Installation and Upgrade Guide

Access Manager Appliance 4.3

October 2016

NetIQ

Legal Notice

For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.

© 2016 NetIQ Corporation. All Rights Reserved.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/. All third-party trademarks are the property of their respective owners.

Contents

About this Book and the Library **7**
About NetIQ Corporation **9**

Part I Installing Access Manager Appliance **11**

1 Planning Your Access Manager Environment **13**

1.1 Deployment Models . . . 13
1.2 Access Manager Versus Access Manager Appliance . . . 14
1.3 Network Requirements . . . 21
1.4 Hardware Requirements . . . 22
1.5 Basic Setup . . . 22
1.6 Setting Up Firewalls . . . 22
1.6.1 Required Ports . . . 23
1.6.2 Restricted Ports . . . 25
1.6.3 Sample Configurations . . . 26

2 Installing Access Manager Appliance **29**

2.1 Installation Requirements . . . 29
2.1.1 Hardware Platform Requirements . . . 29
2.1.2 Browser Support . . . 29
2.1.3 Client Access Requirements . . . 30
2.1.4 Installation Mode . . . 30
2.1.5 Virtual Machine Requirements . . . 30
2.1.6 Network Requirements . . . 31
2.2 Installing Access Manager Appliance . . . 32
2.2.1 Prerequisites . . . 32
2.2.2 Installing Access Manager Appliance . . . 32
2.2.3 Removing the Landing Portal . . . 35
2.2.4 Logging In to the Administration Console . . . 36
2.2.5 Administration Console Conventions . . . 37

3 Installing Analytics Server **39**

3.1 Installing Analytics Server . . . 39
3.1.1 System Requirements . . . 39
3.1.2 Installation Checklist . . . 40
3.1.3 Installing Analytics Server . . . 40
3.1.4 Adding And Configuring Multiple Network Interface Card to Analytics Server . . . 42
3.2 Post-Installation Configuration for Analytics Server . . . 42
3.2.1 Registering for Updates . . . 42
3.3 Deploying Analytics Server for High Availability . . . 42
3.3.1 Prerequisite . . . 42
3.3.2 Installing Analytics Server in High Availability Environment . . . 43
3.3.3 Post-Installation Cluster Configuration for Analytics Server . . . 51

Part II Upgrading Access Manager Appliance 53

4 Prerequisites 55

4.1 Maintaining Customized JSP Files for Identity Server . . . 55
4.1.1 Using Customized JSP Pages from Access Manager 4.1 or Prior . . . 55
4.1.2 Using Customized JSP Pages from Access Manager 4.1 or Prior and Enabling the New Access Manager Portal . . . 56
4.2 Maintaining Customized JSP Files for Access Gateway . . . 57

5 Upgrading the Operating System for Access Manager Appliance 59

5.1 Setting Up the Channel After Upgrading Base Operating System . . . 59

6 Upgrading Access Manager Appliance 61

6.1 Upgrading from the Evaluation Version to the Purchased Version . . . 61
6.2 Upgrading Access Manager Appliance . . . 61
6.2.1 Removing Proxy Services And Protected Resources . . . 63

7 Getting the Latest Security Patches 65

7.1 Installing or Updating Security Patches for Access Manager Appliance and Analytics Server . . . 65
7.1.1 Registering to Novell Customer Center . . . 65
7.1.2 Configuring Subscription Management Tool . . . 67

Part III Troubleshooting Installation and Upgrade 69

8 Troubleshooting Installation 71

8.1 Checking the Installation Logs . . . 71
8.2 Some of the New Hardware Drivers or Network Cards Are Not Detected during Installation . . . 72
8.3 Installation Through Terminal Mode Is not Supported . . . 72
8.4 Device Manager Installation Fails During the Appliance Installation . . . 72
8.5 Access Manager Appliance Installation Fails Due to an XML Parser Error . . . 72
8.6 DN Is Added as Provider ID While Installing NMAS SAML Method . . . 73

9 Troubleshooting Upgrade 75

9.1 Access Gateway Throws a 403 Forbidden Page Error for a Resource Protected by a Form Fill Policy . . . 75
9.2 DN Is Added as Provider ID While Installing NMAS SAML Method . . . 75
9.3 Issue in SSL Communication between Access Gateway and Web Applications . . . 75
9.4 Customized Login Pages Are Missing After Upgrading Access Manager . . . 76

Part IV Appendix 77

A Configuring Ports 9000 and 9001 to Listen on the Specified Address 79

About this Book and the Library

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

Intended Audience

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

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

Other Information in the Library

The library provides the following information resources:

- NetIQ Access Manager 4.3 Best Practices Guide
- NetIQ Access Manager Appliance 4.3 Administration Guide
- NetIQ Access Manager 4.3 Developer Guide

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

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

Installing Access Manager Appliance

This part describes how to install Access Manager Appliance:

- Chapter 1, “Planning Your Access Manager Environment,” on page 13
- Chapter 2, “Installing Access Manager Appliance,” on page 29
- Chapter 3, “Installing Analytics Server,” on page 39

1 Planning Your Access Manager Environment

This section includes the following topics:

- Section 1.1, “Deployment Models,” on page 13
- Section 1.2, “Access Manager Versus Access Manager Appliance,” on page 14
- Section 1.3, “Network Requirements,” on page 21
- Section 1.4, “Hardware Requirements,” on page 22
- Section 1.5, “Basic Setup,” on page 22
- Section 1.6, “Setting Up Firewalls,” on page 22

1.1 Deployment Models

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

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

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

For details about these differentiators and other features of Access Manager Appliance, see Section 1.2, “Access Manager Versus Access Manager Appliance,” on page 14.

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

Figure 1-1 *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. But, the differences in the deployment method result in few similarities and differences in 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) 11 SP4 with 64-bit operating system x86-64 hardware.	Supported on the virtual servers based on SUSE Linux Enterprise Server (SLES) 11 SP4, or SLES 12 SP1 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, Red Hat, or Windows). The patch update channel maintains the patches for Access Manager. You must purchase, install, and maintain the underlying operating system.

Feature	Access Manager Appliance	Access Manager
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 generally not recommended. A typical highly available deployment requires 6-8 or more virtual or physical servers (2 Administration Consoles, 2 Identity Servers, 2 Access Gateways).
Administration Console Access	Administration Console is installed on Access Manager Appliance along with all other components. If you use two network interfaces, access to the 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. For more information, see Performance and Sizing Guidelines.	Scales both vertically and horizontally on adding nodes. For more information, see Performance and Sizing Guidelines.
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.

Feature	Access Manager Appliance	Access Manager
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 the 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	The Administration Console and Identity Server are accelerated and protected by Access Gateways. Only HTTPS port 443 is required to access the 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.
Certificate Management: 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.
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. Note: This is a feature that was introduced in Access Manager 3.2 SP2.
Associating different certificates to Identity Server	Not applicable because the Identity Server is accelerated by the Access Gateway.	Supported. The Identity Server can be behind the Access Gateway or can be placed separately in the DMZ.

Feature	Access Manager Appliance	Access Manager
Sample Portal	After a successful installation, a sample Web portal is deployed for the administrator's reference. The administrator can access the sample portal by using the http://hostname URL. This portal provides detailed example of Access Manager Appliance usage and policy configuration.	Not available.
Ready-made Access Manager	The following configuration is automatically done when Access Manager Appliance is installed: ◆ Importing Identity Server and Access Gateway components. ◆ Automatic cluster creation of Identity Server and Access Gateway component. ◆ Automatic configuration of Identity Server to bring it to green state. ◆ Automatic configuration of Access Gateways and Identity Server association. ◆ Automatic service creation to accelerate or protect the Identity Server, Administration Console, and sample portal. As the inter-component configuration is automated, the administrator only needs to add the existing user store and accelerate, protect, sso-enable existing Web applications.	Each component is manually configured and set up before Web applications can be federation enabled, accelerated, 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 NetIQ Access Manager Appliances and configure them to act as a single server. You can cluster any number of Identity Servers and Access Gateways, and up to three of Administration Consoles. The first three nodes of Access Manager Appliance contain the Administration Console, Identity Server, and Access Gateway. Fourth installation onwards, the node has all components except for the Administration Console. A typical Access Manager Appliance deployment in a cluster is described in Figure 1-2 on page 19.	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 1-3 on page 20.

Figure 1-2 *Access Manager Appliance Cluster*

Figure 1-3 *Access Manager Cluster*

General Guidelines

- It is not possible to add an Access Gateway Service or Access Gateway Appliance to an Access Manager Appliance cluster.
- Deploying the 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 an Access Manager. This may result in corruption of the configuration store. However, you can modify the Listening IP address of reverse proxy or the outbound IP address used to communicate with the Web server. For more information, see Changing the IP Address of Access Manager Appliance in the NetIQ Access Manager Appliance 4.3 Administration Guide.
- You cannot have different certificates for signing, encryption in a Federation setup.
- You cannot install any monitoring software to monitor statistics on an 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 cost by consolidating Access Manager services on fewer servers.
- You want to quickly set up a test environment to verify changes.
- You want to quickly setup and evaluate Access Manager.

1.3 Network Requirements

In addition to the servers on which software is installed, your network environment needs to have the following:

- A server configured with an LDAP directory (eDirectory, Sun ONE, or Active Directory) that contains your system users. The Identity Server uses the LDAP directory to authenticate users to the system.
- Web servers with content or applications that need protection.
- Clients with an Internet browser.
- Domain name server, which resolves DNS names to IP addresses and which has reverse lookups enabled.

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

1.4 Hardware Requirements

The hardware requirements for each component is added in the installation section for the respective components. The below table provides the link to hardware requirements for each component:

Component	Requirements in Linux	Requirements in Windows
Analytics Server	"System Requirements" on page 39	Not applicable

1.5 Basic Setup

Figure 1-4 illustrates the basic Access Manager Appliance installation, where Access Manager Appliance is installed outside your firewall. The figure provides an overview of the flexibility built into Access Manager Appliance. You can use it to design a deployment strategy that fits the needs of your company.

Figure 1-4 *Basic Configuration*

For more information, see Section 2.2.2, "Installing Access Manager Appliance," on page 32.

The firewall protects the LDAP server, which contains a permanent store of sensitive data. The Web servers are also installed behind the firewall for added protection. This is a tested and recommended configuration. We have also tested this configuration with an L4 switch in place of the router so that the configuration can support clusters of Access Manager Appliance.

1.6 Setting Up Firewalls

Access Manager Appliance should be used with firewalls. Figure 1-5 illustrates a simple firewall setup for a basic Access Manager Appliance configuration.

Figure 1-5 *Access Manager Appliance and Firewall*

The first firewall separates the Access Manager Appliance from the Internet, allowing browsers to access the resources through specific ports. This is one of many possible configurations. This section describes the following:

- Section 1.6.1, “Required Ports,” on page 23
- Section 1.6.3, “Sample Configurations,” on page 26

1.6.1 Required Ports

The following tables list the ports that need to be opened when a firewall separates Access Manager Appliance from Internet.

With these tables, you should be able to place Access Manager Appliance of your system anywhere within your existing firewalls and know which ports need to be opened in the firewall.

Table 1-2 *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 Analytics Dashboard.
Browsers	TCP 8443	For HTTPS communication with Analytics Server for Reports console.
Syslog	TCP 1468	For updating Syslog messages from Access Manager components to Analytics Server.
Control Center	TCP 10013	For communicating from a computer to the control center on Analytics Server.
Remote Linux Administration Workstation	TCP 22	For communication from your remote administration workstation to Analytics Server.

Component	Port	Description
High availability configuration	TCP 7360	For communicating between the servers in Analytics server high availability mode.

Component	Port	Description
NTP Server	UDP 123	Access Manager components must have time synchronized else the authentication fails. We highly recommend that all components be configured to use an NTP (network time protocol) server. Depending upon where your NTP server is located in relationship to your firewalls, you might need to open UDP 123 so that the Access Manager component 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 the Access Manager component can resolve DNS names.
Remote Linux Administration Workstation	TCP 22	If you use SSH for remote administration and want to use it for remote administration of Access Manager components, you need to open TCP 22 to allow communication from your remote administration workstation to your Access Manager components.
Access Manager Appliance	TCP 1443	For communication from the Administration Console to the devices.
	TCP 8444	For communication from the devices to the Administration Console.
	TCP 1290	For communication from the devices to the Syslog server on the Administration Console.
	TCP 524	For NCP certificate management with NPKI. The port needs to be opened so that both the device and the Administration Console can use the port.
	TCP 636	For secure LDAP communication from the devices to the Administration Console.
	TCP 524	Required to synchronize the configuration data store.
	TCP 636	Required for secure LDAP communication.
	TCP 8080, 8443	Used for Tomcat communication.
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 the Administration Console. It is not used in day-to-day operations.

Component	Port	Description
Browsers	TCP 8080	For HTTP communication from browsers to the Administration Console.
	TCP 8443, 2443, 2080.	For HTTPS communication from browsers to the Administration Console.
	TCP 8028, 8030	To use iMonitor or DSTrace from a client to view information about the configuration store on the Administration Console.
	TCP 80	For HTTP communication from the client to the Access Gateway. This is configurable.
	TCP 443	For HTTPS communication from the client to the Access Gateway. This is configurable.
Web Servers	TCP 80	For HTTP communication from the Access Gateway to the Web servers. This is configurable.
	TCP 443	For HTTPS communication from the Access Gateway to the Web servers. This is configurable.

NOTE: On SLES 11 SP4, you can edit this file or use YaST to configure UDP ports and internal networks.

1.6.2 Restricted Ports

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

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

If required, use port redirection by using IP tables.

1.6.3 Sample Configurations

- Section 1.6.3.1, “Access Manager Appliance in DMZ,” on page 26

1.6.3.1 Access Manager Appliance in DMZ

- “First Firewall” on page 26
- “Second Firewall” on page 26

First Firewall

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

See, Figure 1-5 on page 23

Table 1-3 *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 the Identity Server.
TCP 8443	For HTTPS communication with the Identity Server.
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 the Administration Console from the Identity Server and the Access Gateway. You need the following ports opened in the second firewall:

Table 1-4 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 the Administration Console to the devices.
TCP 8444	For communication from the devices to the Administration Console.
TCP 1290	For communication from the devices to the Syslog server installed on the 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 the Administration Console can use the port.
TCP 636	For secure LDAP communication of configuration information.

You need to open ports on the second firewall according to the offered services.

2 Installing Access Manager Appliance

This chapter explains how to install Access Manager Appliance. Topics include:

- Section 2.1, “Installation Requirements,” on page 29
- Section 2.2, “Installing Access Manager Appliance,” on page 32

2.1 Installation Requirements

This section explains requirements for installing Access Manager Appliance. For a list of current filenames and for information about installing the latest release, see the Release Notes of that release on the NetIQ Access Manager Documentation Web site.

The Access Manager Appliance installer installs all components on a single server, so software and hardware requirements are same for all components. *Section 1.2, “Access Manager Versus Access Manager Appliance,” on page 14* lists differences between previously shipped Access Manager versus Access Manager Appliance.

Access Manager Appliance is based on the SUSE Linux Enterprise Server (SLES) 11 SP4 64-bit operating system. The hard disk, RAM, and CPU requirements are same for all components.

For network requirements, see Section 1.3, “Network Requirements,” on page 21.

2.1.1 Hardware Platform Requirements

The following are the hardware requirements:

- 8 GB RAM
- Dual CPU or core (3.0 GHz or comparable chip)
- 100 GB hard disk

  The hard disk should have ample space for logging in a production environment. This disk space must be local and not remote.

  2 to10 GB per reverse proxy that requires caching and for log files. The amount varies with the rollover options and logging level that you configure.
- The static IP address and an assigned DNS name (hostname and domain name) for your Access Manager Appliance.

2.1.2 Browser Support

The following browsers are supported for users to log in to Access Manager Appliance:

- Internet Explorer 11 and later
- Mozilla Firefox
- Chrome

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

2.1.3 Client Access Requirements

Clients can use any browser or operating system when accessing resources protected by the Access Gateway.

2.1.4 Installation Mode

You must install Access Manager Appliance by burning the Access Manager Appliance ISO on a DVD.

2.1.5 Virtual Machine Requirements

The virtual machine must have enough resources. The requirements for a virtual machine need to match the requirements for a physical machine. To achieve the performance similar to a physical machine, increase the memory and CPU requirements.

For the hard disk, RAM, and CPU requirements, each virtual machine should meet the following minimum requirements:

- 100 GB of disk space
- 8 GB RAM
- 2 CPUs

Access Manager can be installed on the virtual machines that support an operating system supported by your Access Manager version and component. For example, SUSE Linux Enterprise Server (SLES) 11 SP3 and SLES 12 with 64-bit operating system x86-64 hardware.

NOTE: SLES 11 SP4 64-bit Access Manager Appliance does not support XEN paravirtualization.

The following sections contain installation tips for virtual machines:

- Section 2.1.5.1, “Keeping Time Synchronized on Access Manager Appliances,” on page 30
- Section 2.1.5.2, “Number of Virtual Machines Per Physical Machine,” on page 31
- Section 2.1.5.3, “Using a Network Adapter for VMWare ESX,” on page 31

2.1.5.1 Keeping Time Synchronized on Access Manager Appliances

Even when virtual machines are configured to use a network time protocol (NTP) server, time does not stay synchronized because the machines periodically lose their connection to the NTP server. The easiest solution is to configure primary Access Manager Appliance to use an NTP server and configure other Access Manager Appliance to use a cron job to synchronize their time with primary Access Manager Appliance.

SLES 11 SP4: The `ntpdate` command is not supported by SLES 11 SP4 64-bit. You can use the `sntp` command. Add the following command to the `/etc/crontab` file of the device:

```
*/5 * * * *   root   /usr/sbin/sntp -P no -r 10.20.30.108 >/dev/null 2>&1
```

Replace 10.20.30.108 with the IP address of your NTP server.

2.1.5.2 Number of Virtual Machines Per Physical Machine

How you deploy your virtual machines can greatly influence the Access Manager Appliance performance. Deploy maximum of four Access Manager Appliance virtual machines on a single piece of hardware. When you start deploying more than four, components of Access Manager Appliance start competing with each other for same hardware resources at the same time. You can include other types of services that the machine can support if they do not use the same hardware resources that Access Manager Appliance components use.

The configured CPUs must match the hardware CPUs on the machine. Performance is drastically reduced if you allocate more virtual CPUs than actually exist on the machine.

Another potential bottleneck is IO. For best performance, each virtual machine should have its own hard disk, or you need a SAN that is capable of handling the IO traffic.

For example, if you have one 16-CPU machine, you get better performance when you configure the machine to have four Access Gateways with 4 assigned CPUs than you get when you configure the machine to have eight Access Gateways with 2 assigned CPUs. If the machines are dedicated to Access Manager Appliance components, you get better performance from two 8-CPU machines than you get from one 16-CPU machine.The setup depends on your unique environment and hardware and virtualization configuration for your cluster.

2.1.5.3 Using a Network Adapter for VMWare ESX

Use the E1000 network adapter for Access Manager Appliance installation on VMWare ESX.

2.1.6 Network Requirements

Your network environment must meet the following requirements:

- A server configured with an LDAP directory (eDirectory, Sun ONE, or Active Directory) that contains your system users. The Identity Server uses the LDAP directory to authenticate users to the system.
- Web servers with content or applications that need protection.
- Clients with an Internet browser.
- Static IP addresses for each Access Manager Appliance. If the IP address of the machine changes, Access Manager Appliance components cannot start.
- Domain name server, which resolves DNS names to IP addresses and that has reverse lookups enabled.

  Access Manager Appliance components know each other by their IP addresses. 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 the reverse lookups are not available, host table entries can be used.
- Network time protocol (NTP) server 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.

2.2 Installing Access Manager Appliance

Installation time: 45 to 90 minutes, depending on the hardware.

What you need to know	◆ Root password of Access Manager Appliance. ◆ Username and password of the Administration Console administrator. ◆ Static IP address for Access Manager Appliance. ◆ DNS name (host and domain name) for the Access Gateway that resolves to the IP address. ◆ Subnet mask that corresponds to the IP address for the 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. ◆ The tree for the configuration store is named after the server on which you install Access Manager Appliance. Check the hostname and rename the machine if the name is not appropriate for a configuration tree name.

Access Manager Appliance can be installed on all supported hardware platforms for SLES 11 SP4 (64-bit).

2.2.1 Prerequisites

- ❒ Ensure that you have backed up all data and software on the disk to another machine. The Access Manager Appliance installation completely erases all the data on your hard disk.
- ❒ Ensure that the machine meets the minimum hardware requirements. See Section 2.1, "Installation Requirements," on page 29.
- ❒ (Optional) If you want to try any advanced installation options such as driver installation or network installation, see the *Deployment Guide* (http://www.suse.com/documentation/sles11/book_sle_deployment/data/book_sle_deployment.html).

2.2.2 Installing Access Manager Appliance

Access Manager Appliance is installed with the following default partitions:

- **boot:** The size is automatically calculated and the mount point is `/boot`.
- **swap:** The size is double the size of the RAM and the mount point is `swap`.

The remaining disk space after the creation of the /boot and swap partitions is allocated as the extended drive. The extended drive has the following partitions:

- **root:** The default size is approximately one-third the size of the extended drive and the mount point is `/`.
- **var:** The default size is approximately one-third the size of the extended drive and the mount point is `/var`.

NOTE

- Do not install or import any non- 4.3 Appliance devices during installation.
- Platform Agent and Novell Audit are no longer supported. From Access Manager 4.2 onwards Platform Agent and Novell Audit is unavailable for auditing. If you upgrade from an older version of Access Manager to 4.3, Platform Agent is still available. It is recommended to use Syslog for auditing.

Access Manager Appliance does not support configuring multiple network interfaces during installation. The eth0 interface is configured by default, and if you require multiple interfaces, you can configure them through the Administration Console after installation.

1. Insert the Access Manager Appliance CD into the CD drive.

   The boot screen appears.
2. By default, the **Boot From Hard Disk** option is selected in the boot screen.

   Use the Down-arrow key to select **Install Appliance**.
3. Press Enter.
4. Review the agreement on the License Agreement page, then click **I Agree**.
5. Select the region and time zone on the Clock and Time Zone page.
6. Click **Next**.
7. Configure the details on the Appliance Configuration page:

Field	Description
Host Name	The hostname for the Access Manager Appliance machine.
Domain Name	The domain name for your network.
Public IP	Configure the following options for the public IP: ◆ **IP Address:** The public IP address of Access Manager Appliance. ◆ **Subnet Mask:** The subnet mask of Access Manager Appliance. ◆ **Default Gateway:** The IP address of the default gateway.
Private IP	Configure the following options for the private IP. This is an optional configuration. If this is configured, the Administration Console listens on this IP. ◆ **IP Address:** Private IP address of Access Manager Appliance. ◆ **Subnet Mask:** Subnet mask of Access Manager Appliance. ◆ **Gateway:** IP address of the gateway.
DNS Server 1	IP address of your DNS server. You must configure at least one DNS server.
DNS Server 2	IP address of your additional DNS server. This is an optional configuration.
In the Root Password section, specify password for the `root` user and name of the NTP server.	

8. Click **Next**.

Configure the following details under the Administration Console Configuration:

Field	Description
Primary	Deselect this option to specify if this Access Manager Appliance is not primary. If you are installing it as a secondary Access Manager Appliance then ensure that the primary Access Manager Appliance is reachable.
Admin Console IP	Specify the IP address of the primary Access Manager Appliance if this is secondary.
Username	The name of the Administration Console user. **NOTE:** The Administration Console username does not accept special characters # (hash), & (ampersand), and ( ) (round brackets).
Password	Specify and confirm the password for the user. **NOTE:** The Administration Console password does not accept special characters : (colon) and " (double quotes).

9 Click **Next**.

The Installation Settings page appears. This page displays the options and software you selected in the previous steps. Use the **Overview** tab for a list of selected options, or use the **Expert** tab for more details.

Do not change the software selections listed on this screen.

10 (Optional) To modify the installation settings for partitions, click **Change**.

11 Click **Install** > **Install**.

This process might take 45 to 90 minutes depending on the configuration and hardware.

The machine reboots after the installation is completed. It runs an auto configure script, and then the Access Gateway and Identity Server components are configured.

12 (Optional) Verify if Access Manager Appliance is installed and configured successfully.

Log in to the Administration Console. See Section 2.2.4, “Logging In to the Administration Console,” on page 36), then click **Devices** > **Access Gateways**.

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

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

The Access Gateway health is displayed as green. The configuration takes care of establishing a trust relationship between an embedded service provider and the Access Gateway and also the trust relationship with the Identity Server before you proceed with any other configuration.

12a In a browser, enter the Access Manager Appliance URL. The Access Manager Appliance URL is formed by using the Host Name and Domain Name provided in the Step 8. For example, if the host name is `accessapp` and the domain name is novell.com, then the URL will be `https://accessapp.novell.com`. You will be redirected to the Sample Portal Page.

12b Click the Administration Console link and log in to.

12c Click **Devices**> **Access Gateways**. The Servers tab displays AG-Cluster with one Access Gateway. The IP Address of the Access Gateway is same as the Access Manager Appliance IP Address. The health of both the AG-Cluster and Access Gateway should display green.

13 Continue with one of the following sections:

- Section 2.2.3, “Removing the Landing Portal,” on page 35
- Setting up User Stores for Identity Server Configuration and Configuring Access Gateway in the NetIQ Access Manager Appliance 4.3 Administration Guide.

2.2.3 Removing the Landing Portal

The landing portal is enabled by default during the installation of Access Manager Appliance. The portal also has a sample application, which you can configure to learn Access Manager Appliance capabilities. The landing portal is visible to users, hence it is not recommended to use in the production setup. Use it for demonstration and trial purposes. Remove the landing portal after you verify all your configurations in a staging environment.

Perform the following steps to remove the landing portal:

1 In the Administration Console, click **Access Gateway** > **Cluster** > **Edit** > **NAM - RP.**

2 Select the **namportal** path based service.

3 Click **Delete**.

4 Click **Protected Resources**.

Delete the following protected resources:

- portal_employee
- portal_manager
- portal_public
- portal_users

5 Click **OK** > **Update**.

6 In the Administration Console, click **Devices** > **Identity Servers** > **Servers** > **Edit** > **Roles**.

7 Select the role policy check box, select the **portal_roles** role from the Roles Policy List, and click **Disable**.

8 Click **OK** > **Update**.

9 To remove the portal web application from the Access Manager Appliance filesystem, perform the following steps:

9a Log in to Access Manager Appliance by using any SSH client (for example, SSH in Linux and PuTTY in Windows).

9b Stop the Administration Console by using the `/etc/init.d/novell-ac stop` command.

9c Go to the portal directory by running the `cd /opt/novell/nam/adminconsole/webapps` command.

9d Remove the portal by running the `rm -rf portal` command.

9e Start the Administration Console by running the `/etc/init.d/novell-ac start` command.

10 The portal creates two default users Alice and Bob in the Appliance Configuration store.

You can remove the users by performing the following steps:

10a In the Administration Console, click **Roles and Tasks** > **Users** > **Delete User**.

10b In the Delete User page, specify the Object Name as bob.novell to delete Bob and alice.novell to delete Alice.

10c Click **OK**.

NOTE: If required, you can delete Employee, Manageronly, portal_formfill, portal_id_injection, portal_roles policies on the Policies page.

2.2.4 Logging In to the Administration Console

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

You cannot use it to log into other eDirectory trees and manage them.

You should not download and add iManager plug-ins to this customized version. If you do, you can destroy the Access Manager Appliance schema, which can prevent you from managing the Access Manager Appliance components. This can also prevent communication among the modules.

You should not start multiple sessions of the Administration Console on the same machine through the same browser. Because the browser shares session information, this can cause unpredictable results in the Administration Console. You can, however, start different sessions with different brands of browsers.

To log in to:

1. Enable browser pop-ups.
2. From a client machine external to your Administration Console server, launch your preferred browser and enter the URL for the Administration Console.

   If the hostname of your Access Manager Appliance is www.host.com, you would enter `http://www.host.com:8080/nps`.
3. Click **OK**. You can select either the permanent or temporary session certificate option.
4. Specify the administrator name and password that you defined during installation and click **Login**. Access Manager Appliance Dashboard opens.

   For more information about this view or about configuring the Administration Console for Access Manager Appliance 4.3 view, see Configuring the Default View in the NetIQ Access Manager Appliance 4.3 Administration Guide.

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

To understand the conventions of the Administration Console, see Section 2.2.5, “Administration Console Conventions,” on page 37.

2.2.5 Administration Console Conventions

- The required fields on a configuration page contain an asterisk by the field name.
- All actions such as delete, stop, and purge require verification before they are executed.
- Changes are not applied to a server until you update the server.
- Sessions are monitored for activity. If your session becomes inactive, you are asked to log in again and unsaved changes are lost.

3 Installing Analytics Server

You can install Analytics Server after installing Administration Console. You can install it on any server without the requirement for any base operating system because Analytics Server is packaged with SLES operating system. Before you install Analytics Server, review new functionality and known issues in the supported SLES Release Notes.

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

This chapter includes the details on installing and deploying Analytics Server.

- Section 3.1, “Installing Analytics Server,” on page 39
- Section 3.2, “Post-Installation Configuration for Analytics Server,” on page 42
- Section 3.3, “Deploying Analytics Server for High Availability,” on page 42

3.1 Installing Analytics Server

This section provides information about installing Analytics Server. This image format allows you to generate a full disk image format that can be deployed directly to hardware, either physical (bare metal) or virtual (uninstalled virtual machine in a hypervisor) by using a bootable ISO DVD image.

- Section 3.1.1, “System Requirements,” on page 39
- Section 3.1.2, “Installation Checklist,” on page 40
- Section 3.1.3, “Installing Analytics Server,” on page 40
- Section 3.1.4, “Adding And Configuring Multiple Network Interface Card to Analytics Server,” on page 42

3.1.1 System Requirements

Ensure that the environment where you are going to install this ISO, meets the following prerequisites:

- (Conditional) If you are installing the ISO on bare metal hardware, download the ISO disk image from the support site, unpack the file, and make a DVD.
- It is recommended to use 24 GB for production environment. However, the minimum memory of 6.5 GB can be used for demonstration purpose.
- Ensure that the minimum hard disk space is 50 GB for the installer to make the automatic partition proposal.
- Ensure that you use (4 core) CPUs (8 cores total).

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

To store 500 EPS for an year, you require the following:

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

- **Memory:** 24 GB

3.1.2 Installation Checklist

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

- ❒ Verify that your hardware and software meet the system requirements listed in Section 3.1.1, "System Requirements," on page 39.
- ❒ If there was a previous installation of Analytics Server, ensure that there are no files or system settings remaining from a previous installation.
- ❒ Ensure that the ports listed in Section 1.6, "Setting Up Firewalls," on page 22 are opened in the firewall.

3.1.3 Installing Analytics Server

To install Analytics Server perform the following:

NOTE: If you plan to include multiple Network Interface Card (NIC), then you must install Analytics Server with one NIC and then proceed with configuring other network interfaces. For more information, see Section 3.1.4, "Adding And Configuring Multiple Network Interface Card to Analytics Server," on page 42.

---

1. Download the ISO for the Analytics Server image from the NetIQ Download Website.
2. (Conditional) If you are using a hypervisor:

   Set up the virtual machine using the ISO virtual appliance image, and power it on.

   or

   Copy the ISO image into a DVD, set up the virtual machine using the DVD, and power it on.
3. (Conditional) If you are installing the Analytics Server on bare metal hardware:

   3a Boot the physical machine from the DVD drive with the DVD.

   3b Follow the installation wizard on-screen instructions.

   3c Run the Live DVD appliance image by selecting the top entry in the boot menu.

   The installation checks for the available memory. If the available memory is less than 6.5 GB, the installation will not proceed further. Enter y if you want to continue with the installation, or enter n if you do not want to proceed.
4. Select the language of your choice and keyboard Configuration, then click **Next**.
5. Read and accept the Access Manager Analytics Server End User License Agreement. Click **Next**
6. On the Hostname and Domain Name page, specify the hostname and domain name. Deselect **Assign Hostname to Loopback IP**, then click **Next**.
7. Choose one of the following connection settings options:
   - To use the current network connection settings, select **Use the following configuration** on the Network Configuration II page.
   - To change the network connection settings, click **Change**, then make the desired changes.
8. Click **Next**.
9. Set the Time and Date, then click **Next**.

To change the NTP configuration after installation, use YaST from the appliance command line.

If the time appears out of sync immediately after the install, run the following command to restart NTP:

```
rcntp restart
```

10 Set the `root` password, then click **Next**.

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

12 In the **Administration console server Information** screen, specify the following to import Analytics server to the specified Administration Console:

IP Address: IP address of the Administration Console.

Admin User: The name of the user accessing Administration Console.

Password: Password of the Administration Console user.

Confirm the password, then click **Next**.

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

---

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

14 Select **Install** to confirm the Installation.

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

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

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

16 Select **OK** to reboot the system.

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

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

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

The default value for the username is `root` and the password is the password you set in Step 10.

20 Proceed with Section 3.2, "Post-Installation Configuration for Analytics Server," on page 42.

NOTE: For installing Analytics Server in high-availability mode, see Section 3.3.2, "Installing Analytics Server in High Availability Environment," on page 43.

3.1.4 Adding And Configuring Multiple Network Interface Card to Analytics Server

If you want to install multiple Network Interface Card, and configure multiple IP addresses for Analytics Server, then perform the following:

1. Install Analytics Server with one Network Interface Card that is configured with the IP address that must be used for communicating with Administration Console. For installation steps refer Section 3.1.3, “Installing Analytics Server,” on page 40.
2. After the installation completes, configure the other required network interfaces by using YaST.

3.2 Post-Installation Configuration for Analytics Server

After you install Analytics Server, you need to perform additional configuration for it to work properly.

3.2.1 Registering for Updates

You must register Analytics Server with the server update channel to receive patch updates. For more information about registering the server, see Section 7.1.1, “Registering to Novell Customer Center,” on page 65.

3.3 Deploying Analytics Server for High Availability

This section provides information about how to install Analytics Server in an Active-Passive High Availability mode, which allows the server to fail over to a redundant cluster node in case of hardware or software failure. For more information on implementing high availability and disaster recovery in the Analytics Server environment, contact NetIQ Technical Support.

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

For more information about high availability, see the SUSE High Availability Guide.

- Section 3.3.1, “Prerequisite,” on page 42
- Section 3.3.2, “Installing Analytics Server in High Availability Environment,” on page 43
- Section 3.3.3, “Post-Installation Cluster Configuration for Analytics Server,” on page 51

3.3.1 Prerequisite

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

- ☒ Ensure that each cluster node that hosts the Analytics Server services meet the requirements specified in Section 3.1.1, “System Requirements,” on page 39.
- ☒ Ensure that sufficient shared storage is available for the Analytics Server data and application.

- ☒ Ensure that you use a virtual IP address for the services that can be migrated from node to node on failover.
- ☒ Ensure that your shared storage device meets the performance and size characteristics requirements. It is recommended to use a standard SUSE Linux VM configured with iSCSI Targets as shared storage.
- ☒ Ensure that you have only two cluster nodes that meet the resource requirements for running Analytics Server in the cluster environment.
- ☒ Ensure you have a virtual IP that can be migrated from one node to another node in a cluster to serve as the external IP address for Analytics Server.
- ☒ Ensure you create a method for the cluster nodes to communicate with the shared storage, such as FibreChannel for a SAN. NetIQ recommends a dedicated IP address to connect to the iSCSI Target.
- ☒ Ensure you have at least one IP address per cluster node for internal cluster communications. NetIQ recommends a simple unicast IP address, but multicast is preferred for production environments.

3.3.2 Installing Analytics Server in High Availability Environment

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

- Section 3.3.2.1, “Initial Setup,” on page 43
- Section 3.3.2.2, “Shared Storage Setup,” on page 44
- Section 3.3.2.3, “Configuring Analytics Server for High Availability on the Nodes,” on page 46
- Section 3.3.2.4, “Cluster Installation and Configuration,” on page 47
- Section 3.3.2.5, “Resource Configuration,” on page 49

3.3.2.1 Initial Setup

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

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

- The CPU, RAM, and disk space characteristics for each cluster node must meet the system requirements defined in Section 3.1.1, “System Requirements,” on page 39 based on the expected event rate.
- If you want to configure the operating system firewalls to restrict access to Analytics Server and the cluster, refer to Table 1-2 on page 23, for details of which ports must be available depending on your local configuration and the sources that will be sending event data.
- Ensure that all cluster nodes are time-synchronized. You can use NTP or a similar technology for this purpose.
- The cluster requires reliable host name resolution. Enter all internal cluster host names into the `/etc/hosts` file to ensure cluster continuity in case of DNS failure.
- Ensure that you do not assign a host name to a loopback IP address.
- When configuring host name and domain name while installing the operating system, deselect **Assign Hostname to Loopback IP**.
- The nodes will have one NIC for external access and one for iSCSI communications.

- Configure the external NICs with IP addresses that allow for remote access through SSH or similar. For this example, we will use 172.16.0.1 (node01) and 172.16.0.2 (node02).
- Each node should have sufficient disk for the operating system, and Analytics Server. For system requirements, see Section 3.1.1, “System Requirements,” on page 39.
- One SUSE Linux 11 SP3 VM configured with iSCSI Targets for shared storage
  - (Conditional) You can install X Windows if you require GUI configuration. Set the boot scripts to start without X (runlevel 3), so you can start them only when needed.
  - The system will have two NICs: one for external access and one for iSCSI communications.
  - Configure the external NIC with an IP address that allows for remote access using SSH or similar. For example, 172.16.0.3 (storage03).
  - The system should have sufficient space for the operating system, temp space, a large volume for shared storage to hold Sentinel data, and a small amount of space for an SBD partition. See the SUSE Linux system requirements, and Sentinel event data storage requirements.
- Perform the steps mentioned in the following sections.

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

3.3.2.2 Shared Storage Setup

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

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

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

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

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

   ```
   dd if=/dev/zero of=/localdata count=20480000 bs=1024
   ```

Configure iSCSI targets

Configure the files `localdata` as iSCSI Targets:

1. Run YaST from the command line (or use the Graphical User Interface, if preferred): `/sbin/yast`
2. Select **Network Devices** > **Network Settings**.

3 Ensure that the **Overview** tab is selected.

4 Select the secondary NIC from the displayed list, then tab forward to Edit and press `Enter`.

5 On the **Address** tab, assign a static IP address of 10.0.0.3. This will be the internal iSCSI communications IP.

6 Click **Next**, then click **OK**.

7 On the main screen, select **Network Services** > **iSCSI Target**.

8 If prompted, install the required software (`iscsitarget RPM`) from the SUSE Linux 11 SP3 media.

9 Click **Service**, select the **When Booting** option to ensure that the service starts when the operating system boots.

10 Click **Global**, and then select **No Authentication** because the current OCF Resource Agent for iSCSI does not support authentication.

11 Click **Targets** and then click **Add** to add a new target.

The iSCSI Target will auto-generate an ID and then present an empty list of LUNs (drives) that are available.

12 Click **Add** to add a new LUN.

13 Leave the LUN number as 0, then browse in the **Path** dialog (under Type=fileio) and select the `/localdata` file that you created. If you have a dedicated disk for storage, specify a block device, such as `/dev/sdc`.

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

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

16 Exit YaST.

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

Configuring iSCSI initiators

Use the following procedure to format the devices:

1 Connect to one of the cluster nodes (node01) and start YaST.

2 Select **Network Devices** > **Network Settings**.

3 Ensure that the **Overview** tab is selected.

4 Select the secondary NIC from the displayed list, then tab forward to Edit and press Enter.

5 Click **Address**, assign a static IP address of 10.0.0.1. This will be the internal iSCSI communications IP.

6 Select **Next**, then click **OK**.

7 Click **Network Services** > **iSCSI Initiator**.

8 If prompted, install the required software (open-iscsi RPM) from the SUSE Linux 11 SP3 media.

9 Click **Service**, select **When Booting** to ensure the iSCSI service is started on boot.

10 Click **Discovered Targets**, and select **Discovery**.

11 Specify the iSCSI Target IP address (10.0.0.3), select **No Authentication**, and then click **Next**.

12 Select the discovered iSCSI Target with the IP address 10.0.0.3 and then select **Log In**.

13 Switch to automatic in the **Startup** drop-down and select **No Authentication**, then click **Next**.

14 Switch to the **Connected Targets** tab to ensure that we are connected to the target.

15 Exit the configuration. This should have mounted the iSCSI Targets as block devices on the cluster node.

16 In the YaST main menu, select **System** > **Partitioner**.

17 In the System View, you should see new hard disk (such as `/dev/sdb`) in the list - they will have a type of IET-VIRTUAL-DISK. Tab over to this hard disk, select it, then press **Enter**.

18 Select **Add** to add a new partition to the empty disk. Format the disk as a primary ext3 partition, but do not mount it. Ensure that the option Do not mount partition is selected.

19 Select **Next**, then **Finish** after reviewing the changes that will be made. Assuming you create a single large partition on this shared iSCSI LUN, you should end up with a `/dev/sdb1` or similar formatted disk (referred to as `/dev/<SHARED1>` below).

20 Exit YaST.

21 Repeat steps 1-15 to ensure that each cluster node can mount the local shared storage. Replace the node IP in step 5 with a different IP for each cluster node.

3.3.2.3 Configuring Analytics Server for High Availability on the Nodes

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

First node

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

1 Connect to one of the cluster nodes (node01) and open a console window.

2 Navigate to the following directory:

```
cd /opt/novell/sentinel/setup
```

3 Record the configuration:

3a Execute the following command:

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

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

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

3c Specify `2` to enter a new password.

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

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

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

```
/etc/init.d/novell-offline stop
/etc/init.d/novell-realtime stop
/etc/init.d/novell-jcc stop
rcsentinel stop
insserv -r sentinel
```

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

```
mkdir -p /tmp/new

mount /dev/<SHARED1> /tmp/new

mv /var/opt/novell/sentinel /tmp/new

umount /tmp/new/
```

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

```
mount /dev/<SHARED1>  /var/opt/novell/

umount /var/opt/novell/
```

Subsequent node

1 Connect to second cluster node (node02) and open a console window.

2 Execute the following command:

```
insserv -r sentinel
```

3 Stop Analytics Server services.

```
rcsentinel stop
```

4 Remove Analytics Server directory.

```
rm -rf /var/opt/novell/sentinel
```

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

3.3.2.4 Cluster Installation and Configuration

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

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

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

NetIQ Recommends the following procedure for cluster configuration:

SBD Setup

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

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

2 Create a 1MB file filled with zeros copied from the `/dev/zero` pseudo-device.

3 Run YaST from the command line or the Graphical User Interface: `/sbin/yast`

4. Select **Network Services** > **iSCSI Target**.
5. Click **Targets** and select the existing target.
6. Select **Edit**. The UI will present a list of LUNs (drives) that are available.
7. Select **Add** to add a new LUN.
8. Leave the LUN number as 1. Browse in the **Path** dialog and select the `/sbd` file that you created.
9. Leave the other options at their defaults, then select **OK** then **Next**, then click **Next** again to select the default authentication options.
10. Click **Finish** to exit the configuration. Restart the services if needed. Exit YaST.

NOTE: The following steps require that each cluster node be able to resolve the hostname of all other cluster nodes (the file sync service csync2 will fail if this is not the case). If DNS is not set up or available, add entries for each host to the `/etc/hosts` file that list each IP and its hostname (as reported by the hostname command). Also, ensure that you do not assign a hostname to a loopback IP address.

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

Node Configuration

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

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

20 Select **Finish** to complete the configuration.

21 Exit YaST.

22 Run the command `/etc/rc.d/openais restart` to restart the cluster services with the new sync protocol.

Connect to other cluster node (node02) and open a console:

1 Run YaST.

2 Open **Network Services** > **iSCSI Initiator**.

3 Select **Connected Targets**, then the iSCSI Target you configured above.

4 Select the **Log Out** option and log out of the Target.

5 Switch to the **Discovered Targets** tab, select the **Target**, and log back in to refresh the list of devices (leave the **automatic** startup option and **No Authentication**).

6 Select **OK** to exit the iSCSI Initiator tool.

7 Run the following command: `sleha-join`

   Enter the IP address of the first cluster node.

8 Run `crm_mon` on each cluster node to verify that the cluster is running properly.

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

1 Manually copy `/etc/corosync/corosync.conf` from `node01` to `node02`, or run `csync2 -x -v` on `node01`, or manually set the cluster up on `node02` through YaST.

2 Run `/etc/rc.d/openais start` on `node02`

   (Conditional) If the `xinetd` service does not properly add the new `csync2` service, the script will not function properly. The `xinetd` service is required so that the other node can sync the cluster configuration files down to this node. If you see errors like `csync2 run failed`, you may have this problem.

   To resolve this issue, execute the `kill -HUP `cat /var/run/xinetd.init.pid` command and then re-run the `sleha-join` script.

3 Run `crm_mon` on each cluster node to verify that the cluster is running properly. You can also use 'hawk', the web console, to verify the cluster. The default login name is `hacluster` and the password is `linux`.

Perform the following tasks to modify additional parameters:

1 To ensure that in a single node failure in your two-node cluster does not unexpectedly stop the entire cluster, set the global cluster option `no-quorum-policy` to `ignore`:

```
crm configure property no-quorum-policy=ignore
```

2 To ensure that the resource manager allows resources to run in place and move, set the global cluster option `default-resource-stickiness` to 1:

```
crm configure property default-resource-stickiness=1
```

3.3.2.5 Resource Configuration

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

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

NetIQ recommends the following for resource configuration:

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

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

1. Run the following commands on both nodes:
   - `mkdir -p /var/log/agg-analytics-var`
   - `mkdir -p /var/log/agg-analytics-var/nam/logs/dashboard/tomcat`
   - `chown -R novell.novell /var/log/agg-analytics-var/`
2. On the primary node, run the following commands in the same sequence, where `<SHARED1>` is the shared volume you created previously:

   ```
   mount /dev/<SHARED1> /var/opt/novell
   ln -s /var/log/agg-analytics-var/nam /var/opt/novell/nam
   cd /usr/lib/ocf/resource.d/novell
   ./install-resources.sh
   ```

   The `install-resources.sh` script will prompt you for a couple values, namely the virtual IP that you would like people to use to access Analytics Server and the device name of the shared storage, and then will auto-create the required cluster resources. Note that the script requires the shared volume to already be mounted, and also requires the unattended installation file which was created during Analytics Server install to be present (`/tmp/install.props`). You do not need to run this script on any but the first installed node; all relevant config files will be automatically synced to the other nodes.

   After running the install-resources script, if you get the error for the file syncronization, then run `csync2 -x -v`. If you get the message that file is up to date and is with no errors, then you can continue the deployment.
3. Run the following commands on the primary node:
   - `/etc/init.d/novell-offline start`
   - `/etc/init.d/novell-realtime start`
   - `/etc/init.d/novell-jcc start`
4. Run `/etc/rc.d/openais restart` on node02.
5. If your environment varies from this NetIQ recommended solution, you can edit the `resources.cli` file (in the same directory) and modify the primitives definitions from there. For example, the recommended solution uses a simple Filesystem resource; you may wish to use a more cluster-aware cLVM resource.
6. After running the shell script, you can issue a `crm status` command and the output should look like this:

   ```
   crm status
   ```

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

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

7 Add the following entry to `/etc/csync2/csync2.cfg`:

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

8 Run `csync2 -x -v`.

Run the command again if you get any error.

NOTE: The preceeding steps are used for installing and configuring the cluster for high availability. However, to use this cluster configuration, you must enable clustering from Administration Console. For more information, refer Section 3.3.3, “Post-Installation Cluster Configuration for Analytics Server,” on page 51.

3.3.3 Post-Installation Cluster Configuration for Analytics Server

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

- Section 3.3.3.1, “Enable Clustering,” on page 51
- Section 3.3.3.2, “Configure the settings for auditing,” on page 51

3.3.3.1 Enable Clustering

1 Click **Devices > Analytics Server**.

2 In the cluster row, click **Edit**.

3 In the **Cluster Configuration** section, set the **Clustering is Configured:** field to **Yes** and specify the same virtual IP address in the **Cluster’s Virtual IP:** field that you had specified during resource configuration. For more information, seeStep 2 on page 50.

3.3.3.2 Configure the settings for auditing

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

1 Perform the steps mentioned in “Enable Clustering” on page 51.

2 In the **Admin Tasks** pane, click **Auditing**.

3 In the **Audit Messages Using:** field, Select **Syslog: > Send to Analytics Server**

The Server Listening Address gets auto-populated with the virtual IP address that you had specified when performing step 1.

II Upgrading Access Manager Appliance

This section discusses how to upgrade Access Manager Appliance to the newer version. You must take a backup of the existing configurations before upgradingAccess Manager Appliance.

For more information, see "Back Up and Restore" in the *NetIQ Access Manager Appliance 4.3 Administration Guide*.

IMPORTANT: After upgrading to Access Manager 4.3, you must clear the browser cache to view the upgraded Administration Console. For more information, see TID 7018166.

If you are upgrading to 4.3 Service Pack 1, then you do not require to clear the browser cache.

NOTE

- By default, Access Manager 4.3 configuration uses stronger TLS protocols, ciphers, and other security settings. After upgrading if you want to revert these settings, see Restoring Previous Security Level After Upgrading Access Manager Appliance in the NetIQ Access Manager Appliance 4.3 Security Guide.
- Platform Agent and Novell Audit are not supported from Access Manager 4.2 onwards. If you upgrade from an older version of Access Manager to latest version, Platform Agent is still available. It is recommended to use Syslog for auditing.

This part describes how to upgrade Access Manager Appliance:

- Chapter 4, "Prerequisites," on page 55
- Chapter 5, "Upgrading the Operating System for Access Manager Appliance," on page 59
- Chapter 6, "Upgrading Access Manager Appliance," on page 61
- Chapter 7, "Getting the Latest Security Patches," on page 65

4 Prerequisites

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

- Any option that is configured through the `nidpconfig.properties` file will be overwritten after upgrade. Hence, ensure to back up the `nidpconfig.properties` file before upgrading to 4.3. After the upgrade, replace the new `nidpconfig.properties` file with the backed up file.
- Access Manager 4.2 onwards, some of the options are supported only through the Administration Console. After the upgrade, you must configure those options through the 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 Appliance 4.3 Administration Guide.
- The upgrade process overwrites all customized JSP files. If you have customized JSP files for the Identity Server or the Access Gateway, you must perform manual steps to maintain the customized JSP files. For more information, see Section 4.1, “Maintaining Customized JSP Files for Identity Server,” on page 55 or Section 4.2, “Maintaining Customized JSP Files for Access Gateway,” on page 57.
- If you have customized any changes to `tomcat.conf` or `server.xml`, you must back up the files. After the upgrade, restore the files.
- If you have installed the unlimited strength java crypto extensions before upgrade, you must re-install it after the upgrade because a new Java version will be used.
- If you are using Kerberos, ensure that you back up the `/opt/novell/nids/lib/webapp/WEB-INF/classes/kerb.properties` file.

4.1 Maintaining Customized JSP Files for Identity Server

Access Manager Appliance 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

4.1.1 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/nidp/lib/webapp/jsp` directory and place the copy somewhere else.

   WARNING: The upgrade overwrites all existing JSP files.

2. Upgrade Access Manager Appliance.

3 Create an empty folder `legacy` in Identity Server: `/opt/novell/nids/lib/webapp/WEB-INF/legacy`.

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

4 Copy your all backed up JSP files into the `/opt/novell/nids/lib/webapp/jsp` directory.

5 Refresh the browser to see the changes.

4.1.2 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/nidp/lib/webapp/jsp` directory and place the copy somewhere else.

WARNING: The upgrade overwrites all existing JSP files.

2 Upgrade Access Manager Appliance.

3 Create an empty folder `legacy` in Identity Server: `/opt/novell/nids/lib/webapp/WEB-INF/legacy`.

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

4 Copy your all backed up JSP files into the `/opt/novell/nids/lib/webapp/jsp` directory.

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

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

```
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.

5d Save the file.

5e Repeat the steps for the second JSP file.

6 Refresh the browser to see the changes.

4.2 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 Manager Appliance.
3. Create an empty folder `legacy` in Access Gateway: `/opt/novell/nesp/lib/webapp/WEB-INF/legacy`.

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

4. Copy your all backed up JSP files into the `/opt/novell/nesp/lib/webapp/jsp` directory.
5. Refresh the browser to see the changes.

5 Upgrading the Operating System for Access Manager Appliance

Access ManagerAppliance bundles the latest SUSE kernel. During fresh installation of Access ManagerAppliance, the latest kernel is installed automatically. You must upgrade the base operating system before upgrading Access ManagerAppliance.

NOTE: After upgrading base operating system, you also need to re-register the new channel. For more information, Section 5.1, “Setting Up the Channel After Upgrading Base Operating System,” on page 59.

Perform the following steps to upgrade the base operating system:

1. Get the Access Manager 4.3 Appliance ISO and mount it in the Access Manager server where you want to upgrade. For example, if you want to mount on `/root/iso`, use the following command:

   ```
   mount -o loop /dev/dvd /root/iso/
   ```

   NOTE: Create `/root/iso` by using the `mkdir -p /root/iso` command before executing the above command.

   ---

2. Use the following command to add the mounted ISO as the upgrade repository:

   ```
   zypper ar /root/iso/ 43appiso
   ```

3. Refresh the new repository by using the following command:

   ```
   zypper ref
   ```

4. Use the following command to upgrade the base operating system from the repository you added:

   ```
   zypper dup --from 43appiso
   ```

5. You will be prompted a dependency resolution for `open-iscsi` and `crash-sial-6.0.7-0.10.1.x86_64`. Select **1** from the solutions.
6. Accept the license. The operating system will start upgrading.
7. After upgrade, view the notification.
8. Restart Access Manager Appliance.

5.1 Setting Up the Channel After Upgrading Base Operating System

You must set up the channel if the base operating system is upgraded. If you had an existing channel for an older version of Access Manager and SLES operating system, then after upgrading to the latest operating system and Access Manager 4.3, you must re-register the new channel.

NOTE: If you are upgrading from Access Manager 4.2 and you have already set up the 4.2 channel, then you do not require to re-register the channel for 4.3.

Perform the following steps to set up the SLES 11 SP4 channel.

1. Upgrade the base Operating System to SLES 11 SP4. For more information about upgrading the base operating system, see Section 5, “Upgrading the Operating System for Access Manager Appliance,” on page 59.
2. Upgrade the Access Manager Appliance.
3. If the version mentioned in the `/etc/products.d/NAM_APP.prod` file is other than 4.2, edit the file and change the version to 4.2. The line will look like the following:

   ```
   <version>4.2</version>
   ```
4. Remove all the old NCC credentials using the following commands:

   ```
   rm /etc/zypp/credentials.d/NCCcredentials
   ```

   ```
   rm /etc/zypp/repos.d/nu*
   ```

   ```
   rm /etc/zypp/services.d/nu*
   ```
5. Use the `zypper lr` command to verify that the old channel is removed.
6. Re-register to get the latest updates. For more information, see Section 7.1, “Installing or Updating Security Patches for Access Manager Appliance and Analytics Server,” on page 65.
7. Use the `zypper lr` command to verify if the new channel `NAM42-APP-Updates` is added.

6 Upgrading Access Manager Appliance

- Section 6.1, “Upgrading from the Evaluation Version to the Purchased Version,” on page 61
- Section 6.2, “Upgrading Access Manager Appliance,” on page 61

6.1 Upgrading from the Evaluation Version to the Purchased Version

1. Log in as `root`.
2. Download the upgrade file from dl.netiq.com and extract the `tar.gz` file by 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.

3. Change to the directory where you extracted the file, then run the following command:

   ```
   ./sb_upgrade.sh
   ```

4. The system displays a message regarding restoring customized files.

   For more information about how to sanitize jsp pages, see Preventing Cross-site Scripting Attacks in the NetIQ Access Manager Appliance 4.3 Administration Guide.

5. A confirmation message is displayed.

   ```
   Would you like to continue this upgrade?
   ```

   Type **Y** to continue.

6. Enter the Access Manager Administration Console user ID.
7. Enter the Access Manager Administration Console password.
8. Re-enter the password for verification.

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

   ```
   Upgrade completed successfully.
   ```

6.2 Upgrading Access Manager Appliance

Prerequisite: Before upgrading Access Manager Appliance, perform the following actions:

1. Before upgrading, you must first upgrade the base operating system to the latest operating system that is included in the 4.3 Access Manager Appliance ISO. For more information about how to upgrade, see Section 5, “Upgrading the Operating System for Access Manager Appliance,” on page 59.
2. If you are upgrading Access Manager, and want to use syslog for auditing, you must first upgrade the base operating system.

3. (Optional) On RHEL, ensure that the SELinux configuration allows communication with local TCP port 1290.
4. If you have customized the `tomcat.conf` file or the `server.xml` file, back up these files before upgrading. These files are overwritten during the upgrade process.

NOTE: If you do not upgrade the base operating system before upgrading to 4.3, upgrade will display a warning message, but still allow upgrading to 4.3. If you are using unsupported versions for upgrade, it displays an error and terminates.

NOTE: Platform Agent and Novell Audit are no longer supported. Access Manager 4.2 onwards, the installation no longer installs Platform Agent and Novell Audit for auditing. If you upgrade from an older version of Access Manager to 4.3, Platform Agent is still available. It is recommended to use syslog for auditing. For more information about auditing, see Configuring Access Manager Appliance for Auditing in the NetIQ Access Manager Appliance 4.3 Administration Guide

---

Perform the following steps to upgrade Access Manager Appliance.

1 Log in as `root`.

2 Download the `tar.gz` file of Access Manager Appliance from dl.netiq.com and extract the `tar.gz` file using the following command:

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

NOTE: For information about the name of the file, see the Access Manager Appliance 4.3 Release Notes on theAccess Manager Documentation website.

3 Change to the directory where you extracted the file, then run the following command:

```
./sb_upgrade.sh
```

4 A confirmation message is displayed.

```
Platform Agent is no longer supported for auditing. It is recommended to use
Syslog instead. To use Syslog, ensure that you upgrade the base Operating
System followed by Access Manager/Gateway Appliance upgrade. After upgrading,
enable Syslog on the Auditing user interface of the Administration Console. Do
you want to proceed? (Y/N)
```

Type **Y** to continue.

5 The system displays a message regarding restoring customized files:

```
Before you restore your existing custom pages, ensure that you read and
understand the changes in steps from the Installation and Upgrade guide
available online.
# It is recommended that you run XSS checks for restored JSP files as
instructed in the Installation and Upgrade guide available online.
```

Type **Y** to confirm.

For more information about how to sanitize JSP pages, see Preventing Cross-site Scripting Attacks in the NetIQ Access Manager Appliance 4.3 Administration Guide.

6 Type **Y** and press Enter.

The system displays an information message to upgrade the base operating system and enable Syslog.

7 Type **Y** to continue with the upgrade, then press Enter.

The system displays a warning message to back up the existing JSP files.

8 Type **Y** to continue with the upgrade, then press Enter.

9 Enter the Access Manager Administration Console user ID.

10 Enter the Access Manager Administration Console password.

11 Re-enter the password for verification.

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

```
Upgrade completed successfully.
```

NOTE: If you have customized the Java settings in the `/opt/novell/nam/idp/conf/tomcat.conf` file, then copy the customized setting to the new file after the upgrade.

NOTE: If you have enabled history for risk-based authentication in a prior version of Access Manager, you must upgrade the database for risk-based authentication after upgrading to 4.3. You can find the upgrade script here: `/opt/novell/nids/lib/webapp/WEB-INF/RiskDBScripts.zip`.

MySQL: Run `netiq_risk_mysql_upgrade.sql`

Oracle: Run `netiq_risk_oracle_upgrade.sql`

Microsoft SQL Server: Run `netiq_risk_sql_server_upgrade.sql`

NOTE: To use Syslog for auditing, you need to upgrade the base operating system. After the upgrade, install the Syslog RPMs manually. To install the RPMs, execute the following command: `zypper in -t pattern NetIQ-Access-Manager`.

6.2.1 Removing Proxy Services And Protected Resources

After upgrading Access Manager, manually remove the portal and SSL VPN related proxy service and protected resources.

6.2.1.1 Removing Portal Related Proxy Service And Protected Resources

1 In the Administration Console, click **Access Gateway > Cluster > Edit > NAM - RP**.

2 Select the `namportal` path based service. Click **Delete**.

3 Click **Protected Resources**. Delete the following Protected Resources: **portal** and **portal_public**.

4 Click **OK** until the Access Gateway Servers page appears. Click **Update**.

6.2.1.2 Removing SSLVPN Related Proxy Service And Protected Resources

1 In the Administration Console, click **Access Gateway > Cluster > Edit > NAM - RP**.

2 Select the `sslvpn` path based service. Click **Delete**.

3 Click **Protected Resources**. Delete the following Protected Resources: **sslvpn** and **sslvpn_public**.

4 Click **OK** until the Access Gateway Servers page appears. Click **Update**.

7 Getting the Latest Security Patches

The OpenSSL open source project team regularly releases updates to known OpenSSL vulnerabilities. Access Manager Appliance and Analytics Server use the OpenSSL library for cryptographic functions. It is recommended that you keep Access Manager Appliance and Analytics Server updated with the latest OpenSSL patch.

Prerequisites

- ❒ Before upgrading the kernel, ensure that you have updated the operating system to a supported version.
- ❒ Access Manager Appliance and Analytics Server install a customized version of SLES 11 SP4. If you want to install the latest patches as they become available, you must have a user account to receive the Linux updates.
- ❒ Ensure that you have obtained the activation code for Access Manager Appliance from Novell Customer Center.

WARNING: Installing additional packages other than security updates breaks your support agreement. If you encounter a problem, Technical Support can require you to remove the additional packages and to reproduce the problem before receiving any help with your problem.

- Section 7.1, “Installing or Updating Security Patches for Access Manager Appliance and Analytics Server,” on page 65

7.1 Installing or Updating Security Patches for Access Manager Appliance and Analytics Server

To get the latest security updates for Access Manager Appliance and Analytics Server, you can follow any of these options:

- Section 7.1.1, “Registering to Novell Customer Center,” on page 65
- Section 7.1.2, “Configuring Subscription Management Tool,” on page 67

7.1.1 Registering to Novell Customer Center

To get the latest security updates for Access Manager Appliance and Analytics Server, the user must register with the Novell Customer Center by using the activation code obtained with the product:

NOTE: You must perform the proceeding steps to register with Novell Customer Center for Access Manager Appliance and Analytics Server separately.

If you face issues while using the activation code to register, see TID 3303599.

1. Go to **YaST > Support > Novell Customer Center Configuration**.
2. Select **Configure Now (Recommended)**. In addition to the options that are selected by default, select **Registration Code**.
3. Click **Next**.

   The Manual Interaction Required screen appears. It might take a few minutes to connect to the server.

   This screen indicates that to activate the product, you must provide a valid e-mail ID associated with the Novell account and the activation code.
4. Click **Continue**.
5. To specify the e-mail address, activation code, and system name in the relevant fields:

   5a Select the relevant option, then press **Enter**. A text field appears in the bottom left corner of the screen.

   5b Specify value for the selected option in this text field, then press **Enter** to return to the screen.

   5c Repeat these steps for each field.
6. Click **Submit** after you have specified all the relevant information to complete the registration.
7. Enter `Q` to close the window.
8. Enter `Y` at the prompt.

   The Manual Interaction Required screen is displayed. It indicates that the software repositories are created. You will receive a message from the Novell Customer Center Configuration indicating that the configuration was successful.
9. Click **OK** to return to YaST Control Center.
10. Click **Quit** to exit YaST.
11. Open a shell prompt and specify the following command to verify if the repository named `NAM4x-APP-Updates` was created:

    ```
    zypper lr
    ```

    An output similar to the following appears:

    Access Manager Appliance

    ```
    # | Alias                                | Name
    | Enabled | Refresh
    --+--------------------------------------+----------------------------------
    1 | NetIQAccessManagerAppliance-4.x.x-x | NetIQAccessManagerAppliance-4.x.x-x
    | Yes     | No
    2 | nu_novell_com:NAM4x-APP-Updates      | NAM4x-APP-Updates
    | Yes     | Yes
    ```

    Analytics Server

    ```
    # | Alias                                | Name
    | Enabled | Refresh
    --+--------------------------------------+----------------------------------
    1 | NetIQAnalyticsServer-4.x.x-x | NetIQAnalyticsServer-4.x.x-x
    | Yes     | No
    2 | nu_novell_com:NAM4x-APP-Updates      | NAM4x-APP-Updates
    | Yes     | Yes
    ```

12 Run the `zypper up` command to install the patches

13 After the patches are installed, restart the machine.

14 Confirm that all the patches are installed by running `zypper up` command again.

7.1.2 Configuring Subscription Management Tool

You can register Access Manager Appliance and Analytics Server to local Subscription Management Tool (SMT) server and download software updates from there instead of communicating directly with the Novell Customer Center and the NU servers.

To use an SMT server for client registration and as a local update source, you must configure the SMT server in your network first. The SMT server software is distributed as an add-on for SUSE Linux Enterprise Server. For information about configuring the SMT server, see Subscription Management Tool (SMT) for SUSE Linux Enterprise 11.

The following sections describe the configuration required for Access Manager Appliance:

- Section 7.1.2.1, “SMT Configuration,” on page 67
- Section 7.1.2.2, “Configuring Access Manager Appliance and Analytics Server,” on page 67

7.1.2.1 SMT Configuration

You must configure the SMT server and set up subscription for `NAM4x-APP-Updates` channel to receive the updates for Access Manager Appliance and Analytics Server.

1 Install the SMT server in a SLES 11 SP4 Server. For more information, see Subscription Management Tool (SMT) for SUSE Linux Enterprise 11.

2 Log in to you Novell Customer Center account.

3 Select **My Products > Mirroring Credentials**, then click **Generate Credentials**.

4 Copy the mirroring credentials before logging out of your Novell Customer Center account.

5 Run the *SMT Configuration* tool from YAST, then specify the mirroring credentials.

6 Run the **SMT Management** tool.

The `NAM4x-APP-Updates, sle-11-x86_64` repository is displayed in the **Repositories** tab.

7 Select `sle-11-x86_64`, then click **Toggle Mirroring** to ensure mirroring is selected for this repository.

8 Click **Mirror Now**. This step ensures that the *NAM4x-APP-Updates* channel updates are mirrored from **nu.novell.com** to your local SMT server.

9 When mirroring is complete, click **OK** to close the tool.

7.1.2.2 Configuring Access Manager Appliance and Analytics Server

1 Copy `/usr/share/doc/packages/smt/clientSetup4SMT.sh` from the SMT server to the client machine.

You can use this script to configure a client machine to use the SMT server or to reconfigure it to use a different SMT server.

2 Specify the following command as `root` to execute the script on the client machine:

```
./clientSetup4SMT.sh --host server_hostname
```

For example,

```
./clientSetup4SMT.sh --host smt.example.com.
```

You can get the SMT server URL by running the SMT Configuration tool at the server. The URL is set by default.

3. Enter `y` to accept the CA certificate of the server.
4. Enter `y` to start the registration.
5. The script performs all necessary modifications on the client.
6. Execute the following command to perform registration:

   ```
   suse_register
   ```

7. Specify the following command to get online updates from the local SMT server:

   ```
   zypper up
   ```

8. Reboot the machine if prompted at the end of any patch install.
9. Confirm that all the patches are installed by running `zypper up` command again.

III Troubleshooting Installation and Upgrade

- Chapter 8, “Troubleshooting Installation,” on page 71
- Chapter 9, “Troubleshooting Upgrade,” on page 75

8 Troubleshooting Installation

- Section 8.1, “Checking the Installation Logs,” on page 71
- Section 8.2, “Some of the New Hardware Drivers or Network Cards Are Not Detected during Installation,” on page 72
- Section 8.3, “Installation Through Terminal Mode Is not Supported,” on page 72
- Section 8.4, “Device Manager Installation Fails During the Appliance Installation,” on page 72
- Section 8.5, “Access Manager Appliance Installation Fails Due to an XML Parser Error,” on page 72
- Section 8.6, “DN Is Added as Provider ID While Installing NMAS SAML Method,” on page 73

8.1 Checking the Installation Logs

If Access Manager Appliance fails to install, check the installation logs.

The installation logs are located in the `/tmp/novell_access_manager` directory. The following log files should contain useful content. Check them for warning and error messages.

Log File	Description
`install_main_2011-06-06_17:28:19.log`	Contains messages generated for installing and configuring Access Manager Appliance.
`iinstall_edir_2011-06-06_17:38:35.log`	Contains messages generated for installing and configuring Administration Console configuration store.
`install_audit_2011-06-06_17:38:35.log`	Contains messages generated for installing and configuring NetIQ Auditing components.
`Novell_iManager_2.7_InstallLog.log`	Contains messages generated for installing and configuring iManager.
`install_iman_2011-06-06_17:38:35.log`	Contains messages generated for installing and configuring iManager.
`install_adminconsole_2011-06-06_17:38:35.log`	Contains messages generated for installing and configuring Administration Console.
`install_jcc_2011-06-06_17:38:36.log`	Contains messages generated for installing and configuring the Communications module.
`install_mag_2011-06-06_17:38:37.log`	Contains messages generated for installing and configuring Access Gateway.
`install_idp_2011-06-06_17:38:36.log`	Contains messages generated for installing and configuring Identity Server.
`configure_cluster_2011-06-06_17:28:19.log`	Contains messages generated for configuring Identity Server and Access Gateway.

8.2 Some of the New Hardware Drivers or Network Cards Are Not Detected during Installation

Installation of Access Manager Appliance might fail if some of the hardware drivers or network cards are not detected. If this happens, you must upgrade the hardware drivers manually:

1. Start the Access Manager Appliance installation.

   See Installing Access Manager Appliance in the NetIQ Access Manager Appliance 4.3 Installation and Upgrade Guide.
2. Select **Kernel Module (Hardware Driver)** in the main menu, then click **OK**.
3. Select **Add Driver Update**, then click **OK**.
4. Select the driver update medium.

   The driver update medium can be CD-ROM or floppy disk.
5. Click **OK** and continue with the installation.

8.3 Installation Through Terminal Mode Is not Supported

Installation through terminal mode is supported on GUI mode only. To work around this issue, initiate the installation in the GUI mode. After entering the required input, switch to the terminal mode. The installation is completed successfully.

8.4 Device Manager Installation Fails During the Appliance Installation

To workaround this issue, reinstall the appliance.

8.5 Access Manager Appliance Installation Fails Due to an XML Parser Error

This error may happen if the Appliance is installed by using a remotely mounted installer. Use a locally mounted installer to avoid this issue.

8.6 DN Is Added as Provider ID While Installing NMAS SAML Method

While installing the NMAS SAML method in an external user store, DN is added as Provider ID instead of the metadata URL.

To resolve this issue, perform the following steps:

1. Log in to Administration Console which has the external user store.
2. Go to **Roles and Tasks** > **NMAS** > **NMAS Login Methods** > **SAML Assertion** > **Affiliates**.
3. Select the respective Affiliate and change the provider ID to the identity provider metadata URL.

   For example, https://www.trunk2.com:8443/nidp/idff/metadata.

9 Troubleshooting Upgrade

- Section 9.1, “Access Gateway Throws a 403 Forbidden Page Error for a Resource Protected by a Form Fill Policy,” on page 75
- Section 9.2, “DN Is Added as Provider ID While Installing NMAS SAML Method,” on page 75
- Section 9.3, “Issue in SSL Communication between Access Gateway and Web Applications,” on page 75
- Section 9.4, “Customized Login Pages Are Missing After Upgrading Access Manager,” on page 76

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

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

9.2 DN Is Added as Provider ID While Installing NMAS SAML Method

While installing the NMAS SAML method in an external user store, DN is added as Provider ID instead of the metadata URL.

To resolve this issue, perform the following steps:

1. Log in to Administration Console which has the external user store.
2. Go to **Roles and Tasks** > **NMAS** > **NMAS Login Methods** > **SAML Assertion** > **Affiliates**.
3. Select the respective Affiliate and change the provider ID to the identity provider metadata URL. For example, https://www.trunk2.com:8443/nidp/idff/metadata.

9.3 Issue in SSL Communication between Access Gateway and Web Applications

After upgrading Access Manager from 3.1 SP4 or 3.1 SP5 to 4.0.x, applications are not accessible. This issue happens when there is any discrepancy between the cipher suites configured for Access Gateway and the applications protected by this Access Gateway. To workaround this issue, see TID 7016872.

9.4 Customized Login Pages Are Missing After Upgrading Access Manager

After upgrading Access Manager, you cannot view the customized login JSP pages. This happens when the customized JSP files are not restored or the `legacy` filesystem directory is not created.

To resolve this issue, see Maintaining Customized JSP Files for Identity Server in the NetIQ Access Manager Appliance 4.3 Installation and Upgrade Guide.

IV Appendix

- Appendix A, “Configuring Ports 9000 and 9001 to Listen on the Specified Address,” on page 79

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

In Access Manager Appliance 4.3, ports 9000 and 9001 listen on 127.0.0.1 by default. Access Manager Appliance 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 `tomcat7.conf` file:

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

```
"com.microfocus.nam.adminconsole.localhost.ipaddress"
```

For example:

```
JAVA_OPTS="${JAVA_OPTS} -
Dcom.microfocus.nam.adminconsole.localhost.ipaddress=10.0.0.0"
```