DISCOVERY AND INVENTORY OF DELL EMC DEVICES BY USING DELL EMC OPENMANAGE ESSENTIALS (OME)

ABSTRACT
This technical white paper describes the discovery, inventory, and other features of OME.

August, 2017

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2017 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA [8/9/2017]

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.
## CONTENTS

**EXECUTIVE SUMMARY** ................................................................. 4
**INTRODUCTION** ............................................................................. 4
**SCOPE** .......................................................................................... 4

**DISCOVERY AND INVENTORY** .......................................................... 4
  Prerequisites ...................................................................................... 4
  Performing discovery and inventory using guided wizard.................................. 5
    Configuring discovery range ................................................................ 5
    IP Address or IP Range ...................................................................... 6
  Device type filtering ........................................................................... 8
  Configuring ICMP ............................................................................ 9
  Configuring SNMP .......................................................................... 9
  Configuring WMI ........................................................................... 11
  Configuring WS-Man ....................................................................... 11
    WS-Man configuration field descriptions ........................................... 11
    WS-Man configuration screen options for discovering CMC and all associated components .......... 12
  Configuring SSH ........................................................................... 14
  Summary ....................................................................................... 14

**DEVICE-BASED DISCOVERY** ................................................................ 16
  Note for upgrade scenarios .............................................................. 16
  Excluding range ............................................................................. 17
  Skipping ICMP ping during discovery .............................................. 18

**PERFORMING DISCOVERY AND INVENTORY USING STANDARD WIZARD** ............ 19
  Configuring Storage ....................................................................... 20
  Configuring IPMI ........................................................................... 21
  Discovery range action ................................................................. 22
Executive summary

A fundamental element of any Device Management is discovery and inventory of devices an organization is trying to manage in its IT and data center environment. Discovery must be non-invasive, easy to administer, efficient, thorough, accurate, broad in scope, and responsive to network changes.

Discovery is a process of identifying all Dell EMC hardware devices in your network, such as PowerEdge servers, EqualLogic storage, and PowerConnect switches. It is an unobtrusive way of searching for all networked devices and providing an analysis of each device such as software, memory, components, and serial number. The Inventory Report provides information about all discovered devices such as device health, available memory, and installed software.

Introduction

OME is a hardware management application that provides a comprehensive view of Dell EMC systems, devices, and components in the enterprise network. OME is a web-based and one-to-many systems management application. For Dell EMC systems and other devices and components, you can discover and inventory the systems, monitor the systems' health, and perform system updates.

Scope

The purpose of this technical white paper is to help you with the necessary steps to perform discovery and inventory of Dell EMC devices. The high-level tasks described in this technical white paper:

- Discovery and inventory
  - Guided Wizard
  - Standard Wizard
- Device Based Discovery
- Skipping ICMP ping during discovery
- Providing a holistic view of the data center.
- Searching specific devices.

Discovery and inventory

Discovery and inventory enables understanding about the hardware and software installed across an organization and it is the basic step to effective systems management. Areas such as license compliance, health monitoring, security and upgrades, and migrations require the networked hardware to be available to the System Administrator on a single console to help simplify the process. OME provides these capabilities to initialize the discovery and inventory process and perform required actions on these devices.

Prerequisites

Credentials: The discovery process in OME communicates to the devices by using the following supported protocols:

Table 1. Protocols and Credentials

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Required Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP</td>
<td>SNMP Community string</td>
</tr>
<tr>
<td>WMI</td>
<td>Windows Administrator credentials</td>
</tr>
<tr>
<td>IPMI</td>
<td>IPMI operator credentials</td>
</tr>
<tr>
<td>WS-Man</td>
<td>WS-Man Administrator credentials</td>
</tr>
<tr>
<td>Dell EMC Array</td>
<td>EMC credentials</td>
</tr>
<tr>
<td>SSH</td>
<td>SSH Administrator credentials</td>
</tr>
</tbody>
</table>
Setting up the systems to be managed: There are a few settings to be performed on the managed node to make it discoverable over the network. For more information, see the *Make your Environment Manageable with Dell OpenManage Essentials* white paper on the Dell TechCenter.

OpenManage Server Administrator (OMSA): OMSA must be installed on all the systems that must be managed by using OME.

**Performing discovery and inventory using guided wizard**

- Discovery Range Configuration
- Device Type Filtering
- ICMP Configuration
- SNMP Configuration
- WMI Configuration
- WS-Man Configuration
- SSH Configuration
- Summary

**Configuring discovery range**

Mention the device IP ranges in the environment to perform discovery and inventory.

1. Click Manage → Discovery and Inventory → Discovery Ranges → All Ranges.
2. Right-click All Ranges and click Add Discovery Range.

*Figure 1. Adding Discovery Range*
**IP Address or IP Range**

Sample IP ranges that can be used as an IP range for discovery:

<table>
<thead>
<tr>
<th>Table 2. Sample IP range</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP range</td>
</tr>
<tr>
<td>192.109.112.*</td>
</tr>
<tr>
<td>192.109.110-112.*</td>
</tr>
<tr>
<td>192.109.<em>.</em></td>
</tr>
<tr>
<td>192.109.110-112.11-19</td>
</tr>
<tr>
<td>192.109.110.11-19</td>
</tr>
<tr>
<td>Host name</td>
</tr>
<tr>
<td>WIN-XPDF17J</td>
</tr>
<tr>
<td>Single IP</td>
</tr>
<tr>
<td>192.109.112.113</td>
</tr>
</tbody>
</table>

The Import functionality provided in OME enables you to import a Discovery Range which is defined in a .csv file format. The maximum numbers of devices that can be imported by using this method is 500.

**Figure 3. .csv file**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1750-win-r03-03</td>
<td>Host (A)</td>
<td>10.94.172.180</td>
</tr>
<tr>
<td>1750-win-r03-04</td>
<td>Host (A)</td>
<td>10.94.172.181</td>
</tr>
<tr>
<td>1750-win-r03-05</td>
<td>Host (A)</td>
<td>10.94.172.182</td>
</tr>
<tr>
<td>1750-win-r03-06</td>
<td>Host (A)</td>
<td>10.94.172.183</td>
</tr>
<tr>
<td>1750-win-r03-07</td>
<td>Host (A)</td>
<td>10.94.10.184</td>
</tr>
<tr>
<td>1750-win-r03-08</td>
<td>Host (A)</td>
<td>10.94.172.185</td>
</tr>
<tr>
<td>1750-win-r03-09</td>
<td>Host (A)</td>
<td>10.94.172.186</td>
</tr>
<tr>
<td>2890-win2k12R2</td>
<td>Host (A)</td>
<td>10.94.17.187</td>
</tr>
<tr>
<td>2891-esx</td>
<td>Host (A)</td>
<td>10.94.12.188</td>
</tr>
</tbody>
</table>
The following example demonstrates adding a Discovery Range by using SNMP or WMI protocol in the Add Discovery Range Wizard.

1. Enter the IP range to be discovered.
2. Type the Range Name (optional) and click **Add**.
3. If necessary, repeat steps 1–2.
4. Click **Next**.

**Figure 4. Specifying IP range**
**Device type filtering**

Enables selection of the type of devices that must be discovered. Each selected device has an associated protocol and the types of devices and associated devices that can be selected are listed in 0 and the screen shot is shown in Figure 5.

For example, to select an out-of-band IP, select the **iDRAC (server out of band)** check box, and then type the WS-Man credentials (see Figure 5).

Device type and associated protocols:

<table>
<thead>
<tr>
<th>Sl. No</th>
<th>Device Type</th>
<th>Required Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>iDRAC (Server out of band)</td>
<td>WS-MAN</td>
</tr>
<tr>
<td>2</td>
<td>Server with OMSA</td>
<td>SNMP</td>
</tr>
<tr>
<td>3</td>
<td>Windows Server without OMSA</td>
<td>WMI</td>
</tr>
<tr>
<td>4</td>
<td>Linux Server without OMSA</td>
<td>SSH</td>
</tr>
<tr>
<td>5</td>
<td>ESXi Host</td>
<td>SNMP + WS-MAN</td>
</tr>
<tr>
<td>6</td>
<td>HyperV Host + Guests</td>
<td>SNMP + WMI</td>
</tr>
<tr>
<td>7</td>
<td>Chassis (CMC) Discovery - All Components</td>
<td>WS-MAN</td>
</tr>
<tr>
<td>8</td>
<td>Windows Desktops and Laptops</td>
<td>WMI</td>
</tr>
<tr>
<td>9</td>
<td>PowerVault MD Array</td>
<td>MD Array</td>
</tr>
<tr>
<td>10</td>
<td>Other Devices</td>
<td>SNMP</td>
</tr>
</tbody>
</table>

![Figure 5. Device Type Filtering screen](image)

**Note:**

To select Chassis (CMC) Discovery, you must type the group name. See Figure 4.
Configuring ICMP

1. Set the time after which the PING task must time out.
2. Specify the number of attempts.
3. Click Next.

Figure 6. ICMP Configuration screen

Configuring SNMP

You can configure SNMP on:

- A server that has OMSA installed
- An ESXi Host
- A HyperV Host and guest servers
- Other devices

On the SNMP Configuration page, following options are displayed:

- Option to select SNMP V1/V2C
  - Get Community Name
  - Set community name
- Option to select SNMP V3
  - Authentication protocols (SHA1, MD5, None)
  - User Name
  - Authentication Password
  - Encryption Protocol (AES, DES, None)
- Encryption Password
- Timeout
- Number of retries to be performed

For more information about the SNMP V3 configuration, see the SNMP v3 based discovery and monitoring technical white paper on Dell TechCenter.

Figure 7. SNMP Configuration screen
Configuring WMI
The WMI Configuration dialog box is displayed when the following options are selected:

- Domain \ User name
- Password

Figure 8. WMI Configuration screen

Configuring WS-Man
The WS-Man Configuration dialog box is displayed when the following options are selected:

- iDRAC (Server out of band)
- ESXi Host
- Chassis (CMC) Discovery – All Components

WS-Man configuration field descriptions
Select iDRAC (Server out-of-band) and ESXi Host, and type or select data in the fields:

- **WS-MAN User ID**, where the iDRAC or ESXi host user name must be typed.
- Type the iDRAC or ESXi host name and password.
- Type the duration after which the discovery task must time out, number of attempts to discover, and the port to access a device.
- **Secure Mode**, provides the options related to security
  - Skip Common name check: to skip authenticating common name
  - Weather Trusted site or not: to skip authenticating certifying authority
  - Certificate file, if the WS-MAN server(s) needs to be provided
WS-Man configuration screen options for discovering CMC and all associated components

In case of **Chassis (CMC) Discovery – All Components**, the following tabs are displayed:

- WS-Man Configuration of the CMC Device
- WS-Man configuration for iDRACs and switches

The first tab screen is exactly same as WS-Man configuration. Second tab (Alternate WS-Man Configuration for iDRACs) has additional options, mentioned below and shown in Figure 11:

- Auto-discover iDRACs and switches in CMC – Select to discover switches and iDRACs installed on a CMC
- Use the same credentials of CMC for discovering iDRACs – If you clear the check box, type the iDRAC credentials
Figure 10. CMC WS-Man Configuration Screen, tab 1

Figure 11. CMC WS-Man Configuration Screen, tab 2
Configuring SSH

This screen appears when SSH is selected in the device type filtering screen. It is as shown in Figure 12.

- User Name
- Password
- Port, Retries and Timeout

Figure 12. SSH Configuration screen

Summary

This screen displays a list that summarizes the options selected from the first screen. After reviewing the summary, you can modify the settings or complete the process.

1. Click Back to navigate to the previous screens.
2. Click Finish to complete the range configuration, the range will be added to the Include Range list.
3. Select the required label to directly go to a specific screen.
Review your inputs and click Finish to continue or click Back to change your inputs.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action to be taken</td>
<td>Perform both Discovery and Inventory.</td>
</tr>
<tr>
<td>Include Range</td>
<td>192.168.1-2.10.255.255-255.9</td>
</tr>
<tr>
<td>ICMP Timeout (milliseconds)</td>
<td>1000</td>
</tr>
<tr>
<td>ICMP Retry</td>
<td>1</td>
</tr>
<tr>
<td>WSMAN Discovery</td>
<td>Enabled</td>
</tr>
<tr>
<td>WSMAN UserName</td>
<td>root</td>
</tr>
<tr>
<td>WSMAN Port #</td>
<td>443</td>
</tr>
<tr>
<td>WSMAN Timeout</td>
<td>60</td>
</tr>
<tr>
<td>WSMAN Retries</td>
<td>3</td>
</tr>
<tr>
<td>Certificate Path</td>
<td></td>
</tr>
<tr>
<td>SNMP Discovery</td>
<td>Enabled</td>
</tr>
<tr>
<td>SNMP v3 Discovery</td>
<td>Disabled</td>
</tr>
<tr>
<td>SNMP v1v2c Discovery</td>
<td>Enabled</td>
</tr>
<tr>
<td>SNMP Timeout (seconds)</td>
<td>4</td>
</tr>
<tr>
<td>Number of SNMP Retry attempts</td>
<td>2</td>
</tr>
<tr>
<td>SNMP Get Community</td>
<td>public</td>
</tr>
<tr>
<td>SNMP Set Community</td>
<td></td>
</tr>
<tr>
<td>WMI Discovery</td>
<td>Enabled</td>
</tr>
<tr>
<td>WMI User Name</td>
<td>localhost/Administrator</td>
</tr>
</tbody>
</table>
**Device-based discovery**

Enables discovering only the device types selected in the **Device Type Filtering** screen mentioned in Figure 5.

For example, if **iDRAC (server out-of-band)** is selected in the **Device Type Filtering** screen, only iDRAC servers that match the credentials are discovered, and CMCs or ESXi servers are not discovered.

By default, OME has device-based discovery. To disable this filter:

- Click **Settings** → **Discovery Settings**.
- Clear the **Discover the selected Device Types only** check box.
- Click **Apply**.

![Figure 13. Device Based Discovery screen](image)

**Note for upgrade scenarios**

If OME was upgraded from either 2.1 or 2.2 to 2.3 and later versions, you observe a change in the guided wizard. By default, the guided wizard in OME 2.3 shows the behavior of device-based discovery.

By default, the Discovery/Inventory uses Device-based discovery in the following cases:

- Any new discovery configuration created after upgrade
- The discovery configuration that was created in the previous version by using guided wizard
Excluding range
OME allows excluding a particular range from being discovered or rediscovered. To exclude a range from discovery task:

1. Click Manage → Discovery and Inventory → Add Exclude Range.
2. Right-click Add Exclude Range and select Add Exclude Range when prompted.
3. Click OK.
4. Type the IP address or IP range, discovery range name, or host name.
5. Click Add.
6. Click Finish.

Figure 14. Exclude Discovery Range screen
Skipping ICMP ping during discovery

In many organizations, ICMP protocol is disabled in the servers. Therefore, OME does not support ICMP ping by default during discovery and any other tasks. However, it is possible to disable this feature by doing the following:

- Click Settings → Discovery Settings.
- Clear the Skip ICMP ping during discovery check box.
- Click Apply.

Figure 15. Skip ICMP screen
Performing Discovery and Inventory using Standard Wizard

It is also possible to discover the devices using legacy standard wizard if required at any point. It is possible to use standard wizard during discovery by doing the following:

1. Click Settings → Discovery Settings.
2. Select the Standard Wizard – Choose protocols for use to discovery check box.
3. Click Apply.

Because the discovery is based on protocols and not based on device type, Device type filtering screen does not appear in the standard wizard.

Figure 16. Wizard selection screen

The discovery and inventory of devices using standard wizard can be summarized as follows:

- Discovery Range Configuration
- ICMP Configuration
- SNMP Configuration
- WMI Configuration
- Storage Configuration
- WS-Man Configuration
- SSH Configuration
- IPMI Configuration
- Discovery Range Action
- Summary
For more information about Discovery Configuration, ICMP, SNMP, WMI, WS-Man, SSH Configurations and Summary screen, see Steps for Performing Discovery and Inventory using Guided Wizard.

**Configuring Storage**

Set the options to discover PowerVault Modular drives or Dell EMC Devices. Any required credentials for the devices must be provided.

**Figure 17. Storage Configuration screen**
Configuring IPMI

Set the options to configure IPMI credentials for discovering DRAC or iDRAC devices.

Figure 18. IPMI Configuration screen

[Image of IPMI Configuration screen showing configuration options such as User Name, Password, KG key, Timeout, and Retries.]
**Discovery range action**

Select one of the following:

- Do not perform discovery or inventory
- Perform only discovery
- Perform both discovery and inventory

**Figure 19. Discovery Range Action Screen**
Discovery and Inventory Portal

The Discovery and Inventory Portal provides a single point of access to view the details of discovered or inventoried devices at any given point of time. To view the portal, click Manage → Discovery and Inventory → Discovery Ranges → All Ranges → preferred range. Using this screen, a System Administrator can monitor the progress of the Discovery Inventory process.

Figure 20. Discovery and Inventory Portal Page

The screen is divided into three sub-screens:

- **Discovery Ranges**: The range of IPs which is added.
- **Discovery Range Details**: A graphical representation of discovered and inventoried devices to visually separate the devices from the previously executed discovery and inventory task.
- **Discovery Range Configuration Details**: The details of discovery configuration range.
Device Tree

After the discovery and inventory process is completed, the System Administrator can view the detailed information of all the devices using the Device Tree screen.

To view the Device Tree, navigate to the Manage → Devices tab, and then select the All Devices node to view the devices classified under specific nodes as per the device category. The icon corresponding to each device represents the current health status.

This screen gives a glance of all the discovered and inventoried devices, the type of devices, and the health of each device (green-normal, yellow-warning, and red-critical).

Figure 21. Device Tree
Device Inventory Details

To view a detailed inventory of a particular device, select the device, and view the details in the working pane.

Figure 22. Device Details

The inventory details table displays all the details based on the discovery protocol used.

The following table shows all possible inventory headers captured and displayed by OME:

Figure 23. Inventory Details

<table>
<thead>
<tr>
<th>Device Summary</th>
<th>Physical Disk</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Information</td>
<td>Virtual Disk</td>
</tr>
<tr>
<td>Software Agent Information</td>
<td>Contact</td>
</tr>
<tr>
<td>NIC Information</td>
<td>Software Inventory</td>
</tr>
<tr>
<td>RAC information</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>iDRAC</td>
<td>FRU</td>
</tr>
<tr>
<td>Processor Information</td>
<td>Acquisition Information</td>
</tr>
<tr>
<td>Memory Device Info</td>
<td>Depreciation Information</td>
</tr>
<tr>
<td>Firmware Information</td>
<td>Extended Warranty</td>
</tr>
<tr>
<td>Power Supply</td>
<td>Ownership Information</td>
</tr>
<tr>
<td>Embedded Device</td>
<td>Outsource Information</td>
</tr>
<tr>
<td>Controller Device</td>
<td>Virtual Machine Guest Info.</td>
</tr>
<tr>
<td>Enclosure Information</td>
<td>Virtual Machine NIC Info.</td>
</tr>
</tbody>
</table>
Device Search

If there are many devices under the tree, managing them might be difficult. Searching manually for a particular device for monitoring can be a tedious process. To overcome this situation, OME includes a Device Search option.

1. Click **Manage → Device Search**.
2. Type a name for the new search query.
3. Select the required options from the **Where** drop-down menu.
4. Select any supporting sub-criteria.
5. Type a part of the device name.
6. Click **Run Query**.

   The result is displayed in the lower horizontal pane.

Figure 24. **Device Search Screen**

Learn More

For more information about other System Management software of Dell EMC, visit:

- [http://en.community.dell.com](http://en.community.dell.com)