

NOTE: These are the minimum free disk spaces that must be available before installation or upgrade. However, it is recommended to maintain more than the specified free disk space based on the requirement of your production environment.

- (Conditional) For SLES, ensure that the following packages are installed:
    - rsyslog-module-gtls - The required TLS encryption support module for rsyslog
    - rsyslog - The required software for forwarding audit messages
    - bind-utils - The package contains utilities (host, dig, and nslookup) used to test and query the Domain Name System (DNS) and also the libraries required for the base 'Bind' package
    - glibc-32bit - To install the 32bit glibc libraries on 64 bit Ubuntu
    - iputils - This package contains small network tools for IPv4 and IPv6 like ping, arping, and tracepath
- (Conditional) For installing RHEL packages manually, see *Installing Packages and Dependent RPMs on RHEL for Access Manager*.

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)

IMPORTANT:

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

◆ 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.

For information about browser support, see Browser Support in *NetIQ Access Manager System Requirements*.

For information about network requirements, see Section 1.3, "Network Requirements," on page 20.

3.2 Installing Identity Server

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.

   For software download instructions, see the release-specific Readme.

   3b 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 information about configuring NAT, see Configuring Administration Console Behind NAT.

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.

11 The following components are installed:

Component	Description
Access Manager Server Communication	Enables network communications, including identifying devices, finding services, moving data packets, and maintaining data integrity.
Identity Server	Provides authentication and identity services for the other Access Manager components and third-party service providers.
Identity Server Configuration	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.
Access Manager Server Communications Configuration	Enables Identity Server to auto-import itself into Administration Console.

12 Continue with one of the following actions:

- Verify the installation. See "Verifying Identity Server Installation" on page 56.
- Install Access Gateway. See Section 4.2.2, "Installing Access Gateway Appliance," on page 65 or Section 4.3, "Installing Access Gateway Service," on page 71.
- Configure Identity Server. See Setting Up a Basic Access Manager Configuration in the NetIQ Access Manager 5.0 Administration Guide.

NOTE: After installing Identity Server, you must create a cluster configuration. See Configuring Identity Servers Clusters in the NetIQ Access Manager 5.0 Administration Guide.

3.3   Verifying Identity Server Installation

1 Log in to Administration Console.

See .

2 Click **Devices** > **Identity Servers**.

3.4 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.

The Identity Server service (hosted on Tomcat) runs as a non-privileged user 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 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.
- 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.

For information about iptables, see "Iptable Tutorial 1.2.2" and "NAM Filters for 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.

3.4.1 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 60.

Ensure that you have enabled port forwarding. See "Port Forwarding" on page 57.

Perform the following steps to configure a simple redirect script:

On SLES 12 SP5 or SLES 15 server

1 Click **Devices** > **Identity Server**.

2 Select the Identity Server name and click **Edit**, and configure **Base URL** with HTTPS protocol and Port 443.

3 Click **OK**.

4 Update Identity Server.

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

6 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.

NOTE: Do not create the file in the `/etc/init.d` directory because it may cause some issues. For information about the issues, see 13.3.3 System V Compatibility.

---

7 Copy the following example script and paste it in the file that you created in Step 6 on page 58.

The following is an example of a redirect startup file:

```
#!/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
```

For more information about init scripts for SLES 12, see "Managing Services in a Running System" in the *SLES 12 Administration Guide*.

8 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`.

9 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
```

10 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`.

11 Execute the following commands:

1. `systemctl daemon-reload`

2. `systemctl enable <unit-name>.service`

   For example, `systemctl enable redirect-idp.service`

12 Reboot the Identity Server machine.

13 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.

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

3.4.2 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.

Adding Identity Server Commands

1 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 On Identity Server, edit the `/etc/sysconfig/SuSEfirewall2` file.

    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 .

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.

In this Chapter

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 the Linux 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*

Feature	Access Gateway Appliance	Access Gateway Service
Platform support	SLES 12 SP5	◆ SLES 12 SP5 ◆ SLES 15 SP2 ◆ Red Hat Enterprise Linux 8.2 ◆ Red Hat Enterprise Linux 7.9
Network configuration ◆ DNS servers ◆ Gateways ◆ Network interface cards ◆ Host names	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 > Access Gateways > Select the device > New IP > click OK**.	Configurable with standard operating system utilities.
Date and time	Configurable from Administration Console.	Configurable with standard operating system utilities.
Cache directory	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".	Uses filesystem provided by the Apache mod_cache module. For more information about the Apache model, see "Caching Guide".

4.2 Installing Access Gateway Appliance

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 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 4-2 *Access Gateway Appliance Partitions*

Partition Type	Requirements
root	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.
swap	This partition is twice the size of RAM installed on the machine.
var	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.

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 70.

- Section 4.2.1, "Prerequisites for Installing Access Gateway Appliance," on page 65
- Section 4.2.2, "Installing Access Gateway Appliance," on page 65
- Section 4.2.3, "Configuring Access Gateway Appliance," on page 66

4.2.1 Prerequisites for Installing Access Gateway Appliance

- Ensure that the server meets the minimum hardware requirements. See *NetIQ Access Manager System Requirements*.
- 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.

For information about network requirements, see Section 1.3, "Network Requirements," on page 20.

4.2.2 Installing Access Gateway Appliance

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

What you need to know	- Username and password of the administrator - IP address of Administration Console - Static IP address for Access Gateway - DNS name (host and domain name) for Access Gateway that resolves to the IP address - Subnet mask that corresponds to the IP address for Access Gateway - IP address of your network's default gateway - IP addresses of the DNS servers on your network - IP address or DNS name of an NTP server

IMPORTANT: After Access Gateway Appliance installation, upgrade the Linux kernel to the latest security patch to avoid any security vulnerabilities.

Perform the following steps to install Access Gateway Appliance:

1 Deploy the Access Gateway Appliance OVF template to your enterprise virtual environment.

For more information, see Deploy an OVF Template in the *vSphere Virtual Machine Administration Documentation*.

2 Select the desired language, review the license agreement, then click **Accept**.

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

Field	Description
root Password	Specify the password for `root`.
NTP Server	Specify the name of the primary and secondary NTP server.
Region and Time Zone	Select a region and time zone.

4 Specify the hostname for the Access Gateway Appliance server and click **Next**.

5 Specify the following network setting details:

Field	Description
IP Address	The IP address of Access Gateway.
Network Mask	The subnet mask of Access Gateway Appliance network.
Gateway	The IP address of the default gateway.
DNS Server	The IP address of your DNS server. You must configure at least one DNS server.
	Specify the IP address of your additional DNS server, if you have configured. This is an optional configuration.
Domain Search	Specify the domain name.

6 Click **Next**.

7 Continue with Configuring Access Gateway Appliance.

To add a new hard disk to the virtual machine, see Add a New Hard Disk to a Virtual Machine in the *vSphere Virtual Machine Administration Documentation*.

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.

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.

Perform the following steps to configure 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 67
- Section 4.2.3.2, "Setting Administrative Passwords," on page 70
- Section 4.2.3.3, "Performing an Online Update," on page 70
- Section 4.2.3.4, "Using Additional Hard Disk," on page 70
- Section 4.2.3.5, "Rebooting or Shutting Down the Appliance," on page 71

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 67
- "Using an Existing Certificate and Key Pair" on page 69
- "Activating the Certificate" on page 69

Using the Digital Certificate Tool

- "Creating a New Self-Signed Certificate" on page 68
- "Getting Your Certificate Officially Signed" on page 68

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 68.

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 69.

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 69.

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

See Section 4.2, "Installing Access Gateway Appliance," on page 64.

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`). 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 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

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

- Section 4.3.1, "Prerequisites for Installing Access Gateway Service," on page 71
- Section 4.3.2, "Installation Procedure," on page 73

4.3.1 Prerequisites for Installing Access Gateway Service

❏ Ensure that the system meets the requirements for installing Access Gateway. For information about the requirements, see *NetIQ Access Manager System Requirements*.

❏ An Administration Console is installed. See Installing Administration Console.

❏ An Identity Server is installed and configured. See Installing Identity Server

❏ 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.

❏ (Conditional) For SUSE Linux Enterprise Server (SLES). 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

NOTE: Install the `insserv-compat` package for SLES installation.

> **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`.

❒ (Conditional) For installing the RHEL packages manually, see Appendix 6, "Installing Packages and Dependent RPMs on RHEL for Access Manager," on page 77.

> **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.

❒ 2 to10 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:

Partition	Disk Space
/opt/novell	1 GB
/opt/volera	5 MB
/var/opt/novell	1 GB
/var	512 MB
/usr	25 MB
/etc	1 MB
/tmp/novell_access_manager	10 MB
/tmp	10 MB
/	512 MB

> **NOTE:** These are the minimum free disk spaces that must be available before installation or upgrade. However, it is recommended to maintain more than the specified free disk space based on the requirement of your production environment.

❒ 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 20.

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

4.3.2 Installation Procedure

You must install Access Gateway Service on a separate machine.

Installation time: about 10 minutes.

What you need to know	◆ Username and password of the administrator.
	◆ IP address of Administration Console.

1 Log in to the Micro Focus Customer Center and follow the link that allows you to download software.

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.

9 Continue with one of the following sections:

◆ Verify the installation. See "Verifying Access Gateway Installation" on page 74

◆ Configure Access Gateway. See Configuring Access Gateway in the NetIQ Access Manager 5.0 Administration Guide.

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.

4.4 Verifying Access Gateway Installation

1 Log in to Administration Console.

See Section 2.2, "Logging In to Administration Console," on page 50.

2 Click **Devices** > **Access Gateways**.

If the installation is 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.

This section includes information about how to install the latest Analytics Server. For information about installing the earlier version, see Installing Analytics Server in the NetIQ Access Manager 4.4 Installation and Upgrade Guide.

IMPORTANT: Before installing the new Analytics Server, ensure to delete Analytics Server nodes of the earlier version from Administration Console. Ensure to use only three node cluster for Analytics Server as two node cluster is no longer supported.

Installation time: 10 minutes approximately

What you need to know to install Analytics Server	- Username and password of the Administration Console administrator. - Install Administration Console and Analytics Server on separate servers. - Do not perform any configuration tasks in Administration Console during the installation.

Prerequisites for Installing Analytics Server

❐ Ensure that the system meets the requirements for installing Analytics Server. For information about the requirements, see System Requirements of Analytics Server.

❐ When installing Access Manager components on multiple machines, ensure that the time and date are synchronized on all machines.

❐ Ensure that Administration Console is running.

❐ Install Analytics Server on a separate machine and ensure that the following ports in Analytics Server are open:

- 8445
- 1444
- 22 (Optional)
- 1468
- 9200
- 9300

❐ If you have custom partitioned your hard disk as follows, ensure that the free disk space mentioned against each partition is available.

Partition	Disk Space
/opt	2 GB
/var	3 GB

❐ Edit the /etc/hosts files on each instance and add an entry to resolve its hostname to its private IP address. For example, *10.10.10.11   kubew1*

NOTE: Install the `insserv-compat` package for SLES installation.

To Install Analytics Server

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.

   3b If you downloaded the `tar.gz` file, unzip the file by using the following command:

   `tar -xzvf <filename>`

   3c Change to the `Analytics_Dashboard` directory.

4 At the command prompt, run the following install script:

   `./ar_install.sh`

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

6 Re-enter the password for verification. Analytics Server installation starts.

   If the installation program rejects credentials and IP address, ensure that the required ports are open on both Administration Console and Analytics Server.

7 Verify the installation. You can check the logs in `/tmp/novell_access_manager/ install_ar_`.

Analytics Server Cluster Configuration

You can configure Analytics Server cluster for high availability. For a cluster, you can install Analytics Server on three servers in a sequential order one after the other, using the `tar.gz` file.

NOTE: It is highly recommended to take snapshots to avoid data loss. For more information, see Snapshot and Restore.

After you install the second node of Analytics Server, perform the following steps in Administration Console:

1 **Devices** > **Analytics Servers** > **[Name of Server]** > **Health**.

2 Click **Refresh**.

Perform the same steps after installing the third node. Update one device at a time from top to down and wait for the Elasticsearch database server's health to turn green and then refresh other servers for the update. The cluster health will be red till the second node is updated.

If the server does not come up, click **Restart** to bring all the services up and running, and then manually click **Refresh** for each service.

After all servers' health turn green, the cluster is ready for use.

NOTE: Analytics Server cluster logs named `as_elasticsearch` cannot be downloaded from Administration Console if you have not configured a cluster setup. The error message "`There were logs that failed to download...Requested resource is unavailable`" appears.

6 Installing Packages and Dependent RPMs on RHEL for Access Manager

IMPORTANT: You do not need to manually install the RPMs listed in Table 6-1 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 6-1.

◆ The version of RPMs varies based on the base operating system version of RHEL. Table 6-1 lists RPMs for RHEL 8.3.

◆ You must install these RPMs in the same sequence as they appear in Table 6-1.

Table 6-1   *RHEL Packages and Dependent RPMs*

Package	Dependent RPM
iManager	
glibc-2.28-127.el8.i686.rpm	◆ nss-softokn-freebl-3.36.0-5.el7_5.i686 This must be installed along with glibc-2.17-260.el7.i686.rpm. To install these rpm files together, run the following: `rpm -ivh glibc-2.28-127.el8.i686.rpm nss-softokn-freebl-3.36.0-5.el7_5.i686.rpm`
libstdc++-8.3.1-5.1.el8x86_64.rpm (Part of the RHEL base installation)	◆ glibc-2.28-127.el8.x86_64.rpm ◆ libgcc-8.3.1-5.el8.x86_64.rpm
libXau-1.0.9-3.el8.x86_64.rpm	◆ glibc-2.28-127.el8.i686.rpm
libxcb-1.13-1.el8.x86_64.rpm	◆ glibc-2.28-127.el8.i686.rpm ◆ libXau-1.0.9-3.el8.x86_64.rpm
libX11-1.6.8-3.el8.x86_64.rpm	◆ glibc-2.28-127.el8.i686.rpm ◆ libXau-1.0.9-3.el8.x86_64.rpm

Package	Dependent RPM
libXext-1.3.4-1.el8.x86_64.rpm	• libX11-1.6.8-3.el8.x86_64.rpm • glibc-2.28-127.el8.i686.rpm
libXi-1.7.10-1.el8.x86_64.rpm	• libX11-1.6.8-3.el8.x86_64.rpm • libXext-1.3.3-9.el8.x86_64.rpm • glibc-2.28-127.el8.i686.rpm
libXtst-1.2.3-7.el8.x86_64.rpm	• libX11-1.6.5-2.el7.x86_64.rpm • libX11-1.6.8-3.el8.x86_64.rpm • libXext-1.3.3-9.el8.x86_64.rpm • libXi-1.7.10-1.el8.x86_64.rpm • libXext-1.3.3-9.el8.x86_64.rpm • glibc-2.28-127.el8.i686.rpm
libxcb-1.13.1-1.el8.x86_64.rpm	• libXau-1.0.9-3.el8.x86_64.rpm
libX11-1.6.8-3.e18.x86_64.rpm	• libxcb-1.13.1-1.el8.x86_64.rpm
libXrender-0.9.10-7.el8.x86_64.rpm	• No dependency
Administration Console	
gettext-0.19.8.1-17.el8.x86_64	• No dependency
glibc-2.28-127.el8.i686.rpm	• nss-softokn-3.44.0-15.el8.x86_64.rpm
libstdc++-8.3.1-5.1.el8.i686.rpm	• glibc-2.28-127.el8.i686.rpm • libgcc-8.3.1-5.el8.i686.rpm
ncurses-libs-6.1-7.20180224.el8.i686.rpm	• glibc-2.28-127.el8.i686.rpm
libgcc-8.3.1-5.1.el8.i686.rpm	• No dependency
rsyslog-8.1911.0-6.el8.x86_64	• No dependency
rsyslog-gnutls-8.1911.0-6.el8.x86_64	• No dependency
binutils-2.30-79.base.el8.x86_64	• No dependency
Identity Server	
glibc-2.28-127.el8.i686.rpm	• nss-softokn-3.44.0-15.el8.x86_64
libstdc++-4.8.5-36.el7.i686	• glibc-2.28-127.el8.i686.rpm • libgcc-8.3.1-5.el8.i686.rpm
ncurses-libs-6.1-7.20180224.el8_4.i686.rpm	• glibc-2.28-127.el8.i686.rpm
libgcc-8.3.1-5.el8.i686.rpm	• No dependency
rsyslog-8.1911.0-3.el8.x86_64	• No dependency
rsyslog-gnutls-8.1911.0-3.el8.x86_64	• No dependency
binutils-2.30-79.base.el8.x86_64	• No dependency

Package	Dependent RPM
Access Gateway	
glibc-2.28-127.el8.i686.rpm	• nss-softokn-freebl-3.44.0-15.el8.i686
apr-1.6.3-11.el8.x86_64.rpm	• glibc-2.28-127.el8.i686.x86_64.rpm
apr-util-1.6.1-6.el8.x86_64.rpm	• apr-1.6.3-11.el8.x86_64.rpm • glibc-2.28-127.el8.x86_64.rpm
libtool-ltdl-2.4.6-25.el8_3.x86_64.rpm	• glibc-2.28-127.el8.x86_64.rpm
unixODBC-2.3.7-1.el8.x86_64.rpm	• libtool-ltdl-2.4.6-25.el8_3.x86_64.rpm • glibc-2.28-127.el8.x86_64.rpm
rsyslog-8.1911.0-3.el8.x86_64	• No dependency
rsyslog-gnutls-8.1911.0-3.el8.x86_64	• No dependency
binutils-2.30-79.base.el8.x86_64	• No dependency
patch-2.7.6-11.el8.x86_64.rpm	• No dependency

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

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-5.8-14.el8.x86_64.rpm
- net-snmp-5.8-14.el8.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-5.8-14.el8.x86_64.rpm

```
yum install --nogpgcheck net-snmp-5.8-14.el8.x86_64
```

3 After installation, run `/etc/init.d/novell-snmpd start`. This will succeed for a successful installation.

7 Uninstalling Components

7.1 Uninstalling Identity Server

Uninstalling Identity Server is a two-step process:

1. Removing Identity Server from Administration Console. See Deleting Identity Server References.

2. Removing the Identity Server software from the machine. See Uninstalling Identity Server.

7.1.1 Deleting Identity Server References

As part of the complete Identity Server uninstall process, you must delete Identity Server from Administration Console. Identity Server must first be removed from the cluster configuration before deleting from Administration Console.

1 In Administration Console, click **Devices** > **Identity Servers**.

2 Select Identity Server that you want to uninstall and 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 7.1.2, "Uninstalling Identity Server," on page 81.

7.1.2 Uninstalling Identity Server

If you have installed Identity Server with Administration Console, you have to uninstall both and will not be able to uninstall only the Identity Server.

1 Unzip the `tar.gz` file by using the following command:

```
tar -xzvf <filename>
```

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`.

7.2   Reinstalling an Identity Server to a New Hard Drive

If your Identity Server hard drive fails, you must reinstall Identity Server (see Installing Identity Server) 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 53.)

5 On the 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**.

7.3   Uninstalling Access Gateway

1 In Administration Console, click **Access Gateways**.

2 If Access Gateway belongs to a cluster, remove it from the cluster.

    2a Select Access Gateway, then click **Actions** > **Remove from Cluster**:

    2b Confirm the action, then click **OK**.

3 On the 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 NetIQ Access Manager 5.0 Administration Guide.

5 Unzip the `tar.gz` file by using the following command:

`tar -xzvf <filename>`

6 Navigate to the `novell-access-gateway` directory.

7 Enter `./uninstall.sh` to initiate the uninstallation script.

8 Enter the name of the admin user.

9 Enter the password of the admin user.

Uninstall removes Access Gateway Service. A log file is created at `/tmp/novell_access_manager/uninstall.log`.

7.4   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 NetIQ Access Manager 5.0 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.

Uninstalling Administration Console

1 Unzip the `tar.gz` file by using the following command:

`tar -xzvf <filename>`

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`.

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**.

7.4.1 Restoring a Failed Secondary Console

If a secondary console fails, you need to remove its configuration from the primary console before installing a new secondary console. If the failed console is part of the configuration, other Access Manager devices try to contact it.

1 On the primary console, click **Troubleshooting**.

2 In **Other Known Device Manager Servers**, click **Remove** next to the failed secondary console.

3 Remove traces of the secondary console from the configuration datastore:

   3a In the Access Manager menu bar, select **View Objects**.

   3b In the Tree view, select **novell**.

   3c Delete all objects that reference the failed secondary console.

      You should find the following types of objects:

- SAS Service object with the hostname of the secondary console
- An object that starts with the last octet of the IP address of the secondary console
- DNS AG object with the hostname of the secondary console
- DNS IP object with the hostname of the secondary console
- SSL CertificateDNS with the hostname of the secondary console
- SSL CertificateIP with the hostname of the secondary console

4 Install a new secondary console. See Installing Secondary Administration Console in the NetIQ Access Manager 5.0 Administration Guide.

7.5 Uninstalling Analytics Server Service

NOTE: Before uninstalling Analytics Server Service, ensure that you have uninstalled all the plug-ins.

For more information about how to uninstall NetIQ SecureLogin plug-ins, refer Uninstalling Analytics Dashboard Plug-in in the SecureLogin 9.0 Installation Guide.

For more information about how to uninstall SAPIM plug-ins, refer Configure Analytics in the NetIQ Secure API Manager 2.1 Administration Guide.

To uninstall the Analytics Server service, perform the following steps:

1 Navigate to the `/opt/novell/nam/scripts` directory.

2 Enter `./uninstall.sh` to initiate the uninstallation script.

3 For the uninstall confirmation, **This will Uninstall Analytics Server.Would you like to continue (y/ n) ?**

   Enter **y**

4 Enter the name and password of the admin user.

   Uninstall removes Analytics Server. A log file is created at `/tmp/novell_access_manager/ uninstall.log`.

7.6 Uninstalling Access Manager Containers

To uninstall the Access Manager containers, perform the following steps:

1 Navigate to the `access-manager` directory.

2 Run command `sh uninstall.sh release=<release-name> namespace=<name-of- the-namespace>`

3 Make sure that all the pods are terminated. You can check the pod status by running the following command:

   `kubectl get pods --namespace <name-of-the-namespace>`

NOTE: Uninstalling Access Manager does not delete the persisted directories (`am-edir`, `am-ac`, `am-idp`, and `am-ag`) that got created during installation. If you do not need the directories for future use, you must delete them manually from the node.

Use command `rm -rf <location>/am-*`.

For example, to delete the `am-ac` directory, use command `rm -rf /mnt/am-ac`, where `/mnt` is the location of the directory.

7.7 Uninstalling the Analytics Server Containers

1 Navigate to the `analytics-dashboard` directory.

2 Run command `sh uninstall.sh release=<release-name> namespace=<name-of- the-namespace>`

3 Make sure that all the pods are terminated. You can check the pods status by running the following command:

```
kubectl get pods --namespace <name-of-the-namespace>
```

NOTE: Uninstalling Analytics Server does not delete the persisted directories that got created during installation. If you do not need the directories for future use, you must delete them manually from the node.

Use command `rm -rf <location>/am-*`.

For example, to delete the `am-dashboard` directory, use command `rm -rf /mnt/am-dashboard`, where `/mnt` is the location of the directory.

NOTE: On multiple nodes, ensure all the folders located at `/mnt/am-dashboard` are deleted on all nodes before you re-install the application.

II Installing Access Manager Components on Cloud

This section includes the following topics:

8 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 is not supported on Azure.

For more information about the operating systems supported by Access Manager on Azure, see NetIQ Access Manager System Requirements.

This section includes the following topics:

8.1 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>`.

8.2 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 23 illustrates the recommended way for deploying Access Manager on Azure.

8.2.1 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 **Create a resource**.

  2b Search for `resource group` and select **Resource group**.

  2c Click **Create**.

For more information about resource groups, see Azure Resource Manager Overview > Terminology > resource group (https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-overview).

NOTE: All administrators may not 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 **Create a resource**.

  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`.

> **NOTE:** Keep the default values as is in other fields.

    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 .

8.2.2 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 SP5 or Red Hat Enterprise Linux 8.3 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. For more information about creating a Windows virtual machine, see Quickstart: Create a Windows virtual machine in the Azure portal (https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal).

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 SP5 has been selected here as an example configuration.

4 Select **SLES 12 SP5**.

5 Click **Create**.

6 Configure the following settings in step **1 Basics**:

Field	Description
Name	Specify a name for the virtual machine.
VM disk type	Select **SSD** or **HDD** based on your requirements.
	This selection affects the list of templates displayed for selection in Step 8.
User name	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.
Authentication type	Select **SSH public key**.
SSH public key	Copy the content of your `id_rsa.pub` file that you have generated earlier, and paste it.
Subscription	Select the Azure subscription that should be used for the virtual machine.
Resource group	Select the resource group that you have created or determined in Step 2.
Location	Select from the list of the supported Azure location where you want to create the virtual machine.

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.

Section	Action
High Availability	While deploying a virtual machine for identity Server or Access Gateway, select the appropriate availability set that was created for each type in Step 3.
	For clustering and load balancing, place Identity Server virtual machines in one availability set and Access Gateway virtual machines in a different availability set.

Section	Action
Storage	keep the default value `Yes` for **Use managed disks**.
Network > **Virtual network**	Click **Virtual network** and select the virtual network that you created in Step 4.
Network > **Public IP Address** (Optional)	Configure the **Public IP Address** for this virtual machine or you can keep the default selection (dynamic addressing). If you do not specify a static address (adds an additional cost), the external IP address used to reach each virtual machine changes with each reboot.
Network > **Network Security Group (firewall)**	Accept the default network security group to allow incoming SSH access requests to the virtual machine used for Access Manager. The instructions to further configure these security groups are in a later section of the guide. In an advanced setup where you install multiple Administration Consoles, Identity Servers, and Access Gateways, these virtual machines should use the security group created for the first virtual machine running that component type.
Extension	Keep the default value.
Auto-shutdown	By default, this is set to `Off`. It is recommended to not set this option to on in a production environment. Enabling this option might result in a corrupted Access Manager setup. If it is necessary to enable **Auto Shutdown**, the system admin must set up a cron job to run several minutes prior to the shutdown time specified on the affected virtual machines. The cron script must be placed in the root user's crontab and it must execute the following commands: 1. `/etc/init.d/novell-idp stop` (on the virtual machine containing Identity Server) 2. `/etc/init.d/novell-ac stop` (on the virtual machine containing Administration Console) This script shuts down Access Manager safely prior to the Azure Auto-Shutdown happens. **IMPORTANT:** Before you manually shut down an Azure virtual machine containing an Access Manager installation, first run the `/etc/init.d/novell-[ac|idp] stop` command. This ensure that the Access Manager instance is in a safe state.
Monitoring	Disable **Boot diagnostics** and **Guest OS diagnostics** if you do not want to monitor for those options. You can change these settings later if you need these functionalities.

11 Click **OK**.

12 In **4 Summary**, review the summary of settings, terms of use, privacy policies, and cost of use.

13 Click **Create**.

Azure begins provisioning the virtual machine as you have configured it. This process may take a few minutes.

14 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 92 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.

16 Continue with Section 8.2.3, "Configuring Network Security Groups," on page 94.

8.2.3 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 36, and Table 1-9, "Access Gateway on Cloud," on page 37.

1 In the Azure portal, click **All resources**.

You can filter the list can using the fields at the top of the page.

2 Find and click the desired network security group created in Step 10 on page 92.

3 Click **Inbound security rules** > **Add**.

4 Specify details in fields.

The following is an example configuration:

Field	Value
Source	Any
Source port range	*
Destination	Any
Destination port range	8443
Protocol	TCP
Action	Allow
Priority	100
Name	Administration Console HTTPS

Field	Value
Description	HTTPS port for Access Manager Administration Console.

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 36, 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 Changing the Private IP Address from Dynamic to Static.

8.2.4 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**.

8.2.5 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.

See Section 8.2.3, "Configuring Network Security Groups," on page 94.

❒ Before starting Access Manager installations, ensure that the additional packages listed in the prerequisites sections of each Access Manager component are added.

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 259.

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 Installing Administration Console, Installing Identity Server, and Installing Access Gateway.

   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 *NetIQ Access Manager 5.0 Administration Guide*.

8.3 (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 100.

NOTE: For scaling recommendations, see Recommendations for Scaling Access Manager Components in Public Cloud.

- Section 8.3.1, "Creating a Load Balancer," on page 97
- Section 8.3.2, "Configuring a Load Balancer," on page 98

8.3.1 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:

Field	Description
Name	Specify a name for the load balancer.
Type	Select Public.
Public IP address	Create a new public IP address for this load balancer. 1. Click **>**. 2. Click **Create new**. 3. Specify a name. 4. Select **Static**. 5. Click **OK**.
Subscription	Select the same Azure subscription that you have selected for virtual machines on which Access Manager is installed.
Resource group	Select the same resource group that you have selected for virtual machines on which Access Manager is installed.
Location	Select the same location that you have used for virtual machines.

4 Click **Create**.

5 Continue with "Configuring a Load Balancer" on page 98.

8.3.2　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:

Field	Description
Protocol	Select **HTTP**.
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. **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.
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:

Field	Description
Name	Specify a name for the rule.
IP Version	Select **IPv4**.
Frontend IP address	Select the frontend IP address for this rule.

Field	Description
Protocol	Select **TCP**.

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.

Field	Description
Port	For Access Gateway, specify the following values: ◆ For HTTPS traffic, specify `443`. ◆ For HTTP traffic, specify `80`. For an Identity Server listening on the default ports of 8080/8443, specify the following values: ◆ For HTTPS traffic, specify `8443`. ◆ For HTTP traffic, specify `8080`.
Backend port	For Access Gateway, specify the following values: ◆ For HTTPS traffic, specify `443`. ◆ For HTTP traffic, specify `80`. For an Identity Server listening on the default ports of 8080/8443, specify the following values: ◆ For HTTPS traffic, specify `8443`. ◆ For HTTP traffic, specify `8080`.
Backend pool	Select the backend pool for this rule.
Health probe	Select the health probe for this rule.
Session persistence	Keep the default value.
Idle timeout	Keep the default value.
Floating IP (direct server return)	Keep the default value.

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:

1 Click **Devices** > **Access Gateways** > **Edit** > **Reverse Proxy / Authentication**.

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	Description
Proxy Service Name	Specify a name that identifies the purpose of this proxy service.
Published DNS Name	Specify a value, such as HealthProbe. A value is required, however it is not used for connection purposes.
Web Server IP Address	Specify `127.0.0.1`.
Host Header	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.

9 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 is not supported on AWS EC2.

For more information about the operating systems supported by Access Manager on Azure, see NetIQ Access Manager System Requirements.

This section includes the following topics:

- Prerequisites for Deploying Access Manager on AWS
- Deployment Procedure
- Auto Scaling Access Manager on AWS
- Monitoring Access Manager in AWS Using CloudWatch
- Deploying Access Manager in Multiple AWS Regions

9.1 Prerequisites for 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.

For Access Manager system requirements, see *NetIQ Access Manager System Requirements*.

9.2 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

For information about the recommended way for deploying Access Manager on AWS EC2, see Figure 1-7.

IMPORTANT: The LDAP server and web services must be deployed in the public cloud 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.

9.2.1 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:

Service	Steps
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.
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.

Service	Steps
Internet gateways	1. In the left menu, click **Internet Gateways**. 2. Locate the Internet gateways associated with this VPC. 3. Select the Internet gateways, verify the details, and edit if required.
Route table	1. In the left menu, click **Route Tables**. 2. Select the route table that was automatically created for this VPC. 3. In the **Routes** tab, click **Edit**. 4. Click **Add another route**. 5. In **Destination**, specify `0.0.0.0/0`. 6. In **Target**, select the IGW table that has been created in **Internet gateways**. 7. Click **Save**.

3 Continue with .

9.2.2 Creating and Deploying Instances

This section outlines steps to create and deploy instances for a basic setup of Access Manager. A basic setup 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 SP5` or `RHEL 8.3` 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 (SLES or RHEL).

4 Select the instance type that meets requirements of the base operating system and deployment of Access Manager components. See *NetIQ Access Manager System Requirements*.

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

5 Click **Next: Configure Instance Details**.

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

Field	Action
Auto-assign Public IP	Set to `Enable`.
Network Interfaces	Specify a static IP address in **Primary IP**.

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.

For more information, see Amazon EC2 Security Groups for Linux Instances (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html).

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, and Table 1-9.

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 106.

9.2.3 Installing Access Manager

Prerequisites

❒ Ensure that you meet the requirements listed in Network Requirements.

❒ 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 Creating and Deploying Instances. For the list of ports, see Table 1-7 on page 36, Table 1-8 on page 36, and Table 1-9 on page 37.

❒ Before starting Access Manager installation, ensure that the additional packages listed in the prerequisites 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: Re-importing Identity Server and Access Gateway is not supported.

Installation Procedure

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

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 Installing Administration Console, Installing Identity Server, and Installing Access Gateway Service.

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 *NetIQ Access Manager 5.0 Administration Guide*.

9.2.4 (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.

Repeat the steps in Creating Target Groups, Creating an Elastic IP Address, and Creating a Load Balancer, and create separate target groups, elastic IP addresses, and load balancers for Identity Server and Access Gateway clusters.

9.2.4.1 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, 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:

Field	Description
Target group name	Specify a name for the target group.
Protocol	Select **TCP**.
Port	Specify the port on which the server is configured for listening.
	IMPORTANT: You need to create two separate target groups for each load balancer, one for HTTP and one for HTTPS.
	For Access Gateway
	Specify the following values:
	• If you are creating the target group for the HTTPS traffic, specify 443.
	• If you are creating the target group for the HTTP traffic, specify 80.
	For an Identity Server listening on the default ports of 8080/8443
	Specify the following values:
	• If you are creating the target group for the HTTPS traffic, specify 8443.
	• If you are creating the target group for the HTTP traffic, specify 8080.
	You can use iptables to configure the listeners on Identity Server to use other ports. See Translating Identity Server Configuration Port.
Target type	Select **ip**.
VPC	Select the same VPC that you have selected for the instances of Access Manager components.
Health Check Settings	

Field	Description
Protocol	When creating a target group for the HTTPS protocol, select **HTTPS**.
	When creating a target group for the HTTP protocol, select **HTTP**.
	The load balancer uses this protocol while performing health checks.
Path	Specify the destination path for health checks.
	For Identity Server, specify `/nidp/app/heartbeat`.
	For Access Gateway, specify `/nesp/app/heartbeat`.
Advanced health check settings	Keep the default values.

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.

   6c Specify the following details:

Field	Description
Network	Populated with the VPC that you have selected under **VPC** in Step 3.
IP	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.
Port	Populated with the port value that you have specified for **Port** in Step 3.

   6d Click **Add to list**.

   6e Click **Register**.

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

9.2.4.2 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**.

9.2.4.3 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:

Field	Description
Name	Specify a name for the load balancer.
Scheme	Select **internet-facing**.
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 109.
Tags	Do not make any change.

5 Click **Next: Configure Routing**.

6 Under **Target group**, specify the following details:

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

7 Under **Health Checks**, review the following details:

Field	Description
Protocol	Populated with **HTTPS** or **HTTP** based on the configuration of the target group you selected in Step 6. See "Creating Target Groups" on page 108.
Path	Populated with the health URL that you configured in the target group selected in Step 6. See "Creating Target Groups" on page 108.
Advanced health check settings	Keep the default values.

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 Recommendations for Scaling Access Manager Components in Public Cloud.

9.3 Auto Scaling Access Manager on AWS

AWS 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.

Benefits

- Detects a non-responding instance, terminates it, and replaces it with a new one.
- Adds instances only when needed and scales 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/).

For more information about deploying Access Manager auto scaling on AWS, see Sample Auto Scaling Deployment of Access Manager on AWS (https://www.microfocus.com/documentation/access-manager/developer-documentation-5.0/aws-autoscaling/aws-autoscaling.html).

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

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

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

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

9.4 Monitoring Access Manager in AWS Using CloudWatch

Amazon CloudWatch provides real-time monitoring of 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 Access Manager instances and AWS resources. It includes AWS servers and on-premises servers.

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

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

For more information about 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 server and run the following commands:

   ◆ `curl -O https://bootstrap.pypa.io/get-pip.py` (to download the `get-pip.py` installer package)

   ◆ `pip install --upgrade awscli` (to install AWS CLI)

   For 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 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 AWS IAM credentials and AWS Region by 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 information about using this 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 through the 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 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 by 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:

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

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

For information about installing 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, such as 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).

9.5 Deploying Access Manager in Multiple AWS Regions

You can deploy Access Manager components across different AWS regions. You can use Amazon Virtual Private Cloud (VPC) peering service to communicate among Access Manager components and AWS resources deployed in different VPCs in different AWS regions. Deploying Access Manager across different AWS regions provides the following benefits:

- **High Availability**: Deploying Access Manager components in multiple regions ensures availability even when a region is unavailable.

- **Reduced Latency**: Deploying Access Manager components in a region where majority of users reside reduces the latency.

- **Compliance Requirements**: Some regions require local data hosting. Deploying Access Manager components in a region allows you to adhere to regional compliance requirements.

The following diagram illustrates the recommended Access Manager deployment in a multiple AWS regions:

Figure 9-1   *Deployment of Access Manager in Multi-Region AWS*
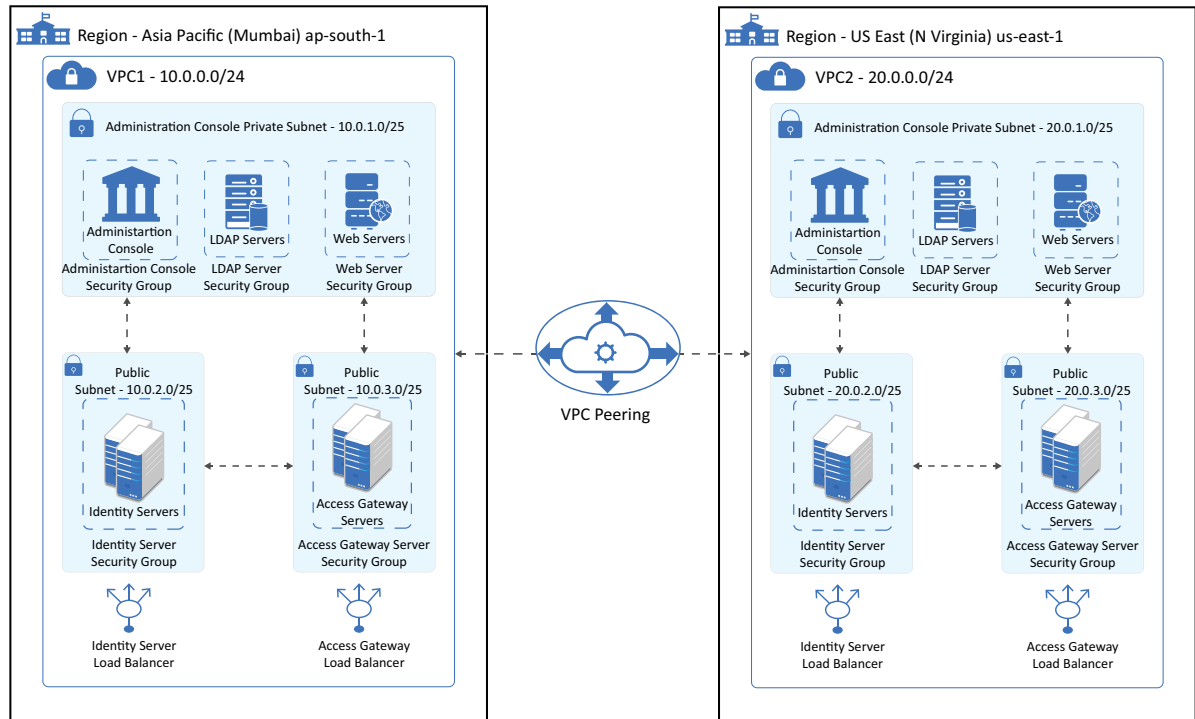
You can deploy the following components in a multi-region environment:

- Administration Console
- Identity Server
- Access Gateway
- LDAP user store
- Web servers

NOTE: You can deploy all Access Manager components in different regions. However, you must determine the need of this solution in before you deploy this solution.

Use the following AWS services to allow communication among Access Manager components:

- **Route 53:** Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service. It provides features such as domain name resolution, latency based routing, Geo DNS, Amazon ELB integration, and DNS Failover. These services help you to enable the multi region deployment of Access Manager components and resources.

  For more information, see Amazon Route 53 (https://aws.amazon.com/route53/).

◆ **VPC Peering:** Access Manager components are deployed in AWS VPCs. These VPCs are local to specific regions. To enable communication across VPCs available in multiple regions, VPC Peering is required between two VPCs from two different regions.

For more information about VPC peering and how to configure it, see What is VPC peering (https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html).

Limitation

Auto scaling Access Manager on AWS is not supported in a multi-region deployment environment. For information about auto scaling of Access Manager, see Auto Scaling Access Manager on AWS.

III Installing Access Manager Containers

Access Manager provides the flexibility of deploying Access Manager Components through a containerized mechanism. Access Manager uses Kubernetes for managing Docker containers. Access Manager components are delivered as Docker images. Access Manager Docker images can be deployed on Kubernetes clusters configured on your on-premises servers or cloud.

NOTE: This release supports deploying Access Manager containers only on Kubernetes. The Kubernetes cluster must be deployed in Linux, AWS, or Azure platforms.

This section includes the following topic:

- Chapter 10, "Planning Access Manager Container Deployment," on page 119
- Chapter 11, "Deploying Access Manager on On-Premises Linux Servers," on page 131
- Chapter 12, "Deploying Access Manager Containers on AWS," on page 141
- Chapter 13, "Deploying Access Manager Containers on Azure Kubernetes Services," on page 151
- Chapter 14, "Scaling Access Manager Components," on page 161

IMPORTANT: For the troubleshooting information, see Troubleshooting Access Manager Container Deployment.

10 Planning Access Manager Container Deployment

10.1 What Is Docker and Why Should You Use It

Docker is a tool that uses OS-level virtualization to deliver software in packages called containers. Containers make it easy to create, deploy, and run applications. Containers are isolated from one another and bundle their software, libraries, and configuration files. They can communicate with each other through well-defined channels.

Docker benefits system administrators as it provides flexibility and reduces the number of systems needed because of its small footprint and lower overhead. Access Manager containers can be deployed quickly on your on-premises Kubernetes or Kubernetes services provided by AWS and Azure, thereby reducing downtime. Access Manager containers are also highly scalable to meet your requirements.

Kubernetes is a container orchestration engine for Docker. Access Manager is deployed on Kubernetes clusters to automate the manual processes of deploying and managing Access Manager containers.

Figure 10-1 Access Manager Deployment on Kubernetes Cluster
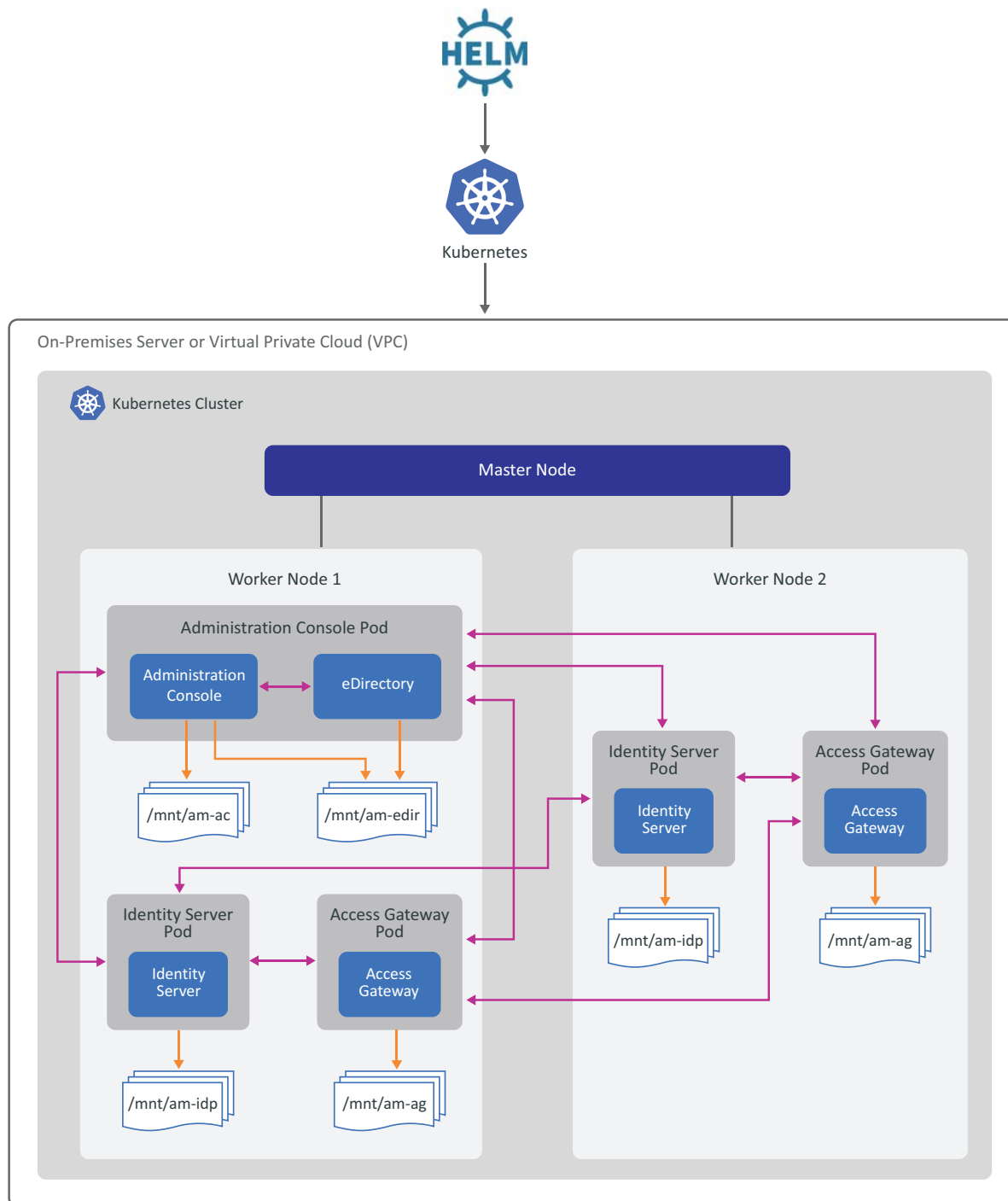
Advantages of Docker

Enterprise software built as Docker containers is easier to assemble and maintain. Some of the parameters that Docker containers enable are:

- Isolation
- Portability

- Composability
- Orchestration and Scaling

Isolation: Docker container isolates the applications from one another, and also from the primary system. This makes the software stack clean, and it becomes easier to monitor an application's usage of system resources, such as CPU, memory, and networking.

Portability: Docker containers can run on any system that supports the container's runtime environment. Access Manager containers can be moved from an on-premises system to a cloud environment easily.

Composability: Access Manager contains many components, Docker makes it possible to compose these components into a functional unit. Each component can be part of different containers, which can be maintained, updated, and swapped independently.

Orchestration and Scaling: You can deploy many Access Manager containers on a single system as the containers are lightweight. You can also have multiple systems with containers. Containers can also be used to scale Access Manager components across clusters of systems when required.

10.2 Basic Terminologies of Kubernetes

10.2.1 Kubernetes Keywords and Their Usage in Access Manager

The following table includes the basic terminologies that are used in the proceeding sections.

Term	Description
Container	An executable image that contains the Access Manager components (Administration Console, Identity Server, or Access Gateway) and all of its dependencies.
Pod	A pod consists of a set of running Access Manager containers that share the same networking and storage resources.
Worker Node or Node	A worker node is a virtual or physical machine where the Access Manager pods run.
Master Node	The master node controls and manages the worker nodes.
Kubernetes Cluster	A set of master and worker nodes to run the Access Manager pods.
Kubelet	An agent that runs on each node in the cluster to ensure that the containers are running in a pod.
Kube-scheduler	Scheduling means assigning a pod to a node. Kube-scheduler is the default Kubernetes scheduler that finds and assigns the optimal node for every newly created pod. It also assigns node for any other unscheduled pod. Kubelet runs the pods in a node. For more information, see Kubernetes Scheduler.
Namespace	A virtual Kubernetes cluster. For more information, see Namespaces.
Release	An instance of a chart that is running in a Kubernetes cluster. You can install the same chart multiple times to create many releases.

Term	Description
Ingress	Ingress manages the external access to the Access Manager services in a Kubernetes cluster. For more information, see Ingress.
Ingress Controller	Ingress controller makes the Ingress resources to work. For more information, see Ingress Controllers.
IngressClassName	From Access Manager 5.0 Service Pack 2 onwards this additional attribute can be used to configure the ingress controller provider.

10.2.2 Helm Charts

Helm is a package manager for Kubernetes. The Helm packaging format is called Charts or Helm Charts. Using Helm, you can deploy, configure, and upgrade Access Manager components on Kubernetes clusters. Helm provides this functionality through a command-line tool called `Kubectl`.

The Access Manager Helm chart defines several Kubernetes resources as a set. The default Access Manager chart contains a minimum of a deployment template and a service template. This reduces the number of Kubernetes commands that you need to run to create and configure resources.

The following table describes the files and directories of Helm:

File or Directory	Description
Helm Charts or Charts	A collection of YAML template files that describe the Kubernetes resources.
Chart.yaml	A YAML file that contains general information about the Access Manager chart such as chart name and version, version number, and search keywords.
values.yaml	A YAML file that contains the default Access Manager configuration values for the chart. As per your requirement, modify this file before installing Access Manager. See Configuring Ingress to configure the Ingress rules. **NOTE:** Do not modify any other configuration file.
charts/	This directory that contains the charts of Access Manager components.
templates/	This directory that contains the following template files that are combined with configuration values and rendered into Kubernetes manifests: ◆ _am-templates.tpl ◆ _helpers.tpl ◆ image-secret.yml ◆ ingress-http-rule.yml ◆ ingress-https-rule.yml ◆ NOTES.txt

File or Directory	Description
templates/NOTES.txt	A text file which prints to a user's terminal when the user installs the chart. This file contains the following post-installation information:

     ◆ Command to check the status of the components.

     ◆ Command to retrieve the Administration Console URL.

     ◆ Administration Console Service URL.

     ◆ Identity Server Service URL.

     ◆ Access Gateway Service URL.

     NOTE: The service URLs of Administration Console, Identity Server, and Access Gateway will be displayed when Ingress is enabled.

To check the version of the Helm client installed on your machine, run command `helm version`.

To view the Kubernetes version running on the client and server, run command `kubectl version`.

For more information about Helm and Helm Charts, see Helm (https://helm.sh/) and Kubernetes. (https://kubernetes.io/releases/)

10.2.2.1 Helm Upgrade

Access Manager 5.0 Service Pack 1 supports Helm chart version 1.0.1. You can check the version of the Helm client installed on your machine, by using the command `helm version` and then update to this version using the command `helm upgrade`. For more information, see Helm Version. (https://helm.sh/docs/topics/version_skew/)

10.3 Planning your Access Manager Deployment on Kubernetes

10.3.1 Deployment Considerations

A few important points to understand to deploy Access Manager:

◆ The Kubernetes cluster should contain one Master node and at least one Worker node.

◆ Each worker node can run only one replica of an Access Manager component. However, two different components can run in the same node.

    For example, two instances of Administration Console, Identity Server, or Access Gateway cannot run in the same node. An instance of Administration Console and another of Identity Server can run in the same node.

- If the number of users or your requirement of resource usage is low, it is possible to run all the components in a single worker node.

- In a node, the port used by one container cannot be used by another container because Access Manager uses host networking.

- To scale up, you must increase the number of worker nodes. For example, to run three instances of Identity Server, you must have three worker nodes.

- Ensure that the system meets the requirements for installing Access Manager containers. See System Requirements of Administration Console, Identity Server, Access Gateway Containers.

The following table lists the maximum number of Access Manager pods that can be deployed on a given number of worker nodes:

Number of Worker Nodes	Administration Console Pod	Identity Server Pod	Access Gateway Pod
1	1	1	1
2	1	2	2
3	1	3	3

NOTE: As you increase the number of worker nodes, you can increase Identity Server and Access Gateway to that many instances.

Memory Allocation of Pods

The default resource memory limit of Access Manager pods are as follows:

Pod	Default Memory
eDirectory	1 Gi
Administration Console	2 Gi
Identity Server	2 Gi
Access Gateway	2 Gi

However, based on your need, you might need to allocate more memory to Tomcat as per the performance sizing recommendations for a production environment.

To determine the JAVA memory that you should allocate for Identity Server, see JAVA Memory Allocations, and for Access Gateway, see JAVA Memory Allocations.

To increase the pods' memory, replace the respective values in the `access-manager/values.yaml` file.

IMPORTANT: You must update the memory values before running the Access Manager helm chart.

Docker containers usually have a default list of Linux capabilities enabled. You must ensure to keep only the following capabilities enabled for Primary Administration Console, secondary Administration Console, Identity Server, Access Gateway, and eDirectory containers and do not use the others:

- ◆ CHOWN
- ◆ FOWNER
- ◆ SYS_CHROOT
- ◆ DAC_OVERRIDE
- ◆ SETGID
- ◆ SETUID
- ◆ NET_BIND_SERVICE
- ◆ AUDIT_WRITE

Adding Privileges for Access Manager Docker

To add any extra privileges:

1 Navigate to the `access-manager/templates/_am-templates.tpl` file.

2 Add or Drop privileges as relevant in the following format:

```
{{/******  Spec for capabilities required by Access Manager  ****/}}
{{- define "access-manager.capabilities" -}}
capabilities:
  drop:
  - all
  add:
  - CHOWN
  - KILL
  - FOWNER
  - DAC_OVERRIDE
  - SETGID
  - SETUID
  - AUDIT_WRITE
  - NET_BIND_SERVICE
{{- end }}
```

Similarly, for Analytics Dashboard you can add extra privileges in the section in file named `_am-templates.tpl`. After you add, helm install can be done (for fresh install) or helm upgrade (if already installed)

3 Enter the `helm install` (if installing for the first time) or `helm upgrade` (if you are upgrading) command as applicable.

10.3.2 Protecting Access Manager Secrets

By default, Kubernetes does not hide the secrets while encrypting, managing, and sharing secrets across a Kubernetes cluster, if the secrets are decoded with Base64. Therefore, Access Manager Secrets could be visible.

You can protect the Access Manager Secrets by performing one or all of the following options:

* Encrypt secret data at rest. For more information, see Encrypting Secret Data at Rest.
* Enable SSL for `etcd` communication. For more information, see PKI certificates.
* Add authorization policies. For more information, see Authorization Overview.

10.3.3 Conditions for Creating Administrator Username and Password

Access Manager administrator username and password must conform to the following conditions:

* The username and password must begin with an alphanumeric character or _ (underscore).
* The last character must not contain any special character.
* The username must not contain # (hash), & (ampersand), and ()(round brackets).
* The password must not contain : (colon) and " (double quotes).

10.3.4 Installing Ingress

Ingress manages the external access to the Access Manager services in a Kubernetes cluster. To make the Ingress resources work, you need an Ingress controller. Configuring Ingress is mandatory while deploying Access Manager on Azure. However, on AWS, if the worker nodes are on public IP, configuring Ingress is optional. Below section shows an example with NginX controller:

Installing the NginX Ingress Controller

1 Add the NginX stable to the master node by using the following command:

```
helm repo add ingress-nginx "https://kubernetes.github.io/ingress-nginx"
```

2 Update the repository:

```
helm repo update
```

3 Install the NginX Ingress Controller:

```
helm install nginx-ingress ingress-nginx/ingress-nginx --set controller.publishService.enabled=true
```

NOTE: An alternative to accessing Administration Console safely without exposing it through Ingress is by deploying a Kubernetes cluster in a private network. Administration Console can only be accessed through a Windows machine which is located in a public subnet.

To configure the Ingress rules, see Section 10.3.5, "Configuring Ingress," on page 127.

10.3.5 Configuring Ingress

Ingress manages the external access to the Access Manager services in a Kubernetes cluster. To make the Ingress resources work, you need an Ingress controller. Configuring Ingress is mandatory while deploying Access Manager on Azure. However, on AWS, if the worker nodes are on public IP, configuring Ingress is optional.

Configuring the Ingress Rules

Configure the Ingress controller chart before running the Access Manager Helm chart.

1 Open the `access-manager/values.yaml` file. Access Manager 5.0 Service Pack 2 onwards, additional attribute ingressClassName can be configured. This attribute is used to configure the ingress controller provider.

2 Enable `ingress` by specifying `enabled: true`.

3 Specify the service ports for the respective components:

Component	Value
Administration Console	2443
Identity Server	8443
Access Gateway	8000 9099 You can specify more port numbers if Access Gateway needs another ports to open.

4 Configure the Administration Console service by specifying the following details:

Element	Value
host	Domain name or Administration Console service URL. For example, `www.cloudac.com`.
https	Specify `true` to enable the backend communication between Ingress and pods.
paths	`:2443/nps`

5 Configure the Identity Server service by specifying the following details:

Element	Value
host	Domain name or Identity Server service URL. For example, `www.cloudidp.com`.
https	Specify `true` to enable the backend communication between Ingress and pods.
paths	`/nidp: 8443`

6 Configure the Access Gateway service by specifying the following details:

Element	Value
host	Domain name or Access Gateway service URL. For example, `www.cloudag.com`.
https	Specify `true` when you want to enable backend communication between Ingress and pods.

paths	`/path1: 8000`
	
	`/path2: 9099`
	
	For example, specify
	
	`/mag: 8000`
	
	`/apache: 9099`

7 Save and close the `values.yaml` file.

8 Create a TLS secret to use with the self-signed certificate. Use the following command:

```
kubectl create secret tls $<cert-name> --key $<KEY_FILE> --cert
$<CERT_FILE>
```

Use this TLS secret when front-end SSL communication is required.

9 Proceed to Deploying Access Manager Containers on Azure Kubernetes Services or Deploying Access Manager Containers on AWS.

NOTE: If you modify any value in the `values.yaml` file of an existing helm release, you must perform a helm upgrade to apply the changes.

Run the following command to perform the helm upgrade:

```
helm upgrade <release-name> access-manager -n <name-of-the-namespace>
```

10.3.6   Limitations of Docker Deployment

 - Installing a tertiary Administration Console is not supported. You can install only primary and secondary Administration Consoles.

 - Customizing the path of the log files is not supported.

 - Combining components (Identity Server, Access Gateway, or Analytics Server) from various platforms is not supported. For example, you cannot use Identity Server deployed on Docker environment with Access Gateway deployed on a non-docker environment.

 - The release name used in one namespace cannot be used in another namespace. In a particular namespace, each cluster must be created as a separate release. The release name is a value that you specify in the Helm install or upgrade command.

 - If the release name contains many characters, the secondary Administration Console pod can go into an error state.

 - If you scale down any pod while upgrading to a new version, the deleted pod's persistent volume does not bind to the pod on performing a rollback.

 - Upgrading the Kubernetes cluster to a later version after installing Access Manager disrupts the Access Manager setup.

- If Administration Console and device pods restart after an unexpected crash and if Administration Console is unable to restart, Identity Server pods, and Access Gateway pods will also be in the waiting state.
- Converting a secondary Administration Console into a primary console is not supported.
- In cloud deployments, such as EKS or AKS, upgrading a Kubernetes cluster is not supported.

11 Deploying Access Manager on On-Premises Linux Servers

You can deploy Access Manager containers on Kubernetes, installed on On-premises Linux servers, using the Helm charts.

- Prerequisites for Deploying Access Manager Containers on On-Premises Linux Servers
- Deploying Access Manager Containers on On-Premises Linux Servers
- Deploying Analytics Server Containers on On-Premises Linux Servers

11.1 Prerequisites for Deploying Access Manager Containers on On-Premises Linux Servers

- ❒ A Kubernetes cluster (v1.19 or later) with Role-Based Access Control enabled.
- ❒ One master node and one worker node (minimum) available in the Kubernetes cluster.

  You can check the status of the nodes by using the following command:

  ```
  kubectl get nodes -o wide
  ```
- ❒ Host entries of the worker nodes added. For example, *10.10.10.11   kubew1*
- ❒ The host entry `127.0.1.1    <hostname>` is removed.
- ❒ The `kubectl` command-line tool is installed on your machine and configured to connect to your cluster.

  You can test your connectivity by using the following command:

  ```
  kubectl cluster-info
  ```
- ❒ Helm 3.*x* is installed.

NOTE: To view the latest Kubernetes version see, Kubernetes version (https://kubernetes.io/releases/). To view the latest Helm version, see Helm version (https://helm.sh/docs/topics/version_skew/).

11.2 Deploying Access Manager Containers on On-Premises Linux Servers

You must have the following details to install Access Manager containers:

— Name of the namespace

— Release name

— IP address of the worker node where you will install Administration Console

— Name of the worker node where you will install Administration Console

Run command `kubectl get nodes -o wide` to view the name, IP address, status, and additional information of the available nodes. You need these details to run the helm install command.

NOTE: In this release, only a fresh installation of Access Manager is supported. You cannot upgrade from a previous version of Access Manager.

Procedure to Install Access Manager:

NOTE: During the installation, Access Manager creates the following directories for data persistence. These directories get created in the corresponding worker node in which you install the particular Access Manager component. The default location of these directories is `/mnt`.

- **eDirectory:** `<release-name>-am-edir`
- **Administration Console:** `<release-name>-am-ac`
- **Identity Server:** `<release-name>-am-idp`
- **Access Gateway:** `<release-name>-am-ag`

NOTE: If you decide not to install all Access Manager components, you can specify the details in the `values.yaml` file before running the helm chart.

For example, if you do not want to install Access Gateway, then specify `enabled: false` under Access Gateway in the `values.yaml` file. In this scenario, only Administration Console and Identity Server will get installed.

Similarly, if you do not want to install Identity Server, then specify `enabled: false` under Identity Server in the `values.yaml` file. In this scenario, only Administration Console and Access Gateway will get installed.

NOTE: If the node contains multiple IP addresses, Kubernetes schedules the Identity Server and Access Gateway pods in the primary IP address. Therefore, you must ensure that the IP address you want to schedule these pods is the primary interface.

1 Create a namespace under which you will deploy Access Manager.

   ```
   kubectl create namespace <name-of-the-namespace>
   ```

   NOTE: Creating a namespace is not mandatory. However, it is recommended to create one to deploy Access Manager. For more information about namespace, see "Kubernetes Keywords and Their Usage in Access Manager" on page 121.

2 Download the Access Manager helm chart (`AM_50_HelmChart-1.0.1.tgz`) to the Master node from Micro Focus Downloads.

3 Unzip the Access Manager helm chart by using the following command:

   ```
   tar -xzvf AM_50_HelmChart-1.0.1.tgz
   ```

4 Run the helm chart by using one of the following approaches:

- Approach 1: Specify the required values in the helm install command and run the command. In this approach, you specify the elements and the values after the `--set` string. The `--set` string overrides any value configured in the `access-manager/values.yaml` file.

- Approach 2: Specify the required values in the `access-manager/values.yaml` file and run the helm install command.

NOTE: Ensure that you execute the helm install command from the location where you have extracted the helm chart, which contains the `access-manager` directory.

Approach 1

Run the following command to install Access Manager:

```
helm install --namespace <name-of-the-namespace> <release-name> access-
manager --set global.amconfig.primaryAcIp=<primary-administration-
console-IP> --set global.amsecret.adminName=<administrator-username> --
set global.amsecret.adminPassword=<administrator-password> --set am-
ac.primary.node=<name-of-the-primary-administration-console-node> --set
am-ac.secondary.enabled=false
```

Drafting a Sample Command

Let us consider that the values of the command's elements are as follows:

Element	Value
Name of the Namespace	development
Release name	my-deployment
	NOTE: You must use the following RegEx, which the Helm package manager enforces while assigning a release name:
	`[a-z0-9]([-a-z0-9]*[a-z0-9])?(\.[a-z0-9]([-a-z0-9]*[a-z0-9])?)*`
Primary Administration Console IP	10.10.10.11
	You can run the `kubectl get nodes -o wide` command to view the IP addresses of the worker nodes, and then choose a node to install Administration Console. You must always install Administration Console in one of the worker nodes, not in the master node.
Name of the Primary Administration Console node	kubew1
	`kubectl get nodes -o wide` command also displays the corresponding name of the node in which you have decided to install Administration Console.
Administrator Username	admin
Administrator Password	password

IMPORTANT: Ensure that the administrator username and password meet the Conditions for Creating Administrator Username and Password.

Then the command will look as follows:

```
helm install --namespace development my-deployment access-manager --set
global.amconfig.primaryAcIp=10.10.10.11 --set
global.amsecret.adminName=admin --set
global.amsecret.adminPassword=password --set am-ac.primary.node=kubew1
--set am-ac.secondary.enabled=false
```

(Optional) To install Secondary Administration Console, change `--set am-ac.secondary.enabled=false` to `true`, and append the following string to the command:

```
--set global.amconfig.secondaryAcIp=<secondary-administration-console-
IP> --set am-ac.secondary.node=<name-of-the-administration-console-
node> --set am-ac.secondary.enabled=true
```

(Optional) If you host the docker images on a separate repository, then append the following string to the command:

```
 --set global.image.repository=<path-of-the-Access-Manager-docker-
images-repository>
```

(Optional) If you use a private registry, then you must also specify the registry's username and password. Append the following string to the command:

```
 --set global.image.pullSecrets.name=<registry-username> --set
global.image.pullSecrets.password=<registry-password>
```

Approach 2

Configure the values and run the helm chart:

1. Open the `access-manager/values.yaml` file.

2. Specify the following details:

Element	Value
repository (Optional)	Path of the Access Manager Docker images
pullPolicy: IfNotPresent (Optional)	If you are using a private registry, then replace `pullPolicy: IfNotPresent` with `pullPolicy: Always`
pullSecrets (Optional)	If you are using a private registry, then specify the registry's username and password
primaryAcIp	IP address of the worker node where you will install primary Administration Console You can run the `kubectl get nodes -o wide` command to view the IP addresses of the worker nodes, and then choose a node to install Administration Console. You must always install Administration Console in one of the worker nodes, not in the master node.

Element	Value
adminName	Administrator Username
adminPassword	Administrator Password
node	Name of the Administration Console worker node The `kubectl get nodes -o wide` command also displays the corresponding name of the node in which you have decided to install Administration Console.

IMPORTANT: Ensure that the administrator username and password meet the Conditions for Creating Administrator Username and Password.

NOTE: To install Secondary Administration Console along with the Primary Administration Console, specify `enabled: true` under Secondary Administration Console.

3. Run the following command to install Access Manager:

```
helm install --namespace <name-of-the-namespace> <release-name>
access-manager
```

NOTE: You must use the following RegEx, which the Helm package manager enforces while assigning a release name:

```
[a-z0-9]([-a-z0-9]*[a-z0-9])?(\.[a-z0-9]([-a-z0-9]*[a-z0-9])?)*
```

5 After you run the helm chart in Step 4, you get a message that Access Manager is installed. However, the Access Manager pods are not yet deployed. The deployment of pods takes about 10 minutes.

Check the progress of the pods deployment by running the following command:

```
kubectl get statefulset,pods --namespace <name-of-the-namespace>
```

An output similar to the following is displayed:

```
lakhil@kubem:~$ kubectl get pods
NAME                       READY    STATUS    RESTARTS    AGE
access-manager-am-ac-0     2/2      Running   0           31h
access-manager-am-ag-0     1/1      Running   0           9h
access-manager-am-idp-0    1/1      Running   0           31h
lakhil@kubem:~$ 
```

The following table describes the output:

Title	Description
Name	Name of the Access Manager pods
Ready	This column displays the deployment status of the Access Manager containers in the pod. Explanation of the status: `0/2` - None of the containers in the pod is deployed `1/2` - One out of two containers is deployed `2/2` - Two out of two containers are deployed
Status	After the containers are pulled from the repository, and the configuration starts, the status changes to `Running`. However, it does not mean that the pods deployment is complete. Check the `Ready` column to verify the deployment status.
Restarts	Number of time that the pod has restarted
Age	Amount of time that the pod is alive

If the deployment does not complete in 10 minutes, proceed to "Checking the Status of Access Manager Resources" on page 236 or "Troubleshooting Access Manager Container Deployment" on page 236.

Proceed to Step 6 if the deployment is complete.

6 Log in to Administration Console. (URL: `https://<administration-console-IP>:2443/nps`)

7 After installing Access Manager, you must create cluster configurations. See Configuring Identity Servers Clusters and Access Gateways Clusters.

11.3 Deploying Analytics Server Containers on On-Premises Linux Servers

You can deploy Analytics Server containers on Kubernetes, installed on On-premises Linux servers, using the Helm charts.

You must have the following details to install Analytics Server:

— Name of the namespace

— Release name

— IP address of the Administration Console

Run command `kubectl get pods -o wide` to view the name, IP address, status, and additional information of the available nodes. You need these details to run the helm install command.

Procedure to Install Analytics Server:

NOTE: During the installation, Analytics Server creates directory for data persistence. The default location of this directory is `/mnt/<release-name>-am-dashboard`.

NOTE: If the node contains multiple IP addresses, Kubernetes schedules the Analytics Server pod in the primary IP address. Therefore, you must ensure that the IP address you want to schedule the pod is the primary interface.

---

1 Create a namespace under which you will deploy Analytics Server

   `kubectl create namespace <name-of-the-namespace>`

   NOTE: Creating a namespace is not mandatory. However, it is recommended to create one to deploy Analytics Server. For more information about namespace, see "Kubernetes Keywords and Their Usage in Access Manager" on page 121.

   ---

2 Label the Kubernetes nodes using `$ kubectl label node <name-of-the-node> nam.app/name=am-dashboard`

   NOTE: Refer to Section 11.3.1, "Label Nodes," on page 140 for more information.

   ---

3 Download the Analytics Server helm chart (`Dashboard_50_HelmChart-1.0.1.tgz`) to the Master node from Micro Focus Downloads.

4 Unzip the Analytics Server helm chart by using the following command:

   `tar -xzvf Dashboard_50_HelmChart-1.0.1.tgz`

5 Run the helm chart by using one of the following approaches:

   ◆ Approach 1: Specify the required values in the helm install command and run the command. In this approach, you specify the elements and the values after the `--set` string. The `--set` string overrides any value configured in the `am-dashboard/values.yaml` file.

   ◆ Approach 2: Specify the required values in the `am-dashboard/values.yaml` file and run the helm install command.

   NOTE: Ensure that you execute the helm install command from the location where you have extracted the helm chart, which contains the `am-dashboard` directory.

Approach 1

Run the following command to install Analytics Server:

```
helm install --namespace <name-of-the-namespace> <release-name> my-
deployment --set global.amconfig.primaryAcIp=<primary-console-IP> --set
global.amsecret.adminName=<administrator-username> --set
global.amsecret.adminPassword=<administrator-password>
```

Drafting a Sample Command

Let us consider that the values of the command's elements are as follows:

Element	Value
Name of the Namespace	as-deploy
Release name	my-deployment
	NOTE: You must use the following RegEx, which the Helm package manager enforces while assigning a release name:
	`[a-z0-9]([-a-z0-9]*[a-z0-9])?(\.[a-z0-9]([-a-z0-9]*[a-z0-9])?)*`
Primary Administration Console IP	IP address of the Administration Console. Example: 10.10.10.11
Administrator Username	admin
Administrator Password	password
Replica	It is the number of replicas you require. You can set this using `--set replicaCount=1`. The replica count number depends on how many replicas are required.

IMPORTANT: Ensure that the administrator username and password meet the Conditions for Creating Administrator Username and Password.

Then the command will look as follows:

```
$ helm install RELEASE_NAME my-deployment \
--namespace NAMESPACE as-deploy \
--set global.amconfig.primaryAcIp=10.10.10.11 \
--set global.amsecret.adminName=admin \
--set global.amsecret.adminPassword=password \
```

(Optional) If you host the docker images on a separate repository, then append the following string to the command:

` --set global.image.repository=<path-of-the-Analytics-Dashboard-docker-images-repository>`

(Optional) If you use a private registry, then you must also specify the registry's username and password. Append the following string to the command:

` --set global.image.pullSecrets.name=<registry-username> --set global.image.pullSecrets.password=<registry-password>`

Approach 2

Configure the values and run the helm chart:

1. Open the `am-dashboard/values.yaml` file.
2. Specify the following details:

Element	Value
repository (Optional)	Path of the Analytics Server Docker images
pullPolicy: IfNotPresent (Optional)	If you are using a private registry, then replace `pullPolicy: IfNotPresent` with `pullPolicy: Always`
pullSecrets (Optional)	If you are using a private registry, then specify the registry's username and password
primaryAcIp	IP address of the primary Administration Console
adminName	Administrator Username
adminPassword	Administrator Password
Replica	It is the number of replicas you require. You can set this using `--set replicaCount=1`. The replica count number depends on how many replicas are required.

IMPORTANT: Ensure that the administrator username and password meet the Conditions for Creating Administrator Username and Password.

3. Run the following command to install Analytics Server:

```
helm install --namespace <name-of-the-namespace> <release-name> am-
dashboard
```

NOTE: You must use the following RegEx, which the Helm package manager enforces while assigning a release name:

```
[a-z0-9]([-a-z0-9]*[a-z0-9])?(\.[a-z0-9]([-a-z0-9]*[a-z0-9])?)*
```

6 After you run the helm chart in Step 4, you get a message that Analytics Server is installed. However, the Analytics Server pods are not yet deployed. The deployment of pods takes about 10 minutes.

Check the progress of the pod deployment by running the following command:

```
kubectl get pods --namespace <name-of-the-namespace>
```

An output similar to the following is displayed:

```
nadmin@kube-master:~/kubernetes$ kubectl get statefulset,pods --
namespace deployment
NAME                                     READY    AGE
statefulset.apps/access-manager-am-dashboard    1/1      18h
NAME                               READY    STATUS    RESTARTS    AGE
pod/access-manager-am-dashboard-0    1/1      Running   0           18h
nadmin@kube-master:~/kubernetes$
```

The following table describes the output:

Title	Description
Name	Name of the Analytics Server pods
Ready	This column displays the deployment status of the Analytics Server containers in the pod. Explanation of the status: `1/1` - Dashboard container is deployed
Status	After the containers are pulled from the repository, and the configuration starts, the status changes to `Running`. However, it does not mean that the pods deployment is complete. Check the `Ready` column to verify the deployment status.
Restarts	Number of time that the pod has restarted
Age	Amount of time that the pod is alive

If the deployment does not complete in 10 minutes, proceed to "Checking the Status of Access Manager Resources" on page 236 or "Troubleshooting Access Manager Container Deployment" on page 236.

Proceed to Step 6 if the deployment is complete.

7 Log in to Administration Console and access Analytics Server from the menu.

11.3.1 Label Nodes

Analytics Server cannot run on nodes where the Access Manager components such as, Administration Console is already present. To ensure that Access Manager and Analytics Server deployments are separate, you must label the nodes to identify where they should run to avoid conflict. You must label all the nodes where the pods would be running.

12 Deploying Access Manager Containers on AWS

You can deploy Access Manager containers on Kubernetes clusters by using the Helm charts.

- Prerequisites for Deploying Access Manager Containers on AWS
- Deploying Access Manager Containers on AWS
- Deploying Analytics Server Containers on AWS

12.1 Prerequisites for Deploying Access Manager Containers on AWS

- ❒ A Kubernetes cluster (v1.19 or later) with Role-Based Access Control enabled.
- ❒ Created an account on Amazon Elastic Kubernetes Service (Amazon EKS).
- ❒ Created an Amazon EKS cluster.

  For more information about how to create an Amazon EKS cluster, see Getting Started with Amazon EKS.
- ❒ One master node and one worker node (minimum) available in the Kubernetes cluster.
- ❒ The `kubectl` command-line tool installed on your machine and configured it to work with Amazon EKS.
- ❒ Helm 3.*x* is installed.
- ❒ (Optional) NginX Ingress Controller is configured.

NOTE: For information about using Amazon EKS, see Best practices for using Amazon EKS.

12.2 Deploying Access Manager Containers on AWS

NOTE: In this release, only a fresh installation of Access Manager is supported. You cannot upgrade from a previous version of Access Manager.

NOTE: During the installation, Access Manager creates the following directories for data persistence. These directories get created in the corresponding worker node in which you install the particular Access Manager component. The default location of these directories is `/mnt`.

- **eDirectory:** `<release-name>-am-edir`
- **Administration Console:** `<release-name>-am-ac`

⬥ **Identity Server:** `<release-name>-am-idp`

⬥ **Access Gateway:** `<release-name>-am-ag`

NOTE: If you decide not to install all Access Manager components, you can specify the details in the `values.yaml` file before running the helm chart.

For example, if you do not want to install Access Gateway, then specify `enabled: false` under Access Gateway in the `values.yaml` file. In this scenario, only Administration Console and Identity Server will get installed.

Similarly, if you do not want to install Identity Server, then specify `enabled: false` under Identity Server in the `values.yaml` file. In this scenario, only Administration Console and Access Gateway will get installed.

---

1 Create a namespace under which you will deploy Access Manager.

```
kubectl create namespace <name-of-the-namespace>
```

NOTE: Creating a namespace is not mandatory. However, it is recommended to create one to deploy Access Manager. For more information about namespace, see "Kubernetes Keywords and Their Usage in Access Manager" on page 121.

---

2 Download the Access Manager helm chart (`AM_50_HelmChart-1.0.1.tgz`) to the Master node from Micro Focus Downloads.

3 Unzip the Access Manager helm chart by using the following command:

```
tar -xzvf AM_50_HelmChart-1.0.1.tgz
```

4 (Optional) Configure the Ingress rules. See "Configuring Ingress" on page 127.

5 Run the helm chart by using one of the following approaches:

⬥ Approach 1: Specify the required values in the helm install command and run the command. In this approach, you specify the elements and the values after the `--set` string. The `--set` string overrides any value configured in the `access-manager/values.yaml` file.

⬥ Approach 2: Specify the required values in the `access-manager/values.yaml` file and run the helm install command.

NOTE: Ensure that you execute the helm install command from the location where you have extracted the helm chart, which contains the `access-manager` directory.

Approach 1

Run the following command to install Access Manager:

```
helm install --namespace <name-of-the-namespace> <release-name> access-
manager --set global.amconfig.primaryAcIp=<primary-administration-
console-IP> --set global.amsecret.adminName=<administrator-username> --
set global.amsecret.adminPassword=<administrator-password> --set am-
ac.primary.node=<name-of-the-primary-administration-console-node> --set
am-ac.secondary.enabled=false
```

Drafting a Sample Command

Let us consider that the values of the command's elements are as follows:

Element	Value
Name of the Namespace	development
Release name	my-deployment **NOTE:** You must use the following RegEx, which the Helm package manager enforces while assigning a release name: `[a-z0-9]([-a-z0-9]*[a-z0-9])?(\.[a-z0-9]([-a-z0-9]*[a-z0-9])?)*`
Administration Console IP	10.10.10.11 You can run the `kubectl get nodes -o wide` command to view the IP addresses of the worker nodes, and then choose a node to install Administration Console. You must always install Administration Console in one of the worker nodes, not in the master node.
Name of the Administration Console node	kubew1 `kubectl get nodes -o wide` command also displays the corresponding name of the node in which you have decided to install Administration Console.
Administrator Username	admin
Administrator Password	password

IMPORTANT: Ensure that the administrator username and password meet the Conditions for Creating Administrator Username and Password.

Then the command will look as follows:

```
helm install --namespace development my-deployment access-manager --set
global.amconfig.primaryAcIp=10.10.10.11 --set
global.amsecret.adminName=admin --set
global.amsecret.adminPassword=password --set am-ac.primary.node=kubew1
--set am-ac.secondary.enabled=false
```

(Optional) To install Secondary Administration Console, change `--set am-ac.secondary.enabled=false` to `true`, and append the following string to the command:

```
--set global.amconfig.secondaryAcIp=<secondary-administration-console-
IP> --set am-ac.secondary.node=<name-of-the-administration-console-
node> --set am-ac.secondary.enabled=true
```

(Optional) If you want to use Ingress, then append the following string to the command:

```
 --set ingress.enabled=true
```

(Optional) If you host the docker images on a separate repository, then append the following string to the command:

```
 --set global.image.repository=<path-of-the-Access-Manager-docker-
images-repository>
```

(Optional) If you use a private registry, then you must also specify the registry's username and password. Append the following string to the command:

```
--set global.image.pullSecrets.name=<registry-username> --set
global.image.pullSecrets.password=<registry-password>
```

Approach 2

Configure the values and run the helm chart:

1. Open the `access-manager/values.yaml` file.
2. Specify the following details:

Element	Value
repository (Optional)	Path of the Access Manager Docker images
pullPolicy: IfNotPresent (Optional)	If you are using a private registry, then replace `pullPolicy: IfNotPresent` with `pullPolicy: Always`
pullSecrets (Optional)	If you are using a private registry, specify the registry's username and password
primaryAcIp	IP address of the worker node where you will install the primary Administration Console You can run the `kubectl get nodes -o wide` command to view the IP addresses of the worker nodes, and then choose a node to install Administration Console. You must always install Administration Console in one of the worker nodes, not in the master node.
adminName	Administrator Username
adminPassword	Administrator Password
node	Name of the Administration Console worker node The `kubectl get nodes -o wide` command also displays the corresponding name of the node in which you have decided to install Administration Console.
ingress (Optional)	Specify `enabled: true` To configure Ingress rules, see Configuring Ingress.

IMPORTANT: Ensure that the administrator username and password meet the Conditions for Creating Administrator Username and Password.

NOTE: To install Secondary Administration Console along with the Primary Administration Console, specify `enabled: true` under Secondary Administration Console.

3. Run the following command to install Access Manager:

```
helm install --namespace <name-of-the-namespace> <release-name>
access-manager
```

> **NOTE:** You must use the following RegEx, which the Helm package manager enforces while assigning a release name:
>
> ```
> [a-z0-9]([-a-z0-9]*[a-z0-9])?(\.[a-z0-9]([-a-z0-9]*[a-z0-9])?)*
> ```

6 After you run the helm chart in Step 5, you get a message that Access Manager is installed. However, the Access Manager pods are not yet deployed. The deployment of pods takes about 10 minutes.

Check the progress of the pods deployment by running the following command:

```
kubectl get statefulset,pods --namespace <name-of-the-namespace>
```

An output similar to the following is displayed:

```
lakhil@kubem:~$ kubectl get pods
NAME                        READY    STATUS     RESTARTS    AGE
access-manager-am-ac-0      2/2      Running    0           31h
access-manager-am-ag-0      1/1      Running    0           9h
access-manager-am-idp-0     1/1      Running    0           31h
lakhil@kubem:~$
```

The following table describes the output:

Title	Description
Name	Name of the Access Manager pods
Ready	The deployment status of the Access Manager containers in a pod.
	Explanation of the status:
	`0/2` - None of the containers in the pod is deployed
	`1/2` - One out of two containers is deployed
	`2/2` - Two out of two containers are deployed
Status	After the containers are pulled from the repository, and the configuration starts, the status changes to `Running`. However, it does not mean that the pods deployment is complete. Check the `Ready` column to verify the deployment status.
Restarts	Number of time that the pod has restarted
Age	Amount of time that the pod is alive

If the deployment does not complete in 10 minutes, proceed to "Checking the Status of Access Manager Resources" on page 236 or "Troubleshooting Access Manager Container Deployment" on page 236.

Proceed to Step 7 if the deployment is complete.

7 Log in to Administration Console. (URL: `https://<administration-console-IP>:2443/nps`)

8 After installing Access Manager, you must create cluster configurations. See Configuring Identity Servers Clusters and Access Gateways Clusters.

12.3 Deploying Analytics Server Containers on AWS

NOTE: During the installation, Analytics Server creates directory for data persistence. The default location of this directory is `/mnt/<release-name>-am-dashboard`.

1 Create a namespace under which you will deploy Analytics Server.

```
kubectl create namespace <name-of-the-namespace>
```

NOTE: Creating a namespace is not mandatory. However, it is recommended to create one to deploy Analytics Server. For more information about namespace, see "Kubernetes Keywords and Their Usage in Access Manager" on page 121.

2 Label the Kubernetes nodes using `$ kubectl label node <name-of-the-node> nam.app/name=am-dashboard`

NOTE: Refer to Section 11.3.1, "Label Nodes," on page 140 for more information.

3 Download the Analytics Server helm chart (`tar -xzvf Dashboard_50_HelmChart-1.0.1.tgz`) from Micro Focus Downloads.

4 Unzip the Access Manager helm chart by using the following command:

```
tar -xzvf Dashboard_50_HelmChart-1.0.1.tgz
```

5 (Optional) Configure the Ingress rules. See "Configuring Ingress" on page 127.

6 Run the helm chart by using one of the following approaches:

   ◆ Approach 1: Specify the required values in the helm install command and run the command. In this approach, you specify the elements and the values after the `--set` string. The `--set` string overrides any value configured in the `am-dashboard/`

`values.yaml` file.

   ◆ Approach 2: Specify the required values in the `am-dashboard/`

`values.yaml` file and run the helm install command.

NOTE: Ensure that you execute the helm install command from the location where you have extracted the helm chart, which contains the `am-dashboard` directory.

Approach 1

Run the following command to install Analytics Server:

```
helm install --namespace <name-of-the-namespace> <release-name> my-
deployment --set global.amconfig.primaryAcIp=<primary-console-IP> --set
global.amsecret.adminName=<administrator-username> --set
global.amsecret.adminPassword=<administrator-password>
```

NOTE: If you require replicas you can use the command `--set replicaCount=1`. The replica count number depends on how many replicas are required.

Drafting a Sample Command

Let us consider that the values of the command's elements are as follows:

Element	Value
Name of the Namespace	as-deploy
Release name	my-deployment **NOTE:** You must use the following RegEx, which the Helm package manager enforces while assigning a release name: `[a-z0-9]([-a-z0-9]*[a-z0-9])?(\.[a-z0-9]([-a-z0-9]*[a-z0-9])?)*`
Administration Console IP	10.10.10.11
Administrator Username	admin
Administrator Password	password
Replica	It is the number of replicas you require. You can set this using `--set replicaCount=1`. The replica count number depends on how many replicas are required.

IMPORTANT: Ensure that the administrator username and password meet the Conditions for Creating Administrator Username and Password.

Then the command will look as follows:

```
$ helm install RELEASE_NAME my-deployment \
--namespace NAMESPACE as-deploy \
--set global.amconfig.primaryAcIp=10.10.10.11 \
--set global.amsecret.adminName=admin \
--set global.amsecret.adminPassword=password \
```

(Optional) If you want to use Ingress, then append the following string to the command:

```
--set ingress.enabled=true
```

(Optional) If you host the docker images on a separate repository, then append the following string to the command:

```
--set global.image.repository=<path-of-the-AnalyticsDashboard-docker-images-repository>
```

(Optional) If you use a private registry, then you must also specify the registry's username and password. Append the following string to the command:

```
--set global.image.pullSecrets.name=<registry-username> --set global.image.pullSecrets.password=<registry-password>
```

Approach 2

Configure the values and run the helm chart:

1. Open the `am-dashboard/values.yaml` file.

2. Specify the following details:

Element	Value
repository (Optional)	Path of the Analytics Server Docker images
pullPolicy: IfNotPresent (Optional)	If you are using a private registry, then replace `pullPolicy: IfNotPresent` with `pullPolicy: Always`
pullSecrets (Optional)	If you are using a private registry, specify the registry's username and password
primaryAcIp	IP address of the primary Administration Console
adminName	Administrator Username
adminPassword	Administrator Password
Replica	It is the number of replicas you require. You can set this using `--set replicaCount=1`. The replica count number depends on how many replicas are required.
ingress (Optional)	Specify `enabled: true` To configure Ingress rules, see Configuring Ingress.

IMPORTANT: Ensure that the administrator username and password meet the Conditions for Creating Administrator Username and Password.

3. Run the following command to install Access Manager:

```
helm install --namespace <name-of-the-namespace> <release-name>
analytics-dashboard
```

NOTE: You must use the following RegEx, which the Helm package manager enforces while assigning a release name:

```
[a-z0-9]([-a-z0-9]*[a-z0-9])?(\.[a-z0-9]([-a-z0-9]*[a-z0-9])?)*
```

7 After you run the helm chart in Step 5, you get a message that Analytics Server is installed. However, the Analytics Server pods are not yet deployed. The deployment of pods takes about 10 minutes.

Check the progress of the pods deployment by running the following command:

```
kubectl get statefulset,pods --namespace <name-of-the-namespace>
```

An output similar to the following is displayed:

```
nadmin@kube-master:~/kubernetes$ kubectl get statefulset,pods --
namespace deployment
NAME                                       READY   AGE
statefulset.apps/access-manager-am-dashboard   1/1     18h
NAME                              READY   STATUS    RESTARTS   AGE
pod/access-manager-am-dashboard-0   1/1     Running   0          18h
nadmin@kube-master:~/kubernetes$
```

The following table describes the output:

Title	Description
Name	Name of the Analytics Server pods
Ready	This column displays the deployment status of the Analytics Server containers in a pod. Explanation of the status: `1/1` - Analytics Server container is deployed
Status	After the containers are pulled from the repository, and the configuration starts, the status changes to `Running`. However, it does not mean that the pods deployment is complete. Check the `Ready` column to verify the deployment status.
Restarts	Number of time that the pod has restarted
Age	Amount of time that the pod is alive

If the deployment does not complete in 10 minutes, proceed to "Checking the Status of Access Manager Resources" on page 236 or "Troubleshooting Access Manager Container Deployment" on page 236.

Proceed to Step 7 if the deployment is complete.

8 Log in to Administration Console and access Analytics Server from the menu. (URL: `https://<administration-console-IP>:2443/nps`)

13 Deploying Access Manager Containers on Azure Kubernetes Services

You can deploy Access Manager containers on Kubernetes clusters by using the Helm charts.

- Prerequisites for Deploying Access Manager Containers on Azure Kubernetes Services
- Deploying Access Manager Containers on Azure Kubernetes Services
- Deploying Analytics Server Containers on Azure Kubernetes Services

13.1 Prerequisites for Deploying Access Manager Containers on Azure Kubernetes Services

- ❑ A Kubernetes cluster (v1.19 or later) with Role-Based Access Control enabled.
- ❑ Created an administrative account on Azure Kubernetes Services (AKS).
- ❑ Configured a Microsoft AKS cluster.

  For more information about how to configure a Microsoft AKS cluster, see Quickstart.

  To workaround the AKS system name limitation, see Administration Console Pod Does Not Deploy in Azure Kubernetes Services.

- ❑ One master node and one worker node (minimum) available in the Kubernetes cluster.
- ❑ The `kubectl` command-line tool installed on your machine and configured it to work with Microsoft AKS.
- ❑ Helm 3.*x* is installed.
- ❑ NginX Ingress Controller is configured.

NOTE: For information about using AKS, see Best practices for using AKS.

13.2 Deploying Access Manager Containers on Azure Kubernetes Services

---

NOTE: During the installation, Access Manager creates the following directories for data persistence. These directories get created in the corresponding worker node in which you install the particular Access Manager component. The default location of these directories is `/mnt`.

- **eDirectory:** `<release-name>-am-edir`
- **Administration Console:** `<release-name>-am-ac`
- **Identity Server:** `<release-name>-am-idp`
- **Access Gateway:** `<release-name>-am-ag`

NOTE: If you decide not to install all Access Manager components, you can specify the details in the `values.yaml` file before running the helm chart.

For example, if you do not want to install Access Gateway, then specify `enabled: false` under Access Gateway in the `values.yaml` file. In this scenario, only Administration Console and Identity Server will get installed.

Similarly, if you do not want to install Identity Server, then specify `enabled: false` under Identity Server in the `values.yaml` file. In this scenario, only Administration Console and Access Gateway will get installed.

1 Create a namespace under which you will deploy Access Manager.

```
kubectl create namespace <name-of-the-namespace>
```

NOTE: Creating a namespace is not mandatory. However, it is recommended to create one to deploy Access Manager. For more information about namespace, see "Kubernetes Keywords and Their Usage in Access Manager" on page 121.

2 Download the Access Manager helm chart (`AM_50_HelmChart-1.0.1.tgz`) to the Master node from Micro Focus Downloads.

3 Unzip the Access Manager helm chart by using the following command:

```
tar -xzvf AM_50_HelmChart-1.0.1.tgz
```

4 Configure the Ingress rules. See "Configuring Ingress" on page 127.

5 Run the helm chart by using one of the following approaches:

- Approach 1: Specify the required values in the helm install command and run the command. In this approach, you specify the elements and the values after the `--set` string. The `--set` string overrides any value configured in the `access-manager/values.yaml` file.

- Approach 2: Specify the required values in the `access-manager/values.yaml` file and run the helm install command.

NOTE: Ensure that you execute the helm install command from the location where you have extracted the helm chart, which contains the `access-manager` directory.

Approach 1

Run the following command to install Access Manager:

```
helm install --namespace <name-of-the-namespace> <release-name> access-
manager --set global.amconfig.primaryAcIp=<primary-administration-
console-IP> --set global.amsecret.adminName=<administrator-username> --
set global.amsecret.adminPassword=<administrator-password> --set am-
ac.primary.node=<name-of-the-primary-administration-console-node> --set
am-ac.secondary.enabled=false
```

Drafting a Sample Command

Let us consider that the values of the command's elements are as follows:

Element	Value
Name of the Namespace	development
Release name	my-deployment **NOTE:** You must use the following RegEx, which the Helm package manager enforces while assigning a release name: `[a-z0-9]([-a-z0-9]*[a-z0-9])?(\.[a-z0-9]([-a-z0-9]*[a-z0-9])?)*`
Administration Console IP	10.10.10.11 You can run the `kubectl get nodes -o wide` command to view the IP addresses of the worker nodes, and then choose a node to install Administration Console. You must always install Administration Console in one of the worker nodes, not in the master node.
Name of the Administration Console node	kubew1 `kubectl get nodes -o wide` command also displays the corresponding name of the node in which you have decided to install Administration Console.
Administrator Username	Administrator Username
Administrator Password	Administrator Password

IMPORTANT: Ensure that the administrator username and password meet the Conditions for Creating Administrator Username and Password.

Then the command will look as follows:

```
helm install --namespace development my-deployment access-manager --set
global.amconfig.primaryAcIp=10.10.10.11 --set
global.amsecret.adminName=admin --set
global.amsecret.adminPassword=password --set am-ac.primary.node=kubew1
--set am-ac.secondary.enabled=false
```

(Optional) To install Secondary Administration Console, change `--set am-ac.secondary.enabled=false` to `true`, and append the following string to the command:

```
--set global.amconfig.secondaryAcIp=<secondary-administration-console-
IP> --set am-ac.secondary.node=<name-of-the-administration-console-
node> --set am-ac.secondary.enabled=true
```

(Optional) If you want to use Ingress, then append the following string to the command:

```
 --set ingress.enabled=true
```

(Optional) If you host the docker images on a separate repository, then append the following string to the command:

```
 --set global.image.repository=<path-of-the-Access-Manager-docker-
images-repository>
```

(Optional) If you use a private registry, then you must also specify the registry's username and password. Append the following string to the command:

```
--set global.image.pullSecrets.name=<registry-username> --set
global.image.pullSecrets.password=<registry-password>
```

Approach 2

Configure the values and run the helm chart:

1. Open the `access-manager/values.yaml` file.
2. Specify the following details:

Element	Value
repository (Optional)	Path of the Access Manager Docker images
pullPolicy: IfNotPresent (Optional)	If you are using a private registry, then replace `pullPolicy: IfNotPresent` with `pullPolicy: Always`
pullSecrets (Optional)	If you are using a private registry, then specify the registry's username and password
primaryAcIp	IP address of the worker node where you will install the Primary Administration Console You can run the `kubectl get nodes -o wide` command to view the IP addresses of the worker nodes, and then choose a node to install Administration Console. You must always install Administration Console in one of the worker nodes, not in the master node.
adminName	Administrator Username
adminPassword	Administrator Password
node	Name of the Administration Console worker node The `kubectl get nodes -o wide` command also displays the corresponding name of the node in which you have decided to install Administration Console.
ingress (Optional)	Specify `enabled: true` To configure Ingress rules, see Configuring Ingress.

IMPORTANT: Ensure that the administrator username and password meet the Conditions for Creating Administrator Username and Password.

NOTE: To install Secondary Administration Console along with the Primary Administration Console, specify `enabled: true` under Secondary Administration Console.

3. Run the following command to install Access Manager:

```
helm install --namespace <name-of-the-namespace> <release-name>
access-manager
```

> **NOTE:** You must use the following RegEx, which the Helm package manager enforces while assigning a release name:
>
> ```
> [a-z0-9]([-a-z0-9]*[a-z0-9])?(\.[a-z0-9]([-a-z0-9]*[a-z0-9])?)*
> ```

6 After you run the helm chart in Step 5, you get a message that Access Manager is installed. However, the Access Manager pods are not yet deployed. The deployment of pods takes about 10 minutes.

Check the progress of the pods deployment by running the following command:

```
kubectl get statefulset,pods --namespace <name-of-the-namespace>
```

An output similar to the following is displayed:

```
lakhil@kubem:~$ kubectl get pods
NAME                         READY    STATUS     RESTARTS    AGE
access-manager-am-ac-0       2/2      Running    0           31h
access-manager-am-ag-0       1/1      Running    0           9h
access-manager-am-idp-0      1/1      Running    0           31h
lakhil@kubem:~$
```

The following table describes the output:

Title	Description
Name	Name of the Access Manager pods
Ready	The deployment status of the Access Manager containers in the pod. Explanation of the status: `0/2` - None of the containers in the pod is deployed `1/2` - One out of two containers is deployed `2/2` - Two out of two containers are deployed
Status	After the containers are pulled from the repository, and the configuration starts, the status changes to `Running`. However, it does not mean that the pods deployment is complete. Check the `Ready` column to verify the deployment status.
Restarts	Number of time that the pod has restarted
Age	Amount of time that the pod is alive

If the deployment does not complete in 10 minutes, proceed to "Checking the Status of Access Manager Resources" on page 236 or "Troubleshooting Access Manager Container Deployment" on page 236.

Proceed to Step 7 if the deployment is complete.

7 Log in to Administration Console. (URL: `https://<administration-console-IP>:2443/nps`)

8 After installing Access Manager, you must create cluster configurations. See Configuring Identity Servers Clusters and Access Gateways Clusters.

Configuring Identity Server and Access Gateway Ports

After configuring Identity Server and Access Gateway clusters, you must modify the port configuration. The configured ports are hardcoded to the hyperlinks of HTML pages, and Access Manager sends back the 302 redirection URL with the cluster's configured port. However, only 80 and 443 ports are open in the load balancer, and the redirection goes through the configured port such as 8443. Therefore, the load balancer cannot accept the redirection URL.

So, you must perform the following additional configurations:

For Identity Server

1 Configure Identity Server in the 443 port.

2 Add host entries of Access Gateway and the load balancer IP address.

For Access Gateway

1 Configure the primary reverse proxy (Embedded Service Provider's URL) in the 80/443 port.

IMPORTANT: If you want to create reverse proxies in any other port, you must open the port.

NOTE: The proxy name must not contain any upper case alphabet, and must comply with the following RegEx:

```
[a-z0-9]([-a-z0-9]*[a-z0-9])?(\.[a-z0-9]([-a-z0-9]*[a-z0-9])?)*
```

---

2 Add the host entry of Identity Server configured to load balancer's IP.

3 (Optional) Configure domain-based multi-homing proxy services in the 80/443 port.

Continue with Configuring Ingress Front-End SSL.

Configuring Ingress Front-End SSL

Let us consider that the DNS of Access Gateway is `www.cloudag.com`, and a certificate for the DNS is generated in Access Manager. Also, Ingress is configured with the same DNS.

Perform the following steps to configure the front-end SSL:

1 Download the certificate (`.pfx` format) from Administration Console.

2 Extract the certificate using the following command:

```
openssl pkcs12 -in <certificate-name>.pfx -clcerts -nokeys -out ag.cert
```

3 Extract the certificate key using the following command:

```
openssl pkcs12 -in <certificate-name>.pfx -nocerts -out ag_pwd.key
```

4 Remove the password from the key using the following command:

```
openssl rsa -in ag_pwd.key -out ag.key
```

5 Create a secret in Kubernetes:

```
kubectl create secret tls cloudag --key ag.key --cert ag.cert -n <name-of-the-namespace>
```

where, `cloudag` is the secret name.

6 Open and modify the `access-manager/values.yaml` as follows:

```
tls:
  - secretName: cloudag
    hosts:
      - www.cloudag.com
```

7 Perform a helm upgrade on the same helm release with the Access Manager helm chart.

13.3 Deploying Analytics Server Containers on Azure Kubernetes Services

NOTE: During the installation, Analytics Server creates directory for data persistence. The default location of this directory is `/mnt/<release-name>-am-dashboard`.

1 Create a namespace under which you will deploy Analytics Server.

```
kubectl create namespace <name-of-the-namespace>
```

NOTE: Creating a namespace is not mandatory. However, it is recommended to create one to deploy Analytics Server. For more information about namespace, see "Kubernetes Keywords and Their Usage in Access Manager" on page 121.

2 Label the kubernetes nodes using `$ kubectl label node <name-of-the-node> nam.app/name=am-dashboard`

NOTE: Refer to Section 11.3.1, "Label Nodes," on page 140 for more information.

3 Download the Access Manager helm chart (`tar -xzvf Dashboard_50_HelmChart-1.0.1.tgz`) to the Master node from Micro Focus Downloads.

4 Unzip the Access Manager helm chart by using the following command:

```
tar -xzvf Dashboard_50_HelmChart-1.0.1.tgz
```

5 Configure the Ingress rules. See "Configuring Ingress" on page 127.

6 Run the helm chart by using one of the following approaches:

- ◆ Approach 1: Specify the required values in the helm install command and run the command. In this approach, you specify the elements and the values after the `--set` string. The `--set` string overrides any value configured in the `am-dashboard/values.yaml` file.

- ◆ Approach 2: Specify the required values in the `am-dashboard.yaml` file and run the helm install command.

NOTE: Ensure that you execute the helm install command from the location where you have extracted the helm chart, which contains the `analytics-dashboard` directory.

Approach 1

Run the following command to install Analytics Server:

```
helm install --namespace <name-of-the-namespace> <release-name> my-
deployment --set global.amconfig.primaryAcIp=<primary administration-
console-IP> --set global.amsecret.adminName=<administrator-username> --
set global.amsecret.adminPassword=<administrator-password>
```

(Optional) If you want to use Ingress, then append the following string to the command:

```
--set ingress.enabled=true
```

Drafting a Sample Command

Let us consider that the values of the command's elements are as follows:

Element	Value
Name of the Namespace	as-deploy
Release name	my-deployment **NOTE:** You must use the following RegEx, which the Helm package manager enforces while assigning a release name: `[a-z0-9]([-a-z0-9]*[a-z0-9])?(\.[a-z0-9]([-a-z0-9]*[a-z0-9])?)*`
Administration Console IP	10.10.10.11
Administrator Username	admin
Administrator Password	password
Replica	It is the number of replicas you require. You can set this using `--set replicaCount=1`. The replica count number depends on how many replicas are required.

IMPORTANT: Ensure that the administrator username and password meet the Conditions for Creating Administrator Username and Password.

Then the command will look as follows:

```
$ helm install RELEASE_NAME my-deployment \
--namespace NAMESPACE as-deploy \
--set global.amconfig.primaryAcIp=10.10.10.11 \
--set global.amsecret.adminName=admin \
--set global.amsecret.adminPassword=password \

```

(Optional) If you want to use Ingress, then append the following string to the command:

```
--set ingress.enabled=true
```

NOTE: If you require replicas you can use the command `--set replicaCount=1`. The replica count number depends on how many replicas are required.

(Optional) If you host the docker images on a separate repository, then append the following string to the command:

```
--set global.image.repository=<path-of-the-Analytics-Dashboard-docker-
images-repository>
```

(Optional) If you use a private registry, then you must also specify the registry's username and password. Append the following string to the command:

```
--set global.image.pullSecrets.name=<registry-username> --set
global.image.pullSecrets.password=<registry-password>
```

Approach 2

Configure the values and run the helm chart:

1. Open the `analytics-dashboard/values.yaml` file.

2. Specify the following details:

Element	Value
repository (Optional)	Path of the Analytics Server Docker images
pullPolicy: IfNotPresent (Optional)	If you are using a private registry, then replace `pullPolicy: IfNotPresent` with `pullPolicy: Always`
pullSecrets (Optional)	If you are using a private registry, then specify the registry's username and password
primaryAcIp	IP address of the Primary Administration Console
adminName	Administrator Username
adminPassword	Administrator Password
ingress (Optional)	Specify `enabled: true` To configure Ingress rules, see Configuring Ingress.
Replica	It is the number of replicas you require. You can set this using `--set replicaCount=1`. The replica count number depends on how many replicas are required.

IMPORTANT: Ensure that the administrator username and password meet the Conditions for Creating Administrator Username and Password.

3. Run the following command to install Access Manager:

```
helm install --namespace <name-of-the-namespace> <release-name>
analytics-dashboard
```

NOTE: You must use the following RegEx, which the Helm package manager enforces while assigning a release name:

```
[a-z0-9]([-a-z0-9]*[a-z0-9])?(\.[a-z0-9]([-a-z0-9]*[a-z0-9])?)*
```

7 After you run the helm chart in Step 5, you get a message that Analytics Server is installed. However, the Analytics Server pods are not yet deployed. The deployment of pods takes about 10 minutes.

Check the progress of the pods deployment by running the following command:

```
kubectl get statefulset,pods --namespace <name-of-the-namespace>
```

An output similar to the following is displayed:

```
nadmin@kube-master:~/kubernetes$ kubectl get statefulset,pods --
namespace deployment
NAME                                          READY    AGE
statefulset.apps/access-manager-am-dashboard    1/1      18h
NAME                              READY   STATUS    RESTARTS    AGE
pod/access-manager-am-dashboard-0    1/1    Running   0          18h
nadmin@kube-master:~/kubernetes$
```

The following table describes the output:

Title	Description
Name	Name of the Access Manager pods
Ready	This column displays the deployment status of the Analytics Server containers in the pod. Explanation of the status: `1/1` - Analytics Server is deployed
Status	After the containers are pulled from the repository, and the configuration starts, the status changes to `Running`. However, it does not mean that the pods deployment is complete. Check the `Ready` column to verify the deployment status.
Restarts	Number of time that the pod has restarted
Age	Amount of time that the pod is alive

If the deployment does not complete in 10 minutes, proceed to "Checking the Status of Access Manager Resources" on page 236 or "Troubleshooting Access Manager Container Deployment" on page 236.

Proceed to Step 7 if the deployment is complete.

8 Log in to Administration Console and access Analytics Server from the menu. (URL: `https://<administration-console-IP>:2443/nps`)

14 Scaling Access Manager Components

As the number of users and demands for web resources increase, you can add another Identity Server or Access Gateway to handle the load.

NOTE: Scaling Administration Console is not supported in Access Manager 5.0 release.

14.1 Scaling Identity Server

IMPORTANT: Administration Console pod will restart while scaling Identity Server up or down.

1 Make sure that additional worker nodes are available.

For example, if you want to scale Identity Server from one instance to three, two additional worker nodes must be available.

2 Run the following command:

```
helm upgrade --namespace <name-of-the-namespace> <release-name> access-manager --set am-idp.replicaCount=<number-of-Identity-Server-instances> --reuse-values
```

For example, if you want three instances of Identity Server and the values of the command's elements are as follows:

Element	Value
Name of the Namespace	development
Release name	my-deployment
Number of Identity Server instances	3

Then the command will look as follows:

```
helm upgrade --namespace development my-deployment access-manager --set am-idp.replicaCount=3 --reuse-values
```

3 Log in to Administration Console, and add the nodes to the cluster.

To scale down, perform the following steps:

1 Reduce the value of `am-idp.replicaCount` and run the following command:

```
helm upgrade --namespace <name-of-the-namespace> <release-name> access-manager --set am-idp.replicaCount=<number-of-Identity-Server-instances> --reuse-values
```

2   Delete the persistent volume and persistent volume claim:

```
kubectl delete pvc $(kubectl get pv | grep am- | grep Terminating | awk
'{print $6}' | cut -d "/" -f2) -n <name-of-the-namespace>
```

3   Delete the unused worker nodes.

4   Log in to Administration Console, then remove the nodes from the cluster.

14.2   Scaling Access Gateway

IMPORTANT: Administration Console pod will restart while scaling Access Gateway up or down.

1   Make sure that additional worker nodes are available.

For example, if you want to scale Access Gateway from one instance to four, three additional worker nodes must be available.

2   Run the following command:

```
helm upgrade --namespace <name-of-the-namespace> <release-name> access-
manager --set am-ag.replicaCount=<number-of-Access-Gateway-instances> -
-reuse-values
```

For example, if you want four instances of Access Gateway and the values of the command's elements are as follows:

Element	Value
Name of the Namespace	development
Release name	my-deployment
Number of Access Gateway instances	4

Then the command will look as follows:

```
helm upgrade --namespace development my-deployment access-manager --set
am-ag.replicaCount=4 --reuse-values
```

3   Log in to Administration Console, and add the nodes to the cluster.

To scale down, perform the following steps:

1   Reduce the value of `am-ag.replicaCount` and run the following command:

```
helm upgrade --namespace <name-of-the-namespace> <release-name> access-
manager --set am-ag.replicaCount=<number-of-Access-Gateway-instances> -
-reuse-values
```

2   Delete the persistent volume and persistent volume claim:

```
kubectl delete pvc $(kubectl get pv | grep am- | grep Terminating | awk
'{print $6}' | cut -d "/" -f2) -n <name-of-the-namespace>
```

3   Delete the unused worker nodes.

4   Log in to Administration Console, then remove the nodes from the cluster.

IV Upgrading or Migrating Access Manager

This section discusses how to upgrade or migrate Access Manager to the newer version. You must take a backup of the existing configurations before upgrading or migrating Access Manager components.

For more information, see "Back Up and Restore" in the *NetIQ Access Manager 5.0 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 5.0 Security Guide* .

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: For information about the latest supported upgrade paths, see the specific Release Notes on the Access Manager Documentation website.

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 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:

15 Prerequisites for Upgrading or Migrating 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

IMPORTANT: ◆ Access Manager 5.0 onwards, modification of nidp.jar is not recommended. If you have modified nidp.jar in the earlier release, then move those properties to nidp_custom_resources_*.properties as instructed in Customizing the Error Pages and upload the properties file to the Identity Server cluster using Advanced File Configurator. For information about how to add a file, see Adding Configurations to a Cluster in the NetIQ Access Manager 5.0 Administration Guide.

   ◆ From Access Manager 5.0, modifying a configuration file directly on a device is not supported. Any modification made directly on a device is replaced when modifications made through Administration Console are applied. You must customize a configuration file using Advanced File Configurator on Administration Console. See Modifying Configurations.

Before performing an upgrade, ensure that the following prerequisites are met:

❐ Back up your current Access Manager configuration using `./ambkup.sh` command. For more information, see Back Up and Restore in the NetIQ Access Manager 5.0 Administration Guide.

❐ 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 Maintaining Customized JSP Files for Identity Server or Maintaining Customized JSP Files for Access Gateway.

❐ If you have customized any changes to `tomcat.conf` or `server.xml`, back up the files. After the upgrade, restore the files. For information about how to restore the file, see "Managing Configuration Files" in the "NetIQ Access Manager 5.0 Administration Guide".

❐ 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. For information about how to restore the file, see "Managing Configuration Files" in the "NetIQ Access Manager 5.0 Administration Guide".

   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 `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:

```
<!-- Force use the old Cookie processor (because this new tomcat version
uses RFC6265 Cookie Specification) -->

<!--  <CookieProcessor
className="org.apache.tomcat.util.http.LegacyCookieProcessor" /> -->
```

```
</Context>
```

For information about how to modify a file, see "Modifying Configurations" in the "NetIQ Access Manager 5.0 Administration Guide".

❒ 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 NetIQ Access Manager 5.0 Administration Guide.

❒ 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.

❒ Edit the /etc/hosts files on each instance and add an entry to resolve its hostname to its private IP address. For example, `10.10.10.11     kubew1`

NOTE: Post-Upgrade: (Applicable for upgrading from Access Manager 5.0 release only) To avoid any mismatch of customizations seen on Advanced File Configurator user interface and the file present

in the VM server, it is recommended to click the **Send Configurations to Servers** icon (⬆) on all non-temporary files and folders in Identity Server, Administration Console, and Access Gateway from the Advanced File Configurator user interface. This action must be performed even if file status is displayed as Configuration sent successfully on the Advanced File Configurator user interface post-upgrade.

In addition to the these prerequisites, ensure that you also meet the hardware requirements. For more information about hardware requirements, see NetIQ Access Manager System Requirements.

15.1 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

15.1.1 Using Customized JSP Pages from Access Manager 4.1 or Prior

1 Before upgrade, create a copy of all JSP files inside the `/opt/novell/nids/lib/webapp/jsp` directory and place the copy somewhere else.

   WARNING: The upgrade overwrites all existing JSP files.
   ---

2 Upgrade Identity Server.

3 Create an empty folder `legacy`.

4 Add the `legacy` folder to Identity Server in the`/opt/novell/nids/lib/webapp/WEB-INF/` directory using Advanced File Configurator.

For information about how to add a folder, see "Adding Configurations to a Cluster" in the *NetIQ Access Manager 5.0 Administration Guide*.

NOTE: If you do not create the `legacy` folder, Access Manager uses the logic of the default new login pages.

---

5 Add all backed up JSP files into the `/opt/novell/nids/lib/webapp/jsp` directory using Advanced File Configurator. For information about how to add files, see "Adding Configurations to a Cluster" in the *NetIQ Access Manager 5.0 Administration Guide*.

6 Refresh the browser to see the changes.

15.1.2 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 `/opt/novell/nids/lib/webapp/jsp` directory and place the copy somewhere else.

WARNING: The upgrade overwrites all existing JSP files.

---

2 Upgrade Identity Server.

3 Create an empty folder `legacy`.

4 Add the `legacy` folder to Identity Server in the `/opt/novell/nids/lib/webapp/WEB-INF/` directory using Advanced File Configurator.

For information about how to add a folder, see "Adding Configurations to a Cluster" in the *NetIQ Access Manager 5.0 Administration Guide*.

NOTE: If you do not create the `legacy` folder, Access Manager uses the logic of the default new login pages.

---

5 Open customized nidp.jsp and content.jsp files and make the following changes in both files:

For information about how to modify a file, see "Adding Configurations to a Cluster" in the *NetIQ Access Manager 5.0 Administration Guide*.

   5a In the top Java section of the JSP file, find the `ContentHandler` object that looks similar to the following:

   ```
   ContentHandler handler = new ContentHandler(request,response);
   ```

   5b In the code, add the following Java line under `ContentHandler`:

   ```
   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:

```
<% if (bGotoAlternateLandingPageUrl) { %>
      document.location =
"<%=handler.getAlternateLandingPageUrl()%>";
<%  } %>
```

This redirects control to the default portal page that contains appmarks.

6 Refresh the browser to see the changes.

15.2 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 `/opt/novell/nesp/lib/webapp/jsp` directory and place the copy somewhere else.

WARNING: The upgrade overwrites all existing JSP files.

2 Upgrade Access Gateway.

3 Create an empty folder `legacy`.

4 Add the `legacy` folder to Access Gateway in the `/opt/novell/nesp/lib/webapp/WEB-INF/` directory using Advanced File Configurator.

For information about how to add a folder, see "Adding Configurations to a Cluster"in the *NetIQ Access Manager 5.0 Administration Guide*.

NOTE: If you do not create the `legacy` folder, Access Manager uses the logic of the default new login pages.

5 Add all backed up JSP files into the `/opt/novell/nesp/lib/webapp/jsp` directory using Advanced File Configurator.

For information about how to add files, see "Adding Configurations to a Cluster"in the *NetIQ Access Manager 5.0 Administration Guide*.

6 Refresh the browser to see the changes.

16 Upgrading Administration Console

IMPORTANT: If the base operating system is RHEL 7.8, you must first upgrade to Access Manager 5.0, and then upgrade to RHEL 7.9.

Access Manager by default supports Tomcat 9.0.41 and OpenSSL 1.0.2x. 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, backup these files or allow the upgrade program to back them up for you.

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 *NetIQ Access Manager 5.0 Administration Guide*.

Perform the following steps to upgrade Administration Console:

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 and log in as the `root` user.

3 Download the upgrade file from Micro Focus Downloads and extract the `tar.gz` file using the `tar -xzvf <filename>` command.

NOTE: For information about the name of the upgrade file, see the specific Release Notes on the Access Manager Documentation website (https://www.microfocus.com/documentation/access-manager/5.0/).

4 Change to the directory where you unpacked the file using the `./upgrade.sh` command.

5 A confirmation message is displayed 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.

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.

7 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.

8 Enter the Access Manager Administration Console user ID. For example, `admin`

9 Enter the Access Manager Administration Console password.

10 Re-enter the password for verification.

11 The system displays the following confirmation message:

   ```
   Do you want to back up the configuration before the upgrade (y/n)?
   ```

12 Type **Y** and press Enter.

13 The system displays the following message when the upgrade is complete:

   ```
   Upgrade completed successfully.
   ```

NOTE: If the configuration backup fails, the system displays the following message:

```
The configuration backup failed. Do you want to continue the upgrade
without a backup (y/n)?
```

You can complete the upgrade by typing **Y**. However, the configuration will not have a backup.

---

14 (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 using Advanced File Configurator. See "Modifying Configurations" in the *NetIQ Access Manager 5.0 Administration Guide*.

NOTE: Post-Upgrade: To avoid any mismatch of customizations seen on Advanced File Configurator user interface and the file present in the VM server, it is recommended to click the **Send Configurations to Servers** icon () operation for all non-temporary files and folders in

Administration Console from the Advanced File Configurator user interface. This action must be performed even if file status is displayed as Configuration sent successfully on the Advanced File Configurator user interface post-upgrade.

If you encounter an error, see Troubleshooting Administration Console Upgrade.

17 Upgrading Identity Server

In this Chapter

- Upgrading Identity Server
- (Conditional) Upgrading the Database Schema for Risk Service

---

IMPORTANT: If the base operating system is RHEL 7.8, you must first upgrade to Access Manager 5.0, and then upgrade to RHEL 7.9.

17.1 Upgrading Identity Server

Use the following procedure to upgrade stand-alone Identity Server. If you installed Identity Server and Administration Console both on the same machine, see Upgrading Administration Console.

Prerequisites for Upgrading Identity Server

❒ 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 *NetIQ Access Manager 5.0 Administration Guide*.

NOTE: If you have configured risk-based authentication, perform the following steps before you upgrade Identity Server:

- Copy all the custom risk rules and database-connector jars from `/opt/novell/nids/lib/webapp/WEB-INF/lib` to `/opt/novell/rba-core/lib/webapp/WEB-INF/lib`.
- (Conditional) Upgrade the database schema for Risk Service. For more information, see Section 17.2, "(Conditional) Upgrading the Database Schema for Risk Service," on page 175.

---

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 Micro Focus Downloads and extract the `tar.gz` file by using the `tar -xzvf <filename>` command.

> **NOTE:** For information about the name of the upgrade file, see the specific Release Notes.

5 Change to the directory where you unpacked the file, then run the following command in a terminal window:

```
./upgrade.sh
```

6 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)?
```

7 Type **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 **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. For example, `admin`

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 files, add files to the respective locations using Advanced File Configurator:

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

    Also, add the following line to the server.xml file:

```
<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" />
```

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

 ◆ `/opt/novell/nam/idp/conf/tomcat.conf`

NOTE: Post-Upgrade: To avoid any mismatch of customizations seen on Advanced File Configurator user interface and the file present in the VM server, it is recommended to click the

Send Configurations to Servers icon ( ) for all non-temporary files and folders in Identity Server from the Advanced File Configurator user interface. This action must be performed even if file status is displayed as `Configuration sent successfully` on the Advanced File Configurator user interface post-upgrade.

For information about how to add files using Advanced File Configurator, see "Adding Configurations to a Cluster" and how to modify a file, see Modifying Configurationsin the *NetIQ Access Manager 5.0 Administration Guide*.

Important Notes:

 ◆ If you use 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.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 using Advanced File Configurator. See "Modifying Configurations" in the *NetIQ Access Manager 5.0 Administration Guide*

 ◆ 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 NetIQ Access Manager 5.0 Administration Guide.

17.2 (Conditional) Upgrading the Database Schema for Risk Service

If you have configured the risk-based authentication, you must upgrade the database schema for the external database feature to work.

NOTE: It is recommended to run the database schema upgrade script on a non-production database or in a test environment. If any error occurs while upgrading, contact technical support before proceeding.

The upgrade script performs the following actions:

- Modifies few constraints in the `usrtransaction` table (PRIMARY and FOREIGN keys)
- Alters certain indexes
- Modifies certain columns of the table

The upgrade script assumes the same names for the constraints as defined in the original SQL script file (earlier bundled with Access Manager, see in 'nam-upgrade/original/'). However, sometimes the constraint names might be different than the ones used in the SQL script. If you find that the constraint names are different for your instance than what was used in the database creation process, replace the same in the upgrade script with the constraint name that was generated in your instance. To avoid such issues, it is recommended to run the upgrade script on a new test database instance. This ensures that no syntax error occurs while upgrading.

IMPORTANT: Before upgrading the production database, take a backup of the entire `netiq_risk` production database or at least of the `usrtransaction` table.

To upgrade the database schema, perform the following steps after upgrading Identity Server:

1 Download the `RiskDBScripts` package from the following location using Advanced File Configurator:

`/opt/novell/rba-core/lib/webapp/WEB-INF/RiskDBScripts.zip`

For information about how to download a file, see "Downloading Files from a Server" in the *NetIQ Access Manager 5.0 Administration Guide*.

2 Copy the package to your external database server and unzip it by running the following command:

`unzip RiskDBScripts.zip`

3 Go to the `nam-upgrade/upgrade/` directory on your external database and run one of the following scripts based on your database:

- **MySQL:** `netiq_risk_mysql_upgrade_to_risk_service.sql`
- **Microsoft SQL Server:** `netiq_risk_sql_server_upgrade_to_risk_service.sql`
- **Oracle:** `netiq_risk_oracle_upgrade_to_risk_service.sql`

NOTE: It is assumed that you have the basic knowledge of the database.

To validate the schema and table, refer to the following resources:

- **MySQL:** See "*mysqlshow — Display Database, Table, and Column Information*" in the MySQL 5.5 Reference Manual.
- **Microsoft SQL Server:** See View the Table Definition.
- **Oracle:** See Managing Schema Objects.

Troubleshooting the Database Schema Upgrade

The older SQL files, used to create the database in Access Manager 4.5.x or earlier, are available in the `nam-upgrade/original/` directory.

If a constraint violation error occurs, perform the following steps:

1 Verify that the constraint names in your server are the same as used in the upgrade script (`pk_transaction_uuid` and `fk_transction_id`).

  ◆ For MySQL and Microsoft SQL Server, use the following command for fetching constraints:

    `select * from information_schema.table_constraints where table_name = 'usrtransaction';`

  ◆ For Oracle, use the following command for fetching constraints:

    `select * from user_constraints where table_name = 'USRTRANSACTION';`

  Verify the constraint_name column of the above query result is the same as used in the following commands in the upgrade script:

  MySQL:

  ◆ `ALTER TABLE netiq_risk.usrtransaction DROP PRIMARY KEY;`

  ◆ `ALTER TABLE netiq_risk.usrtransaction DROP FOREIGN KEY fk_transction_id;`

  Microsoft SQL Server:

  ◆ `ALTER TABLE usrtransaction DROP CONSTRAINT pk_transaction_uuid;`

  ◆ `ALTER TABLE usrtransaction DROP CONSTRAINT fk_transction_id;`

  Oracle:

  ◆ `ALTER TABLE netiq_risk.usrtransaction DROP CONSTRAINT pk_transaction_uuid;`

  ◆ `ALTER TABLE netiq_risk.usrtransaction DROP CONSTRAINT fk_transction_id;`

2 Similarly, check from the database that the index names being referred in the upgrade scripts have the same identifiers.

18 Upgrading Access Gateway

In this Chapter

- Upgrading Access Gateway Appliance
- Migrating Access Gateway Appliance
- Upgrading Access Gateway Service

IMPORTANT: If the base operating system is RHEL 7.8, you must first upgrade to Access Manager 5.0, and then upgrade to RHEL 7.9.

18.1 Upgrading Access Gateway Appliance

18.1.1 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" on page 183.

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

For information about upgrading from 4.4 to any of the supported upgrade version of Access Gateway, see Upgrading Access Gateway Appliance in the NetIQ Access Manager 4.4 Installation and Upgrade Guide.

NOTE: You cannot directly upgrade from Access Gateway Appliance 4.4.*x* to the latest version.

18.1.2 Upgrading from Access Gateway Appliance 4.5.x

From Access Manager 5.0 onwards, in order to upgrade Access Manager Gateway Appliance you must complete the following actions:

1. Upgrade the base operating system using **Online Update**. For more information, see "Upgrading the base Operating System and Common Appliance Framework" on page 180.

2. Run the product upgrade script. For more information, see "Steps to upgrade from 4.5.x to the latest version of Access Gateway Appliance:" on page 181.

NOTE: You can use the latest upgrade file to upgrade from 4.5.x 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 Section 18.1.1, "Upgrading from Access Gateway Appliance 4.4.x," on page 179.

18.1.2.1 Upgrading the base Operating System and Common Appliance Framework

You must update the base operating system and CAF before upgrading Access Gateway Appliance to the 5.0 version. Perform the following steps:

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

2. Click **Online Update**.

3. Click **Update Now** to apply all patches.

IMPORTANT: For Upgrading Access Gateway Appliance from Access Manager 5.0 to Access Manager 5.0 Service Pack 1 only steps 1-3 are required.

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.

---

4. Click **Product Upgrade** > **Start**.

5. Review and accept the License Agreement.

6. Register for the Online Update Service. For registering for the Online Update Service, see "To register for the Online Update Service:" on page 200.

7. Click **OK** to install all the required updates.

8. In the upper right corner of the Appliance Configuration pane, click **Reboot**.

Verifying the version of the base Operating System and Common Appliance Framework

(Applicable for upgrading Access Gateway Appliance to 5.0)

1 Open a terminal window and log in as the `root` user.

2 Use the following command to check the version of the operating system:

`cat /etc/os-release`

Ensure that the version is SLES 12 SP5.

The output is similar to the following:

```
cat /etc/os-release
NAME="SLES"
VERSION="12-SP5"
VERSION_ID="12.5"
PRETTY_NAME="SUSE Linux Enterprise Server 12 SP5"
ID="sles"
ANSI_COLOR="0;32"
CPE_NAME="cpe:/o:suse:sles:12:sp5"
```

NOTE: If the SLES version points to SLES 12 SP4, run the `zypper up` command to perform upgrade to `grub2-x86_64-xen-2.02-12.47.1.noarch`, `sles-release-12.5-1.171.x86_64`, and `sles-release-POOL-12.5-1.171.x86_64` RPMs. Reboot the system after the upgrade and check the operating system version again using `cat /etc/os-release` command.

3 Use the following command to check the CAF version:

`cat /etc/Novell-VA-base`

Ensure that the version is 2.1.

The output is similar to the following:

```
cat /etc/Novell-VA-base
product=Micro Focus Base Appliance
version=2.1
arch=x86_64
```

NOTE: However, the actual CAF version is 2.0.3. The Configuration console also displays the version number as 2.0.3. The mismatch in version numbers occurs because of the updated `vabase-datamodel-15.1.1-14.1.x86_64 rpm`.

18.1.2.2 Steps to upgrade from 4.5.x 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 Micro Focus Downloads 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. For example, `admin`

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 files, add or merge the backed up files and folders to the respective locations as appropriate using Advanced File Configurator:

- `/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`
  For information about how to merge or modify files, see "Modifying Configurations" in the *NetIQ Access Manager 5.0 Administration Guide*.

18.1.3 Upgrading from Access Gateway Appliance 5.0.*x*

1 Register to Access Gateway Appliance 5.0 update service on the Common Appliance Framework user interface using `https://<IP>:9443` URL. Ignore this step if you have already registered to this service.

NOTE: For information on registration, see "Upgrading the base Operating System and Common Appliance Framework" on page 180.

2 Log in to the Access Gateway terminal as a `root` user.

3 Run command `zypper install nam-ag-channel-meta`.

4 Navigate to the `/opt/novell/channel` directory.

5 Run the `./upgrade_nam.sh` command.

6 Follow the on-screen prompts to complete the upgrade.

18.2 Migrating Access Gateway Appliance

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 provide a new IP address and host name or reuse an existing IP address and host name.

18.2.1 Prerequisites for Migrating Access Gateway Appliance

In addition to the Section 4.2.1, "Prerequisites for Installing Access Gateway Appliance," on page 65, ensure that the following prerequisites are met before migrating Access Gateway Appliance:

❐ Upgrade all instances of Administration Console and Identity Server before migration.

❐ (If the services are managed by an L4 switch) Remove the device, which needs to be migrated, from the L4 switch. This prevents the L4 switch from sending the user requests to that device during migration.

   Ensure to 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.

   If the version of Access Gateway Appliance is prior to 4.4 Service Pack 4, first upgrade from a supported upgrade path to 4.4 Service Pack 4 using the instructions in Upgrading Access Gateway Appliance in the Access Manager 4.4 Installation and Upgrade Guide.

❐ Determine if you want to reuse the existing IP address or a new IP address to setup the system.

❐ For using an existing IP address:

   ◆ Take a backup of the following Access Gateway 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/agm/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/
   ```

- ◆ 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.

- ◆ The number of network interfaces along with their values are same for both the new Access Gateway Appliance and the existing Access Gateway Appliance.

❒ (For using new IP address) Adding the new Access Gateway Appliance in the existing cluster restores 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 these files because these files are not restored automatically.

❒ 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. See Setting Up Firewalls.

❒ 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.

18.2.2 Upgrading from Access Gateway Appliance 5.0.*x*

1 Register to Access Gateway Appliance 5.0 update service on the Common Appliance Framework user interface using `https://<IP>:9443` URL. Ignore this step if you have already registered to this service.

NOTE: For information on registration, see "Upgrading the base Operating System and Common Appliance Framework" on page 180.

---

2 Log in to the Access Gateway terminal as a `root` user.

3 Run command `zypper install nam-ag-channel-meta`.

4 Navigate to the `/opt/novell/channel` directory.

5 Run the `./upgrade_nam.sh` command.

6 Follow the on-screen prompts to complete the upgrade.

18.2.3 Migrating Access Gateway Appliance

Migrating the existing Access Gateway Appliance to new Access Gateway Appliance does 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.x:

- Section 18.2.3.1, "Using the Existing IP Address," on page 185
- Section 18.2.3.2, "Using a New IP Address," on page 186

18.2.3.1 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 4 (4.4 SP4) to Access Manager 5.0. After upgrading Administration Console and Identity Server to 5.0 version, you require to migrate Access Gateway Appliance to the 5.0 version using the existing IP address.

It is assumed that your server meets the system requirements mentioned in *NetIQ Access Manager System Requirements*.

Consider that the setup includes the following components:

- Access Manager 5.0 Administration Console (primary Administration Console: AC 1)
- Access Manager 5.0 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 A G 3)

Migration process:

1 If you are first migrating AG 2 using the existing IP address of AG 2, ensure to perform the following actions:

   1a Shut down AG 2

   1b Ensure that Prerequisites for Migrating Access Gateway Appliance are met

2 Install Access Gateway Appliance (newAGA 2) with the same IP address and hostname as of 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 64.

   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 members of Access Gateway Appliance to Access Gateway Appliance 5.0 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 for Migrating Access Gateway Appliance" on page 183.

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 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.

```
<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 merge the changes to the new server.xml file using Advanced File Configurator. For information about how to add or merge files using the Configuration Files page, see "Managing Configuration Files" in the *NetIQ Access Manager 5.0 Administration Guide*. After upgrading to 5.0, to restore the customization, you can upload the backup files or make the changes in file and add to Advanced File Configurator to make the changes effective.

NOTE: **Post-Upgrade**: To avoid any mismatch of customizations seen on Advanced File Configurator user interface and the file present in the VM server, it is recommended to click the

Send Configurations to Servers icon (⬆) for all non-temporary files and folders in Access Gateway from the Advanced File Configurator user interface. This action must be performed even if file status is displayed as Configuration sent successfully on the Advanced File Configurator user interface post-upgrade.

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 5.0.

6 On the newly added Access Gateway Appliance, restart Tomcat by using the /etc/init.d/ novell-mag restart or systemctl restart novell-mag.service command.

18.2.3.2 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 64.

3 Restore the customized files from the backup taken earlier. For information about how to add or merge files using the Configuration Files page, see "Managing Configuration Files" in the *NetIQ Access Manager 5.0 Administration Guide*.

Use case

You are upgrading Access Manager 4.4 SP2 to Access Manager 5.0. After upgrading Administration Console and Identity Server to 5.0 version, you require to migrate Access Gateway Appliance to the 5.0 version using the new IP address.

This scenario assumes that you have a server with the system requirements as mentioned in *NetIQ Access Manager System Requirements* to install the new Access Gateway Appliance.

Consider that the setup includes the following components:

- Access Manager 5.0 Administration Console (primary Administration Console: AC 1)
- Access Manager 5.0 Identity Server cluster (primary Identity Server: IDP 1 and secondary Identity Server: IDP2)
- Access Manager 4.4 SP2 Access Gateway Appliance cluster (primary Access Gateway: AG 1 and secondary Access Gateway: AG 2).

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). See Installing Access Gateway Appliance.

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 for Migrating Access Gateway Appliance" on page 183.

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, apply the corresponding changes the `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 merge the changed values in the new `server.xml` file. For information about how to add or merge files using the Configuration Files page, see "Managing Configuration Files" in the *NetIQ Access Manager 5.0 Administration Guide*.

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 5.0.

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 `systemctl restart novell-mag.service` command.

18.3   Upgrading Access Gateway Service

- Section 18.3.1, "Prerequisites for Upgrading Access Gateway Service," on page 189
- Section 18.3.2, "To Upgrade Access Gateway Service," on page 190

18.3.1   Prerequisites for Upgrading Access Gateway Service

☐ Manually back up `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.

☐ **(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.

18.3.2 To Upgrade Access Gateway Service

1 Download the `AM_50_AccessGatewayService_Linux_64.tar.gz` file from the Micro Focus download site and extract it by using the following command:

`tar -xzvf <AM_50_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 for Upgrading Access Gateway Service" on page 189.

Restore the customized files from the backup taken earlier. For information about how to add or merge files using the Configuration Files page, see "Managing Configuration Files" in the *NetIQ Access Manager 5.0 Administration Guide*.

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

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 merge the changed values to 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/agm/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 `systemctl restart novell-mag.service` 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.

---

19 Upgrading Analytics Server

You can upgrade to the 5.0 version of Analytics Server only from the early access beta release and the Analytics Server 4.5 Service Pack 3 Hotfix 1 releases.

Hence, you cannot migrate the existing events realtime or offline indices from any earlier version other than the early access beta release and Analytics Server 4.5 Service Pack 3 Hotfix 1 release to the 5.0 version. However, you can use the new Analytics Server along with the earlier Sentinel-based Analytics Server for events to be captured in both until all the data become available in the new dashboard. For this, you need to configure two target servers, one for the old and one for the new Analytics Server. For more information, see "Setting Up Logging Server and Console Events" in the *NetIQ Access Manager 5.0 Administration Guide*.

You cannot launch the old Analytics Server and reports from Administration Console. Instead, you can access the old data using the following direct access links:

- Dashboard: https://<Analytics IP>:8445/amdashboard/login
- Reports: https:// <Analytics IP>:8443/sentinel

IMPORTANT: Before installing the new Analytics Server, ensure to delete Analytics Server nodes of the earlier version from Administration Console. Ensure to use only three node cluster for Analytics Server as two node cluster is no longer supported.

NOTE: For upgrading Analytics Server in the cluster environment, see Section 19.1, "Upgrade Analytics Server Cluster," on page 194.

Use the following procedure to upgrade Analytics Server.

1. Ensure to delete Analytics Server nodes of the earlier version from Administration Console.
2. Open a terminal window.
3. Log in as the `root` user.
4. Download the upgrade file from Micro Focus Downloads and extract the `tar.gz` file by using the `tar -xzvf <filename>` command.

   NOTE: For information about the name of the upgrade file, see the specific Release Notes on the Access Manager Documentation website (https://www.microfocus.com/documentation/access-manager/5.0/).

5. Change to the directory where you unpacked the file, then run the following command in a terminal window:

   ```
   ./ar_upgrade.sh
   ```

6 The system displays the following confirmation message:

```
This will upgrade Analytics Server. Would you like to continue (y/n) ?
[y]:
```

7 Type **Y** and press Enter.

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. For example, `admin`

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.
```

19.1 Upgrade Analytics Server Cluster

Follow the below procedure to upgrade Analytics Server in the cluster environment:

1 Take a snapshot of the data from the primary Analytics Server.

For more information, see Snapshot and Restore.

2 Upgrade the analytics servers one by one, for more information, see Chapter 19, "Upgrading Analytics Server," on page 193.

3 Run `/opt/novell/nam/scripts/restore_elk_objects.sh` script on any one of the nodes.

NOTE: This step is optional if you are upgrading the Analytics Server cluster from 5.0.1 to 5.0.2.

---

20 Upgrading Access Manager Containers

This section includes following topics:

20.1 Upgrading Access Manager Containers

1 Get a list of all the helm deployments present in your kubernetes cluster using the following command:

```
helm list —A
```

2 From the list displayed, select the Access Manager deployment release name as relevant and the deployed namespace. This information will be used during the upgrade.

3 View history of upgrades done on the selected Access Manager release deployment using the following command:

```
helm history <release_name> --namespace <namespace>
```

4 Download the latest Access Manager helm chart, example, `AM_50_HelmChart-1.0.x.tgz`, to the master node from the Software License and Download (https://sld.microfocus.com/) portal.

5 Unzip the helm chart by using the following command for Access Manager:

```
tar -xzvf AM_50_HelmChart-1.0.x.tgz
```

6 Copy all the values from existing Access Manager deployments `values.yaml` file to the recently downloaded `access-manager-1.0.x/values.yaml`.

7 Open the `access-manager-1.0.x/values.yaml` file and edit the following values:

- `am-ac.primary.mode=upgrade`
- If a secondary Administration Console is deployed, then set `am-ac.secondary.mode=upgrade`

8 Run the helm chart to upgrade the deployment, the sample format is as follows:

```
helm upgrade --namespace <name-of-the-namespace> <release-name> access-manager-1.0.x --reuse-values
```

9 Use the following command to verify if all the pods are in ready state after upgrade:

```
kubectl get pods -o wide --namspace <namespace>
```

10 The Helm history is also updated after a successful upgrade. To view the updated data, use the following command:

```
helm history <release_name> --namespace <namespace>
```

20.2   Upgrading Analytics Server Containers

NOTE: The Access Manager release version should be compatible with release version to which you want to upgrade if your are upgrading the Analytics Server. If versions are not compatible, ensure that before upgrading Analytics Server containers, Access Manager containers are upgraded. For more information, see Chapter 20, "Upgrading Access Manager Containers," on page 195 to upgrade Access Manager deployment.

---

1 Get a list of all the helm deployments present in your kubernetes cluster using the following command:

```
helm list -A
```

2 From the list displayed, select the `am-dashboard` deployment release name as relevant and the deployed namespace. This information will be used during the upgrade.

3 View history of upgrades done on the selected `AM-Dashboard` release deployment using the following command:

```
helm history <release_name> --namespace <namespace>
```

4 Download the latest `AM-Dashboard` helm chart, example, *AM_50x_Dashboard_HelmChart-1.0.x.tgz*, to the master node from the Software License and Download (https:// sld.microfocus.com/) portal.

5 Unzip the helm chart by using the following command for Analytics Server:

```
tar -xzvf AM_50x_Dashboard_HelmChart-1.0.x.tgz
```

6 Copy all the values from existing Analytics Server deployments `values.yaml` file to the recently downloaded `am-dashboard-1.0.x/values.yaml`.

7 Run the helm chart to upgrade the deployment, the sample format is as follows:

```
helm upgrade --namespace <name-of-the-namespace> <release-name> am-
dashboard-1.0.x --reuse-values
```

8 Use the following command to verify if all the pods are in ready state after upgrade:

```
kubectl get pods -o wide --namspace <namespace>
```

9 The Helm history is also updated after a successful upgrade. To view the updated data, use the following command:

```
helm history <release_name> --namespace <namespace>
```

21 Post Upgrade Considerations

In this Chapter

21.1 Database Schema Changes for Risk Service

If you have configured the risk-based authentication, you must upgrade the database schema for the external database feature to work. Perform the following actions after the upgrade:

1. Recomplile the custom rules and database-connector jars against the new libraries (NAMCommon.jar, nidp.jar, risk-service-sdk.jar, risk-auth-nidp.jar) and then copy all custom rules and database-connector jars from `/opt/novell/nids/lib/webapp/WEB-INF/lib` to `/opt/novell/rba-core/lib/webapp/WEB-INF/lib`.

   NOTE: NIDPlog and RiskLog are not supported.

2. (Conditional) Upgrade the Database Schema for Risk Service.

21.2 Configuration Files-specific Changes

- **nidp.jar:** Access Manager 5.0 onwards, modification of `nidp.jar` is not recommended. If you have modified `nidp.jar` in the earlier release, then move those properties to nidp_custom_resources_*.properties as instructed in "To Customize Identity Server Messages" and upload the properties file to the Identity Server cluster using Advanced File Configurator. See "Adding Configurations to a Cluster" in the *NetIQ Access Manager 5.0 Administration Guide*.

  The jsp_resources_<language>.properties files are now placed in `/opt/novell/nam/idp/webapp/nidp/WEB-INF/classes/com/novell/nidp/resource/jsp/` and can be directly modified using Advanced File Configurator.

  You do not need to extract `nidp.jar`. If you have customized "jsp_resources_<language>.properties" in the previous release, extract `nidp.jar` and copy it from `nidp.jar` to `/opt/novell/nam/idp/webapp/nidp/WEB-INF/classes/com/novell/nidp/resource/jsp`.

- **Advanced Authentication Plug-in file:** The `config.xml` file is moved from `/etc/aaplugin` to `/opt/novell/nam/idp/plugins/aa/`.

- **Syslog configuration files:**

File Name	Access Manager 4.5.x and earlier	Access Manager 5.0
nam.conf	/etc/rsyslog.d/	/opt/novell/syslog/rsyslog.d/
Auditlogging.cfg	/etc/	/opt/novell/syslog/rsyslog.d/

- **JCC file:** The following files are moved from `/opt/novell/devman/jcc/conf` to `/opt/novell/devman/jcc/conf/runtime`:

  clientlist.dat
  alertdispatch.dat
  tmp.dat
  jcc.keystore
  jcc.keystore.original
  jcc_devman.keystore
  keystore_info.xml
  keystore_info.xml.original
  Settings.properties

21.3 Changes in Identity Server and Access Gateway Processes

After upgrading to Access Manager 5.0, the Identity Server and Access Gateway processes running as the root user changes to a non-root user. To run the processes as the root user, see Java Communication Channel Processes Run as Non-Root User After Upgrading to Access Manager 5.0.

21.4 Schema Changes of Attributes

After upgrading to Access Manager 5.0, the object type of attributes changes from octet to stream. This update is made to accommodate larger values in attributes.

22 Getting the Latest OpenSSL Updates for Access Manager

The OpenSSL open source project team regularly releases updates to known OpenSSL vulnerabilities. Access Gateway uses the OpenSSL library for cryptographic functions. It is recommended that you keep Access Gateway 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 SP5.

❒ If you want to install the security updates 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 Software Licenses and Downloads.

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.

22.1 Installing or Updating Security Patches for Access Gateway Appliance

Use the **Online Update** option to register to the online update service from Software Licenses and Downloads. It will get you the latest security updates for Access Manager Appliance. You can select to install updates automatically or manually.

If you want to control the updates further, you can configure Access Gateway Appliance to get the updates from a local Subscription Management Tool (SMT). This allows you to download the updates to a single SMT server in your network and all other nodes of Access Gateway Appliance receive updates from this server. For more information, see *Subscription Management Tool Guide (https://www.suse.com/documentation/smt11/book_yep/data/book_yep.html)*. To obtain the proper credentials to use the SMT server, see "Mirroring Credentials (https://www.suse.com/documentation/smt11/book_yep/data/smt_mirroring_getcredentials.html)" in the *Subscription Management Tool Guide (https://www.suse.com/documentation/smt11/book_yep/data/book_yep.html)*.

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 Micro Focus Customer Center 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.

22.2 Updating Security Patches for Access Gateway Service

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-4.2.2-
1.0.2x
```

NOTE: This downloads the 1.0.2x 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 Micro Focus Customer Center Portal the product is registered with.

23 Upgrade Assistant

Online Update Service enables you to get the latest Access Manager product updates. The Upgrade Assistant feature simplifies the usage of this Update Service.

Using this feature, you can perform the following actions on Administration Console:

- Register to Update Service for all devices
- Receive updates when a new release of Access Manager is available.
- View the list of all devices, available updates, their versions, and registration status
- Invoke the Update Service registration for an individual device
- Deregister Update Service

The following diagram illustrates how to use this feature:

| Get the activation key from Customer Center or set up the local SMT server | Register to Update Service | Ensure that all devices are auto-configured | Get notified when a new release of Access Manager is available | Upgrade the product |
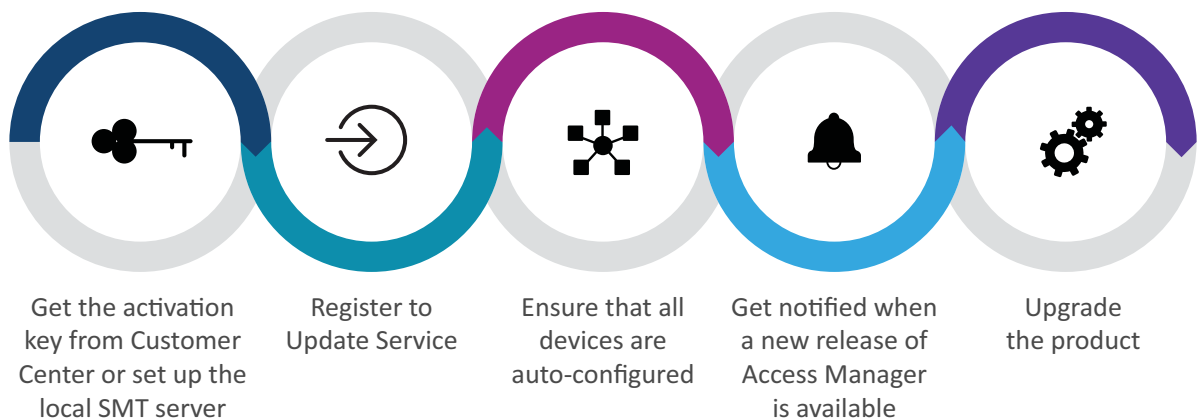
Video

The following video demonstrates how to register to Upgrade Assistant and use it for upgrading the product:

http://www.youtube.com/watch?v=RActAIMhNg8

NOTE: Upgrade Assistant supports the following upgrades:

- A major release version to a service pack (such as 5.0 to 5.0 Service Pack 1)
- A service pack to a service pack (such as 5.0 Service Pack 1 to 5.0 Service Pack 2)
- A service pack to a major release version (such as 5.0 Service Pack 3 to 5.1)

Upgrade Assistant does not support a patch upgrade to a service pack or major release version.

In this section:

NOTE: For troubleshooting information, see Troubleshooting Upgrade Assistant.

How Upgrade Assistant Works

To use the Upgrade Assistant feature, you must register to one of the following services:

- Micro Focus Customer Center on SLES
- Register using Local Repository on RHEL

When you register to any of these services, all devices get registered to Update Service. The new devices are also auto-registered as part of the import process.

Auto-registration while adding a new device into Administration Console works only when the device and Administration Console have the same Access Manager versions installed. Auto-registration does not work in a hybrid environment.

If a device is not registered for the update, you can register it on the Device Status page. For more information, see Registering a Single Device to Update Service.

When a new Access Manager Release is available, you can view the release details in **Available Updates** table.

Click **Device Status** to view various statuses of each device, such as whether the device is on the latest version or any update is pending.

If updates are pending on a device, you can update the device to the latest available Access Manager release version. Follow steps in Upgrading Access Manager through Upgrade Assistant.

You can de-register the service for all devices or an individual device by clicking **Deregister** on the Upgrade Assistant page or on the Device Status page respectively. After de-registering, you can re-register.

The **Upgrade Assistant** agent works with the default certificate. You can change this to the device certificate by re-pushing the certificate. Re-push the connector certificate of devices and keystore of Administration Console. After the certificates are re-pushed, restart the **Upgrade Assistant** agent by running the restart command to apply the certificate changes.

To restart the **Upgrade Assistant** agent, perform the following steps:

1. In Administration Console, click **Troubleshooting**.
2. Click **Certificates**.
3. Select **SSL Connector** for devices.
4. Select **Administration Console Keystore** for Administration Console.

5. Click **Re-push certificates**.

6. Run the `systemctl restart novell-ua-agent.service` command.

Prerequisites before using Upgrade Assistant

❒ Upgrade Assistant is enabled on licensed version of Access Manager.

❒ The Tomcat service and JCC service are up and running on all the devices.

❒ All devices are time synchronized for the registration and upgrade processes to get complete successfully.

❒ The Upgrade Assistant agent service is up and running before you start the upgrade process using the `systemctl status novell-ua-agent` command.

❒ A new port 9968 is opened in firewall and is only used to communicate internally (within Administration Console). This port must not be accessible from the external network due to security reason.

❒ No zypper/yum process or zypper/yum cron job is running on the system during the registration or upgrade process.

❒ To register to Micro Focus Customer Center: You must have obtained the activation key for the product from Micro Focus Customer Care.

❒ To register by using local repository on RHEL: You must have access to a mirror repository of the Access Manager Product channel.

Important Notes

◆ You can use Upgrade Assistant in Access Manager 5.0 and later only.

◆ It is recommended to use Upgrade Assistant in the primary Administration Console only.

◆ For SLES setups, it is recommended to open only one Administration Console tab in any browser. Opening Administration Console in multiple browsers at the same time might cause issues in managing the `am.prod` symbolic link. For more information about the `am.prod` symbolic link, see "Managing the am.prod Symbolic Link on SLES" on page 211.

◆ Upgrading Access Manager 5.0.x to Access Manager 5.0 Service Pack 2 must be done from the command line only. For more information, see "Registration in Access Manager 5.0 or 5.0 Service Pack 1" on page 207.

◆ Upgrading Access Manager 4.5.x to Access Manager 5.0.x must be done using `tar.gz`.

Registering to Micro Focus Customer Center on SLES

Ensure that you have obtained the activation code for Access Manager from Micro Focus Customer Center.

Perform the following steps to register to Micro Focus Customer Center:

1 On Administration Console Dashboard, click **Upgrade Assistant** > **Register**.

2 Specify the following details:

Field	Description
Channel Type	Select **Micro Focus Customer Center**.
Email	Specify your email address to which the updates will be sent.
Activation Key	Specify the activation key that you have obtained for the product from Micro Focus Customer Care.

3 Click **OK**.

> **NOTE:** If you are registering in Access Manager 5.0 or in Access Manager 5.0 Service Pack 1, you need to manage the `am.prod` symbolic link. For more information, see Managing the am.prod Symbolic Link on SLES.

Registration Using Local Repository on RHEL

On the RHEL system, you need to create a local repository of Access Manager. Perform the following steps to register to the local repository:

1 On Administration Console Dashboard, click **Upgrade Assistant > Register**.

2 Specify the following details:

Field	Description
Repository Name	Default Repository Name is `AM-5.0-Product.`
Base URL	Specify Access Manager's local URL to which you want to register. The valid URL format is: https://<Mirror_ID>:<Repository_key>@nu.novell.com/repo/$RCE/AM-5.0-Product/sle-15-x86_64/ The URL is appended with 'repodata/repomd.xml' automatically and it is verified for its validity. An error is displayed on the user interface if the URL is invalid.
Repository is Enabled	By default, Access Manager's repository (`AM-5.0-Product`) used for getting Online Updates will be enabled post-registration.
GPG Check	By default, GPG check for Access Manager's repository is disabled.

3 Click **OK**.

You can use Upgrade Assistant from Access Manager 5.0 Service Pack 2 onwards. To register in Access Manager 5.0 or 5.0 Service Pack 1 release, see "Registration in Access Manager 5.0 or 5.0 Service Pack 1" on page 207.

Registering using Local SMT on SLES

On SLES, you can register using local SMT.

Prerequisites to set up Local SMT

NOTE: Before performing the following steps, ensure that Access Manager is installed on the same machine.

Perform the following steps to setup Local SMT:

1. Navigate to **yast** > **Software** > **Add System Extensions or Modules** > **Web and Scripting Module 12 x86_64** to enable Web Scripting repositories.

   You can also enable Web Scripting repositories through CLI. Run the following commands:

   SLES 12:

   ```
   SUSEConnect -p sle-module-web-scripting/12/x86_64
   ```

   SLES 15:

   ```
   SUSEConnect -p sle-module-web-scripting/<version>/x86_64
   ```

2. Extract the tar ball and change the directory to `smt_packages`.

   For example: `cd /home/novell-access-manager-5.0.3.0-118/smt_packages`

3. Run the `ua_smt_packages.sh` script as a root or root equivalent user.

Local SMT on SLES

On SLES system, you need to create a local repository of the Access Manager product.

Perform the following steps to register to the local repository:

1. On the Administration Console Dashboard, click **Upgrade Assistant > Register**.

2. Select **Local SMT**.

3. Provide the required host details and click **OK**.

Registration in Access Manager 5.0 or 5.0 Service Pack 1

If you are using Access Manager 5.0 or 5.0 Service Pack 1 on the RHEL server, perform the following steps on each device:

1 Create file `/etc/yum.repos.d/nam.repo` and update the following information:

```
[AM-5.0-Product]
name=AM-5.0-Product
baseurl=https://<Mirror_ID>:<Repository_key>@nu.novell.com/repo/$RCE/
AM-5.0-Product/sle-15-x86_64/
enabled=1
gpgcheck=0
```

2 Assign the `novlwww:novlwww` ownership to the file by using the following command:

```
chown novlwww:novlwww /etc/yum.repos.d/nam.repo
```

3 Assign the following permission:

```
chmod 644 /etc/yum.repos.d/nam.repo
```

4 Verify if the Access Manager repository is added successfully by using the following command:

```
yum repolist
```

The `AM-5.0-Product` will be listed in the repository list.

5 Verify if `AM-5.0-Product` can fetch the available updates by using the following command:

```
yum list updates | grep AM-5.0-Product
```

Perform the following procedure if you have registered to Access Manager's Online Update Service in Access Manager 5.0 or 5.0 Service Pack 1 and you have upgraded to Access Manager 5.0 Service Pack 2.

1 Verify `/etc/yum.repos.d/nam.repo` has `nowlwww:novlwww` ownership and 644 file permission by using the following command:

```
ll /etc/yum.repos.d/nam.repo
```

The sample output will look similar to the following:

```
-rw-r-----. 1 novlwww novlwww 143 Mar 11 10:35 /etc/yum.repos.d/
nam.repo
```

2 If the `/etc/yum.repos.d/nam.repo` file ownership and file permission are not as expected, then run the following commands:

To assign expected ownership:

```
chown novlwww:novlwww /etc/yum.repos.d/nam.repo
```

To assign file permission on each device:

```
chmod 644 /etc/yum.repos.d/nam.repo
```

3 If a repository is created with a name such as `xyz.repo` instead of `nam.repo`, then delete the file from all devices.

4 Log in to Administration Console and register by using Upgrade Assistant by following the procedure mentioned in "Registration Using Local Repository on RHEL" on page 206. Use the same base URL that you used in Access Manager 5.0 or 5.0 Service Pack 1.

After successful synchronization of registration information into Administration Console, in the Access Manager 5.0 Service Pack 2 or later, you can use Upgrade Assistant to receive future Access Manager release updates and to update devices to the latest Access Manager version.

Registering a Single Device to Update Service

You can invoke the registration for an individual device in the following scenarios:

- If a new secondary Administration Console is added.
- An issue occurred during the auto-registration of a device.

Perform the following steps to register an individual device:

1 On Administration Console Dashboard, click **Upgrade Assistant** > **Device Status**.

2 Click the **Register** icon associated with the device which you require to register to Update Service.

Upgrading Access Manager through Upgrade Assistant

Whenever a new Access Manager release is available, you can view the new release details, such as latest Access Manager release version and its description, on the Upgrade Assistant page. You can also view the latest available version for each device on **Upgrade Assistant > Device Status** page.When

Access Manager release updates are available for any of the devices, the Update icon ⊕ on the **Device Status** page is enabled for the respective devices. Clicking the **Update** icon will start the update process in a new tab called Upgrade Console. Once the update process is complete successfully, the **Update Status** of the device will display as **Up to date** in green color on **Device Status** page.

When a user initiates an upgrade from Upgrade Assistant, a default backup of configuration is taken during the upgrade at `/root/nambkup/` and the default certificate encryption password is `password`.

NOTE: When you are on 5.0 Service Pack 2, and if 5.0 Service Pack 3 updates are available in the repository, the **Available Updates** still displays the description of the previous version. Ignore this description and consider the `Version`.

Upgrading from Access Manager 5.0 or 5.0 Service Pack 1

To upgrade from Access Manager 5.0 to Access Manager 5.0 Service Pack 2, follow steps 1 to 5.

To upgrade from Access Manager 5.0 Service Pack 1 to Access Manager 5.0 Service Pack 2, follow steps 2 to 5.

1 Navigate to the `/opt/novell/channel` directory. You can install `meta.rpm` for Administration Console, Access Gateway, Analytics Dashboard, and Identity server manually by using the following procedure. On the SLES setup, change the symbolic link to `am.prod` before proceeding with following steps. For more information, see "Managing the am.prod Symbolic Link on SLES" on page 211.

   ◆ For Administration Console, run the command [SLES] `zypper install nam-ac-channel-meta` or [RHEL] `yum install nam-ac-channel-meta`

   ◆ For Identity Server, run the command [SLES] `zypper install nam-idp-channel-meta` or [RHEL] `yum install nam-idp-channel-meta`

   ◆ For Access Gateway, run the command [SLES] `zypper install nam-ag-channel-meta` or [RHEL] `yum install nam-ag-channel-meta`

   ◆ For Analytics Dashboard, run the command [SLES] `zypper nam-dashboard-channel-meta` or [RHEL] `yum install nam-dashboard-channel-meta`. If you are upgrading from Access Manager 5.0 or Access Manager 5.0 SP1, remove the old RPM and install the new RPM. Remove the old meta RPM by using the command, `zypper rm -y nam-dashboard-channel-meta` for SLES and `yum remove -y nam-dashboard-channel-meta` for RHEL.

   NOTE: After performing step 1, the `/opt/novell/channel/upgrade_assistant` folder is not available. This is an expected behavior. The folder will be ready after step 3.

   ---

2 The following upgrade procedure is identical for all components. After upgrading Administration Console, repeat the same process for Identity Server, Access Gateway, and Analytics Server. Open a terminal window and log in as the root user.

Navigate to the `/opt/novell/channel` directory.

3 Run the `./upgrade_nam.sh` command.

4 Follow the on-screen prompts to complete the upgrade.

Upgrading Access Manager using Major Version Update

You can update to the next major release using the **Major Version Update** option from **Upgrade Assistant**. For example, if you are on 5.0 Service Pack 3, using the **Major Version Update** option you can update to the next major release.

You can either update to the next major version or continue with the existing service pack.

NOTE: After you have updated to the next major version using the **Major Version Update** option, you cannot revert to the previous service pack. The **Major Version Update** option is enabled from 5.0 Service Pack 3.

To use the **Major Version Update** option, you have to first register your device using the **Upgrade Assistant**. See "Registering to Micro Focus Customer Center on SLES" on page 205 and "Registration Using Local Repository on RHEL" on page 206.

After the registration is complete, you can view the **Registration Status** and **Available Updates** for each device.

Perform the following steps:

1. On the Administration Console, click **Upgrade Assistant** > **Device Status**.

   You can view if the registration is successful or not. The upgrades for the current and available version are displayed.

2. Click **Major Version Update**. The following instructions are displayed:

For SLES

Click **OK** to update the currently registered repository to a new repository. To register for the available major version of Access Manager, obtain the activation key from Micro Focus Customer Center. After you register to the major version, you cannot revert to the earlier version.

For RHEL

Click **OK** to update the currently registered repository to a new repository. After you register to the major version, you cannot revert to the earlier version.

3. Click **OK**.

After the release update is successful, a message `Subscription to major available version is successful. Please reregister` is displayed. You will be de-registered from the earlier version and redirected for registering to the new major version. See Registering to Micro Focus Customer Center on SLES and Registration Using Local Repository on RHEL.

Managing the am.prod Symbolic Link on SLES

Follow the procedure while upgrading using Upgrade Assistant from Access Manager 5.0 or Access Manager 5.0 Service Pack 1 to Access Manager 5.0 Service Pack 2.

1 Change the base product symbolic link to `am.prod` by using the following command:

`ln -sf /etc/products.d/am.prod /etc/products.d/baseproduct`

2 Register using Micro Focus Customer Center. For more information, see Registering to Micro Focus Customer Center on SLES.

3 Verify if any product upgrades are available.

4 Run the `/opt/novell/channel/upgrade_nam.sh` script.

5 After the upgrade is complete for all the devices, change the symbolic link to `SLES.prod` for all devices.

6 For using Upgrade Assistant for Access Manager 5.0 Service Pack 2, deregister and re-register from the user interface.

`ln -sf /etc/products.d/SLES.prod /etc/products.d/baseproduct`

7 View **Device Status** to see any updates and continue with the upgrade.

Upgrade Assistant Limitations

- If the registration is already done successfully, but later the Access Manager product repository is deleted from the back- end, Upgrade Assistant continues to display status as registered. However, there might be disruptions in receiving updates from Access Manager Online Update Service. To start receiving the updates again, you must deregister and then re-register on the Upgrade Assistant page.

- Upgrade Assistant is not support when Administration Console and Identity Server are deployed on the same machine.

- Upgrade Assistant is not supported for Access Manager deployed using docker containers, Access Gateway Appliance, and Access Manager Appliance. For more information about how to upgrade Access Manager on docker and Access Gateway Appliance, see Upgrading Access Manager Appliance and Upgrading Access Manager Containers.

- Identity Server details are displayed in Upgrade Assistant's device status page even after Identity Server is uninstalled using the `uninstall.sh` script.

  To overcome this issue, you must delete Identity Server after `uninstall.sh` is executed successfully. To delete Identity Server, click **Devices** > **Identity Server > Servers Actions** > **Delete**.

  After deleting Identity Server, details from Upgrade Assistant's device status page are removed.

- Dashboard registration across operating system platforms is not supported. For example, a dashboard installed on RHEL cannot be registered to Access Manager Online Update Service if it is imported into a SLES Administration Console.

24 Migrating Access Manager from Windows to RHEL

Access Manager 5.0 and later versions do not provide Windows-based installers. To leverage the latest features and functionalities available with version 5.0 Service Pack 1 or later, you can migrate Access Manager from Windows to RHEL.

To migrate to Access Manager 5.0 Service Pack 1 and later, you need to be on one of the following versions of Access Manager:

- 4.5 Service Pack 4
- 4.5 Service Pack 3 Patch Update 3
- 4.5 Service Pack 3 Patch Update 2
- 4.5 Service Pack 3 Hotfix 1
- 4.5 Service Pack 3
- 4.5 Service Pack 2 Hotfix 2
- 4.5 Service Pack 2 Hotfix 1
- 4.5 Service Pack 2

Migrate the Access Manager components in the following sequence:

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

NOTE: Access Manager 5.0 and later does not support Kerberos Constrained delegation (KCD).

In this Chapter

- Migrating Administration Console from Windows to RHEL
- Migrating Identity Server from Windows to RHEL
- Migrating Access Gateway from Windows to RHEL

24.1 Migrating Administration Console from Windows to RHEL

- Prerequisites for Migrating Administration Console
- Supported Migration Scenarios
- Migrating Primary Administration Console
- Migrating Secondary Administration Console

24.1.1 Prerequisites for Migrating Administration Console

In addition to the following prerequisites, ensure that you also meet the hardware and software requirements for Administration Console. See *NetIQ Access Manager System Requirements*.

❒ A new IP address that will be used temporarily during the primary Administration Console migration.

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

   If the **Enable Timeout Per Protected Resource** option has already been applied, it is not displayed.

❒ The time of primary and secondary Administration Consoles time is synchronized. You can ensure this by configuring the machines to use the same network time server for time synchronization.

❒ The health status for all devices in Administration Console is green.

   For more information, see "Monitoring Server Health" in the *NetIQ Access Manager 5.0 Administration Guide*.

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

❒ The required ports are opened in the firewall. For more information about ports, see Section 1.8.1, "Required Ports," on page 31.

❒ Note down the contracts selected under the **Satisfies contract** list of SAML 2.0 and Liberty identity providers. These are under **Devices** > **Identity Servers** > **Edit** > **[Protocol]** > **[Identity Provider]** > **Authentication Card**.

   You must manually configure these contracts after migration. This configuration will be effective after the Identity Server migration is done.

❒ The hostname of the new 5.0.x Administration Console must be different from the existing 4.5.x primary and secondary Administration Consoles.

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

❒ Ensure that the following RHEL RPMs are installed on the machine:
   - ncurses-libs.i686
   - createrepo
   - yum-utils
   - ntp
   - glibc.i686
   - nss-softokn-freebl.i686
   - libgcc.i686
   - libstdc++.i686
   - rsyslog.x86_64
   - rsyslog-gnutls.x86_64
   - unzip

- bind-utils
- net-tools
- zip
- net-snmp
- expat

For installing RHEL packages manually, see *Installing Packages and Dependent RPMs on RHEL for Access Manager*.

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.

24.1.2   Supported Migration Scenarios

Identify the scenario that best describes your migration environment and review the appropriate steps before you begin the process of migration.

- Administration Console, Identity Server, and Access Gateway Service Are Installed on Different Servers
- Administration Console and Identity Server Are on the Same Server, and Access Gateway Service Is on a Different Server
- Secondary Administration Console and Identity Server Are on the Same Server
- Administration Console and Identity Server Are on the Same Server

Administration Console, Identity Server, and Access Gateway Service Are Installed on Different Servers

1 Migrate the primary Administration Consoles.

2 Migrate Identity Server.

3 Migrate Access Gateway Service.

Administration Console and Identity Server Are on the Same Server, and Access Gateway Service Is on a Different Server

1 Migrate the primary Administration Console.

2 Migrate Identity Server.

3 Migrate Access Gateway Service.

Secondary Administration Console and Identity Server Are on the Same Server

1 Migrate the primary Administration Console.

2 Migrate the secondary Administration Console.

3 Migrate Identity Server.

Administration Console and Identity Server Are on the Same Server

1 Migrate Administration Consoles.

2 Migrate Identity Server.

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

To do this run the `system-config-network` command from the terminal. Use the **Device Configuration** option to configure the interfaces.

24.1.3 Migrating Primary Administration Console

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

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

1 Back up the 4.5.x primary Administration Console configuration by using `C:\Program Files\Novell\bin\ambkup.bat`.

2 Copy the backup zip file to `/tmp` or any other folder on the new RHEL machine where you plan to install 5.0.x Administration Console.

3 Download the installer file from Micro Focus Downloads and extract the tar.gz file using the `tar -xzvf <filename>` command.

   For example, `tar -xzvf novell-access-manager-5.0.1.0-760.tar.gz`

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

5 Run the `install_and_migrate.sh` script from the folder to migrate the primary Administration Console from 4.5.x to 5.0.x.

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

7 Type `Y` and press `Enter` when the installation confirmation message is displayed.

8 Specify the following details:

   ◆ Access Manager 4.5.x primary Administration Console IP address

   ◆ Access Manager administration user ID

   ◆ Access Manager administration password. Re-enter the password for verification.

9 Specify `1` in replica number.

10 Select the 5th replica option from the list when prompted.

   5. Designate this server as the new master replica

11 Type `I Agree` when prompted.

12 Specify the administrator name and password. The name must be in leading dot notation. For example, **.admin.novell**

13 Remove the eDirectory replica ring of the Windows server.

    13a Run the `/opt/novell/eDirectory/bin/ndsrepair -P -Ad -a` command. This step might take about 5-7 minutes.

    13b Specify `1` when prompted to enter a replica number.

    13c Specify `10` (10. View Replica Ring).

    13d Specify `1` to remove the Windows replica.

    13e Specify `6` (6. Remove this server from replica ring).

    13f Specify the administrator's username and password. The username must be in leading dot notation. For example, **.admin.novell**

    13g Specify `I Agree` when prompted.

    The Windows replica is removed.

    13h Run the `- ndsstat -r` command and verify whether the Windows replica is removed.

14 Shut down 4.5.x Administration Console.

15 Change the IP address of 5.0.x Administration Console to the old primary Administration Console IP address.

    15a On the 5.0.x Administration Console machine, go to `/etc/sysconfig/network-scripts/`.

    15b Open the `ifcfg-Profile_1` file and replace the IP address with the old Windows Administration Console IP address.

    15c Open the `/etc/hosts` file and replace the IP address with the old Windows Administration Console IP address.

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

17 Specify `Y` for `Would you like to continue this installation (y/n)?`.

18 Specify the location of the 4.5.x backup file with an absolute path. For example, `/tmp/<filename>`.

19 Specify the username and password for decrypting the backup file.

20 Specify Access Manager administration username and password.

21 Continue with "Removing Windows Administration Console Objects" on page 217.

Removing Windows Administration Console Objects

Remove any traces of Windows 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 Windows Administration Console. You should find the following types of objects:

- SAS Service object with the hostname of Windows Administration Console
- An object that starts with the last octet of the IP address of Windows Administration Console
- DNS AG object with the hostname of Windows Administration Console
- DNS IP object with the hostname of Windows Administration Console
- SSL CertificateDNS with the hostname of Windows Administration Console
- SSL CertificateIP with the hostname of Windows Administration Console
- NCP server object

5 Run the `/opt/novell/eDirectory/bin/ndsstat -r` command to view the list of available replicas. If you still see the replica that you deleted from **Other Known Device Manager Servers**, continue with Step 6.

6 (Conditional) 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**.

24.1.4 Migrating Secondary Administration Console

Perform a fresh installation of Administration Console. See "Installing Secondary Administration Console" in the *NetIQ Access Manager 5.0 Administration Guide*.

24.2 Migrating Identity Server from Windows to RHEL

- Prerequisites for Migrating Identity Server
- Supported Migration Scenario
- Migrating Identity Server

24.2.1 Prerequisites for Migrating Identity Server

❏ Ensure that the system meets the requirements for Identity Server.

For information about the requirements, see *NetIQ Access Manager System Requirements*.

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

❏ The time of Identity Server is synchronized with the time of Administration Console.

❏ Ensure that Administration Console is running. See Installing Administration Console.

❒ If you installed Administration Console on a separate machine, ensure that the DNS names resolve between Identity Server and Administration Console.

❒ Ensure that the following ports are open on both Administration Console and Identity Server:

8444
1443
1289
1290
524
636

For information about ports, see Configuring the Administration Console Firewall.

❒ 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.

❒ Ensure that the following RHEL RPMs are installed on the machine:
- ncurses-libs.i686
- createrepo
- yum-utils
- ntp
- glibc.i686
- nss-softokn-freebl.i686
- libgcc.i686
- libstdc++.i686
- rsyslog.x86_64
- rsyslog-gnutls.x86_64
- unzip
- bind-utils
- net-tools
- zip
- net-snmp
- expat

For installing RHEL packages manually, see *Installing Packages and Dependent RPMs on RHEL for Access Manager*.

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)

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

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

For more information about delegated users, "Managing Delegated Administrators" in the *NetIQ Access Manager 5.0 Administration Guide*.

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

❒ Back up the customized files.

24.2.2   Supported Migration Scenario

◆ Using the Existing IP Address
◆ Using a New IP Address

Using the Existing IP Address

1. Back up the customized files on the Access Manager 4.5.x setup.
2. Note down the IP address of Windows Identity Server.
3. Stop and remove Identity Server from the cluster on the Windows machine.
4. Delete Identity Server that is removed from the Identity Servers cluster.
5. Switch off the Windows machine.
6. On the RHEL machine, change the IP address to the IP address of Windows Identity Server that you noted in step 2.
7. On the RHEL machine, use the NetIQ Access Manager 5.0.x installer to install Identity Server.
8. Add 5.0.x Identity Server to the existing Identity Server cluster in 5.0.x Administration Console on RHEL.
9. Update Identity Server and apply changes.
10. Restore customized files from the backup taken earlier.

Using a New IP Address

1. Back up the customized files on the Access Manager 4.5.x setup.
2. Use the NetIQ Access Manager 5.0.x installer to install Identity Server on the RHEL machine.
3. Add Identity Server to the existing Identity Server cluster in 5.0.x Administration Console on RHEL.
4. Update Identity Server and apply changes.
5. Restore any customized files from the backup taken earlier.
6. Delete older Identity Servers on the Windows machine.

24.2.3 Migrating Identity Server

NOTE: If you are migrating Identity Server using a new IP address, skip Step 1 to Step 5.

1 **(When using the existing IP address)** Note down the IP address of Windows Identity Server.

2 **(When using the existing IP address)** Remove the existing Identity Server from Administration Console on the Windows machine.

   Do not delete the Identity Server cluster as this will be used later.

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

   2b Select the server and click **Stop**.

   2c Select the server > **Actions > Remove from cluster**.

   2d Update the cluster configuration.

3 **(When using the existing IP address)** Delete Identity Server that is removed from the Identity Servers cluster.

4 **(When using the existing IP address)** Switch of the Windows machine on which 4.5.x Identity Server was installed.

5 **(When using the existing IP address)** On the RHEL machine, change the IP address.

   5a Go to `/etc/sysconfig/network-scripts/`.

   5b Open the `ifcfg-Profile_1` file and change the IP address to the IP address noted in Step 1.

   5c Open the `/etc/hosts` file and change the IP address to the IP address noted in Step 1.

   5d Reboot the machine.

   5e SSH to the RHEL machine with the changed IP address.

6 On the RHEL machine, download the installer file from Micro Focus Downloads, extract the tar.gz file by using the `tar -xzvf <filename>` command, and change to the `novell-access-manager` directory.

7 At the command prompt, run `./install.sh`.

8 When prompted to install a product, specify `2`, **Install Identity Server**, and press Enter.

   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 information about configuring NAT, see Configuring Administration Console Behind NAT.

9 Specify `Y` to proceed.

10 Review and accept the license agreement.

11 Verify that the required RPMs are of the latest versions. Specify `Y` to proceed.

12 Specify the IP address, user ID, and password of 5.0.x Administration Console that is migrated to RHEL.

13 Specify the IP address of 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.

14 Go to the migrated Administration Console and verify whether this Identity Server is added.

15 Restore customized files from the backup taken earlier. To restore files, add files by using Advanced File Configurator to the locations listed in the following table:

For information about how to add files by using Advanced File Configurator, see "Adding Configurations to a Cluster" in the *NetIQ Access Manager 5.0 Administration Guide*.

Location on Windows	Location on RHEL
`C:\Program Files\Novell\Tomcat\conf\server.xml`	`/opt/novell/nam/idp/conf/server.xml`
`C:\Program Files\Novell\Tomcat\conf\web.xml`	`/opt/novell/nam/idp/webapps/nidp/WEBINF/web.xml`
`C:\Program Files\Novell\Tomcat\webapps\nidp\config`	`/opt/novell/nam/idp/webapps/nidp/config`
`C:\Program Files\Novell\Tomcat\webapps\nidp\images`	`/opt/novell/nam/idp/webapps/nidp/images`
`C:\Program Files\Novell\jre\lib\security\bcsLogin.conf.template`	`/opt/novell/java/jre/lib/security/bcslogin.conf`
`C:\Program Files\Novell\Tomcat\webapps\nidp\jsp`	`/opt/novell/nam/idp/webapps/nidp/jsp`
`C:\Program Files\Novell\Tomcat\webapps\nidp\WEB-INF\classes`	`/opt/novell/nam/idp/webapps/nidp/WEBINF/classes`

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

For more information, see "Configuring Identity Servers Clusters" in the *NetIQ Access Manager 5.0 Administration Guide*.

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

17 On the newly added Identity Server, restart Tomcat by using the `/etc/init.d/novell-idp restart` or `systemctl restart novell-idp.service` command.

18 Repeat these steps to add other Identity Servers to the Identity Server cluster.

24.3 Migrating Access Gateway from Windows to RHEL

- Prerequisites for Migrating Access Gateway
- Supported Migration Scenario
- Migrating Access Gateway

24.3.1   Prerequisites for Migrating Access Gateway

❒ Ensure that the system meets the requirements for Access Gateway.

For information about the requirements, see *NetIQ Access Manager System Requirements*.

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

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

❒ You have physical access to the server or server console (in case of VMWare setups) as a root user and are familiar with firewall configurations. The required ports must be opened in the firewall. For more information about the ports, see Section 1.8.1, "Required Ports," on page 31.

❒ Ensure that you have migrated all Administration Consoles and Identity Servers before migrating Access Gateway Service.

❒ Back up all customized files.

❒ Verify that the time on the machine is synchronized with the time on Administration Console. If the times differ, Access Gateway Service is not imported to 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.

❒ Ensure that the following RHEL RPMs are installed on the machine:
   - ncurses-libs.i686
   - createrepo
   - yum-utils
   - ntp
   - glibc.i686
   - nss-softokn-freebl.i686
   - libgcc.i686
   - libstdc++.i686
   - rsyslog.x86_64
   - rsyslog-gnutls.x86_64
   - unzip
   - bind-utils
   - net-tools
   - zip
   - net-snmp
   - expat

For installing RHEL packages manually, see *Installing Packages and Dependent RPMs on RHEL for Access Manager*.

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.

❑ 2 to 10 GB hard disk space per reverse proxy that requires caching and for log files. The amount varies with rollover options and the 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.

❑ Other Access Manager components must not be installed on the same machine.

24.3.2   Supported Migration Scenario

◆ Migrating Access Gateway Using an Existing IP Address

◆ Migrating Access Gateway Using a New IP Address

Migrating Access Gateway Using an Existing IP Address

1. Back up the customized files on the Access Manager 4.5.x setup.

2. Note down the IP address and hostname of Windows Access Gateway.

3. Switch off the Windows device.

4. On the RHEL machine, change the IP address and hostname to the IP address and hostname of Windows Access Gateway that you noted in step 2.

5. On the RHEL machine, use the NetIQ Access Manager 5.0.x installer to install Access Gateway using the existing IP address you noted in step 2.

6. On the Administration Console RHEL machine, go to the `novell-access-manager` folder and run `sh scripts/migrate_post_ag.sh`.

7. Provide the username and password of the Administration Console administrator.

8. Restart Access Gateway.

9. Restart Administration Console.

10. Update Access Gateway and apply changes.

11. Restore any customized files from the backup taken earlier.

Migrating Access Gateway Using a New IP Address

1. Back up the customized files on the Access Manager 4.5.x setup.

2. Use the NetIQ Access Manager 5.0.x installer to install Access Gateway on RHEL.

3. Add the newly installed Access Gateway with a new IP address to the existing Access Gateway cluster in the migrated Administration Console.

4. Update Access Gateway and apply changes.

5. Restore any customized files from the backup taken earlier.

6. Convert the newly added Access Gateway node to the master node.

7. Delete the older Access Gateway on Windows.

24.3.3 Migrating Access Gateway

1 **(When using the existing IP address)** Note down the IP address and hostname of 4.5.x Access Gateway on the Windows machine.

2 **(When using the existing IP address)** Switch of the Windows machine on which 4.5.x Access Gateway is installed.

3 **(When using the existing IP address)** On the RHEL machine, change the IP address and hostname.

   3a Go to `/etc/sysconfig/network-scripts/`.

   3b Open the `ifcfg-Profile_1` file and change the IP address to the IP address that you noted in Step 1.

   3c Open the `/etc/hosts` file and change the IP address and hostname to the IP address and hostname that you noted in Step 1.

   3d Open the `/etc/hostname` file and change the hostname to the hostname you noted in Step 1.

   3e Reboot the machine.

   3f SSH to the RHEL machine with the changed IP address.

4 On the RHEL machine, download the installer file from Micro Focus Downloads, extract the tar.gz file by using the `tar -xzvf <filename>` command, and change to the `novell-access-manager` directory.

5 At the command prompt, run `./ag_install.sh`.

6 Review and accept the License Agreement.

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

8 Specify the IP address, user ID, and password of the migrated Administration Console.

9 **(When using the existing IP address)** Specify the existing IP address of Access Gateway that you noted in Step 1.

   (When using a new IP address) Specify the IP address of Access Gateway.

10 Go to the migrated Administration Console and verify whether this Access Gateway is added.

11 Add the newly installed Access Gateway to the existing Access Gateway cluster.

   For more information, see "Access Gateways Clusters" in the *NetIQ Access Manager 5.0 Administration Guide.*

   The cluster object stores all the existing Access Gateway configurations. The newly added Access Gateway inherits these configurations.

12 Convert the newly added Access Gateway node to the master node.

   12a Click **Devices** > **Access Gateways** > **[Name of Cluster]** > **Edit**.

   12b In the **Primary Server** list, select Access Gateway and click **OK**.

13 Delete the older Access Gateway on Windows.

14 **(When using the existing IP address)** Perform the following steps on the Administration Console RHEL machine:

   14a Run `sh scripts/migrate_post_ag.sh`.

   14b Specify the username and password of the Administration Console administrator.

   14c Restart Access Gateway by running the `/etc/init.d/novell-appliance` restart command.

   14d Restart Administration Console by running the `/etc/init.d/novell-ac restart` command.

15 Restore customized files from the backup taken earlier. To restore files, add files by using Advanced File Configurator to the locations listed in the following table.

   For information about how to add files by using Advanced File Configurator, see "Adding Configurations to a Cluster" in the *NetIQ Access Manager 5.0 Administration Guide*.

Location on Windows	Location on RHEL
`C:\Program Files\Novell\Tomcat\conf\web.xml`	`/opt/novell/nam/mag/conf/web.xml`
`C:\Program Files\Novell\Tomcat\webapps\nesp\WEB-INF\web.xml`	`/opt/novell/nam/mag/webapps/nesp/WEB-INF/web.xml`
`C:\Program Files\Novell\Tomcat\webapps\nesp\jsp`	`/opt/novell/nam/mag/webapps/nesp/jsp`
`C:\Program Files\Novell\Tomcat\webapps\nesp\html`	`/opt/novell/nam/mag/webapps/nesp/html`
`C:\Program Files\Novell\Tomcat\webapps\nesp\images`	`/opt/novell/nam/mag/webapps/nesp/images`
`C:\Program Files\Novell\Tomcat\webapps\agm\WEB-INF\config\current`	`/opt/novell/nam/mag/webapps/agm/WEB-INF/config/current`
`C:\Program Files\Novell\Tomcat\webapps\nesp\config`	`/opt/novell/nam/mag/webapps/nesp/config`

Repeat these steps to add other Access Gateways to the Access Gateway cluster.

IMPORTANT: 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 the `sysctl -p` command to update changes.

4. Start Apache.

V Troubleshooting Installation and Upgrade

- Troubleshooting Installation
- Troubleshooting Upgrade

25 Troubleshooting Installation

25.1 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.

25.2 (RHEL) The Health Status of Administration Console, Identity Server, and Access Gateway after Installation Is Not Green

The status of the Administration Console, Access Gateway, and Identity Server after installation is not green post installation. Administration Console might display the timed-out error and might not be accessible using a web browser. Identity Server and Access Gateway might display an `Unable to read keystore` error message. This issue occurs if SELinux is enabled on your system. To resolve this issue, you have to enable the Permissive mode.

To enable the Permissive mode, perform the following steps:

1 Open the `config` file located in the `/etc/sysconfig/selinux` directory.

2 Reconfigure SELINUX with edirectory. You must set SELinux to permissive mode on RHEL 9 and above. See eDirectory Install Guide.

3 Save the change.

4 Restart the system.

25.3 Troubleshooting Identity Server Import and Installation

25.3.1 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, 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 233.

25.3.2 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 *NetIQ Access Manager 5.0 Administration Guide*.

4 On the Identity Server machine, change to the `jcc` directory:

`/opt/novell/devman/jcc`

5 Run the following script to configure jcc:

`./conf/reimport_nidp.sh jcc`

6 Run the following reimport script:

`./conf/reimport_nidp.sh nidp`

7 If these steps do not work, reinstall the device.

25.3.3 Check the Installation Logs

Installation logs are located in the `/tmp/novell_access_manager` directory.

Table 25-1 *Installation Log Files for Identity Server*

Log File	Description
`install_idp_<date&time>.log`	Contains the messages generated for Identity Server module.
`install_main_<date&time>.log`	Contains the Tomcat messages generated during the installation.
`install_jcc_<date&time>.log`	Contains the messages generated for the communications module.

25.4 Access Gateway Appliance Installation Fails Due to an XML Parser Error

This error might happen if Access Gateway Appliance is installed by using a remotely mounted installer. Use a locally mounted installer to avoid this issue.

25.5 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, repair the import.

If the repair option does not resolve the problem, see the following sections:

- Section 25.5.1, "Repairing an Import," on page 234
- Section 25.5.2, "Troubleshooting the Import Process," on page 234

25.5.1 Repairing an Import

If Access Gateway does not appear in Administration Console within 10 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 235.

7 If triggering an import retry does not solve the problem, reinstall the device.

25.5.2 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 25.5.2.1, "Understanding the Import Process," on page 234
- Section 25.5.2.2, "Locating the Log Files," on page 235
- Section 25.5.2.3, "Triggering an Import Retry," on page 235

25.5.2.1 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.

25.5.2.2 Locating the Log Files

Various Access Manager components produce log files. Use the following logs on Administration Console or Access Gateway:

- Administration Console log: `/opt/novell/devman/share/logs/app_sc.0.log`
- Tomcat Log on Administration Console: `/opt/novell/nam/device name/logs/catalina.out`

  The device name can be `idp`, `mag`, or `adminconsole`.

- JCC log on Access Gateway: `/opt/novell/devman/jcc/logs/`

25.5.2.3 Triggering an Import Retry

1 Go to the `/opt/novell/devman/jcc/` directory:

2 Run the `sh conf/reimport_ags.sh jcc` script.

Specify details against the following prompts:

- Choose a local listener IP address [x.x.x.x]:
- (Optional) Choose a local NAT IP address [optional]:
- Choose Administration Console's IP address []:
- Enter Admin User's DN [cn=admin,o=novell]:
- Enter Admin Password: *****

  Wait for a few minutes for the configuration to finish.

3 Run the `sh conf/reimport_ags.sh agm` script.

For example, if the username is *admin*, then run conf\reimport_ags.bat agm admin

Specify details against the following prompts:

- (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).
- (Linux) Enter Admin User's DN [cn=admin,o=novell]:
- Enter Admin password:

25.6 Troubleshooting Access Manager Container Deployment

- Administration Console Pod Does Not Deploy in Azure Kubernetes Services
- Checking the Status of Access Manager Resources
- Debugging Pods
- Unable to Use a Release Name
- Kubernetes Gives Error Messages While Retrieving Information About Pods
- Unable to Connect to the DNS Server
- Performance and Stability Issues Because Swap is Enabled
- Communication Between the Kubernetes Master Node and Worker Node Fails
- Health Check of Access Gateway Activemq Fails

25.6.1 Administration Console Pod Does Not Deploy in Azure Kubernetes Services

While creating the Azure Kubernetes Services (AKS) cluster, Azure, by default, creates a certain number of systems with default system names and configurations. The Administration Console pod does not get deployed in the AKS cluster when the system name exceeds 32 characters.

Workaround: Append the `--nodepool-name` string while running the `az aks create` command.

For example, `az aks create --resource-group <resource-group-name> --name <AKS-cluster-name> --node-count 3 --nodepool-name n --generate-ssh-keys --attach-acr <ACR-name>`

25.6.2 Checking the Status of Access Manager Resources

After you run the Access Manager helm chart, the helm chart gets deployed, and a message `STATUS: deployed` is displayed. However, the Access Manager resources do not get deployed immediately. To check the status of the resources, you must run some commands.

To check the status of the Access Manager pods, run the following command:

```
kubectl get --namespace <name-of-the-namespace> pods
```

To check the status of all the Access Manager resources, run the following command:

```
kubectl get --namespace <name-of-the-namespace>
statefulset,pods,pv,pvc,svc,ingress
```

For information about viewing the logs, see Section 25.6.3, "Debugging Pods," on page 236.

25.6.3 Debugging Pods

Run the following command to view the names of the Access Manager pods:

```
kubectl get pods -n <name-of-the-namespace>
```

To view the configuration logs of the Access Manager pods, run the following commands:

- **Administration Console:** `kubectl logs -f pod/<name-of-the-administration-console-pod> am-ac --namespace <name-of-the-namespace>`
- **eDirectory:** `kubectl logs -f pod/<name-of-the-administration-console-pod> am-edir --namespace <name-of-the-namespace>`
- **Identity Server:** `kubectl logs -f pod/<name-of-the-identity-server-pod> --namespace <name-of-the-namespace>`
- **Access Gateway:** `kubectl logs -f pod/<name-of-the-access-gateway-pod> --namespace <name-of-the-namespace>`
- **Analytics Server:** `kubectl logs -f pod/<name-of-the-analytics-dashboard-pod> --namespace <name-of-the-namespace>`

To get inside a pod, run the following commands:

- **Administration Console:** `kubectl exec -it pod/<name-of-the-administration-console-pod> -c am-ac bash --namespace <name-of-the-namespace>`
- **eDirectory:** `kubectl exec -it pod/<name-of-the-administration-console-pod> -c am-edir bash --namespace <name-of-the-namespace>`
- **Identity Server:** `kubectl exec -it pod/<name-of-the-identity-server-pod> bash --namespace <name-of-the-namespace>`
- **Access Gateway:** `kubectl exec -it pod/<name-of-the-access-gateway-pod> bash --namespace <name-of-the-namespace>`
- **Analytics Server:** `kubectl exec -it pod/<name-of-the-analytics-dashboard-pod> bash --namespace <name-of-the-namespace>`

To retrieve more information about each pod, run the following commands:

- **Administration Console:** `kubectl describe pod/<name-of-the-administration-console-pod> --namespace <name-of-the-namespace>`
- **Identity Server:** `kubectl describe pod/<name-of-the-identity-server-pod> --namespace <name-of-the-namespace>`
- **Access Gateway:** `kubectl describe pod/<name-of-the-access-gateway-pod> --namespace <name-of-the-namespace>`
- **Analytics Server:** `kubectl describe pod/<name-of-the-analytics-dashboard-pod> --namespace <name-of-the-namespace>`

25.6.4 Unable to Use a Release Name

Cannot use a Release Name that is currently in use.

Workaround: Uninstall the release.

1 View the available releases:

`helm list -n <name-of-the-namespace>`

2 Uninstall the release:

`helm uninstall --namespace <name-of-the-namespace> <release-name>`

25.6.5 Kubernetes Gives Error Messages While Retrieving Information About Pods

Running the `kubectl describe pod` command can throw the following error messages:

◆ probe errored: rpc error: code = DeadlineExceeded desc = context deadline exceeded

◆ pod has unbound immediate PersistentVolumeClaims

Workaround: Ignore the message.

25.6.6 Unable to Connect to the DNS Server

After deploying, Access Gateway nodes display warnings that the nodes cannot connect to the DNS server.

Workaround: Check and rectify the Container Network Interface (CNI) plugin configuration, or deploy Access Manager again with another CNI plugin applied to the Kubernetes cluster.

25.6.7 Performance and Stability Issues Because Swap is Enabled

This issue can occur if Swap is enabled on the host machine.

Workaround: Disable Swap by one of the following ways:

◆ Use the `swapoff -a` command.

Or,

◆ Open the `/etc/fstab` file, and comment out the swap entry.

25.6.8 Communication Between the Kubernetes Master Node and Worker Node Fails

This issue can occur if you revert the master node. However, the worker nodes still assume the connection with the old master node.

Workaround:

1 Run the following command to retrieve a token from the master node:

```
//get token - kubeadm token create --print-join-command
```

2 Remove the following files from the worker nodes:

◆ ca.crt

```
// sudo rm /etc/kubernetes/pki/ca.crt
```

◆ kubelet.conf

```
// sudo rm /etc/kubernetes/kubelet.conf
```

3 Delete the worker nodes:

3a Run commands:

```
kubectl drain <name-of-the-node> --ignore-daemonsets
```

```
kubectl delete node <name-of-the-node>
```

3b Repeat the previous step for all the nodes.

4 Connect the master node with the worker nodes:

```
// kubeadm join <master-node-IP>:6443 --token n5hxyu.v0wzsc0zk9rosohw --discovery-token-ca-cert-hash sha256:4e891f83f3aaa75832d8a955e25ed50111d6bc3b26146180e2c4d48f9fa5556d
```

25.6.9 Health Check of Access Gateway Activemq Fails

This issue occurs when the host entries are not available.

Workaround: Add the host entries to the worker nodes.

25.7 Troubleshooting Analytics Server

25.7.1 Dashboard Login Fails After Applying An External Signed Certificate to the Administration Console

Access Manager Dashboard returns `Login Failure. Invalid Username or Password` after assigning an external signed x509 Certificate to the Administration Console.

Issue: Dashboard server is missing the Trusted Root Certificate chain in order to validate the external signed / issued certificate running with the administration console server. Using iManager to assign an external signed certificate to the Administration Console service will not add the required Root Certificates to the Dashboard servers truststore: `/opt/novell/devman/jcc/conf/runtime/jcc_devman.keystore`. Adding the required Root Certificates to the Access Manager Certificates = > Trusted Roots will not add certs into the `/opt/novell/devman/jcc/conf/runtime/jcc_devman.keystore`.

Resolution: Use the following steps to manually add the missing Root Certificates into `/opt/novell/devman/jcc/conf/runtime/jcc_devman.keystore`.

1 SSH to your dashboard server.

2 Create a backup copy of the existing `/opt/novell/devman/jcc/conf/runtime/jcc_devman.keystore`

3 Obtain the required password to access the keystore:

3a `cd /opt/novell/devman/jcc/conf`

3b `./ksinfo.sh dump | grep -a2 "jcc_devman.keystore"`

3c Use Keystore Explorer to add the required certificates.

NOTE: Opening the `/jcc_devman.keystore` you will be prompted for the keystore password which we discovered from above mentioned steps.

3d Save the changes and restart Analytics Server.

25.7.2 Intermittent Issue With Cluster Configuration

At times the nodes create their own cluster instead of joining the Elasticsearch cluster. In case the Elasticsearch cluster health displays red color in Administration Console user interface for any of the nodes, follow the steps on non-primary nodes only:

1 Stop the Elasticsearch service in all the nodes where cluster health is displaying red color. Do not stop the service on the primary server.

2 Run the `/opt/novell/nam/scripts/configure_cluster.sh` script on all the non-primary nodes one by one which display the cluster health in red color.

25.8 Rsyslog Fails to Start After Access Manager Installation

Scenario:

Installing the Access Manager installs the updated version of rsyslog and its dependencies. In some cases, the dependencies may not be updated to the latest version as compared to rsyslog. This results in failure to start rsyslog.

Workaround:

Update the ryslog dependency, `libfastjson` to the latest version using `zypper` or `yum` depending on RHEL or SUSE respectively.

NOTE: Updating the Operating System may also result in failure to start rsyslog.

26 Troubleshooting Upgrade

In this Chapter

26.1 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:

1 Click **Devices** > **Access Gateways** > **Edit** > **Advanced Options**.
2 Specify `ProxyErrorOverride off`.
3 Click **OK**.

26.2 Troubleshooting Administration Console Upgrade

26.2.1 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 whether the upgrade should continue. 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 to lists all the files created in the specified directory:

   ```
   tail -f /tmp/novell_access_manager/<file-name>
   ```

   4c Restart the upgrade process.

26.2.2 Multiple IP Addresses

If your server has multiple IP addresses, you might see the following message during upgrading 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 `/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, `driver=mdbds referral=10.10.123.45`.

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.

26.2.3 Certificate Command Failure

Certificate commands are generated when you upgrade Administration Console. Ensure that this process has been completed successfully. Click **Security** > **Command Status**.

If a certificate command fails, note the store, click **Troubleshooting** > **Certificates**. Select the store, then click **Re-push certificates** to push the certificates to the store.

26.3 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 might occur because of some eDirectory issues. You can run the script again. If you access the console remotely, run the script from the machine directly.

26.4 Issue in SSL Communication between Access Gateway and Web Applications

After upgrading Access Manager, applications are not accessible. This issue happens when any discrepancy exists between cipher suites configured for Access Gateway and applications protected by this Access Gateway.

To workaround this issue, see TID 7016872.

26.5 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.

26.6 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 when the compatibility mode is enabled.

To workaround this issue, perform the following steps:

1 Modify the nidp_latest.jsp file.

   For information about how to modify a file, see "Modifying Configurations" in the *NetIQ Access Manager 5.0 Administration Guide*.

2 Add the following entry in the file:

```
response.setHeader("X-UA-Compatible","IE=edge"); after the first <%.
```

Example, add `response.setHeader("X-UA-Compatible","IE=edge");` after

```
<%
```

```
        final String NIDP_JSP_CONTENT_DIV_ID = "theNidpContent";
```

For more information, see TID 7022722.

26.7 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 `context.xml` file if you have customized it.

2 After upgrading Access Manager, add the customized content to the upgraded 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>
```

For more information about how to modify a file, see "Modifying Configurations" in the *NetIQ Access Manager 5.0 Administration Guide*.

26.8 Changes Required in server.xml for Apache Tomcat 8.5.51 after Upgrading to Access Manager 4.5 Service Pack 2

Access Manager 4.5 Service Pack 2 (4.5.2) adds support for Apache Tomcat 8.5.51. This version adds a secret required attribute to the Apache JServ Protocol (AJP) Connector. For fresh Access Manager installations, this string is specified in the `server.xml` file as secret= *"namnetiq"* by default. You do not need to make any change to `server.xml` in this regard.

However, the Tomcat service might not get loaded if you upgrade an existing Access Manager setup to 4.5.2 and Tomcat to version 8.5.51. You might see the following error in the `Tomcat` `catalina.log` file:

```
SEVERE [main] org.apache.catalina.core.StandardService.startInternal
Failed to start connector [Connector[AJP/1.3-8009]]
    org.apache.catalina.LifecycleException: Protocol handler start failed
          Caused by: java.lang.IllegalArgumentException: The AJP Connector
is configured with secretRequired="true" but the secret attribute is either
null or "". This combination is not valid.
'
```

To workaround this issue, after upgrading Tomcat to version 8.5.51, perform the following steps:

1 Modify Access Gateway server.xml.

   For information about how to add a file or folder using the Configuration File page, see "Modifying Configurations" in the *NetIQ Access Manager 5.0 Administration Guide*.

2 Add the `secret required` attribute. Set it to *true* by specifying a a non-null or non-zero length string.

NOTE: The value of this `secret required` attribute must be same in `server.xml` files of each component.

For example:

Embedded Service Provider configuration:

```
<Connector port="9009" enableLookups="false" redirectPort="8443"
protocol="AJP/1.3" address="127.0.0.1" minSpareThreads="25"
maxThreads="600" backlog="0" connectionTimeout="20000"
packetSize="65536" maxPostSize="65536" secret="namnetiq" />^M
```

Administration Console:

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"
secret="namnetiq" />
```

Identity Server:

```
<Connector URIEncoding="utf-8" port="8009" protocol="AJP/1.3"
redirectPort="8443" secret="namnetiq" useBodyEncodingURI="false"/>

<Connector address="127.0.0.1" backlog="0" connectionTimeout="20000"
enableLookups="false" maxPostSize="2097152" maxThreads="600"
minSpareThreads="25" port="9019" protocol="AJP/1.3" scheme="https"
secure="true" secret="namnetiq" />^M
```

The following are examples of `Apache vhost.d/*`snippets:

Embedded Service Provider configuration:

```
ProxyPass /AGLogout ajp://127.0.0.1:9009/nesp/app/plogout secret=namnetiq
ProxyPass /nesp ajp://127.0.0.1:9009/nesp secret=namnetiq

ProxyPass /AGLogout ajp://127.0.0.1:9009/nesp/app/plogout secret=namnetiq
  ProxyPass /nesp ajp://127.0.0.1:9009/nesp secret=namnetiq
```

26.9 Access Gateway Fails to Start After Upgrading SLES 11 SP3 to SLES 12

If you upgrade the operating system for all devices from SLES 11 SP3 to SLES 12, Access Gateway fails to start. The following error message is displayed:

```
/opt/novell/apache2/sbin/httpd: error while loading shared libraries:
libpcrc.so.0: wrong ELF class: ELFCLASS32
```

This happens because Access Gateway dependencies do not get copied during an operating system upgrade.

Workaround: Reinstall Access Gateway or create the following symbolic links at Access Gateway server:

```
ln -s /usr/lib64/libpcre.so.1.2.1 /usr/lib64/libpcre.so.0
ln -s /usr/lib64/libdb-4.8.so /usr/lib64/libdb-4.5.so
ln -s /usr/lib64/libodbc.so.2.0.0 /usr/lib64/libodbc.so.1
ln -s /usr/lib64/libesmtp.so.6 /usr/lib64/libesmtp.so.5
```

26.10 Java Communication Channel Processes Run as Non-Root User After Upgrading to Access Manager 5.0

After upgrading to Access Manager 5.0, the Java Communication Channel (JCC) processes run as a non-root user in Identity Server and Access Gateway. You can revert the changes to run the process as a root user using the following procedure, which is applicable for both SLES and RHEL operating system:

Access Manager Non-Docker Deployment

1 Go to the `/etc/systemd/system/novell-jcc.service` directory.

2 Remove the following lines:
   - `User=novlwww`
   - `Group=novlwww`

3 Execute the following commands:
   - `systemctl daemon-reload`
   - systemctl restart <service_name>

4 Reboot the Identity Server machine.

Access Manager Docker Deployment

Perform the following steps:

1 In Administration Console Dashboard, click **Advanced File Configurator**.

2 Select **Administration Console**.

3 Click the plus icon (╶┼╴) > **Edit Configurations on the Server**, and specify the following details:

Field	Description
Type	1. Select **File**. 2. Select `novell-jcc.xml` in **File Name**. 3. **File Path** displays the default location for the selected file. Example: `/opt/novell/devman/jcc/bin`
Cluster Name	This option does not apply to Administration Console.
Source	Select the device from which you want to import the file, and click **Fetch File**.

Field	Description
File	Click **File Editor** and perform the following steps: 1. Search for `<RUN_AS=novlwww>`. 2. Modify the value to `RUN_AS=root`. 3. Click **Save**.
Restart *Administration Console*	By default, this option is turned on for novell-jcc. Do not turn it off. You will be prompted to restart Administration Console after sending the configuration change to devices.
Temporary Modification	Turn off the toggle to retain this configuration change in the next Access Manager upgrade.
Modification Type	Select the type of modification from the list. You can specify the type manually if the list does not contain the required type. You can later use this information to search for files that are updated for a specific type. For example, you can search for all files for which **Modification Type** is `Security Setting`.
Description	Specify the details of the changes you have made in the file. As you might require to update the configurations many times over the period, you can use these details to track when and what changes were done in the file. You can also use this information as criteria to search for specific files.

4 Click **OK**.

5 Select `novell-jcc`l that you have modified.

6 Click the **Send Configurations to Servers** icon ().

7 Click **OK**.

8 Restart the service using `/etc/init.d/novell-jcc restart`.

26.11 Rsyslog Fails to Start After Access Manager Upgrade

Scenario:

Upgrading the Access Manager upgrades rsyslog and its dependencies. In some cases, the dependencies may not be updated to the latest version as compared to rsyslog. This results in failure to start rsyslog.

Workaround:

Update the ryslog dependency, `libfastjson` to the latest version using `zypper` or `yum` depending on RHEL or SUSE respectively.

NOTE: Updating the Operating System may also result in failure to start rsyslog.

26.12 (Kubernetes) OSP/OAuth2-based Authentication Fails after Upgrading Access Manager

This issue occurs when Access Manager integrated with Advanced Authentication is upgraded. After the upgrade is completed, the pods do not retain the host entries of the Advanced Authentication server. This results in the broken OSP/OAuth2-based authentication.

This is the default behavior of Kubernetes. To resolve this issue, you need to perform one of the following workarounds for Access Manager. No need to make any change in the Advanced Authentication configuration.

Workaround 1: Add the required host entries on worker nodes or on the DNS server configured on workers before installing or upgrading Access Manager. Thus whenever you install or upgrade Access Manager integrated with Advanced Authentication, all pods can resolve DNS.

Workaround 2: Perform the following steps if the entries need to be added inside Access Manager pods:

1 Before the upgrade, note down the host entries of the Advanced Authentication server from Administration Console, Identity Server, and Access Gateway pods.

2 After the upgrade, add the same host entries that you noted before the upgrade to the Administration Console, Identity Server, and Access Gateway pods.

NOTE:

- This issue does not occur when Access Manager is integrated with Advanced Authentication using the IP address.
- By design of Kubernetes, each time when a pod spawns, it inherits the content of /etc/hosts of the worker node.

26.13 Troubleshooting Upgrade Assistant

Troubleshooting Using Log Files

Log File Path	Troubleshooting Information
`/var/opt/novell/nam/logs/adminconsole/tomcat/catalina.out`	**Device:** Primary Administration Console **Purpose:** Captures logs for all user actions performed from Upgrade Assistant available in Primary Administration Console. Use it as first step of debugging for any failure or error message displayed on Upgrade Assistant User Interface.

Log File Path	Troubleshooting Information
`/var/opt/novell/nam/logs/jcc/jcc-0.log.0`	**Device:** Identity Server, Access Gateway, Analytics Server
	Purpose: Captures device registration/de-registration logs.
`/var/opt/novell/nam/logs/ua_registration/registration.log`	**Device:** All devices
	Purpose: Captures device registration/de-registration logs.
`/var/opt/novell/nam/logs/ua_registration/suse_register.log`	**Device:** All devices
	Purpose: Captures logs for `suse_register` command execution which is used in registration.
`/var/opt/novell/nam/logs/ua_agent/application.log`	**Device:** All devices
	Purpose: Captures logs of `novell-ua-agent.service`.
`/tmp/novell_access_manager`	**Device:** All devices
	Purpose: Has upgrade logs which are generated after upgrade process is complete.

Troubleshooting Using Error Messages

The following sections include important error messages along with required actions:

- **Error Message:** `Failed to fetch status from novell-ua-agent service`

  Description: This messages is displayed in scenarios where Primary Administration Console is unable to fetch Upgrade Assistant agent's status from respective devices and communication between Primary Administration Console and Upgrade Assistant agent service is disrupted. Few example scenarios where this can happen:

  - Upgrade Assistant agent service is down.
  - Upgrade Assistant agent service is disabled.
  - Some failure happened during Upgrade Assistant Agent service upgrade and agent service is unable to come up in active state.

  Workaround:

  Use the following command to validate that Upgrade Assistant agent service is up and running on the device:

  `systemctl status novell-ua-agent`

  Restart the service using the following command:

  `systemctl restart novell-ua-agent`

Log in to the Administration Console and check if you are able to resolve this error message and if you are able to initiate upgrade successfully. Keep the `/var/opt/novell/nam/logs/ua_agent/application.log` and `/var/opt/novell/nam/logs/adminconsole/tomcat/catalina.out` log files available for troubleshooting.

- **Error Message:** `Unexpected failure. Please check Administration console log at /var/opt/novell/nam/logs/adminconsole/tomcat/catalina.out.`

  Description: This message is displayed in scenarios where Primary Administration Console does not receive a response from the application (AMService/JCC/Upgrade Assistant agent service).

  Workaround: Use the Primary Administration Console's `catalina.out` file to troubleshoot and resolve the issue accordingly.

- **Error Message:** `Failed to get details about available updates.`

  Description: This message is displayed in scenarios where Primary Administration Console fails to receive updates from Access Manager Online update service to which user has registered.

  Workaround: Ensure that Access Manager Product Channel is accessible and updates are available in the Product Channel. You can use Primary Administration Console's `catalina.out` log to further troubleshoot the issue.

- **Error Message:** `You cannot continue using Upgrade Assistant. Stop any zypper process running on the system OR You cannot continue using Upgrade Assistant. Stop any yum process running on the system.`

  Description: This message is displayed when there is already a `zypper/yum` process or a `zypper/yum` cron job running on the system and user access Upgrade Assistant User Interface. To resolve this, stop the `zypper/yum` process or `zypper/yum` cron job and then access Upgrade Assistant User Interface and perform further operations using Upgrade Assistant. Once you are done using Upgrade Assistant, you can restart the `zypper/yum` process or `zypper/yum` cron job.

- **Error Message:** `Upgrade Failed/Update Failed.`

  Description: This message comes when update process fails due to either of mentioned reasons:

  - The `upgrade_nam.sh` script has failed
  - The `novell-ua-agent` service has issues.

  Workaround:

  - For `upgrade_nam.sh` script failures, check upgrade logs at `/tmp/novell_access_manager`.
  - For issues in `novell-ua-agent` service, restart service using command `systemctl restart novell-ua-agent`. After service is restarted, re-try update from Upgrade Assistant user interface.

- **Error Message:** `WARNING: Killing process`

  Description: By default, the Update Service registration timeout is four minutes. If the registration process takes longer than four minutes, registration fails and the error message is logged in the `JCC` log.

  Workaround: To fix this issue, based on your setup, increase the timeout value in the registration API request body and retry the registration through the *POST /nps/rest/ua/channel Content-Type: application/json* API.

```
{
    "sType":"microFocusCustomerCenter",
    "email":<"email ID">,
    "activationKey":<"activation key">,
    "timeout":240 #in seconds
}
```

The following is an example JSON to set the timeout value to five minutes:

```
{
    "sType":"microFocusCustomerCenter",
    "email":"ht@dfsdf.com",
    "activationKey":"sdfsdff",
    "timeout": 300
}
```

NOTE: Contact Micro Focus customer center if you are unable to successfully troubleshoot any issue using the workarounds mentioned in this section.

26.13.1 An Issue with SLES Registration and Updates After Installing or Upgrading Access Manager

Installing or upgrading to Access Manager 5.0 and Access Manager 5.0 Service Pack 1 might hinder fetching updates from the SLES updates channel.

This issue might occur if `/etc/products.d/baseproduct` is symbolically linked to the `/etc/products.d/am.prod` file instead of the `/etc/products.d/SLES.prod` file. For example,

```
ll /etc/products.d/

total 8

-rw-r--r-- 1 root root 2912 Nov  9  2019 SLES.prod

-rwxr-xr-x 1 root root  818 Aug  4 16:39 am.prod

lrwxrwxrwx 1 root root    9 Aug  5 13:04 baseproduct -> /etc/products.d/
am.prod
```

Workaround: To avoid this issue, perform the following steps:

1 Register to the SLES updates channel before installing or upgrading Access Manager 5.0 and Access Manager 5.0 Service Pack 1 and ensure that SLES updates are being fetched as expected.

2 Before installing and upgrading to Access Manager 5.0 and Access Manager 5.0 Service Pack 1, ensure that the `/etc/products.d/baseproduct` file is symbolically linked to `/etc/products.d/SLES.prod` file. For example,

```
ll /etc/products.d/

total 8

-rw-r--r-- 1 root root 2912 Nov  9  2019 SLES.prod

lrwxrwxrwx 1 root root    9 Aug  5 13:04 baseproduct -> SLES.prod
```

3 If a symbolic link is not present between `/etc/products.d/baseproduct` and `SLES.prod`, then run the following commands:

```
cd /etc/products.d
```

`rm baseproduct` command removes the symbolic link from baseproduct.

    `ln -s SLES.prod baseproduct command` creates a symbolic link between baseproduct and SLES.prod.

4 Install or upgrade to Access Manager 5.0.x.

5 Ensure that a symbolic link between `/etc/products.d/baseproduct` and `SLES.prod` exists post-install or upgrade. Run the following command to validate:

`ll /etc/products.d`

Example result:

```
ll /etc/products.d/

total 8

-rw-r--r-- 1 root root 2912 Nov  9  2019 SLES.prod

-rwxr-xr-x 1 root root  818 Aug  4 16:39 am.prod

lrwxrwxrwx 1 root root    9 Aug  5 13:04 baseproduct -> SLES.prod
```

To use Upgrade Assistant:

Change the `/etc/products.d/baseproduct` symbolic link from `SLES.prod` file to `/etc/products.d/am.prod`:

Commands:

`cd /etc/products.d/`

Verify the baseproduct symbolic link before changing it using the following command:

`ll`

Remove the symbolic link from baseproduct using the following command:

`rm baseproduct`

`ln -s /etc/products.d/am.prod baseproduct`

Verify the baseproduct symbolic link is now pointing to the `am.prod` file.

`ll`

Example output:

```
ll
total 8
-rw-r--r-- 1 root root 2912 Nov  9  2019 SLES.prod
-rwxr-xr-x 1 root root  818 Aug  4 16:39 am.prod
lrwxrwxrwx 1 root root   23 Aug  5 14:24 baseproduct -> /etc/products.d/
am.prod
```

NOTE: ✦If you are already registered then change the symbolic link to `am.prod` file and enable the AM-5.0-Product repository (if present) using the following command:

`zypper mr -e AM-5.0-Product`

- If you are changing the symbolic link back to SLES.prod, you must disable the AM-5.0-Product repository using the following command:

```
zypper mr -d AM-5.0-Product
```

Now, you can register or deregister the update service, or check for available updates on the Upgrade Assistant page.

NOTE: If the symbolic link of baseproduct -> /etc/products.d/am.prod exists, there will be issues in fetching updates from the SLES updates channel. Hence, it is recommended to keep this configuration only for the duration until the user operations are done on the Upgrade Assistant page. When operations are complete on the Upgrade Assistant page, change the baseproduct symbolic link to SLES.prod.

To change the baseproduct symbolic link to SLES.prod, use the following commands:

```
cd /etc/products.d/
```

Verify the baseproduct symbolic link before changing it using the following command:

```
ll
```

Remove the symbolic link from baseproduct using the following command:

```
rm baseproduct
```

```
ln -s SLES.prod baseproduct
```

Verify the baseproduct symbolic link is now pointing to the SLES.prod file.

```
ll
```

Example output:

```
ll
total 8
-rw-r--r-- 1 root root 2912 Nov  9  2019 SLES.prod
-rwxr-xr-x 1 root root  818 Aug  4 16:39 am.prod
lrwxrwxrwx 1 root root    9 Aug  5 14:36 baseproduct -> SLES.prod
```

NOTE:

- The operating system `prod` file name might vary depending on the operating system. For example, `SLES.prod` file.
- This issue mostly occurs when Installing/Upgrading to Access Manager 5.0 or Access Manager 5.0 Service Pack 1.However, it is recommended to verify the /etc/products.d/baseproduct symbolic link before and after performing an upgrading from Access Manager 4.5.X to 5.0.

VI Appendix

This section includes the following topics:

- Appendix A, "Configuring Administration Console Ports 9000 and 9001 to Listen on the Specified Address," on page 257
- Appendix B, "Recommendations for Scaling Access Manager Components in Public Cloud," on page 259
- Appendix C, "Denormalizing SQL Database," on page 261

A 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 "tomcat.conf" (tomcat8.conf) file:

```
"com.microfocus.nam.adminconsole.localhost.ipaddress"
```

For example:

```
JAVA_OPTS="${JAVA_OPTS} -
Dcom.microfocus.nam.adminconsole.localhost.ipaddress=10.0.0.0"
```

For information about how to modify a file, see Modifying Configurations in the NetIQ Access Manager 5.0 Administration Guide.

B 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 259
- "Scaling Down the Access Manager Nodes" on page 260

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 Creating and Deploying Instances and for Azure, see Creating and Deploying Virtual Machines.
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.

C Denormalizing SQL Database

IMPORTANT: You must perform this task only if you are upgrading to Access Manager 4.5 Service Pack 2 (SP2) or later from an older version and your database contains the Risk Based Authentication (RBA) data.

From Access Manger 4.5 SP2, a one-to-one data model is used to store the device information for RBA in SQL database. The older versions of Access Manager uses the many-to-one data model to provide the storage benefits of data normalization. The many-to-one data model can cause performance issues in some versions of SQL database when the system is under heavy load.

If you are upgrading to Access Manager SP2 with existing RBA data in database, you must denormalize the existing data. To denormalize your database, you must run a jar utility supplied along with Access Manager 4.5 SP2. If you do not run this utility, the existing user data can become irrelevant in RBA and may not be used for Risk Score calculation.

Refer the following points to know how this utility works:

- It runs outside Access Manager as a separate JAR utility.
- It runs on a configuration file and the configuration file is bundled with JAR.
- It uses hibernate and native SQL queries to modify the database entries.

Perform the following steps to denormalize your database:

IMPORTANT: ◆ It is recommended to back up your database before you run the utility.

- Make sure that enough Java heap space is available before you run the utility.
- Provide appropriate hibernate connector JARs in classpath.

1 Log in to Administrator Console of Access Manager.

2 Click **Policies > Risk-based policies > User history**. Make a note of the following information provided on this page:

   1. Database Driver
   2. Database Dialect
   3. Username
   4. Password
   5. URL

3 Extract the utility JAR (`RBA_SQL_Cleanup_Util.zip`) outside Identity Server folders.

NOTE: If you want to use c3p0 connection pool libraries to optimize the database connection usage while running the utility, you must place the c3p0 JAR files in the same location where the utility JAR is extracted. Specify the c3p0 properties in the configuration file in the `<key=value>` format.

Download the following c3p0 connection pool libraries from Maven Repository:

- c3p0-0.9.2.1.jar
- hibernate-c3p0-4.3.6.Final.jar
- mchange-commons-java-0.2.3.4.jar

4 Open the `config.properties` file that you extracted from utility JAR.

5 Specify the details that you noted in Step 2 in the `config.properties` file:

For example, see the following information to understand what information is specified in `config.properties` file:

```
hibernate.connection.url=<URL>
hibernate.connection.username=<Username>
hibernate.connection.password=<Password>
hibernate.dialect=<Database Dialect>
hibernate.connection.driver_class=<Database Driver>
```

6 Run command line or terminal as an administrator.

7 Run the following java command to run the utility:

```
java -cp '<directory path where the zip is extracted>/*'
com.novell.nam.nidp.risk.sql.cleanup.SQLApp
<directory path where the zip is extracted>/config.properties
<directory to save log files> denormalization_01
```

IMPORTANT: Make sure that you specify absolute paths in classpath and arguments to avoid platform specific issues.

8 Open the log files to check for errors, if occurred.