ivanti

Data Center Discovery v2017.3

SCAN ENGINE PREREQUISITES GUIDE

Contents

Rev 10/17

Overview

This guide is written for the staff tasked with provisioning a company's hardware and software resources to install the Ivanti Data Center Discovery scan engine. As a technical document, it's assumed that the reader has knowledge of networking, operating systems, and database administration.

Refer to this document to learn about the following:

- **The scan engine:** This chapter gives a description of what the scan engine does and the technology used. It also outlines the server hardware and software requirements.
- **Estate access:** This chapter explains requirements needed for accessing the estate, including Windows and UNIX credentials.
- **Application access:** This chapter discusses virtualization technology and database access.
- **Additional details:** This chapter outlines additional considerations for installing the Data Center Discovery scan engine.

About the scan engine

The Data Center Discovery scan engine is a highly scalable and secure network inventory tool. It uses a number of protocols to access platforms and applications to gather information securely from the hardware and software in the estate.

The data gathered is typically used for (but not limited to):

- Software license management
- IT asset management
- IT security
- IT operations/operational management
- IT support
- Configuration Management Database (CMDB) population

Scan engine components

The Data Center Discovery scan engine is a three-tier, web-based application that consists of a web-based presentation tier, an application-logic tier, and a database tier. These logical tiers map to the following components:

Component	Description
Scan engine	The scan operation uses one or more scan engine servers to discover and scan devices and applications. The scan engine is a 64-bit Windows .NET application.
Scan database	The scan database stores: • Configuration information that controls the scan operations. • Data as reported by the devices from the scan engine. The scan database is a Microsoft SQL Server database.
UI	The User Interface (UI) provides centralized configuration and control of the scanning operation. The web-based application is integrated with Microsoft IIS and ASP.NET.
Rest API	Provides a programmatic access to the scan data. Allows for integration with customer in-house tools.

> **Note:** When setting up the scan engine, you can install the scanning service, scan database, and UI (with Rest API) on a single server. However, if scalability and security are an issue, you can separate and run each of these components on individual servers. In addition, multiple scanning servers can be deployed to spread the load of scanning an estate. Common installation scenarios are covered in the *Data Center Discovery—Scan Engine Deployment Guide*.

Server preparation

The scan engine runs on a Windows Server platform and provides a web-based UI that interfaces with a back-end Microsoft IIS for its administration console. A Microsoft SQL Server Instance is used as the scan data repository. The Windows Server(s) used can be either **physical** or **virtual** machines.

Installation requirements

It is **highly recommended** that you provide a **dedicated** server for the installation. When the scan engine is sharing an environment with other applications, you must ensure that sufficient resources are available for the duration of the scan. SQL Server should be installed on a separate server.

Hardware requirements

Component	Physical Recommended	Physical Minimum	Recommended if using a VM	Minimum if using a VM
CPU physical	2 x 2.6GHz Dual Core CPU	1 x 2.4GHz Dual core CPU	4 x 2.6GHz vCPU	2 x 2.4GHz vCPU
RAM (available)	8GB	4GB	8GB	4GB
HDD (This storage is scaled for an estate scan of 4,000 devices with full logging enabled.)	100MB + SQL DB data (60GB) + 10GB Logs	100MB + SQL DB data (60GB) + 10GB Logs	100MB + SQL DB data (60GB) + 10GB Logs	100MB + SQL DB data (60GB) + 10GB Logs
Additional disk for 3rd-party libraries	1GB	1GB	1GB	1GB

Software requirements

The scan engine runs on a Windows server using MS SQL Server as its data repository and IIS for its presentation layer. The server hosting the scan engine service must be configured to trust Thawte digital signatures.

Requirement	Minimum	Recommended
Common	Windows Server 2012 .NET Framework 4.5.1 SQL Server 2012 Express Service Pack 3 applied (the recommended Collation setting is Latin1_General_CI_AS).	Windows Server 2012 R2 .NET Framework 4.5.1 SQL Server 2012 Standard 64-bit Service Pack 3 applied (the recommended Collation setting is Latin1_General_CI_AS).

Browser	IE 10	IE 11
SQL Server user permissions	**Installation:** • Provide a SQL Server user or Active Directory account that has CREATE ANY DATABASE (**dbcreator**) server permission. • The provided user will become the **db_owner** of the scan engine database (if it doesn't already exist). **Run-Time**: At run time, the user identity is remembered from the installation step: • The user supplied at install time must have VIEW ANY DEFINITION and VIEW SERVER STATE permissions. • If the user supplied at install time is not **db_owner**, the user requires **db_readdata** and **db_writedata** roles. This scenario is only likely to occur if additional scan engine(s) are installed that share a SQL Server scan engine database; a **different** SQL Server installation user could be provided to access the existing scan engine database. **Upgrade:** Supply a user with the **db_owner** role and with VIEW ANY DEFINITION and VIEW SERVER STATE permissions.	
Interface	IIS Server v8.0 with ASP.net (which must be pre-installed) See the "IIS requirements" section for full description of IIS requirements. The default website must be present prior to installation.	IIS Server v8.0 with ASP.net (which must be pre-installed) See the "IIS requirements" section for full description of IIS requirements. The default website must be present prior to installation.

Standard SQL Server configuration

The scan engine database components are installed into a Microsoft SQL server instance. Follow the installation instructions supplied by Microsoft when installing the SQL Server database.

The following configuration changes are required:

- The database user account that is used for **installing** the scan engine should have elevated privileges (with the ability to create a new database).
    - Installation requires a database user that has dbcreate permissions.
    - If the database does not exist, creating the DB will mark the selected user as a member of dbowner.
    - For the scan engine, the database user that is selected during the installation process will continue to be used as the Application login identity for the database. The selection of the 'SA' account is, therefore, not recommended.
- The database logging should be configured to **simple** by default.
- It is recommended that the database growth interval be changed to 256MB (for Database and Logs).
- The **.NET CLR** option in SQL Server must be enabled for the scan engine to function correctly:

```
sp_configure @configname=clr_enabled, @configvalue=1
GO
```

```
RECONFIGURE
GO
```

> **Note:** It's recommended that the **SQL Server Profiler** option is enabled as part of the SQL Server installation; it's a useful troubleshooting tool.

Folder write permissions

The installation user needs **write access** to the folders:

- In which the scan engine is installed.
- Where the log files are updated.

Because the installer must be run with Administrative privileges, access to the following default locations is normally granted:

- <drive>:\Program Files\Ivanti\DataCenterDiscovery ScanEngine 4.0
- <drive>:\ProgramData\Ivanti\DataCenterDiscovery ScanEngine 4.0

The installer creates these folders during installation.

IIS requirements

Add or Remove Role Services > Role Services > Web Server.

Application development features:

- .NET extensibility
- ASP .NET
- ISAPI extensions
- ISAPI filters

Common HTTP features:

- Default document
- Directory browsing
- HTTP errors
- HTTP redirection
- Static content

Security:

- Request filtering
- Windows authentication (optional). The Window Authentication IIS Security feature is only required if Active Directory login is wanted for access to the UI. If this is not enabled, then only application-defined users can log into the UI.
- IIS hostable web core

Estate access requirements

The scan engine is agentless. Agentless access requires that connections between the scanning server and remote target device/application be established over standard protocols. The sections below list the basic access requirements to complete a scan of an estate.

Protocols

This table shows the typical protocols that may be needed, depending on the scan requirements for the estate. All of these protocols may not be available or provisioned on the devices within the estate.

Area	Protocol	Credentials needed
Common	• ICMP (ping) • SNMP	• None • V2 (community); V3 (password)
Windows	WMI	Windows user provided with WMI permissions (scan engine will use impersonation of this user) Required permissions for the user login are: • Enable Account • Remote Enable By default, only the local computer Administrator account has full control of the WMI services on the computer being managed. Members of the Administrators group have access to remote computers but may not have access to all data. All others have read/write/execute permissions on their local computer only. For details, see https://technet.microsoft.com/en-us/library/cc771551.aspx
Windows	• Remote registry • Remote access • Windows file share	Windows Admin group member on target device.
UNIX	• SSH • SSH proxy • Telnet	Privileged (see “UNIX credentials” section for details). For SSH only, see note (in the same section) on the use of sudo and requiretty.

Oracle	PLSQL	Read access to all system tables, views, and dictionaries. Note: when DATABASE VAULT is in use: GRANT PARTICIPANT or OWNER authorization on "Oracle Database Vault Realm" For additional information on the process of defining realm authorization, see the relevant Oracle Documentation related to REALMS.
Certificate analysis provider	Certificate analysis	None
DB2	DB2	Read access to all system tables, views, and dictionaries.
Informix	Informix	Read access to all system tables, views, and dictionaries; Execute access to database configuration stored procedures.
LDAP	LDAP	Windows non-privileged
NaviSphereCLI	NaviSphereCLI	NaviSphereCLI Application Specific setup. Navisphere CLI (NAVCLI) is a command-line interface tool for EMC storage system management. It's used for storage provisioning and managing array configurations from any one of the managed storage systems on the LAN. The NAVCLI software must be installed and configured to connect to any storage platform that is to be scanned. There is no direct discovery process of storage. Only storage connected through the NAVCLI interface will be available.
Packet analysis	Packet analysis	None
TraceRoute	Trace route client provider	None
VMware	vSphere	vSphere user read-only role access to all vSphere items. See the "Application access requirements" section for additional detail.

Ports

The scan engine accesses a number of internet ports to carry out discovery and inventory of devices. These ports must be opened by the relevant firewall teams to ensure that the scan engine can gather all required information. If these ports aren't opened, there is a risk that that devices will be missed or products won't be properly scanned. Refer to Appendix A for a complete list of default ports.

Because the scan engine operates within a customer estate, you're not required to modify the firewall rules or firewall exceptions. However, if you want to scan network segments that are separated by firewalls, suitable modification is required. If modification of internal firewalls isn't possible, you can install and configure multiple scan engines in each segment to forward discovery information to a

central location. If no data forwarding is allowed due to fire-wall restrictions, alternative Out-Of-Band data exchange approaches can be supported.

> **Note:** You can define alternate ports on the scan engine dashboard if necessary. This is covered in more detail in the *Data Center Discovery—Scan Engine User Guide*.

Firewalls

Windows scanning uses Windows Management Instrumentation (WMI), which automatically establishes two connections (one is created on port **135** and the other on a random port between **1024** and **65535**).

Operating system credentials

The scan engine uses a variety of commands over multiple network protocols to retrieve as much inventory data as possible from all devices. It uses different types of network access and credentials, depending on the target device hardware and software products.

The scan engine can discover the existence of devices based solely upon IP address; however, to perform full inventory operations on these discovered devices, the scan engine must be configured with credentials that can log onto the targets. These credentials enable the scan to retrieve detailed information about applications, devices, and operating systems that reside on the network. The scan engine requires the rights and permissions described below to inventory Windows and UNIX/Linux devices.

The credentials provided must allow the commands found in Appendix B to be executed.

Window credentials

On scanned Windows target devices, Windows user-specific rights are required to gather important system information via the Windows Remote Registry and Windows Management Instrumentation (WMI) protocols. Use the following tips for help with this:

- Create a single scan-engine scanning user account that complies with the required credential levels (as specified in the “Estate access requirements” section’s Protocols table).
- Create a Windows scan user for each domain within the estate.
- Give access to default file shares for credentials (admin$, C$, etc.). This is only required if the credential being used is not a member of the Administrator Group. This feature allows a remote file scanning operation to be accomplished.

UNIX credentials

When accessing *NIX variant target systems, the scan engine makes use of Telnet or Secure Shell (SSH). Ivanti recommends the use of SSH to ensure the security of authentication credentials; Telnet uses password sent-in-the-clear for authentication.

A prerequisite for using the *NIX commands (as outlined in Appendix B) is having the user privileges required to execute the commands. The privilege to execute a command is normally directly associated with the login user credentials that are used to access the UNIX target. A set of credentials that provide **elevated** access will automatically provide the required privilege level.

However, some of the methods that can be used to grant access are:

- **Access Control Lists:** Specific users have access to privileged commands (such as a scan engine scanning specific account would be given privileged access).
- **Aliases:** Provide command aliases on specific targets that typically are not accessible by non-root users.
- **Proxy or Gateway Server:** Route commands through a proxy.
- **Account Escalation:** Requires the use of a privilege escalation command, such as sudo or su. The scan engine provides native support for non-privileged accounts to execute a command using a privilege escalation command prefix such as sudo. This functionality is associated with the **SSH connection type** within the UI.

SUDO is a program for UNIX-like computer operating systems that allows users to run programs with the security privileges of another user, by default the superuser (root). Unlike the related command su, users must supply their own password for authentication, rather than the password of the target user.

After authentication, and if the configuration file (typically located at /etc/sudoers) permits the user access, the system invokes the requested command. The configuration file offers detailed access permissions, including enabling commands only from the invoking terminal, requiring a password per user or group, requiring re-entry of a password every time, or never requiring a password at all for a particular command line. It can also be configured to permit passing arguments or multiple commands.

> **Note:** A target device may require that sudo commands can only be run with an attached tty. The Data Center Discovery scan engine typically does not have an attached tty device, so sudo prefixed commands will raise errors. The default operation of sudo is controlled by the /etc/sudoers file. The following entry requires all sudo commands to have an associated tty:
>
> `Defaults   requiretty`
>
> It's possible to override this on a per-user basis with the following line, which enables you to set up a special scan-engine user that is used exclusively for scanning processes on the target device:
>
> `Defaults:<username>      !requiretty`
>
> The scanning user should also be configured to not request a password for running a command with sudo. This can be done with an entry such as the following in the sudoers file:
>
> `<username>      ALL=(ALL) NOPASSWD:ALL`
>
> **Note:** Older AIX OS might have a command-line length limitation of around 200 characters, which will affect scanning. This can be overridden by configuration on AIX 5.1 and newer.

UNIX shells

The UNIX shell created by initiating a remote connection to the UNIX device must:

- **Not run** a restricted shell (unless it's associated with a "standard restricted shell" such as HMC).
- **Not use** a C shell (/bin/csh).
- **Have** read access to the install folder and relevant sub-folders of any software to be scanned.
- **Have** the ability to execute sudo commands without a tty attached.

Language settings

It's recommended that both the scanning server and the target devices have the LANG environment variable setting and other relevant environment variables set to an English language value for the scanning to work correctly:

UNIX devices

LANG=en_US
LC_CTYPE=en_US
LC_NUMERIC="en_US"
LC_TIME="en_US"
LC_COLLATE="en_US"
LC_MONETARY="en_US"
LC_MESSAGES="en_US"
export LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE
export LC_MONETARY LC_MESSAGES LC_ALL

Windows devices

These values can be made available through the **Control Panel > Region** option.

Application access requirements

When performing scans for detailed information, credentials are required to access both the **OS** and **applications** running on a device. Credentials are needed for applications such as Oracle database, SQL Server, and Virtual Device Management software.

Virtualization server access

VMware vSphere access

Access is provided through the use of VMware vSphere PowerCLI. The VMware ESX Product Adapter communicates with the vSphere Installation using the vSphere Web API, and the Simple Object Access Protocol (SOAP) via the PowerCLI Client. You will need to install this on the scanning server before starting the scan operations.

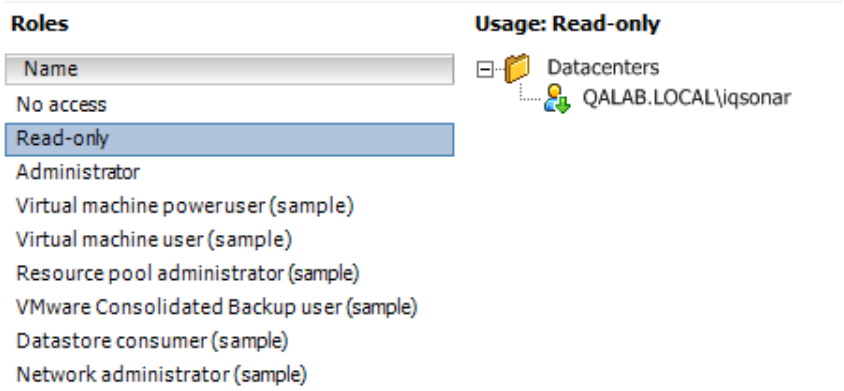
See the Protocols table in the “Estate access requirements” section for the vSphere credential type that’s required.

The vSphere access is used as the primary source of information for VMware virtual machines and the relationships established between VM guest and ESX hosts. If an ESXi/vSphere Hypervisor is not scanned, associated virtual machines will be identified by direct scanning of targets but virtualization/clustering information related to the connections will not be available.

Commands that are issued:

- FindEntityViews:<object name>: Returns the object list
- FindEntityViews:VirtualMachine: List of virtual machines
- FindEntityViews:Datacenter: List of datacenters
- FindEntityViews:Datastore: List of datastores
- FindEntityViews:HostSystem: List of hosts (servers)

In addition, you’ll need to identify credentials that allow access to the console through which the scanning server will log in. The credential that is used to log into vSphere requires Read-Only permissions (on datacenters).



To scan vSphere licenses, a role with permissions for **Global – Licenses** is needed.

Access to the vSphere PowerCLI is provided through the installation of downloadable software. Download the latest release (vSphere PowerCLI 5.5 Release 1 - released 09/22/2013).

All versions are available from VMware at: https://www.VMware.com/support/developer/PowerCLI/. Select the correct version from the drop-down list.

> **Note:** These downloads require the use of a VMware login.

HMC and PowerVM access

To enable the scanning of IBM PowerVM virtualization environments, SSH or Telnet access is required to the Hardware Management Console (HMC) used to manage the systems.

If scanning the IBM HMC, the HMC user must have a minimum setting of **hmcviewer** role.

Read-only access to the following commands is required to allow the scan engine to generate Oracle reports for this hardware type:

- VIOS (all)
- ioslevel (VIOS server code level)
- lparstat (VIOS servers own LPAR config)
- lsdev (Devices defined to VIOS)
- lstcpip (IP addresses of VIOS servers)

WinPcap

WinPcap allows applications to capture and transmit network packets.

WinPcap consists of a driver, which extends the operating system to provide low-level network access, and a library that is used to easily access the low-level network layers.

The WinPcap capabilities extend the ability to detect specific OS versions on a target device; you can use this functionality as part of the discovery operations (i.e., prior to a full scan of the device being achieved). This installation is optional and isn't mandatory for the scanning operations to succeed.

No login is required for this installation; its use doesn't require a credential. Download the latest release (WinPcap v4.1.3 – released 07/04/2014). Install instructions are included in the .EXE file.

Oracle access

Oracle support libraries

Oracle Data Access Components (ODAC) Libraries (DLLs) must be present to support Oracle database scanning. DLL files allow the scan engine to communicate and manage the Oracle database. These are automatically shipped with the scan engine installer.

Multiple versions of the Oracle DLL libraries are available, and each DLL is capable of supporting connections to different versions of the Oracle database. The most recent version of the Oracle client library supports connections to Oracle 10.0+. The previous version supports earlier versions of Oracle. Both versions are installed automatically with the product and are available for immediate use.

Oracle permissions

To gather detailed information required for an audit of Oracle, the scan engine needs to log into the database and read certain tables. The user account used to access Oracle will require the **Select any dictionary** and **Select any table** options**.**

The sample script below creates a user and assigns the correct privileges. It's appropriate for **9i and above**. For earlier versions, modify the creation script as appropriate.

```
CREATE USER <USERNAME> identified BY <PASSWORD>;

GRANT

      CREATE SESSION,

      SELECT ANY DICTIONARY,

      SELECT ANY TABLE TO <USERNAME>;
```

> **Note:** When DATABASE VAULT is in use: Grant PARTICIPANT or OWNER authorization on "Oracle Database Vault Realm." For additional information on the process of defining realm authorization, see the relevant Oracle Documentation related to REALMS.

Oracle background details

To complete the scan of Oracle databases, the scan engine must examine some tables created when the Oracle Management Packs are installed, including **CMPSYSCLASSES**, **CMPINSTALLATION,** and multiple tables with the prefix **MGMT_**.

These system tables can be created in any user schema, depending on how they are installed and the identity of the user that accepted the pack. To complete the scan, the scan engine must read the **DBA_TABLES** dictionary to find all the relevant tables and must have read-only permission on all user schemas to read the contents of the system tables.

> **Note:** The scan engine doesn't query any other tables in the user schema.

MS SQL Server access

MS SQL Server support libraries

Access to MS SQL Server is provided using built-in SQL support libraries. No additional installations are required.

MS SQL Server permissions

To gather information required for an audit of Microsoft SQL Server, the scan engine needs to log into the database instance being scanned and access certain system objects. The following permissions are required for the user identity that is used to scan the target SQL instance:

Permission	Description
Viewer Server State	Required to get sessions, license details, and high-availability configuration.
View Any Definition	Required to get login and database details.
Select On sys.sysaltfiles	Required to get database details on SQL Server (for SQL Server 2000). For details, see https://msdn.microsoft.com/en-us/library/ms181338(v=sql.110).aspx.

Creating user and assigning privileges

These sample scripts create a user and assign the correct privileges.

For SQL Server 2005 and above:

```
CREATE LOGIN [<USERNAME>] WITH PASSWORD='<PASSWORD>',
        DEFAULT_DATABASE=[master],
        DEFAULT_LANGUAGE=[us_english]
GO
        USE master;
        CREATE USER [<USERNAME>] FOR LOGIN [<USERNAME>];
        GO
        GRANT VIEW SERVER STATE TO [<USERNAME>];
        GRANT VIEW ANY DEFINITION TO [<USERNAME>];
        GRANT SELECT ON sys.sysaltfiles TO [<USERNAME>];
GO
```

For SQL Server 2000:

```
USE [master]

GO EXEC master.dbo.sp_addlogin @loginame = N'<USERNAME>',

@passwd = N'<PASSWORD>',

@defdb = N'master'

GO EXEC dbo.sp_grantdbaccess @loginame = N'<USERNAME>',

@name_in_db = N'<USERNAME>'

GO GRANT

SELECT ON dbo.sysaltfiles TO [<USERNAME>];
```

> **Note:** If no SQL Server credentials are supplied, Data Center Discovery is restricted to obtaining information about SQL Server by parsing registry keys. This approach will retrieve only partial information on the installation.

Informix access

Informix support libraries

To scan an Informix database, a special client application must be installed within the scanning server. Download the latest release (64-bit Informix Connect Developer Edition 4.10.FC1DE – released 03/26/2013). Install instructions are included in the .ZIP file.

> **Note:** This download requires the use of an IBM login and the hyperlink links to a search page that will return a list containing the required driver.

To install Informix

1. Right-click **install.bat** and choose **Run as Administrator**.
2. Install the **IBM Informix .NET Provider** installation feature.
3. Complete the installation process (the IBM Data Server Driver installation isn't required).
4. Copy the <client install path>\IBM Informix Client SDK\bin\netf40\IBM.Data.Informix DLL file.
5. Paste the DLL file into <scan engine install path>\Ivanti\DataCenterDiscovery ScanEngine 4.0\bin.
6. Restart the scan engine service after doing so.
7. Add appropriate Informix credentials in the UI.

Informix permissions

To enable Informix scanning, the scan engine user must have read or execute access to all system tables and database configuration stored procedures. It must also be able to run queries.

To gather detailed information required for a DB2 audit, the scan engine needs to log into the database and read certain database views. Because Informix doesn't support internal database users, an appropriate user must exist within the operating system for both Windows and *NIX devices. The user account can be any OS user account on the system.

Windows user permissions

You can create and manage users in Windows from the control panel:

Control Panel > User Accounts > Manage User Accounts

UNIX user permissions

*NIX systems all have different methods for creating users, though the **useradd** command is commonly used.

IBM DB2 access

IBM DB2 support libraries

To scan a DB2 database, a special client application must be installed on the scanning server. Download the latest release (64-bit IBM Data Server Runtime Client (Windows AMD 64) v10.5 – released 03/30/2012).

> **Note:** This download requires the use of an IBM login.

IBM DB2 permissions

Discovery of DB2 on Windows requires the ability to execute the **db2cmd.exe** appropriately; this in turn requires a credential that is in the DB2 Administrators group on the device being scanned.

To enable DB2 scanning, the scan engine user must have read or execute access to all system tables and database configuration stored procedures.

To gather detailed information required for a DB2 audit, the scan engine needs to log into the database and read certain database views. The user account can be any OS user account on the system.

Windows user permissions

You can create and manage users in Windows from the control panel:

Control Panel > User Accounts > Manage User Accounts

UNIX user permissions

*NIX systems all have different methods for creating users, though the **useradd** command is commonly used.

The DB2 user needs to be a part of a DB2 administrators group. You can do this on UNIX by adding the user to the **DB2ADMNS** group, which is automatically created when DB2 is installed. This can be done by adding the user to the **db2iadm1** group account. Again, this account exists on an installed DB2 system—add users to the group using the **usermod** command (-G option).

Storage – EMC (BETA)

Storage (EMC) support libraries

Navisphere CLI (NAVCLI) is a command-line interface tool for EMC storage system management. It can be used for storage provisioning and managing array configurations from any one of the managed storage systems on the LAN.

The scan engine storage product adapter uses a co-located NAVCLI installation (i.e., the Navisphere CLI support tool must be installed on scanning server).

The EMC Navisphere Command Line Interface (CLI) enables you to monitor/manage **CLARiiON** storage systems. The secure CLI communication occurs (over the IP network) with the management server over port **443**, though you can choose to use the alternate port of **2163** for secure communication. The actual port selected is determined during storage-system initialization. Secure CLI requires either port **443** or **2163** to be opened for proper operation.

Download the latest release (32-bit Navisphere CLI [Windows - all supported 32 and 64-bit versions] 7.33.8.1.19 - released 01/09/2014). Install instructions are included in the .EXE file.

> **Note:** This download requires the use of a Navisphere login.

Device setup requirements for EMC CLARiiON arrays

For the latest support information about which CLARiiON CLI is compatible with array firmware versions, see the CommandCentral Storage Hardware and Software Compatibility List.

This document is updated regularly at: https://entsupport.symantec.com/docs/288784

When you install the CLARiiON CLI on Windows, both NaviCLI and NaviSecCLI are installed. Install NaviCLI or NaviSecCLI at the default location:

C:\Program Files\EMC\Navisphere CLI

If you install the CLI at a location other than the default location, note the installation location for later configuration of the scan engine.

Storage (EMC) permissions

Setup user permissions for the NAVCLI interface per the installation instructions provided with the Navisphere CLI installer.

Oracle VM for x86

Oracle VM for x86 is scanned using the Oracle VM Manager REST API and does not require additional libraries.

Oracle VM for x86 REST API permissions

Scanning Oracle VM for x86 requires Oracle VM Manager credentials with read-only access to the REST API. A user in the **Monitor** global role is appropriate.

CyberArk Credential Manager

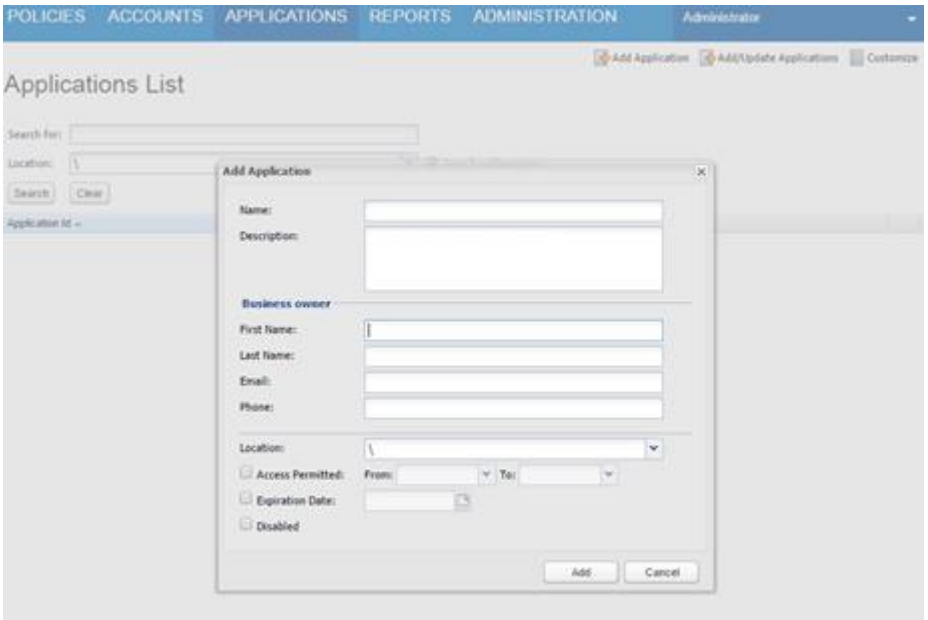
You can configure the scan engine to scan targets using credentials stored within a CyberArk Privileged Account Security Solution vault.

Required components

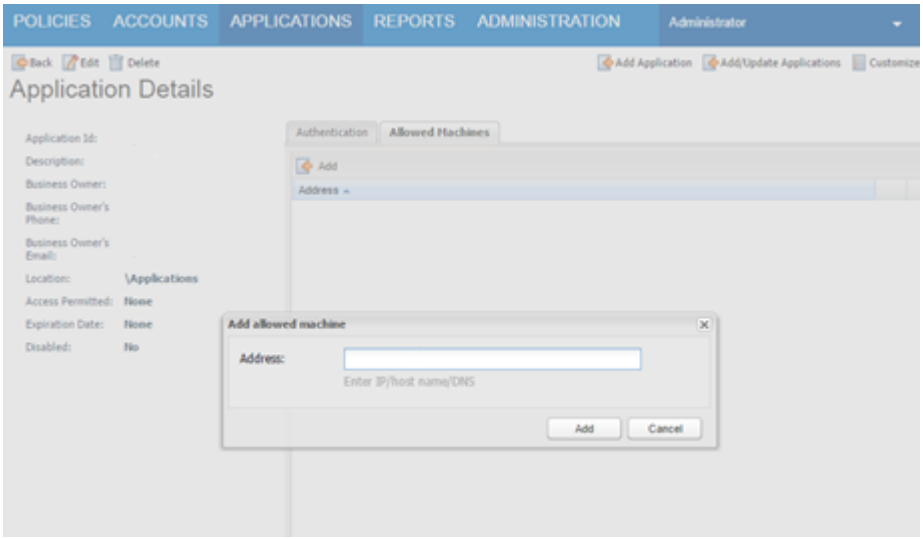
The integration with CyberArk uses the Application Identity Manager Central Credential Provider Web Service to retrieve credentials from CyberArk. The central credential provider web service should be installed as per the *Central Credential Provider Implementation Guide.* This is typically installed on the same device as the Private Vault Web Access.

Required account permissions

To access credentials through the CyberArk CCPWA, you must configure an application account for the scan engine to use—create it through the Private Vault Web Access.



Configure the application account to allow access only from the scan engine server.



Additional details

The scan engine installer provides a step to test that the product prerequisites have been met, verifying that the components needed are installed and running correctly in advance of the scan engine install.

The tool provides visual indicators of success. All checks must run successfully before the installation continues.

Appendix A: Default ports list

Ports used for discovery

You can add or remove ports from this default list during the **discovery** phase with port scanning.

Port	Description
21	FTP control (command)
22	Secure Shell (SSH) used for secure logins file, transfers (scp sftp), and port forwarding
23	Telnet protocol unencrypted text communications
25	Simple Mail Transfer Protocol (SMTP) used for email routing between mail servers
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol 3 (POP3)
135	DCE endpoint resolution
139	NetBIOS Session Service
143	Internet Message Access Protocol (IMAP) used for retrieving, organizing, and synchronizing email messages
443	Hypertext Transfer Protocol over TLS/SSL (HTTPS)
445	Microsoft-DS SMB file sharing
1520	Oracle database common alternative for listener
1521	Oracle database default listener
1522 1529	Oracle database common alternative for listener
3389	Microsoft Terminal Server (RDP) officially registered as Windows Based Terminal (WBT)
7001	Default for BEA WebLogic Servers HTTP server, though often changed during installation

Ports used for inventory

You're required to open all of these ports to facilitate the **inventory** of devices and enterprise applications. Custom ports configured by a DBA may also need to be included.

Port	Protocol	Service	Device or Application
22	TCP	SSH	UNIX/Linux devices, HMC
23	TCP	Telnet	UNIX/Linux devices
80	TCP	HTTP	VMware vCenter, ESX Host scanning
443	TCP	HTTPS	VMware vCenter, ESX Host scanning
135	TCP	RPC	Windows devices
139	TCP	NETBIOS Session	Windows devices
445	TCP	SMB	Windows devices
137	UDP	NETBIOS Datagram	Windows devices
138	UDP	NETBIOS Datagram	Windows devices
139	UDP	NETBIOS Session	Windows devices
49152 to 65535	TCP	WMI dynamic ports	Windows Vista/Server 2008 or higher(1)
1025 to 5000	TCP	WMI dynamic ports	Windows XP/Server 2003 or lower(1)
1433	TCP	SQL Server	Microsoft SQL Server scanning. May also need custom ports opened.
1521	TCP	Oracle Database	Oracle RDBMS scanning, default listener
1526	TCP	Informix	Informix scanning, default port
2025 4100 5000	SSH, WMI	Sybase	Sybase scanning
50000	TCP	DB2	IBM DB2 default. This overlaps with the WMI ports.

Appendix B: Privileged command access

The following commands, namespaces, and registry hives are used by the Data Center Discovery scan engine, and you must be provided access to these commands to successfully retrieve inventory data.

Platform	Commands
***NIX**	
ALL	awk, cat, cd, cut, date, echo, egrep, grep, head, ls, pwd, sed, sort, find, tail, tr, uname, uniq, wc, which
Veritas Clustering	haclus, hastatus, hasys
Oracle DB	lsnrctl
Oracle HA	Srvctl
IBM DB2	db2, db2ls, db2set
Informix	oninit, onstat
AIX	
ALL	df, domainname, ifconfig, lsattr, lscfg, lslpp, lslv, netstat, oslevel, ps, uptime
HMC	lshmc, lshwres, lspartition, lssyscfg
VIO/LPAR	Ioslevel, Iparstat, lsdev, lstcpip
HPUX	
ALL	adb, bc, cstm, df, domainname, getconf, ifconfig, pwdx, ioscan, lanscan, machinfo, model, netstat, nwmgr, pdcinfo, print_manifest, ps, selclass, setboot, swlist, uptime, lsof
Linux	
ALL	blkid, df, dmidecode (requires elevated permissions to execute), dnsdomainname, dpkg-query (Debian distro), free, ifconfig, lshal, ps, rpm (Redhat distro), uptime
HMC	lshmc
Solaris	
ALL	awk, arp, df, domainname, hostid, hostname, kstat, ifconfig, pkginfo, prodreg, prtconf, pargs (requires elevated permissions to execute), prtdiag, pooladm, ps, uptime, zoneadm, zonecfg

Windows (WMI)	root\default root\cimv2\Win32_Bios root\cimv2\Win32_ComputerSystem root\cimv2\Win32_ComputerSystemProduct root\cimv2\Win32_Directory root\cimv2\Win32_DisplayConfiguration root\cimv2\Win32_LogicalDisk root\cimv2\Win32_OperatingSystem root\cimv2\Win32_Process root\cimv2\Win32_Processor root\cimv2\Win32_PhysicalMemory root\cimv2\Win32_Service root\cimv2\Win32_SoundDevice root\cimv2\Win32_SystemEnclosure root\cimv2\Win32_TimeZone root\cimv2\Win32_UserAccount root\MicrosoftExchangeV2 root\virtualization\Msvm_BiosElement root\virtualization\Msvm_ComputerSystem root\virtualization\Msvm_MemorySettingData root\vm\virtualserver\VirtualMachine root\vm\virtualserver\VirtualServerProvider root\mscluster\MSCluster_Cluster root\mscluster\MSCluster_ClusterSharedVolume root\mscluster\MSCluster_Disk root\mscluster\MSCluster_DiskToDiskPartition root\mscluster\MSCluster_NetworkInterface root\mscluster\MSCluster_NetworkToNetworkInterface root\mscluster\MSCluster_Node root\mscluster\MSCluster_Resource root\mscluster\MSCluster_ResourceGroup root\mscluster\MSCluster_ResourceGroupToResource root\mscluster\MSCluster_ResourceType root\mscluster\MSCluster_ResourceTypeToResource

	root\mscluster\MSCluster_Service
Windows (Registry)	HKEY_LOCAL_MACHINE HKEY_USERS
Remote Processes	The commands above are issued directly as RPC calls and SSH/Telnet commands on the remote target. In addition, on a Windows target, the retrieval of process port number association is retrieved through the invocation of a root\cimv2\Win32_Process that invokes the **cmd.exe** program. This command-line program generates the process port information using **netstat** and writes the results to a file. This port information is then retrieved and used to populate the scan engine database for that target.

Appendix C: MS SQL Server system objects

When scanning Microsoft SQL Server, the following system objects need to be accessed and read to gather the required information:

System object	Platform
[MASTER]..[SYSLOGINS]	MS SQL 2000 or higher
[MASTER]..[SYSPROCESSES]	MS SQL 2000 or higher
[MASTER]..[SYSDATABASES]	MS SQL 2000
[MASTER]..[SYSALTFILES]	MS SQL 2000
SYS.SQL_LOGINS	SQL Azure
SYS.DM_OS_SYS_INFO	MS SQL 2005 or higher
SYS.DM_OS_CLUSTER_NODES	MS SQL 2005 or higher
SYS.DATABASE_MIRRORING	MS SQL 2005 or higher
SYS.DATABASES	MS SQL 2005
SERVERPROPERTY('')	MS SQL 2000 or higher
::FN_VIRTUALSERVERNODES()	MS SQL 2000
DB_NAME()	MS SQL 2000 or higher
SYS.MASTER_FILES	MS SQL 2000 or higher
SUSER_SNAME()	MS SQL 2000
@@SERVERNAME	MS SQL 2000 or higher
@@VERSION	MS SQL 2000 or higher

Appendix D: Key terms

Term	Definition
Advanced Encryption Standard (AES)	AES is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.
Dedicated server	A server designated to be a scanning server.
DLL	Dynamic Link Library
Estate access	Access to all devices within a network.
GAC	Global Assembly Cache
Data Center Discovery scan engine	An agentless scanning tool used for discovery and inventory.
Network inventory tool	A tool used to gather data on a network.
SSIS	SQL Server Integration Services
Target device	A device that the scan engine is attempting to discover; defined by the user.
WMI	Windows Management Instrumentation

Appendix E: Oracle EULA

Technology Network Development and Distribution License Terms for Oracle Data Access Components

Export Controls on the Programs

Selecting the "Accept License Agreement" button is a confirmation of your agreement that you comply, now and during the trial term, with each of the following statements:

-You are not a citizen, national, or resident of, and are not under control of, the government of Cuba, Iran, Sudan, Libya, North Korea, Syria, nor any country to which the United States has prohibited export.
-You will not download or otherwise export or re-export the Programs, directly or indirectly, to the above mentioned countries nor to citizens, nationals or residents of those countries.
-You are not listed on the United States Department of Treasury lists of Specially Designated Nationals, Specially Designated Terrorists, and Specially Designated Narcotic Traffickers, nor are you listed on the United States Department of Commerce Table of Denial Orders.

You will not download or otherwise export or re-export the Programs, directly or indirectly, to persons on the above mentioned lists.

You will not use the Programs for, and will not allow the Programs to be used for, any purposes prohibited by United States law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical or biological weapons of mass destruction.

EXPORT RESTRICTIONS
You agree that U.S. export control laws and other applicable export and import laws govern your use of the programs, including technical data; additional information can be found on Oracle®'s Global Trade Compliance web site (http://www.oracle.com/products/export).

You agree that neither the programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Oracle Employees: Under no circumstances are Oracle Employees authorized to download software for the purpose of distributing it to customers. Oracle products are available to employees for internal use or demonstration purposes only. In keeping with Oracle's trade compliance obligations under U.S. and applicable multilateral law, failure to comply with this policy could result in disciplinary action up to and including termination.

Note: You are bound by the Oracle Technology Network ("OTN") License Agreement terms. The OTN License Agreement terms also apply to all updates you receive under your Technology Track subscription.

The OTN License Agreement terms below supercede any shrinkwrap license on the OTN Technology Track software CDs and previous OTN License terms (including the Oracle Program License as modified by the OTN Program Use Certificate).

Oracle Technology Network Development and Distribution License Agreement for Oracle Data Access Client

"We," "us," and "our" refers to Oracle America, Inc. "You" and "your" refers to the individual or entity that wishes to use the Programs from Oracle under this Agreement. "Programs" refers to the Software Products referenced below that you wish to download and use and Program documentation. "License" refers to your right to use the Programs and Program documentation under the terms of this Agreement. The substantive and procedural laws of California govern this Agreement. You and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco, San Mateo, or Santa Clara counties in California in any dispute arising out of or relating to this Agreement.
We are willing to license the Programs to you only upon the condition that you accept all of the terms contained in this Agreement. Read the terms carefully and select the "Accept" button at the bottom of the page to confirm your acceptance. If you are not willing to be bound by these terms, select the "Do Not Accept" button and the registration process will not continue.

Software Product
- Oracle Data Access Components

License Rights

License.
We grant you a non-exclusive right and license to use the Programs solely for your business purposes and development and testing purposes, subject to the terms of this Agreement. You may allow third parties to use the Programs, subject to the terms of this Agreement, provided such third party use is for your business operations only.

Distribution License
We grant you a non-exclusive right and license to distribute the Programs, provided that you do not charge your end users for use of the Programs. Your distribution of such Programs shall at a minimum include the following terms in an executed license agreement between you and the end user that: (1) restrict the use of the Programs to the business operations of the end user; (2) prohibit (a) the end user from assigning, giving, or transferring the Programs or an interest in them to another individual or entity (and if your end user grants a security interest in the Programs, the secured party has no right to use or transfer the Programs); (b) make the Programs available in any manner to any third party for use in the third party's business operations (unless such access is expressly permitted for the specific program license or materials from the services you have acquired); and (c) title to the Programs from passing to the end user or any other party; (3) prohibit the reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs and prohibit duplication of the Programs except for a sufficient number of copies of each Program for the end user's licensed use and one copy of each Program media; (4) disclaim, to the extent permitted by applicable law, our liability for any damages, whether direct, indirect, incidental, or consequential, arising from the use of the Programs; (5) require the end user at the termination of the Agreement, to discontinue use and destroy or return to you all copies of the Programs and documentation; (6) prohibit publication of any results of benchmark tests run on the Programs; (7) require the end user to comply fully with all relevant export laws and regulations of the United States and other applicable export and import laws to assure that neither the Programs, nor any direct product thereof, are exported, directly or indirectly, in violation of applicable laws; (8) do not require us to perform any obligations or incur any liability not previously agreed to between you and us; (9) permit you to audit your end user's use of the Programs or to assign your right to audit the end user's use of the Programs to us; (10) designate us as a third party beneficiary of the end user license agreement; (11) include terms consistent with those contained in the sections of this Agreement entitled "Disclaimer of Warranties and Exclusive Remedies," "No Technical Support," "End of Agreement," "Relationship Between the Parties," and "Open Source"; and (11) exclude the application of the Uniform Computer Information Transactions Act.

You may allow your end users to permit third parties to use the Programs on such end user's behalf for the purposes set forth in the end user license agreement, subject to the terms of such agreement. You shall be financially responsible for all claims and damages to us caused by your failure to include the required contractual terms set forth above in each end user license agreement between you and an end user. We are a third party beneficiary of any end user license agreement between you and the end user, but do not assume any of your obligations thereunder, and you agree that you will not enter into any end user license agreement that excludes us as a third party beneficiary and will inform your end users of our rights.

If you want to use the Programs for any purpose other than as expressly permitted under this Agreement you must contact us to obtain the appropriate license. We may audit your use of the Programs. Program documentation is either shipped with the Programs, or documentation may be accessed online at http://docs.oracle.com/en/.

You agree to: (a) defend and indemnify us against all claims and damages caused by your distribution of the Programs in breach of this Agreement and/or failure to include the required contractual provisions in your end user agreement as stated above; (b) keep executed end user agreements and records of end user information including name, address, date of distribution and identity of Programs distributed; (c) allow us to inspect your end user agreements and records upon request; and, (d) enforce the terms of your end user agreements so as to effect a timely cure of any end user breach, and to notify us of any breach of the terms.

Ownership and Restrictions
We retain all ownership and intellectual property rights in the Programs. You may make a sufficient number of copies of the Programs for the licensed use and one copy of the Programs for backup purposes.

You may not:
-use the Programs for any purpose other than as provided above;
-charge your end users for use of the Programs;
-remove or modify any Program markings or any notice of our proprietary rights;

-assign this agreement or give the Programs, Program access or an interest in the Programs to any individual or entity except as provided under this agreement;
-cause or permit reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs;
-disclose results of any Program benchmark tests without our prior consent.

Export
You agree that U.S. export control laws and other applicable export and import laws govern your use of the Programs, including technical data; additional information can be found on Oracle's Global Trade Compliance web site located at http://www.oracle.com/products/index.html. You agree that neither the Programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Disclaimer of Warranty and Exclusive Remedies

THE PROGRAMS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. WE FURTHER DISCLAIM ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.

IN NO EVENT SHALL WE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. $1,000).

No Technical Support
Our technical support organization will not provide technical support, phone support, or updates to you or end users for the Programs licensed under this agreement.

Restricted Rights
If you distribute a license to the United States government, the Programs, including documentation, shall be considered commercial computer software and you will place a legend, in addition to applicable copyright notices, on the documentation, and on the media label, substantially similar to the following:
NOTICE OF RESTRICTED RIGHTS
"Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065."

End of Agreement
You may terminate this Agreement by destroying all copies of the Programs. We have the right to terminate your right to use the Programs if you fail to comply with any of the terms of this Agreement, in which case you shall destroy all copies of the Programs.

Relationship Between the Parties
The relationship between you and us is that of licensee/licensor. Neither party will represent that it has any authority to assume or create any obligation, express or implied, on behalf of the other party, nor to represent the other party as agent, employee, franchisee, or in any other capacity. Nothing in this Agreement shall be construed to limit either party's right to independently develop or distribute software that is functionally similar to the other party's products, so long as proprietary information of the other party is not included in such software.

Open Source
"Open Source" software - software available without charge for use, modification and distribution - is often licensed under terms that require the user to make the user's modifications to the Open Source software or any software that the user 'combines' with the Open Source software freely available in source code form. If you use Open Source software in conjunction with the Programs, you must ensure that your use does not: (i) create, or purport to create, obligations of us with respect to the Oracle Programs; or (ii) grant, or purport to grant, to any third party any rights to or immunities under our intellectual property or proprietary rights in the Oracle Programs. For example, you may not develop a software program using an Oracle Program and an Open Source program where such use results in a program file(s) that contains code from both the Oracle Program and the Open

Source program (including without limitation libraries) if the Open Source program is licensed under a license that requires any "modifications" be made freely available. You also may not combine the Oracle Program with programs licensed under the GNU General Public License ("GPL") in any manner that could cause, or could be interpreted or asserted to cause, the Oracle Program or any modifications thereto to become subject to the terms of the GPL.

Entire Agreement
You agree that this Agreement is the complete agreement for the Programs and licenses, and this Agreement supersedes all prior or contemporaneous Agreements or representations. If any term of this Agreement is found to be invalid or unenforceable, the remaining provisions will remain effective.
Should you have any questions concerning this License Agreement, or if you desire to contact Oracle for any reason, please write:
Oracle America, Inc.
500 Oracle Parkway,
Redwood City, CA 940