NetIQ Access Manager 3.2

Appliance Whitepaper

NetIQ.

Legal Notice

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

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

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

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

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

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.

Contents

1 Introduction

Access Manager Appliance is a new deployment model introduced in NetIQ Access Manager 3.2. The model includes all 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 components are installed on separate systems. Access Manager Appliance enables organizations to rapidly deploy and secure Web and enterprise applications. This mode simplifies 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 helps lower the total cost of ownership.

This document helps you determine whether Access Manager Appliance suits 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 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 Access Manager and Access Manager Appliance Comparison

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

Figure 1: Typical Deployment of Access Manager

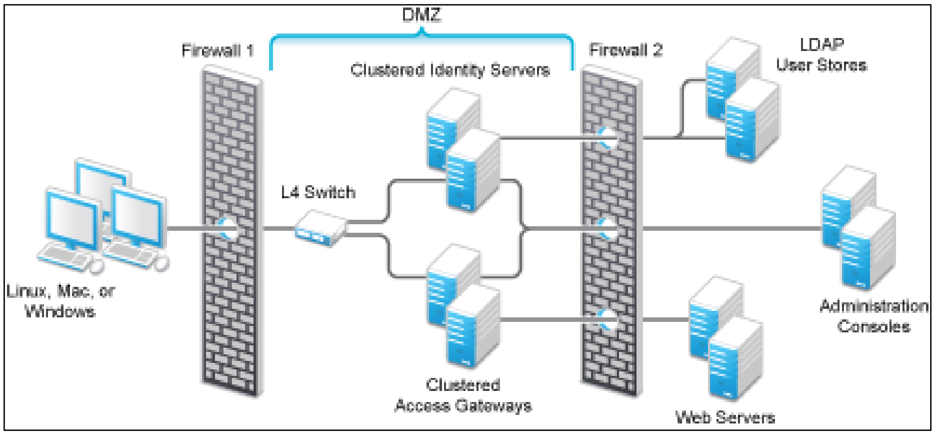
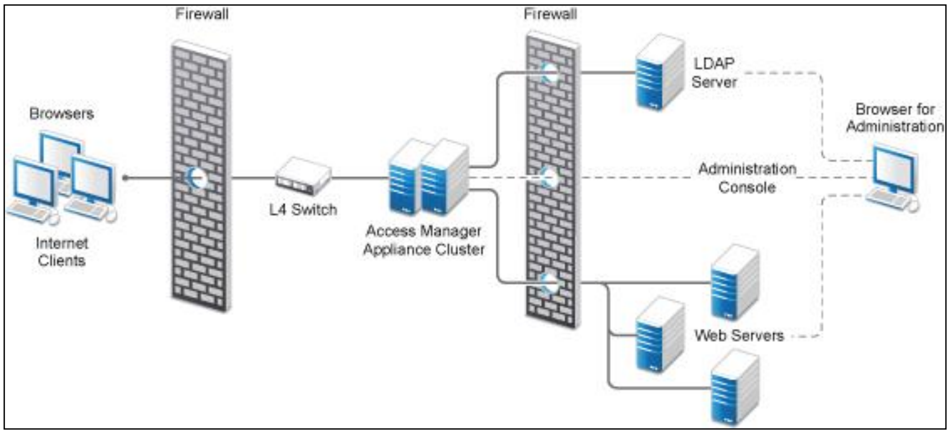


Figure 2: Typical Deployment of Access Manager Appliance



2 When to Choose the Access Manager Appliance

This section describes scenarios in which you can deploy Access Manager.

- You are interested in deploying Access Manager but need fewer servers.
- You still use 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.com.
- 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 set up 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 differences in the deployment method result in few similarities and differences in the features of both models. Refer to the following table to understand the details and determine which solution fits your business:

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.	The operating system choice is more flexible. Install Administration Console, Identity Server, Access Gateway, and SSL VPN 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.
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 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 (two Administration Consoles, two Identity Servers, two Access Gateways, two SSL VPNs).

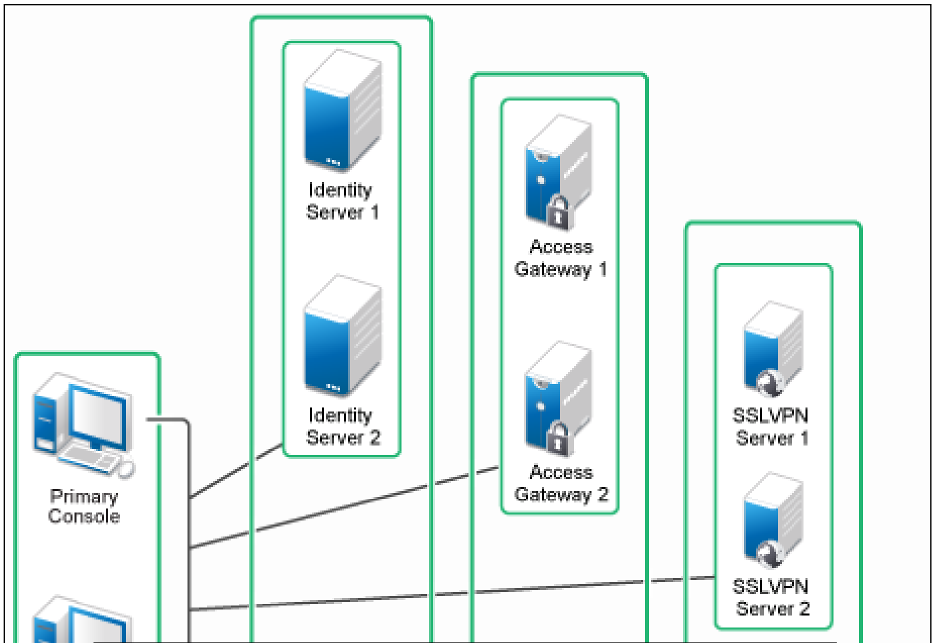
Features	Access Manager Appliance	Access Manager
Administration Console Access	The Administration Console is installed on the Access Manager Appliance along with all other components. If you use two network interfaces, access to the Administration Console can be limited to the private IP network bound to the internal network. The public interface is bound to an externally accessible network.	The 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	The Access Manager Appliance scales vertically on adding CPU and memory resources to each node. For more information, see Performance and Sizing Guidelines.	The Access Manager scales both vertically and horizontally on adding nodes. For more information, see Performance and Sizing Guidelines.
High Availability	High Availability is supported.	High Availability is supported.
Upgrade	You can upgrade from one version of Access Manager Appliance to another version. Upgrading from Access Manager to Access Manager Appliance is not supported.	You can upgrade from one version of Access Manager to another version. Upgrading from Access Manager Appliance to Access Manager is not supported.
Migration between Models	During migration from Access Manager Appliance to Access Manager, the policies can be exported but the rest of the configuration should be done manually.	During migration from Access Manager to Access Manager Appliance, the policies can be exported but the rest of the configuration should be done manually.
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	During installation and configuration of Access Manager Appliance, several steps are automated to quickly set up the system.	Installation and configuration of Access Manager requires more time since 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.	With Access Manager you have more flexibility during installation in terms of selectable parameters.

Features	Access Manager Appliance	Access Manager
		For example: You can either install SSL VPN along with Access Gateway or install SSL VPN separately on a different system.
Installation and Configuration Phases	The installation program takes care of the configuration for each component. The system is ready for use after it is installed.	There are 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 uses this configuration.
Networking: Port Details	The Administration Console, Identity Server, and SSL VPN are accelerated and 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
Networking: General	If Administration Console is in a DMZ, restrict access through the private interface.	Because the Administration Console is a separate component, access can be restricted or the Administration Console can be placed in an internal network.
Certificate Management	Certificate management is simplified. All certificates and key stores are stored in one place making replacing or renewing certificates easier.	Changes are required in multiple places to replace or renew certificates.
Certificate Management: SAML Assertion Signing	The same certificate is used for all communication. (signing, encryption, and transport).	Because there are multiple key stores, you can configure different certificates for the communication.
Signing Certificates for Service Providers	Associating different signing certificates for each service provider is 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 new feature introduced in Access Manager 3.2 SP2.

Features	Access Manager Appliance	Access Manager
Associating Different Certificates to Identity Server	This capability is not applicable because the Identity Server is accelerated by the Access Gateway.	This capability is supported. The Identity Server can be behind the Access Gateway or can be placed separately in the DMZ.
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.	A sample portal is not available.
Ready-Made Access Manager	The following configuration steps are automatically completed 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 components. • 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 or protect the Identity Server, Administration Console, and sample portal. Because the inter-component configuration is automated, the administrator needs only 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 and protected.
J2EE Agents	Access Manager Appliance 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	Access Manager Appliance supports installation of the latest SLES operating system security patches.	You are fully responsible for all operating system maintenance including patching.

Features	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, Access Gateways, SSL VPNs, and up to three Administration Consoles. The first three nodes of Access Manager Appliance contain the Administration Console, Identity Server, Access Gateway, and SSL VPN. For the 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 4	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 3

Figure 3: Clustering Access Manager



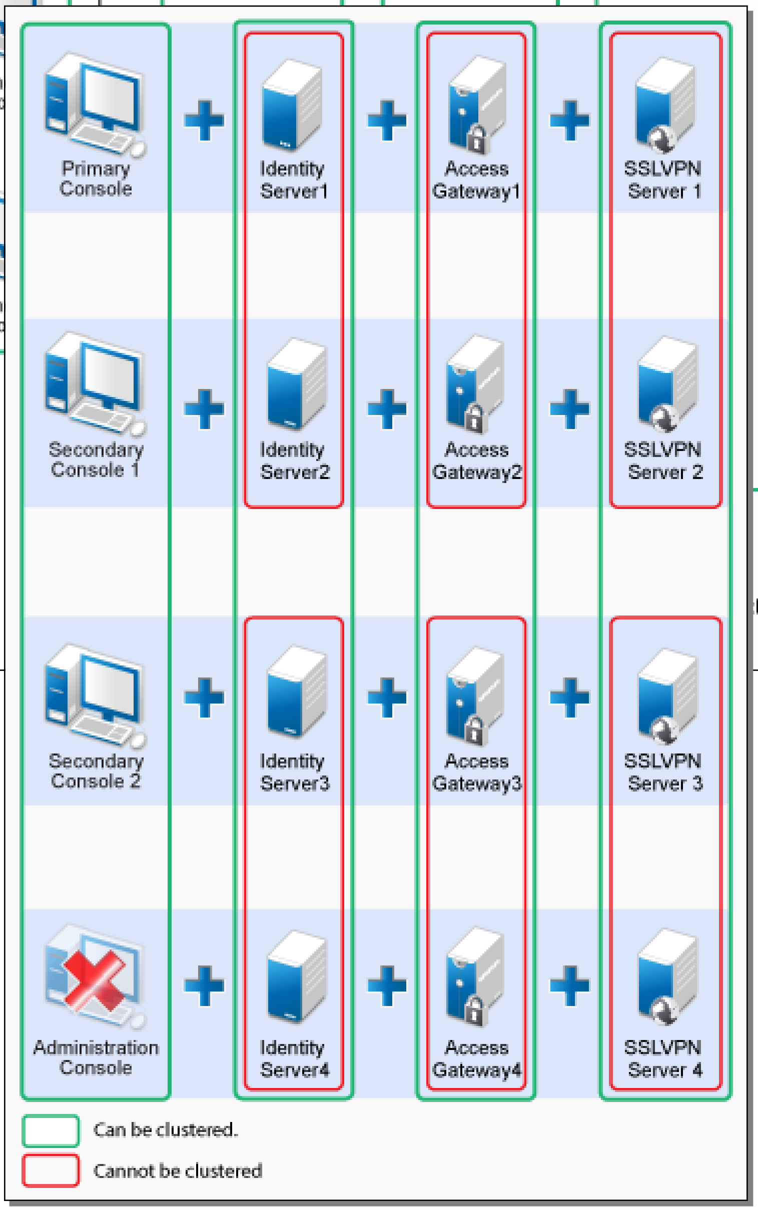


Figure 4: Clustering Access Manager Appliance

4 General Guidelines

Use the following general guidelines when using the 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 or network.
- It is not recommended to change the primary IP Address of an Access Manager. Changing this might result in corruption of the configuration store. However, you can modify the Listening IP address of reverse proxy or the outbound IP address used to communicate with the Web server. For more information, see https://www.netiq.com/documentation/netiqaccessmanager32_appliance/adminconsolehelp/data/b8ilbpe.html
- Clustering between Access Manager and Access Manager Appliance is not supported.
- You cannot install monitoring software to monitor statistics on an Access Manager Appliance.
- You cannot have different certificates for signing and, encryption in a Federation setup.