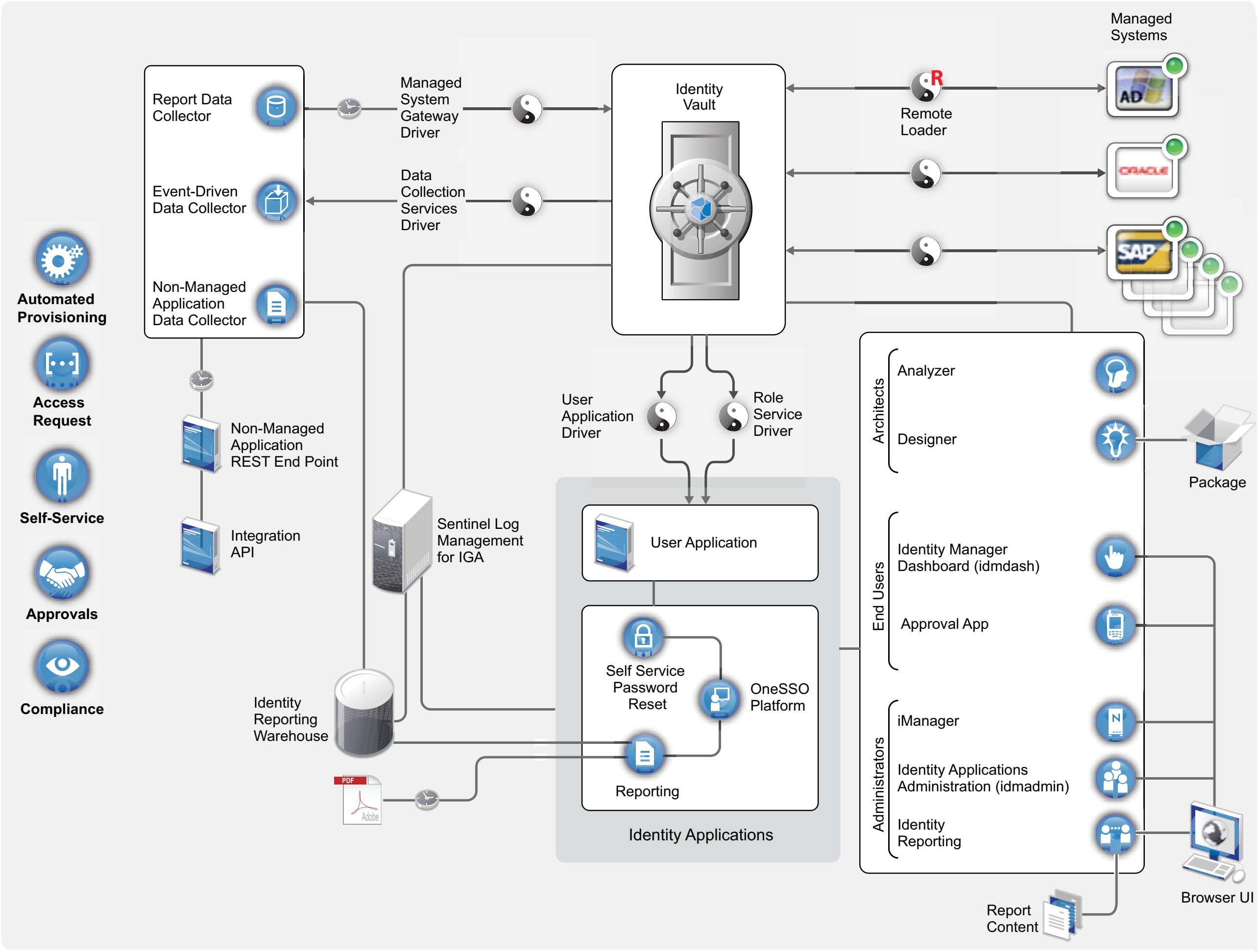
Quick Start

Quick Start Guide for Installing NetIQ Identity Manager 4.8

October 2019

This document provides guidelines to help you quickly understand the Identity Manager 4.8 installation process.

Before beginning, you must understand how different components are integrated in Identity Manager.



For more information, see How Identity Manager Works in the *NetIQ Identity Manager Overview and Planning Guide*.

Installation Overview

Installing Identity Manager includes the following tasks:

1. Planning your installation
2. Installing and configuring the Identity Manager components
3. Verifying the installation for each component
4. Performing any post-installation tasks

For more information about installing the components, see the *NetIQ Identity Manager Setup Guide for Linux* or *NetIQ Identity Manager Setup Guide for Windows*.

Planning Your Installation

Review the following information before installing Identity Manager:

Topic	**See...**
Feature comparison between Identity Manager Advanced and Standard Edition	Release Notes
Downloading the installation files	Release Notes
Locating the executables and default installation paths	Release Notes
Installation prerequisites	Prerequisites for each component in *NetIQ Identity Manager Setup Guide for Linux* or *NetIQ Identity Manager Setup Guide for Windows*.
System requirements	System requirements for each component in the System Requirements for Identity Manager 4.8.

For detailed information, see Planning to Install Identity Manager in the *NetIQ Identity Manager Setup Guide for Linux* or Planning to Install Identity Manager in the *NetIQ Identity Manager Setup Guide for Windows*.

Installing and Configuring Identity Manager

You can install Identity Manager components on the same server or on multiple servers depending on your deployment strategy. Before you start installation, evaluate how you want to implement Identity Manager.

Components Installed

Identity Manager installation programs for Linux and Windows use different approaches for installing the components. The installer for Linux provides options to install a group of components together. However, the installer for Windows provides an option to install the components independently. You must review the following details to understand the installation pattern for your platform:

- **Linux:** The installer obfuscates several underlying components and supporting software required by the Identity Manager components to run. For more information, see "Understanding Linux Installables" on page 3.
- **Windows:** The installer allows you to separately install the individual components. For more information, see "Understanding Windows Installables" on page 4.

Understanding Linux Installables

The installation program provides concise interactive and silent methods for installing and configuring the following Identity Manager components on Linux:

- Identity Manager Engine (Installs Identity Vault, Identity Manager engine, and Identity Manager drivers. The installation process also installs Oracle Java Runtime Environment (JRE).)
- Identity Manager Remote Loader Service (Installs the Remote Loader service and the driver instances in the Remote Loader. The Remote Loader allows you to run Identity Manager drivers on connected systems that do not host the Identity Vault and the Identity Manager engine.)
- Identity Manager Fanout Agent (Installs the Fanout agent for the JDBC Fanout driver. The JDBC Fanout driver uses the Fanout agent to create multiple JDBC Fanout driver instances. The Fanout agent loads the JDBC driver instances based on the configuration of the connection objects in the Fanout driver. For more information, see *NetIQ Identity Manager Driver for JDBC Fanout Implementation Guide*.
- iManager Web Administration (Installs the iManager Web Administration console and iManager plug-ins)
- Identity Applications (Installs several components that provide the underlying framework for Identity Applications: Identity Manager Dashboard, Identity Manager Administration Console, User Application, User Application driver (UAD), Role and Resource Service driver (RRSD), One Single Sign-On Provider (OSP), Password Management component (SSPR), PostgreSQL, PostgreSQL JDBC driver, and Tomcat application server)

  This component is only available for Advanced Edition.
- Identity Reporting (Installs several components that provide the underlying framework for Identity Reporting: Identity Reporting, Managed System Gateway driver (MSGW), and Data Collection Service driver (DCS), OSP, and Tomcat application server)

NetIQ does not support guided installation (GUI) method for these components.

The installer includes two separate phases for installing and configuring these components. The installer also provides default values for most of the common settings. However, you can customize the settings to meet your requirements. Depending on the Identity Manager Edition selected during installation, different components will be installed.

This installer does not include the following components that must be separately installed from the `.iso` file.

- Designer for Identity Manager
- Analyzer for Identity Manager
- Sentinel Log Management for Identity Governance and Administration

Designer for Identity Manager and Analyzer for Identity Manager are also available in separate installation packages. For more information, see Installing Designer and Installing Analyzer in the *NetIQ Identity Manager Setup Guide for Linux*. For information about installing Sentinel Log Management for IGA, see Installing Sentinel Log Management for Identity Governance and Administration in the *NetIQ Identity Manager Setup Guide for Linux*.

Understanding Windows Installables

The installation program separately installs the following Identity Manager components on Windows:

- Identity Vault (eDirectory)
- iManager
- Identity Manager Engine
- Designer (should be installed on a client computer)
- Analyzer (only required for analyzing, cleaning, and preparing an organization's data for synchronization)
- Remote Loader
- Tomcat (supported application server)
- Single Sign-on Provider (OSP)
- Password Management component (SSPR)
- Identity Applications
- Identity Reporting

After completing the installation, you may want to configure the settings for some components to meet your requirements. For more information, see *NetIQ Identity Manager Setup Guide for Windows*.

Installation Order

The installation programs vary for Linux and Windows operating systems. Before starting the installation, review how components are installed for your platform. For more information, see "Understanding Linux Installables" on page 3 and "Understanding Windows Installables" on page 4.

You must install the components in the following sequence on Linux:

1. Sentinel Log Management for Identity Governance and Administration
2. Identity Manager Engine components
3. Identity Applications components (not required for Standard Edition)
4. Identity Reporting components
5. Designer
6. Analyzer

You must install the components in the following sequence on Windows:

1. Identity Vault (eDirectory)
2. iManager
3. Identity Manager Engine
4. Designer
5. Analyzer

6. Remote Loader
7. Tomcat
8. OSP
9. SSPR
10. Identity Applications (not required for Standard Edition)
11. Identity Reporting

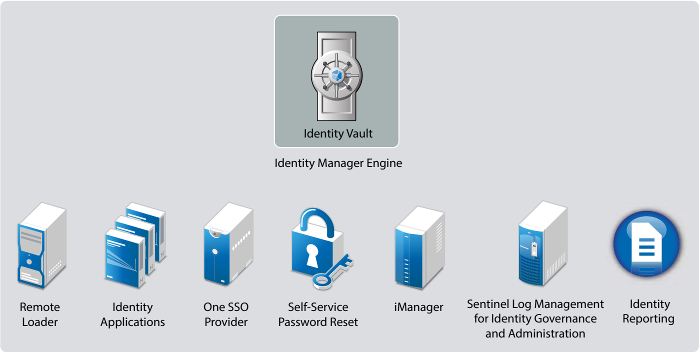
Installation Procedure

There are different ways to install and configure Identity Manager to take advantage of all of its features. The following scenarios provide an overview of the flexibility built into Identity Manager. Use them to design a deployment strategy that fits the needs of your company. Regardless of the deployment option you choose, verify that your server meets the system requirements for each component that you are planning to install. For more information, see *NetIQ Identity Manager Setup Guide for Linux* or *NetIQ Identity Manager Setup Guide for Windows*.

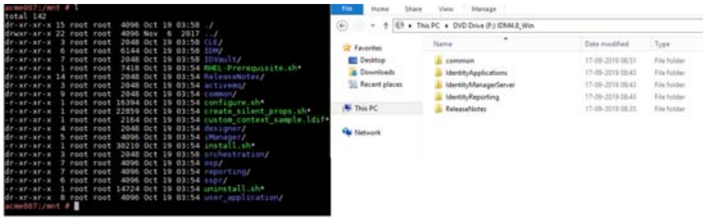
IMPORTANT: These deployment scenarios are examples to help you install Identity Manager. You can use these examples for reference purpose. These examples do not reflect best practices or recommended configuration for a production environment. You must reach out to a NetIQ Consulting Services or a NetIQ Partner Services professional to help you design the Identity Manager system that is suitable for your environment.

Basic Setup

The most basic deployment option is an all-in-one system that contains all Identity Manager components on a single server.



The all-in-one deployment is suitable only for installing Identity Management Proof-of-Concept (POC). This setup may cause performance issues in production environments. You can install all components on one Linux or Windows computer except NetIQ Sentinel Log Management for Identity Governance and Administration component, which can be installed only on Linux computers. You can perform this installation by running the installation files from the Identity Manager installation package for your operating system.

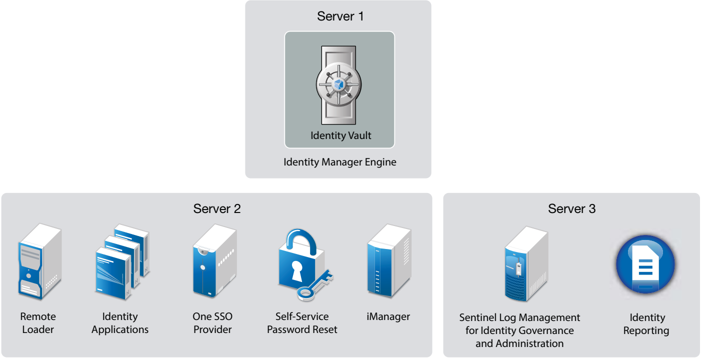


```
acme007:/mnt # l
total 142
dr-xr-xr-x 15 root root  4096 Oct 19 03:58 ./
drwxr-xr-x 22 root root  4096 Nov  6  2017 ../
dr-xr-xr-x  3 root root  2048 Oct 19 03:58 CLE/
dr-xr-xr-x  6 root root  6144 Oct 19 03:58 IDM/
dr-xr-xr-x  7 root root  2048 Oct 19 03:58 IDVault/
-r-xr-xr-x  1 root root  7418 Oct 19 03:54 RHEL-Prerequisite.sh*
dr-xr-xr-x 14 root root  2048 Oct 19 03:54 ReleaseNotes/
dr-xr-xr-x  3 root root  2048 Oct 19 03:54 activemq/
dr-xr-xr-x  9 root root  2048 Oct 19 03:54 common/
-r-xr-xr-x  1 root root 16394 Oct 19 03:54 configure.sh*
-r-xr-xr-x  1 root root 22859 Oct 19 03:54 create_silent_props.sh*
-r-xr-xr-x  1 root root  2164 Oct 19 03:54 custom_context_sample.ldif*
dr-xr-xr-x  4 root root  2048 Oct 19 03:54 designer/
dr-xr-xr-x  5 root root  4096 Oct 19 03:54 iManager/
-r-xr-xr-x  1 root root 38210 Oct 19 03:54 install.sh*
dr-xr-xr-x  3 root root  2048 Oct 19 03:58 orchestration/
dr-xr-xr-x  7 root root  4096 Oct 19 03:54 osp/
dr-xr-xr-x  7 root root  4096 Oct 19 03:54 reporting/
dr-xr-xr-x  6 root root  4096 Oct 19 03:54 sspr/
-r-xr-xr-x  1 root root 14724 Oct 19 03:54 uninstall.sh*
dr-xr-xr-x  8 root root  4096 Oct 19 03:54 user_application/
acme007:/mnt #
```

Name	Date modified	Type
common	17-09-2019 08:51	File folder
IdentityApplications	17-09-2019 08:43	File folder
IdentityManagerServer	17-09-2019 08:43	File folder
IdentityReporting	17-09-2019 08:43	File folder
ReleaseNotes	17-09-2019 08:35	File folder

To provide scalability to different components, you can extend a basic setup to accommodate the requirements of a production environment where services are distributed across multiple servers. This type of installation allows you to install Identity Manager components separately or customize a large portion of the settings.

In a simple approach, you can dedicate one server to the Identity Manager engine and Remote Loader and a second server to the identity applications and its supporting components, and iManager. You can include an additional server to host the components for reporting service to suffice the system requirements for running the Sentinel Log Management for IGA component.



Perform the following steps to install Identity Manager in this setup:

1. Install Sentinel Log Management for IGA on Server 3. This server must be a Linux computer.

   You can generate the required audit reports by using Sentinel Log Management for IGA.

2. Install the Identity Manager engine on Server 1.

   Open the ports required for Identity Vault to communicate with Identity Manager components: 389, 524, 636, 8028, and 8030. For more information about the ports used by Identity Manager, see “Understanding Identity Manager Communication” in the *NetIQ Identity Manager Security Guide*.

3. Install and deploy identity applications on Server 2.

   On Linux, the installer performs the following tasks:

   - Installs the authentication service to support single sign-on access to the identity applications.
   - Installs a password management service that helps you configure Identity Manager to allow users to reset their passwords.
   - Deploys the User Application driver and the Role and Resource Service driver.

   On Windows, you must manually perform these tasks.

   Open the ports required by identity applications: 5432, 8005, 8009, 8080, 8109, 8180 and 8443 (also needed by iManager), 8543, 45654. For more information about these ports, see “Installing Identity Manager ” in the *NetIQ Identity Manager Setup Guide for Linux* or Installing and Configuring Identity Manager Components in the *NetIQ Identity Manager Setup Guide for Windows*.

4. Install iManager and Remote Loader components on Server 2.

   Open port 8090 that is used by Remote Loader. iManager needs port 9009.

5. Install and deploy Identity Reporting on Server 3.

   Identity Reporting connects to Sentinel Log Management for IGA that was earlier installed on this server.

   Open the ports required for Identity Reporting to communicate with Identity Manager components: 435 and 15432. For more information about the ports used by Identity Manager, see “Understanding Identity Manager Communication” in the *NetIQ Identity Manager Security Guide*.

High Availability Configuration with Load Balancing

High availability ensures efficient manageability of critical network resources including data, applications, and services. You can install the following components in a high-availability environment:

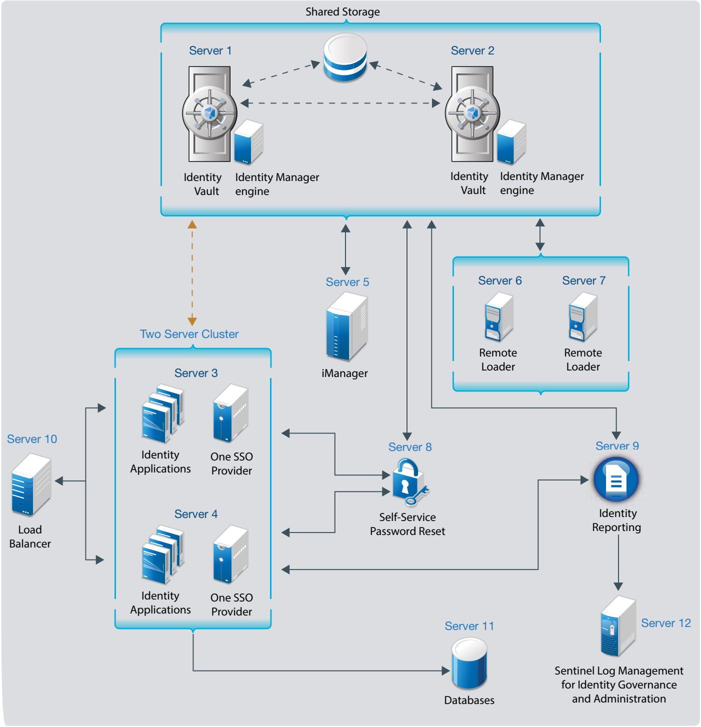
- Identity Vault
- Identity Manager engine
- Remote Loader
- Identity Applications, except Identity Reporting

When you run Identity Vault in a clustered environment, the Identity Manager engine is also clustered. In this configuration, only one node is active at any point of time. If the active node fails, the service fails over to another node in the cluster.

You can cluster identity applications and authentication service to support single sign-on access (OSP on Windows) and configure these components for load balancing and fault tolerance. The load balancer is typically part of the cluster. It understands the cluster configuration as well as failover policies. In this configuration, all the nodes in the cluster are active at any point of time. The load balances performs the following actions:

- Distributes the load across all nodes to ensure that the nodes have roughly the same workload.
- Diverts the requests to the failed node to the surviving nodes when any of the nodes fail.

You must ensure that session stickiness is enabled for the cluster created in the load balancer software for the identity applications nodes.



You can easily add additional identity applications and OSP servers (or nodes) to handle the load, then add new servers to the L4 switch. When the new servers are added to the cluster, they are automatically sent the cluster configuration.

Perform the following steps to install Identity Manager in this setup on Linux:

1 Install Identity Vault on Server 1 and Server 2 with shared storage. State data for Identity Vault is located on the shared storage so that it is available to the cluster node that is currently running the Identity Vault. This data includes eDirectory DIB, NICI (NetIQ International Cryptographic Infrastructure) data, eDirectory configuration, and log data. For more information, see “Sample Identity Manager Cluster Deployment Solution on SLES 12 SP3 or Later Versions” in the *NetIQ Identity Manager Setup Guide for Linux*.

2 Install Sentinel Log Management for IGA on Server 12.

   You can generate the required audit reports by using Sentinel Log Management for IGA.

3 Install the Identity Manager engine on Server 1 and Server 2.

   Open the ports required for Identity Vault to communicate with Identity Manager components: 389, 524, 636, 8028, and 8030. For more information about the ports used by Identity Manager, see “Understanding Identity Manager Communication” in the *NetIQ Identity Manager Security Guide*.

4 Install all databases on Server 11.

   These databases are connected to the identity applications servers.

5 Install and deploy identity applications on Server 3 and Server 4.

   Both Server 3 and Server 4 combine to form a two-server cluster.

   For more information, see Sample Identity Manager Cluster Deployment Solution on SLES 12 SP3 or Later Versions in the *NetIQ Identity Manager Setup Guide for Linux*.

   Open the ports required by identity applications: 5432, 8005, 8009, 8080, 8109, 8180 and 8443 (also needed by iManager), 8543, 45654. For more information about the ports used by Identity Manager, see “Understanding Identity Manager Communication” in the *NetIQ Identity Manager Security Guide*.

6. Install iManager on Server 5.

   The Identity Manager engine installation program includes the installation files for iManager.
7. Open port 9009 that is used by iManager.
8. Install Remote Loader on Server 6 and Server 7.

   The Identity Manager engine installation program includes the installation files for Remote Loader.
9. Open port 8090 that is used by Remote Loader.
10. Install password management service on Server 8.

    The identity applications installer contains the installation files for password management service that helps you configure Identity Manager to allow users to reset their passwords.
11. Install and deploy Identity Reporting on Server 9.

    Open the ports required for Identity Reporting to communicate with Identity Manager components: 435 and 15432. For more information about the ports used by Identity Manager, see "Understanding Identity Manager Communication" in the *NetIQ Identity Manager Security Guide*.
12. Deploy the load balancer on Server 10. This is required to balance the load between the Identity Applications servers.

Perform the following steps to install Identity Manager in this setup on Windows:

1. Install Identity Vault on Server 1 and Server 2 with shared storage. State data for Identity Vault is located on the shared storage so that it is available to the cluster node that is currently running the Identity Vault. This data includes eDirectory DIB, NICI (NetIQ International Cryptographic Infrastructure) data, eDirectory configuration, and log data. For more information, see Sample Identity Manager Cluster Deployment Solution on Windows in the *NetIQ Identity Manager Setup Guide for Windows*.
2. Install Sentinel Log Management for IGA on Server 12.

   You can generate the required audit reports by using Sentinel Log Management for IGA.
3. Install the Identity Manager engine on both Identity Vaults.

   Open the ports required for Identity Vault to communicate with Identity Manager components: 389, 524, 636, 8028, and 8030. For more information about the ports used by Identity Manager, see "Understanding Identity Manager Communication" in the *NetIQ Identity Manager Security Guide*.
4. Install all databases on Server 11.

   These databases are connected to the identity applications servers.
5. Install and deploy identity applications on Server 3 and Server 4.

   Both Server 3 and Server 4 combine to form a two-server cluster.

   For more information, see Sample Identity Applications Cluster Deployment Solution in the *NetIQ Identity Manager Setup Guide for Windows*.

   Open the ports required by identity applications: 5432, 8005, 8009, 8080, 8109, 8180 and 8443 (also needed by iManager), 8543, 45654. For more information about the ports used by Identity Manager, see "Understanding Identity Manager Communication" in the *NetIQ Identity Manager Security Guide*.
6. Install iManager on Server 5.

   Open port 9009 that is used by iManager.
7. Install Remote Loader on Server 6 and Server 7.

   Open port 8090 that is used by Remote Loader.
8. Install OSP on Server 3 and Server 4.

Both Server 3 and Server 4 combine to form a two-server cluster.

9. Install SSPR on Server 8.
10. Install and deploy Identity Reporting on Server 9.

    Open the ports required for Identity Reporting to communicate with Identity Manager components: 435 and 15432. For more information about the ports used by Identity Manager, see "Understanding Identity Manager Communication" in the *NetIQ Identity Manager Security Guide*.
11. Deploy the load balancer on Server 10. This is required to balance the load between the Identity Applications servers.

Deploying Identity Manager on Public Cloud

You can deploy Identity Manager in public cloud on Amazon Web Services (AWS) EC2 or Microsoft Azure. Identity Manager components can be deployed on a private or a public network based on your requirement. However, the deployment procedure is the same for all scenarios.

- Use AWS EC2 to deploy Identity Manager components on Linux platform.
- Use Microsoft Azure to deploy Identity Manager components on Linux platform.

NetIQ provides the flexibility of deploying Identity Manager on on-premises and cloud environments. After determining the cloud provider that suits your environment, ensure that you review the recommended configuration details before beginning the deployment.

Completing Post-Installation Tasks

After completing the installation of Identity Manager components, perform the necessary tasks. For example, configure the drivers you installed to meet the policies and requirements defined by your business processes. You also need to configure Sentinel Log Management for IGA to gather audit events. For more information, see "Final Steps for Completing the Installation" in the *NetIQ Identity Manager Setup Guide for Linux* or Post-Installation Tasks in the NetIQ Identity Manager Setup Guide for Windows.

Verifying Installed Components

After you install and configure Identity Manager components, verify that the components are properly installed. For example, you should log in to the individual identity applications and be able to switch among them without logging out. For more information, see the individual component section in *NetIQ Identity Manager Setup Guide for Linux* or *NetIQ Identity Manager Setup Guide for Windows*.

Legal Notice

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

Copyright © 2019 NetIQ Corporation, a Micro Focus company. All Rights Reserved.