NetIQ Access Manager 3.2

Appliance Whitepaper

Contents

1 Introduction

Access Manager Appliance is a new deployment option introduced in NetIQ Access Manager 3.2 that includes all the major components such as Administration Console (AC), Identity Server (IDS), Access Gateway (AG), and SSL VPN in a single soft appliance. This solution differs from the other Access Manager model where all the components are installed on separate machines.

Access Manager Appliance enables organizations to rapidly deploy and secure web and enterprise thereby simplifying access to any application.

Enhancements to NetIQ Access Manager 3.2 provide the Appliance feature without sacrificing scalability for most deployments. The reduced deployment and configuration time gives quick time to value and lower total cost of ownership.

This paper provides information to help you determine if the Access Manager Appliance is right for your business needs.

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

- Quick installation and automatic configuration
- Single port configuration, one place to manage certificates
- Sample portal for administrator reference
- Fewer DNS Names, SSL Certificates and IP Addresses
- Lower hardware requirements

These differentiators and other features of the Access Manager Appliance are described in detail in Access Manager and Access Manager Appliance Comparison

The following figure describes in a pictorial manner the differences between deployment models of Access Manager and the Access Manager Appliance.

Figure 1:Typical Deployment of Access Manager

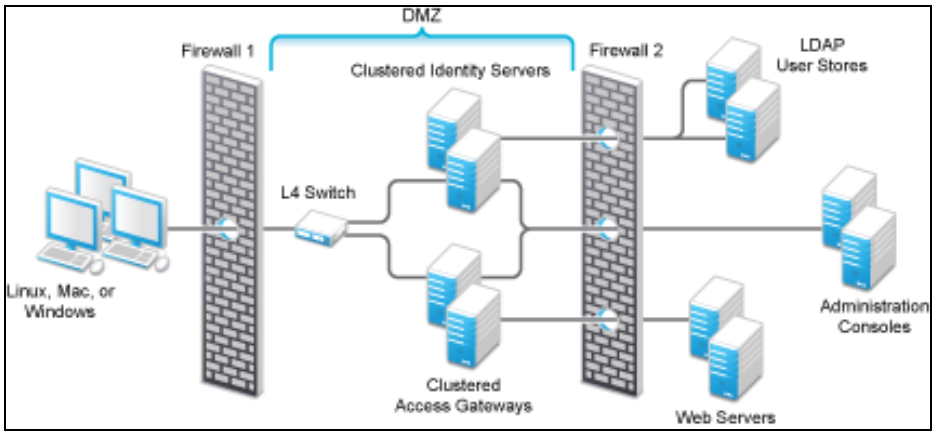
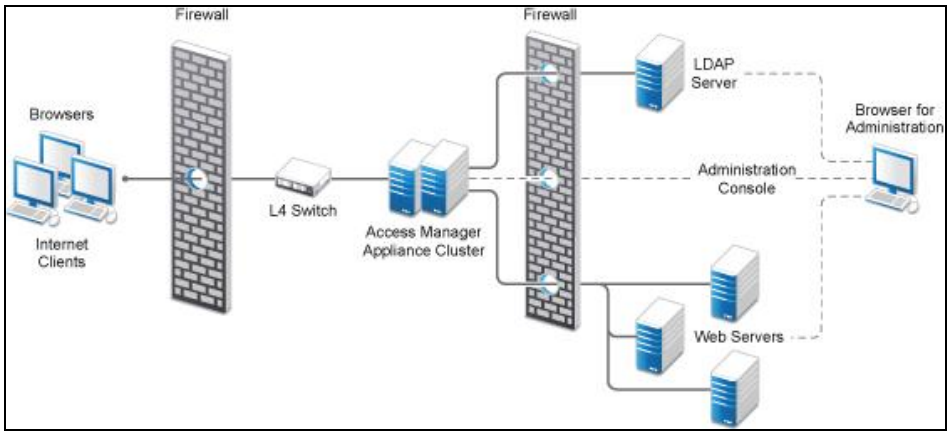


Figure 2: Typical Deployment of Access Manager Appliance



2 Use Cases

This section describes common usage patterns to help you understand the possibilities and functionalities of 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 don't want to go through the long process of designing, installing and configuring a full-fledged Web access management solution.
- You do not have a Web access management/Federation solution and 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.com.
- You want to reduce server hardware and management cost by consolidating Access Manager services on fewer servers.
- You want to quickly setup a test environment to verify changes.
- You want to quickly setup and evaluate Access Manager.

3 Access Manager and Access Manager Appliance Comparison

Both Access Manager and Access Manager Appliance deployment models use a common code base. But the installation differences between both the deployment models result in a few similarities and differences in the features. Refer this table to understand the details and determine which solution fits your business needs:

Features	Access Manager Appliance	Access Manager
Server Virtualization Support	Supported on VMware and Xen For virtual machine requirements, see Virtual Machine Requirements	Supported on VMware and Xen For virtual machine requirements, see Virtual Machine Requirements
Host Operating System	A soft appliance that includes a pre-installed and configured SUSE Linux operating system. Both the operating system and Access Manager patches are maintained by NetIQ through the patch update channel.	Operating System choice is more flexible. Administration Console, Identity Server, Access Gateway and SSL VPN can be installed on a supported operating system (SUSE, Red Hat, or Windows). Access Manager patches are maintained by NetIQ through the patch update channel. You must purchase, install and maintain the underlying operating system.

Features	Access Manager Appliance	Access Manager
Component Installation Flexibility	Access Manager components such as the Administration Console, Identity Server, Access Gateway, and SSL VPN cannot be selectively installed or uninstalled.	Each Access Manager component such as the Administration Console, Identity Server, Access Gateway and SSL VPN, can be 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 will require 6-8 or more virtual or physical servers (2 Administration Consoles, 2 Identity Servers, 2 Access Gateways, 2 SSL VPN).
Administration Console Access	Administration Console is installed on the Access Manager Appliance along with all other components. By using two network interfaces, access to the Administration Console can be limited to the private IP network bound to the internal network while 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 NAM 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. But upgrading from Access Manager to Access Manager Appliance is not supported.	You can upgrade from one version of Access Manager to another version. But upgrading from Access Manager Appliance to Access Manager is not supported.
Migration from Access Manager to Access Manager Appliance or vice-versa.	If you are migrating from Access Manager Appliance to Access Manager, the policies can be exported but the rest of the configuration has to be done manually.	If you are migrating from Access Manager to Access Manager Appliance, the policies can be exported but the rest of the configuration has to be done manually.

Features	Access Manager Appliance	Access Manager
Disaster Recovery	You can use the backup and restore process to save your Access Manager 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.	Takes 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. It takes only a few basic parameters as input. Several options assume default values.	The installation process allows for more flexibility by offering more selectable parameters. For example: You can either install SSLVPN along with Access Gateway or install SSLVPN separately on a different machine.
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.	Delivered in the form of multiple operating system- specific binaries.
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 the internal network.
NIC Bonding	IP address configuration is done through Administration Console. So, NIC bonding is not supported.	NIC bonding can be done through the operating system and NAM in turn uses this configuration
Networking: Port Details	The Administration Console, Identity Server, and SSL VPN are accelerated/protected by Access Gateway(s). Only HTTPS port 443, is required to access the Access Manager Appliance through a firewall.	Multiple ports need to be opened for deployment. For more information, see Installation Requirements
Certificate Management	Certificate management is simplified. All the certificates and key stores are stored in one place making replacing or renewing certificates easier.	Changes are required at multiple places to replace or renew certificates.

Features	Access Manager Appliance	Access Manager
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 communication.
Associating different signing certificates for each Service Provider	Not supported.	A unique signing certificate can be assigned to each Service Provider. For environments with a large number of trust relationships, using this feature can ease the process of replacing expiring certificates. Note: This is a new feature introduced in NAM 3.2.2.
Associating different certificates to Identity Server	Not applicable because Identity Server is accelerated by Access Gateway.	Supported. Identity Server can be behind Access Gateway or can be placed separately in the DMZ.
Sample Portal	After a successful installation, a sample web portal is deployed for administrator reference. The administrator can access the sample portal using the http://hostname URL. This portal provides detailed example of Access Manager Appliance usage and policy configuration.	Not available

Features	Access Manager Appliance	Access Manager
Ready-made Access Manager	The following configuration is automatically done when Access Manager Appliance is installed: • Importing Identity Server, Access Gateway, and SSL VPN components. • Automatic cluster creation of Identity Server, Access Gateway, and SSL VPN component. • Automatic configuration of Identity Server and SSLVPN to bring it to green state. • Automatic configuration of Access Gateways and Identity Server Association. • Automatic service creation to accelerate/protect the Identity Server, Administration Console, and sample portal. As the inter-component configuration is automatic, the administrator only needs to add the existing user store(s) and accelerate/protect/sso-enable existing web applications.	Each component has to be manually configured and set up before web applications can be federation enabled, accelerated or protected.
J2EE Agents	Does not support J2EE agents.	You can install and configure the J2EE Agent components when you need fine-grained access control to Java J2EE applications.
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.
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, Access Gateways, SSL VPNs, and up to three of Administration Consoles. The first three nodes of Access Manager Appliance contain the Administration Console, Identity Server, Access Gateway, and SSL VPN. Fourth installation onwards, the node has all components except for the Administration Console. A typical Access Manager Appliance	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 machines are required A typical Access Manager deployment in a cluster is described in Figure 3

Features	Access Manager Appliance	Access Manager
	deployment in a cluster is described in Figure 4	

Figure 3: Clustering Access Manager

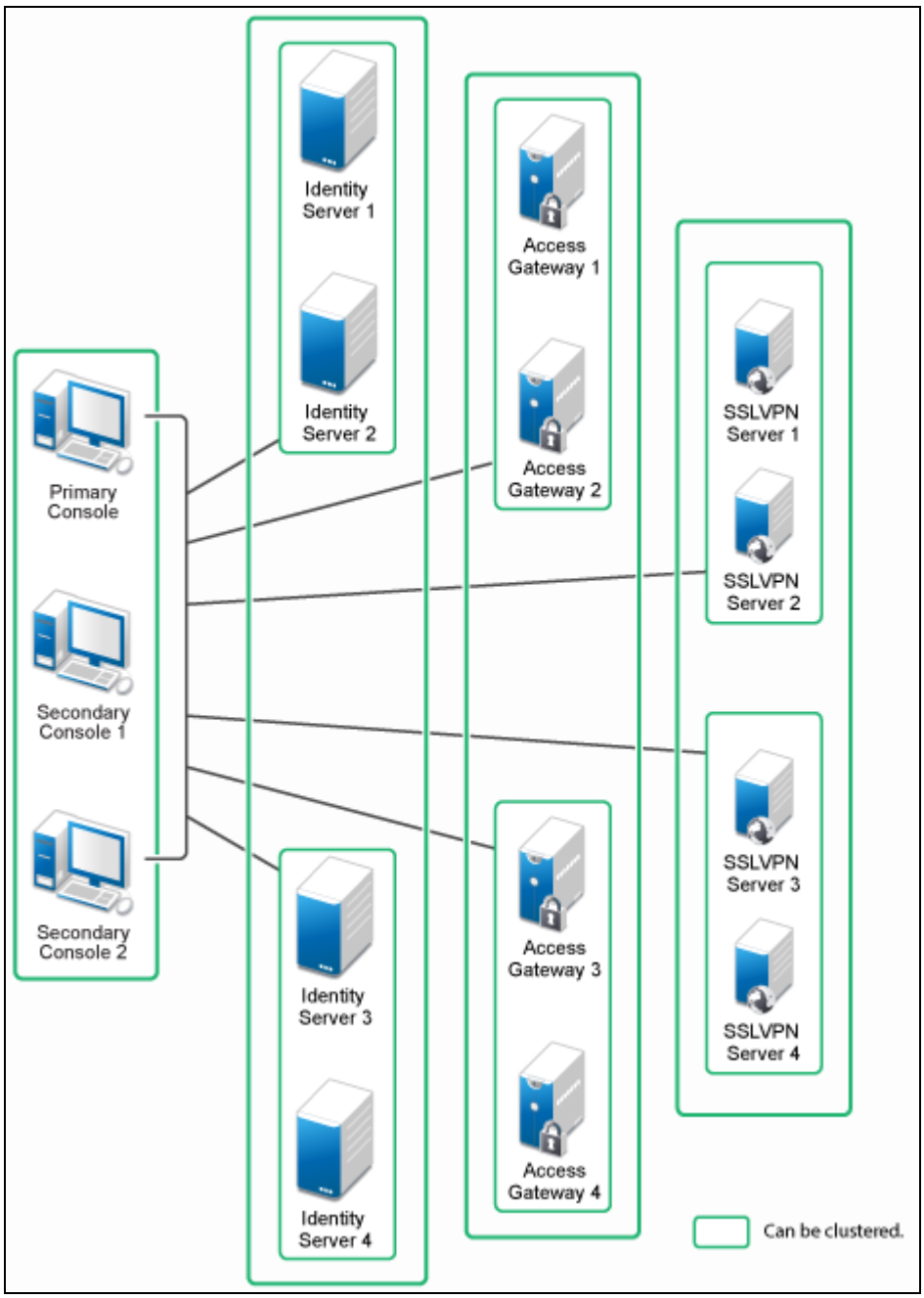
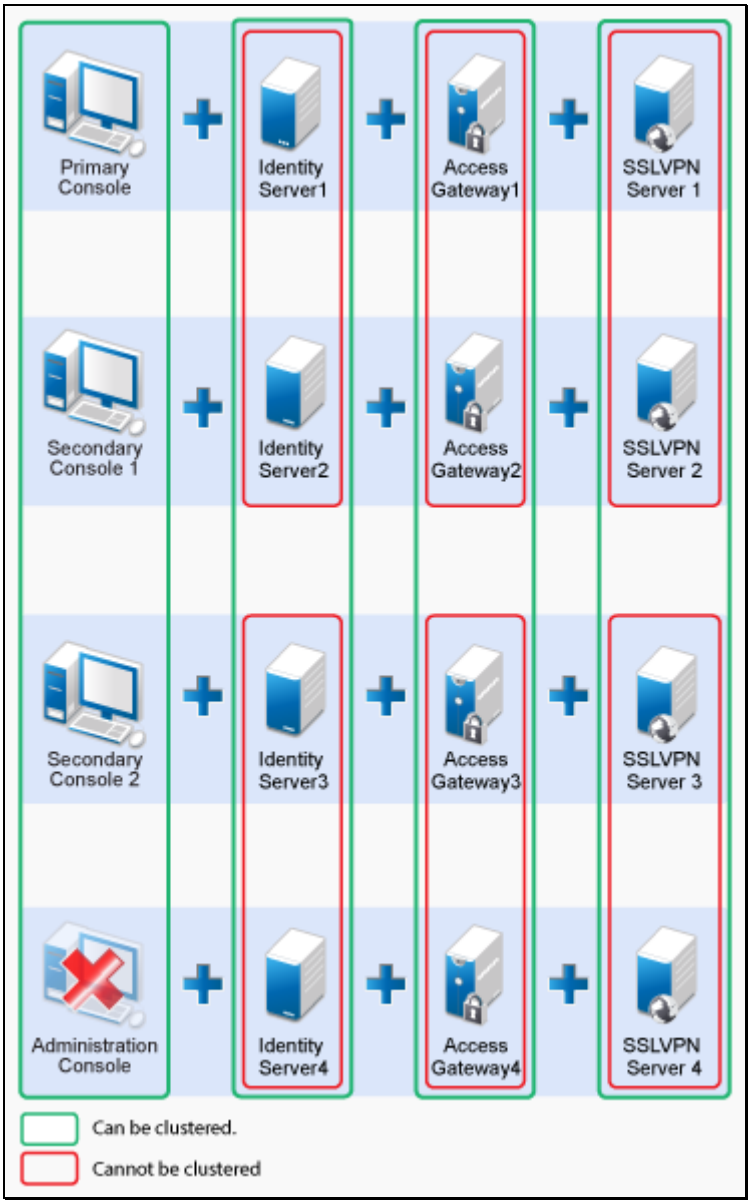


Figure 4: Clustering Access Manager Appliance



4 General Guidelines

This section provides the following guidelines and any potential workarounds for Access Manager Appliance:

- 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/network.
- Changing the primary IP Address of an Access Manager Appliance is not recommended. 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 about https://www.netiq.com/documentation/netiqaccessmanager32_appliance/adminconsolehelp/data/b8ilbpe.html

- Clustering is not supported between Access Manager and Access Manager Appliance.
- It is not possible to install monitoring software to monitor statistics on an Access Manager Appliance.
- It is not possible to different certificates for signing, encryption in a Federation setup.