Data Center Discovery 2020.1

SCAN ENGINE PREREQUISITES GUIDE

Copyright notice
This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti") and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.ivanti.com.

Copyright © 2020, Ivanti. All rights reserved.
Ivanti and its logos are registered trademarks or trademarks of Ivanti, Inc. and its affiliates in the United States and/or other countries. Other brands and names may be claimed as the property of others.

Protected by patents, see http://www.ivanti.com/patents

Rev 04/20

Contents

Overview 5
About the scan engine 6
Scan engine components 6
Server preparation 7
Installation requirements 7
Estate access requirements 12
Protocols 12
Ports 14
Firewalls 14
Operating system credentials 14
Windows credentials 15
UNIX credentials 15
UNIX shells 16
Language settings 16
Application access requirements 18
Virtualization server access 18
VMware vSphere access 18
HMC and PowerVM access 19
Oracle access 19
Oracle support libraries 19
Oracle permissions 19
Restricting system privileges in Oracle 20
Oracle background details 21
MS SQL Server access 22
MS SQL Server support libraries 22
MS SQL Server permissions 22
Informix access 23
Informix support libraries 23
Informix install 23
Informix permissions 23
IBM DB2 access 24
IBM DB2 support libraries 24
IBM DB2 permissions 24

MongoDB 25
MongoDB install 25
MongoDB supported versions 25
MongoDB permissions 25
Cassandra 26
Cassandra install 26
Cassandra supported versions 26
Cassandra database permissions 26
Storage – EMC (BETA) 27
Storage (EMC) support libraries 27
Storage (EMC) permissions 27
Oracle VM for x86 27
Oracle VM for x86 REST API permissions 28
CyberArk Credential Manager 28
CyberArk required components 28
CyberArk required account permissions 28
Additional details 29
Appendix A: Default ports list 30
Ports recommended for discovery 30
Ports required for inventory 31
Appendix B: Privileged command access 32
Appendix C: MS SQL Server system objects 43
Appendix D: Key terms 44
Appendix E: Oracle EULA 45
Appendix F: IBM EULA 48
Appendix G: MongoDB drivers 48

Overview

This guide is written for the staff tasked with provisioning a company's hardware and software resources to ensure a successful installation of Ivanti's 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:

- **Scan engine overview:** This section describes what the scan engine does and the technology used. It also outlines the server hardware and software requirements.
- **Estate access requirements:** This section explains requirements needed for accessing the estate, including Windows and UNIX credentials.
- **Application access requirements:** This section discusses virtualization technology and database access.
- **Additional details:** This section 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 several 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. For details about these possible installation scenarios, see 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.)	260MB + SQL DB data (60GB) + 10GB Logs	260MB + SQL DB data (60GB) + 10GB Logs	260MB + SQL DB data (60GB) + 10GB Logs	260MB + 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 Windows server hosting the scan engine service must be configured to trust Thawte digital signatures.

Requirement	Minimum	Recommended
Common	Windows Server 2016 .NET Framework 4.5.1 SQL Server 2016 Express Service Pack 3 applied (the recommended Collation setting is Latin1_General_CI_AS).	Windows Server 2016 .NET Framework 4.5.1 SQL Server 2016 Standard 64-bit Service Pack 2 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 the 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 v10.0 with ASP.net (which must be pre-installed) See the "IIS requirements" section for full description of IIS requirements. The IIS **default** website must be present prior to installation.	IIS Server v10.0 with ASP.net (which must be pre-installed) See the "IIS requirements" section for full description of IIS requirements. The IIS **default** website must be present prior to installation.

> **Note:** Although not a requirement, it's strongly recommended that *before an installation* you configure a certificate and https binding for the default website for the SLL flag to be set through the installation process.

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.
    - If you choose to use Windows Authentication, then the database user must be a domain user and not a local machine account.
- The database logging should be configured to **simple** by default.
- It's 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 4.5 or above
- ASP .NET 4.5 or above
- 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

Installation on a FIPS-140-enabled target

FIPS (Federal Information Processing Standard) is a standard defined by NIST (National Institute of Standards and Technology) that specifies the security requirements for cryptographic modules. The application of a policy within an enterprise that forces the use of FIPS-certified algorithms and crypto implementations will cause errors when attempting to use Data Center Discovery.

Data Center Discovery makes use of the Microsoft-managed API when executing standard cryptographic operations. The managed version of the System.Security.Cryptography classes (whether invoked directly or indirectly) will fail when invoked in a FIPS-140 policy environment. This problem is not that the managed versions of the CRYPTOAPI are flawed or insecure. The problem is that these libraries have not been submitted for Certification by Microsoft to NIST.

Microsoft's comment on this functionality is as follows:

"Microsoft .NET Framework applications such as Microsoft ASP.NET only allow for using algorithm implementations that are certified by NIST to be FIPS-140 compliant. Specifically, the only cryptographic algorithm classes that can be instantiated are those that implement FIPS-compliant algorithms. The names of these classes end in "CryptoServiceProvider" or "Cng." Any attempt to create an instance of other cryptographic algorithm classes, such as classes with names ending in "Managed," cause an InvalidOperationException exception to occur. Additionally, any attempt to create an instance of a cryptographic algorithm that is not FIPS compliant, such as MD5, also causes an InvalidOperationException exception."

Microsoft does **not** enable FIPS by default: "We're not telling customers to turn it off – our recommendation is that it's each customer's decision to make." This is likely due to the complications and problems it can cause for individuals and corporations who do not need to comply with the FIPS-140 requirement for data processing.

As a result, Ivanti recommends that Data Center Discovery **not** be installed in a FIPS-140 enabled environment.

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 protocols that are standard to the target device OS/application. 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 provider (ping) • SNMP • TCP provider	• None • V2 (community); V3 (password) • None
Windows	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 (SMB)	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.
Cassandra	Cassandra	Premission to connect and execute required commands.
Certificate analysis provider	Certificate analysis	None
Couchbase	Couchbase	Read access to all system tables and views.
DB2	DB2	Read access to all system tables, views, and dictionaries.
DNS	DNS provider	None
Informix	Informix	Read access to all system tables, views, and dictionaries; execute access to database configuration stored procedures.
LDAP	LDAP	Windows non-privileged
Mongo	Mongo database	Premission to execute required commands.
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.
Oracle VM Manager	Oracle VM Manager (REST)	Read access to the REST API. A user in the "Monitor" global role would be appropriate.
SQL Server	MS SQL Server (TSQL)	Read access to all system tables, views, and dictionaries.
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.
WBEM	WBEM	Web-based Enterprise Management specific setup for communicating with SMI-S storage devices. Read access.

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**). More details can be found from Microsoft.

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 into 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 enable the commands found in Appendix B to be executed.

Windows credentials

When scanning 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.

> **Note:** To capture login information for Windows devices, a credential with Administrator permissions is required.

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 (for example, 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 on a device 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's used exclusively for scanning processes on the target device:
>
> ```
> Defaults:<username>      !requiretty
> ```
>
> You should also configure the scanning user 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 OSes might have a command-line length limitation of around 200 characters, which can 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

VMware ESX Product Adapter communicates with the vSphere installation using the vSphere Web API and the Simple Object Access Protocol (SOAP).

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 data centers).

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

> **Note:** The scan engine supports scanning of VMware vCenter servers 5.5, 6.0, and 6.5.

HMC and PowerVM access

To enable 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)

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, you can 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.

Restricting system privileges in Oracle

Because system privileges are so powerful, Oracle recommends that you configure your database to prevent regular (non-DBA) users from exercising ANY system privileges (such as UPDATE ANY TABLE) on the data dictionary. In order to secure the data dictionary, ensure that the O7_DICTIONARY_ACCESSIBILITY initialization parameter is set to FALSE, the default value. This feature is called the dictionary protection mechanism.

The O7_DICTIONARY_ACCESSIBILITY initialization parameter controls restrictions on system privileges when you upgrade from Oracle Database version 7 to Oracle8i and higher releases. If the parameter is set to TRUE, then access to objects in the SYS schema is allowed (Oracle Database version 7 behavior). If this parameter is set to FALSE, then system privileges that allow access to objects in any schema do not allow access to objects in the SYS schema. The default for O7_DICTIONARY_ACCESSIBILITY is FALSE (no SYS schema access allowed).

If you enable dictionary protection (O7_DICTIONARY_ACCESSIBILITY is set to FALSE), then access to objects in the SYS schema (dictionary objects) is restricted to users with the SYS schema. These users are SYS and those who connect as SYSDBA.

System privileges providing access to objects in other schemas **do not** give other users access to objects in the SYS schema. For example, the SELECT ANY TABLE privilege allows users to access views and tables in other schemas, but does not enable them to select dictionary objects (base tables of dynamic performance views, views, packages, and synonyms).

These users can, however, be granted explicit object privileges to access objects in the SYS schema.

- Accessing objects in a **non-SYS** schema:
  Select ANY Table system privilege allows query access to tables, views, or materialized views in any schema (this excludes the SYS schema).
- Accessing objects in the **SYS** schema:
  Users with explicit object privileges or those who connect with administrative privileges (SYSDBA) can access objects in the SYS schema. Additionally, system privilege can be granted to users who require access to tables created in the SYS schema using the following command:

  Select ANY Dictionary system privilege allows query access to any object in the SYS schema, including tables created in that schema. It must be granted individually to each user requiring the privilege. It is not included in GRANT ALL PRIVILEGES, but it can be granted through a role. This privilege lets you selectively override the FALSE setting of the O7_DICTIONARY_ACCESSIBILITY initialization parameter.

- Database Login:
  Finally, data retrieval requires that the user can log into the database. This requires an additional privilege—the **Create Session** system privilege allows the assigned user to establish a connection to the target database. This is required, as the user will need to connect to both CDBs and PDBs remotely.

In conclusion, the Oracle LMS queries require access to a number of the underlying SYS-schema-defined tables, and the user that is required to execute the associated queries must have appropriate privileges.

Examples queries that would make use of these privileges:

- **SELECT** DISTINCT

  c.SET_NAME as CHANGE_SET_NAME

  c.PUBLISHER

  c.QUEUE_TABLE_NAME

  FROM

  SYS.CDC_CHANGE_SETS$ c

- **SELECT count(*) from SYS.MODEL$;**

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 so that you can 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 a 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

In order for Data Center Discovery to scan an Informix database, a special client application must be installed with the scan engine software. Download the latest release (Informix Client SDK Developer Edition for Windows x86_64, 64-bit), which requires an IBM login. Installation instructions are included in the .ZIP file.

Informix install

1. Run the installer as Administrator.
2. Install the IBM Informix .NET Provider installation feature.
3. Complete the installation process. The IBM Data Server Driver installation is *not* required.
4. Add the appropriate Informix credentials in the Data Center Discovery 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 client driver package must be installed on the scanning server. Download the latest release (64-bit IBM Data Server Driver Package), which requires an IBM login. Install instructions are included in the .ZIP file.

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).

MongoDB

MongoDB install

1. Select the appropriate MongoDB installation process for the OS and MongoDB edition. Also ensure that the installed version is of the correct bit architecture and isn't approaching EOL. See https://docs.mongodb.com/ for more information.
2. Read the installation instructions for the version of MongoDB required.
3. Add the appropriate MongoDB credentials in the UI.

MongoDB supported versions

Data Center Discovery currently uses the MongoDB .NET driver v2.6, and this limits the current recommended support to MongoDB v3.6 (or lower).

The following compatibility table specifies the recommended version(s) of the MongoDB C#.NET driver for use with a specific version of MongoDB.

C# .NET driver version	DB 4.2	DB 4.0	DB 3.6	DB 3.4	DB 3.2	DB3.0	DB 2.6
v2.9	x	x	x	x	x	x	x
v2.8		x	x	x	x	x	x
v2.7		x	x	x	x	x	x
v2.6			**x**	**x**	**x**	**x**	**x**
v2.5			x	x	x	x	x
v2.4				x	x	x	x
v2.3					x	x	x
v2.2					x	x	x
v2.0						x	x
v1.11					x	x	x
v1.10						x	x

MongoDB permissions

Connections are established using the username, password, and remote IP address. It's assumed that the username is always available in the adm DB instance for authentication purposes.

Validation of the connection is ensured by forcing a command to be sent to the database, which in turn forces an auth attempt.

To gather the detailed information required for a MongoDB scan, the scan engine needs to log into the database and execute a sequence of commands against the admin database instance. The list of commands that are executed using network protocol against the MongoDB are as follows:

Request Type	Request Query
Force Authentication	{ping: 1}
List Databases	{listDatabases: 1}
Is Master	{isMaster: 1}
Server Status	{serverStatus: 1}

The MongoDB user credential must have permissions to execute these commands and thereby return results. Possible role settings for the login account are: **cluster_admin** (allows hosts to be visible) and **dbAdminAnyDatabase** (provides visibility into the databases). You're free to apply other appropriate roles if required.

Cassandra

Cassandra install

1. Identify the appropriate Cassandra database installation process for the OS and Cassandra database edition. Also ensure that the installed version is of the correct bit architecture and isn't approaching EOL.
2. Read installation instructions for the version of Cassandra database required.
3. Add the appropriate Cassandra database credentials in the UI.

Cassandra supported versions

Data Center Discovery currently uses the Cassandra database .NET driver v3.8. This driver has been tested against both community and enterprise editions.

Cassandra database permissions

Connections are established using the username, password, and remote IP address.

To gather the detailed information required for a Cassandra database scan, the scan engine needs to log into the database (cluster) and execute a sequence of commands. The list of commands that are executed using network protocol against the Cassandra database are as follows:

Request Type	Request Query
Get All Hosts	No explicit query. Host list is established as part of connection establishment.
Version and Edition	SELECT *FROM system.local

The Cassandra database user credential must have permissions to connect and execute these commands and thereby return results.

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 a customer 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). Install instructions are included in the .EXE file. 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, which 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

Set up 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.

CyberArk 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.

CyberArk 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 needed components 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 an install of the product.

Appendix A: Default ports list

Ports recommended for discovery

This is a list of example ports that can be provided during the **discovery** phase. The identification of these as open ports identifies that a device is present.

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
902	VMWare ESX
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)
5985 5986	Windows PowerShell default psSession Port
7001	Default for BEA WebLogic Servers HTTP server, though often changed during installation

Discovery can be achieved by certificate analysis and TCP provider (port scan). Either of these connection types can potentially use ports from this list. The TCP provider uses ports 22, 23, 80, 443, 135, 139, 445, 5985, 5986, 902 by default.

Ports required for inventory

You're required to open the following 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
1025 to 5000	TCP	WMI dynamic ports	Windows XP/Server 2003 or lower
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, or registry hives are used by the Data Center Discovery scan engine, and a user must be provided access to these commands to successfully retrieve inventory data.

Platform Type	Type	Command Run	Protocol Used	What are you trying to Scan?
Windows	ALL	Select	LDAP	Windows Device
		SNMP tree get	SNMP	Windows Device
		get <storage>	WBEMClient	Device
		cfg	Windows File Share	Application
		apache.exe	Windows Remote Process	Application
		appclient.bat	Windows Remote Process	Windows Device
		cmlevel.bat	Windows Remote Process	Windows Device
		dgmgrl	Windows Remote Process	Application
		dspmq	Windows Remote Process	Windows Device
		echo	Windows Remote Process	Windows Device
		httpd.exe	Windows Remote Process	Application
		ipconfig	Windows Remote Process	Windows Device
		iquate_lms_hw.cmd	Windows Remote Process	Windows Device
		manageprofiles.bat	Windows Remote Process	Windows Device
		mongod.exe	Windows Remote Process	Windows Device
		mqsiprofile	Windows Remote Process	Windows Device
		netstat	Windows Remote Process	Windows Device
		opmnctl	Windows Remote Process	Application
		systeminfo	Windows Remote Process	Windows Device
		tasklist	Windows Remote Process	Windows Device
		<registry key>	Windows Remote Registry	Windows Device
		registry key	Windows Remote Registry	Windows Device

		<wmi space>	Windows WMI	Windows Device
		Select	Windows WMI	Windows Device
	BASIC	tail	Windows Remote Process	Application
		ls	Windows Remote Registry	Windows Device
	DB2	db2cmd.exe	Windows Remote Process	Application
		db2ilist	Windows Remote Process	Application
		db2licm	Windows Remote Process	Application
	INFORMIX	onstat	Windows Remote Process	Windows Device
	SMB	Windows direct file access	Windows File Share	Windows Device

Platform Type	Type	Command Run	Protocol Used	What are you trying to Scan?
VSphere	vSphere	get:ClusterComputeResource-domain	VMware	Application
		get:ComputeResource-domain	VMware	Application
		get:Datastore-datastore	VMware	Application
		get:Folder-group	VMware	Application
		get:HostSystem-host	VMware	Application
		get:TestStore	VMware	Application
		get:VirtualMachine-vm	VMware	Application
		Get-Datacenters	VMware	Application
		getview:licensemanager	VMware	Application
		ServiceContent:AboutInfo	VMware	Application
Storage Device	ALL	getall	NavisphereCLI	Storage Device
		getcrus	NavisphereCLI	Storage Device
		storagepool	NavisphereCLI	Storage Device
		Retrieving <attribute>	WBEMClient	Storage Device
		storagepool	WBEMClient	Storage Device

Platform Type	Type	Command Run	Protocol Used	What are you trying to Scan?
Solaris	ALL	arp	SSH-TELNET	Solaris Device
		hostid	SSH-TELNET	Solaris Device
		ifconfig	SSH-TELNET	Solaris Device
		kstat	SSH-TELNET	Solaris Device
		lsof	SSH-TELNET	Solaris Device
		pargs (requires elevated permissions to execute)	SSH-TELNET	Application
		pfiles	SSH-TELNET	Solaris Device
		pkginfo	SSH-TELNET	Solaris Device
		pooladm	SSH-TELNET	Solaris Device
		prtconf	SSH-TELNET	Solaris Device
		prtdiag	SSH-TELNET	Solaris Device
		psrinfo	SSH-TELNET	Solaris Device
		smbios	SSH-TELNET	Solaris Device
		uname	SSH-TELNET	Solaris Device
		uptime	SSH-TELNET	Solaris Device
		zoneadm	SSH-TELNET	Solaris Device
		zonecfg	SSH-TELNET	Solaris Device
		zonename	SSH-TELNET	Solaris Device
	BASIC	cat	SSH-TELNET	Solaris Device
		hostname	SSH-TELNET	Solaris Device
		ls	SSH-TELNET	Solaris Device
		ps	SSH-TELNET	Solaris Device
Scan Engine	ALL	certdiscovery	Certificate Analysis Provider	Device
		Select	LDAP	Windows Device

		Select	MS SQL Server	Application
		SNMP tree get	REST	Device
		cfg	SMB	Windows Device
		portdiscoverytcp	TCP Provider	Device
		get <storage>	WBEM	Storage Device
	BASIC	ping	ICMP Provider	Device
		ping	TCP Provider	Device
	SMB	Windows direct file access	SMB	Windows Device

Platform Type	Type	Command Run	Protocol Used	What are you trying to Scan?
Network Device	ALL	<ipresolve>	DNS Provider	Network Device
		SNMP tree get	SNMP	Network Device
		SNMP tree getnext	SNMP	Network Device
		SNMP tree walk	SNMP	Network Device
Linux (Debian)	ALL	dpkg-query	SSH-TELNET	Linux (Debian) Device
	BASIC	cat	SSH-TELNET	Linux (Debian) Device
Linux	ALL	blkid	SSH-TELNET	Linux Device
		dig	SSH-TELNET	Linux Device
		dmidecode (requires elevated permissions to execute)	SSH-TELNET	Linux Device
		dnsdomainname	SSH-TELNET	Linux Device
		ifconfig	SSH-TELNET	Linux Device
		lsb_release	SSH-TELNET	Linux Device
		lscpu	SSH-TELNET	Linux Device
		lshal	SSH-TELNET	Linux Device
		lsof	SSH-TELNET	Linux Device
		lspci	SSH-TELNET	Linux Device

		nslookup	SSH-TELNET	Linux Device
		rpm	SSH-TELNET	Linux Device
		tune2fs	SSH-TELNET	Linux Device
		uname	SSH-TELNET	Linux Device
	BASIC	cat	SSH-TELNET	Linux Device
		df	SSH-TELNET	Linux Device
		ls	SSH-TELNET	Linux Device
		ps	SSH-TELNET	Linux Device

Platform Type	Type	Command Run	Protocol Used	What are you trying to Scan?
HP-UX	ALL	domain	SSH-TELNET	HP-UX Device
		echo	SSH-TELNET	HP-UX Device
		getconf	SSH-TELNET	HP-UX Device
		kctune	SSH-TELNET	HP-UX Device
		lanscan	SSH-TELNET	HP-UX Device
		lsof	SSH-TELNET	HP-UX Device
		machinfo	SSH-TELNET	HP-UX Device
		model	SSH-TELNET	HP-UX Device
		netstat	SSH-TELNET	HP-UX Device
		nwmgr	SSH-TELNET	HP-UX Device
		pfiles	SSH-TELNET	HP-UX Device
		setboot	SSH-TELNET	HP-UX Device
		swlist	SSH-TELNET	HP-UX Device
		uname	SSH-TELNET	HP-UX Device
		uptime	SSH-TELNET	HP-UX Device
	BASIC	cat	SSH-TELNET	HP-UX Device
		ls	SSH-TELNET	HP-UX Device

		ps	SSH-TELNET	HP-UX Device
	HMC	lshmc	SSH-TELNET	HP-UX Device
Application	ALL	Select	DB2	Application
		Select	Informix	Application
		Select	Oracle Database	Application
		alter session	PLSQL	Application
		Select	PLSQL	Application

Platform Type	Type	Command Run	Protocol Used	What are you trying to Scan?
AIX	ALL	domainname	SSH-TELNET	AIX Device
		entstat	SSH-TELNET	AIX Device
		ifconfig	SSH-TELNET	AIX Device
		lsattr	SSH-TELNET	AIX Device
		lscfg	SSH-TELNET	AIX Device
		lslpp	SSH-TELNET	AIX Device
		lsof	SSH-TELNET	AIX Device
		netstat	SSH-TELNET	AIX Device
		oslevel	SSH-TELNET	AIX Device
		uname	SSH-TELNET	AIX Device
		uptime	SSH-TELNET	AIX Device
	BASIC	cat	SSH-TELNET	AIX Device
		ps	SSH-TELNET	AIX Device

Platform Type	Type	Command Run	Protocol Used	What are you trying to Scan?
*NIX	ALL	adb	SSH-TELNET	Device
		apache2	SSH-TELNET	Application
		appclient.sh	SSH-TELNET	Application

		arp	SSH-TELNET	Device
		blkid	SSH-TELNET	Device
		cmlevel	SSH-TELNET	Application
		dgmgrl	SSH-TELNET	Application
		dig	SSH-TELNET	Device
		dmesg	SSH-TELNET	Linux Device
		dmidecode (requires elevated permissions to execute)	SSH-TELNET	Linux Device
		dnsdomainname	SSH-TELNET	Device
		domain	SSH-TELNET	Device
		domainname	SSH-TELNET	Device
		dpkg-query	SSH-TELNET	Device
		dspmq	SSH-TELNET	Application
		dspmqver	SSH-TELNET	Device
		echo	SSH-TELNET	Application
		entstat	SSH-TELNET	Device
		free	SSH-TELNET	Linux Device
		gedit	SSH-TELNET	Device
		getconf	SSH-TELNET	Device
		ggsci	SSH-TELNET	Application
		haclus	SSH-TELNET	Device
		hastatus	SSH-TELNET	Device
		hostid	SSH-TELNET	Device
		httpd.exe	SSH-TELNET	Application
		ifconfig	SSH-TELNET	Device
		ioscan	SSH-TELNET	Device
		ioslevel	SSH-TELNET	Device
		kctune	SSH-TELNET	Device

		kstat	SSH-TELNET	Device
		lanscan	SSH-TELNET	Device
		lastlog	SSH-TELNET	Device
		list server	SSH-TELNET	Device
		locate	SSH-TELNET	Application
		lsattr	SSH-TELNET	Device
		lsb_release	SSH-TELNET	Device
		lscfg	SSH-TELNET	Device
		lscpu	SSH-TELNET	Device
		lshal	SSH-TELNET	Linux Device
		lslpp	SSH-TELNET	Device
		lslv	SSH-TELNET	Device
		lsof	SSH-TELNET	Device
		lspci	SSH-TELNET	Device
		machinfo	SSH-TELNET	Device
		manageprofiles.sh	SSH-TELNET	Application
		model	SSH-TELNET	Device
		mqsilist	SSH-TELNET	Device
		netstat	SSH-TELNET	Device
		nslookup	SSH-TELNET	Device
		nwmgr	SSH-TELNET	Device
		opmnctl	SSH-TELNET	Application
		oslevel	SSH-TELNET	Device
		pargs (requires elevated permissions to execute)	SSH-TELNET	Device
		pdcinfo	SSH-TELNET	Device
		pfiles	SSH-TELNET	Device
		pkginfo	SSH-TELNET	Device

		pooladm	SSH-TELNET	Device
		print_manifest	SSH-TELNET	Device
		prtconf	SSH-TELNET	LPAR
		prtdiag	SSH-TELNET	Device
		psrinfo	SSH-TELNET	Device
		rpm	SSH-TELNET	Application
		setboot	SSH-TELNET	Device
		show <ovmattr>	SSH-TELNET	Device
		showversion	SSH-TELNET	Device
		smbios	SSH-TELNET	Device
		swlist	SSH-TELNET	Device
		tune2fs	SSH-TELNET	Device
		uname	SSH-TELNET	LPAR
		uptime	SSH-TELNET	Device
		uv	SSH-TELNET	Device
		versioninfo.sh	SSH-TELNET	Application
		vxlicrep	SSH-TELNET	Device
		xl	SSH-TELNET	Device
		zoneadm	SSH-TELNET	Solaris Device
		zonecfg	SSH-TELNET	Solaris Device
		zonename	SSH-TELNET	Solaris Device

Platform Type	Type	Command Run	Protocol Used	What are you trying to Scan?
*NIX	BASIC	cat	SSH-TELNET	Linux Device
		df	SSH-TELNET	Device
		find	SSH-TELNET	Application
		grep	SSH-TELNET	Device

		hostname	SSH-TELNET	Device
		ls	SSH-TELNET	Application
		ping	SSH-TELNET	Application
		ps	SSH-TELNET	Device
		strings	SSH-TELNET	Application
		tail	SSH-TELNET	Application
	DB2	db2	SSH-TELNET	Application
		db2ilist	SSH-TELNET	Application
		db2licm	SSH-TELNET	Application
	HMC	lshmc	SSH-TELNET	Device
	INFORMIX	oninit	SSH-TELNET	Application
		onstat	SSH-TELNET	Application
	LPAR	lparstat	SSH-TELNET	LPAR
		lsdev	SSH-TELNET	LPAR

Protocol	Key
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\virtualization\v2\Msvm_BiosElement root\virtualization\v2\Msvm_ComputerSystem root\virtualization\v2\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
Windows (WMI)	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. The system object accesses are listed below.

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

Appendix F: IBM EULA

iQuate (and resellers) make use of IBM supplied libraries in order to query DB2 and Informix database services. This involves the installation (on behalf of the customer) of supporting client libraries that expose Application Program Interfaces. The customer is still subject to normal licencing of the target software installation. The use of the API is a derived work based on sample programs provided by IBM. As required by IBM, the following copyright notice is provided to identify associated ownership of this API and derived software.

Additional information is available from IBM here:
https://www.ibm.com/support/knowledgecenter/en/SSEPGG_11.1.0/com.ibm.swg.im.dbclient.adonet.doc/doc/c0010960.html

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. 2019. All rights reserved.

Appendix G: MongoDB drivers

Copyright 2010 – present MongoDB Inc.

Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.