Dell Management Plug-in for VMware vCenter: Discovery of Dell Bare-Metal Servers

This Dell technical white paper describes how to discover Dell PowerEdge 11th Generation or later bare metal servers into the Dell Management Plug-in for VMware vCenter for hypervisor deployment.

Michael Hepfer
Sangita Pandit
Umer Shabbir

Enterprise Product Group
This document is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

© 2012 Dell Inc. All rights reserved. Dell and its affiliates cannot be responsible for errors or omissions in typography or photography. Dell, the Dell logo, and PowerEdge are trademarks of Dell Inc. Intel and Xeon are registered trademarks of Intel Corporation in the U.S. and other countries. Microsoft, Windows, and Windows Server are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims proprietary interest in the marks and names of others.

May 2012 | Rev 1.0
Contents

Executive summary ........................................................................................................................................ 5
Introduction .................................................................................................................................................. 5
Prerequisites ................................................................................................................................................ 5
Manual discovery ..................................................................................................................................... 6
Auto-Discovery .......................................................................................................................................... 7
Process overview ..................................................................................................................................... 7
Prerequisites ................................................................................................................................................ 8
Provisioning service location .................................................................................................................... 8
Disabling administrative account access ................................................................................................... 9
  For Dell PowerEdge 11th Generation servers: ................................................................................... 9
  For Dell PowerEdge 12th Generation servers: ................................................................................. 9
Disabling accounts with the administrator role ......................................................................................... 11
Enabling Auto-Discovery ........................................................................................................................... 12
  Timeout limit ......................................................................................................................................... 12
  Manually configuring a PowerEdge 11th Generation server for Auto-Discovery .................... 12
Ordering Auto-Discovery enabled systems .............................................................................................. 13
Undiscovering or deleting bare-metal servers ............................................................................................ 14
Troubleshooting .......................................................................................................................................... 15
  The IDRAC trace log ............................................................................................................................. 15
Conclusion .................................................................................................................................................. 15
Appendix 1. - Configuring advanced security features ........................................................................... 16
  Adding service tags to the white list ..................................................................................................... 16
Certificates .................................................................................................................................................. 16
  Handshake client certificate ................................................................................................................... 17
  Private server certificate .......................................................................................................................... 17
Dell Management Plug-in for VMware vCenter: Discovery of Dell Bare-Metal Servers

Figures

Figure 1. Manual discovery. Deployment Wizard Add Server dialog ........................................ 6
Figure 2. iDRAC LAN user configuration screen ......................................................................... 9
Figure 3. 12th Generation Server, enabling Auto-Discovery ....................................................... 10
Figure 4. 12th Generation Server, disabling an account .............................................................. 11
Figure 5. Dell.com server configuration component selection, system options .......................... 13
Figure 6. Removing a discovered bare-metal server .................................................................... 14
Figure 7. Manually removing discovered servers .......................................................................... 14
Executive summary

The Dell Management Plug-in for VMware vCenter is a virtual appliance that streamlines tools and tasks associated with the management and deployment of Dell servers in your virtual environment. It reduces complexity by natively integrating the key management capabilities into the VMware vCenter console. It enables and speeds up bare metal provisioning from within vCenter and minimizes risk with hardware alarms, streamlined firmware updates, and provides deep visibility into inventory, health, and warranty details.

Discovery is the process of adding a Dell PowerEdge 11th or 12th Generation bare-metal server into a pool of available servers for use by the Dell Management Plug-in for VMware vCenter. Once a server is discovered, you can use it for hypervisor and hardware deployment. This white paper provides sufficient information about discovery to assist you in decision making for server purchasing, system configuration, and provides references to more detailed information on the specific topics covered.

Having a strong understanding of the features and requirements surrounding the purchasing, configuration, and the overall discovery process reduces time and effort in the administrative functions necessary to bring new servers online, and for achieving a successful implementation of security features important to your organization. An example of this would be leveraging the ordering system to use an Auto-Discovery SKU so servers can ship pre-configured to announce them once cabled.

Introduction

This white paper briefly discusses manually discovering servers into the Dell Management Plug-in for VMware vCenter, and discusses Auto-Discovery. The Auto-Discovery section outlines the requirements for adding servers to the Dell Management Plug-in, discusses the processes available to reduce administrative effort, and provides information about how to configure your environment for Auto-Discovery.

Prerequisites

Before attempting to discover Dell PowerEdge 11th or 12th Generation bare-metal servers, first follow the installation instructions for the Dell Plug-in for VMware vCenter. Only Dell PowerEdge 11th Generation or later servers with iDRAC express or iDRAC enterprise can be discovered into the Dell Management Plug-in for VMware vCenter’s pool of bare-metal servers. Network connectivity from the Dell bare-metal server’s iDRAC to the Dell Management Plug-in for VMware vCenter’s virtual machine is required.

NOTE: Hosts with existing hypervisors should not be discovered into the Dell Management Plug-in for VMware vCenter, instead they should be added to the vCenter, added to a connection profile, and then reconciled with the Dell Management Plug-in using the Host Compliance Wizard.
Dell Management Plug-in for VMware vCenter: Discovery of Dell Bare-Metal Servers

**Manual discovery**

The *Add Server* button in the *Select Servers* section of the Deployment Wizard provides a method of specifying a server’s iDRAC IP address and credentials. This manual discovery process is suitable for importing a small quantity of servers where configuration of the servers and environment for Auto-Discovery is not practical.

![Manual discovery. Deployment Wizard Add Server dialog](image-url)

**Figure 1. Manual discovery. Deployment Wizard Add Server dialog**
Auto-Discovery

Auto-Discovery is a Lifecycle Controller feature for setting up a new server and registering it using a console. The advantages of using this capability includes removing the need to do cumbersome manual local configuration of a new server and enabling an automated way for a console to discover a new server that was connected to the network and plugged into power.

Process overview

Auto-Discovery is sometimes referred to as Discovery and Handshake after the process it performs. When a new server with the Auto-Discovery feature enabled is plugged in to AC power and connected to the network, the Dell server’s Lifecycle Controller attempts to discover a deployment console that was integrated with the Dell Provisioning Server, and initiates a handshake between the provisioning server and the Lifecycle Controller.

The Dell Management Plug-in for VMware vCenter is a deployment console with an integrated provisioning server. The location of the provisioning server is provided to the iDRAC using different methods (See Provisioning server location). The IP address or host name for the provisioning server location is set to the IP address or host name of the Dell Management Plug-in for VMware vCenter appliance virtual machine.

NOTE: A new server configured for Auto-Discovery server makes an attempt to resolve the location of the provisioning server every 90 seconds over a period of 24 hours, after which you can manually re-initiate Auto-Discovery.

When iDRAC knows the location of the provisioning server, The Dell server’s Lifecycle Controller announces itself using a SOAP over HTTPS request to the Dell Management Plug-in for VMware vCenter. The iDRAC handshake client verifies that the certificate provided by the provisioning server during the initial SSL exchange is properly signed by the Dell certificate authority. When the Auto-Discovery request is received by the Dell Management Plug-in for VMware vCenter, it validates the SSL certificate and then initiates any optionally configured security procedures, such as client side security certificates and validation against a white list. A second validation request from the new server returns temporary username/password credentials to be configured on the iDRAC. Subsequent calls are initiated by the Dell Management Plug-in for VMware vCenter, which gathers information about the server, remove the temporary credentials, and configure more permanent user defined credentials for administrative access.

If Auto-Discovery was successful, the deployment credentials provided in the Settings->Deployment Credentials page at the time of discovery are created on the target iDRAC, and the Auto-Discovery feature is turned off. The server should now appear in the pool of available bare-metal servers under Deployment in the Dell Management Center.
Prerequisites

For Auto-Discovery to occur, several conditions must be met:

- **Power**: You must connect the server to the power outlet; however, the server does not need to be powered on.

- **Network connectivity**: The server’s iDRAC must have network connectivity and must communicate with the provisioning server over port 4433. You can obtain the IP address using a DHCP server or manually specified in the iDRAC Configuration Utility.

- **Additional network settings**: If using DHCP, enable the *Get DNS server address from DHCP* setting so that DNS name resolution can occur.

- **Provisioning service location**: The iDRAC needs to know the IP address or hostname of the provisioning service server. There are several ways you can accomplish this (See Provisioning service location).

- **Account access disabled**: You must enable the administrative account access to the iDRAC and if there are any iDRAC accounts with administrator privileges, you must first disable them from within the iDRAC Web console. Once Auto-Discovery completes successfully, the administrative iDRAC account is enabled.

- **Auto-Discovery enabled**: The server’s iDRAC must have Auto-Discovery enabled so that the Auto-Discovery process can begin.

Provisioning service location

There are several ways that the Provisioning Service Location is obtained by iDRAC during Auto-Discovery.

- **Manually specified in the iDRAC**: You can manually specify the location in the iDRAC Configuration Utility under LAN User Configuration, Provisioning Server.

- **DHCP Scope Option**: You can specify the location using a DHCP Scope Option.

- **DNS Service Record**: You can specify the location using a DNS Service Record.

- **DNS Known Name**: The DNS server specifies the IP address for a server with the known name DCIMCredentialServer.

If the provisioning service value is not manually specified in the iDRAC console, the iDRAC attempts to use the DHCP scope option value. If the DHCP Scope option is not present, it attempts to use the Service record value from DNS.

Disabling account access

You must disable administrative account access to the iDRAC and if there are any iDRAC accounts with administrator privileges, you must disable them first from within the iDRAC Web console. Note that the discovery process does not run if the admin accounts are enabled. Once Auto-Discovery completes successfully, the administrative iDRAC account is enabled.

Disabling administrative account access

For Dell PowerEdge 11th Generation servers:

1. Reboot the system and enter <CTRL-E> during the system boot when the “Press CTRL-E for Remote Access Setup within 5 seconds....” message appears to enter the iDRAC Configuration Utility.

2. Make sure the Auto-Discovery setting is enabled and the Account Access setting is disabled. The following screenshot depicts the iDRAC Configuration settings needed.

   ![iDRAC LAN user configuration screen](image)

   Figure 2. iDRAC LAN user configuration screen

For Dell PowerEdge 12th Generation servers:

1) Reboot the server and enter F2 to enter System Services.

2) Navigate to the iDRAC Settings -> Remote Enablement.

3) Click the Enabled option button for the Enable Auto Discovery item.

4) Enter the provisioning Server information as Dell Management Center Plug-in appliance IP.

5) Save the changes and exit the System services.
Figure 3. 12th Generation Server, enabling Auto-Discovery
Disabling accounts with the administrator role

Auto-Discovery does not run if the administrator accounts are enabled on the iDRAC. From the iDRAC Web console you can add additional administrator accounts. Any additional accounts you may have enabled must be disabled through the iDRAC Web console before Auto-Discovery can run.

On PowerEdge 12th Generation servers, you can disable the administrative accounts from the iDRAC Settings -> User configuration window. Clearing the option button for the Enable User for all administrative users disables the administrative accounts.

Figure 4. 12th Generation Server, disabling an account
Enabling Auto-Discovery

You can manually initiate Auto-Discovery using the iDRAC console on the server. You can enable Auto-Discovery automatically by ordering it shipped from factory in the enabled state, (See Ordering Auto-Discovery enabled systems), or you can initiated from a WSM-MAN command. For Auto-Discovery to run, all administrative accounts on the iDRAC must be disabled.

Timeout limit

When power is applied to the server and Auto-Discovery is properly enabled, the server attempts to contact the provisioning service until it successfully completes or until it has reached the timeout limit of 24 hours. If the provisioning server cannot contact the server within the timeout limit, you can manually re-initiate Auto-Discovery from the iDRAC Configuration Utility. When you attempt to use Auto-Discovery with a large number of servers, then you must first test the process with a single server or small sampling of servers to avoid having to manually re-initiate Auto-Discovery if the 24 hour timeout is reached.

Manually configuring a PowerEdge 11\textsuperscript{th} Generation server for Auto-Discovery

To manually configure a PowerEdge 11\textsuperscript{th} Generation server for Auto-Discovery, do the following:

1. Press $<\text{Ctrl}-e>$ when prompted within 5 seconds during system start-up.
2. In the iDRAC Configuration Utility page, enable NIC (for modular system only).
3. Enable DHCP.
4. Navigate to LAN Parameters.
5. Select Domain Name from DHCP.
7. Select DNS Server from DHCP.
8. Select On.
9. Navigate to LAN user configuration.
10. Select Account Access.
11. Select Disabled. This disables the default administrative account.
12. Select Auto-Discovery.
13. Select Enable to enable the Auto-Discovery feature
14. Save and Exit iDRAC6 Configuration Utility.
15. Restart your system.
Ordering Auto-Discovery enabled systems

When ordering servers for a large rollout, make sure you specify the Auto-Discovery SKU. You can order Dell servers with the Auto-Discovery feature enabled from the factory. This Auto-Discovery feature is not enabled by default. It is off unless it is explicitly requested when the server is ordered. If the Auto-Discovery is ordered, the machine comes with DHCP enabled on the iDRAC with all of its admin accounts disabled. Therefore, it is not necessary to configure a static IP address for the iDRAC; it gets one from a DHCP server on the network.

Figure 5. Dell.com server configuration component selection, system options
Undiscovering or deleting bare-metal servers
You can delete discovered bare-metal servers from the bare-metal servers list by clicking on the Remove Server button, shown below.

![Figure 6. Removing a discovered bare-metal server](image)

It opens another dialog box where you can select one or more servers to delete. After selecting the servers, click Remove Selected Servers to remove bare-metal servers permanently from the Dell Management Plug-in.

![Figure 7. Manually removing discovered servers](image)
Troubleshooting

The iDRAC trace log

You can obtain information about the Auto-Discovery process by examining the iDRAC trace log of the system that is attempting Auto-Discovery. Access this log in several ways, such as using the RACLOG or using the troubleshooting section of the iDRAC Web console, and invoking `racadm gettracelog` and look for messages with the source `idrac_discovery`. For more information about querying using the RACLOG or the troubleshooting section of the iDRAC Web console, see the *iDRAC6 User’s Guide*.

Conclusion

The Dell Management Plug-in for VMware vCenter has features that simplify the deployment of hypervisors to Dell PowerEdge 11th Generation and later bare-metal servers. You can manually add servers to the pool of bare-metal servers one at a time. The process can be automated for larger rollouts by ordering the servers pre-configured to arrive from the factory ready for Auto-Discovery.
Appendix 1. - Configuring advanced security features

Adding service tags to the white list

The white list is a list of service tags. If white list validation is turned on, only servers with matching service tags in the list are allowed to make the connection to the provisioning server. You can add the white list servers from the Dell Management Plug-in -> Dell Management Center -> Settings -> Security section. Select the Edit button on the Server White List page. You can add White list servers using the Add Server button or by importing the White List CSV file containing the list of service tags of server to be added to the white list.

1. To add the service tags using the Add Server button, click Add Server.

![Add Service Tags](image)

2. Enter up to five service tags of white list servers at a time and click Continue.

3. To add the service tags using the CSV file, click the Import White List button, and then enter the CSV file containing the service tags of white list servers.

4. To enable the white list, select the check box Enforce Server White List, and then click Apply.

Certificates

The Lifecycle Controller uses two certificates for establishing a mutually authenticated encrypted SSL connection between the Lifecycle Controller and the provisioning server.
Handshake client certificate

The iDRAC handshake client certificate is signed with a Dell certificate authority root certificate for which the public key is made available by Dell to console software partners that incorporate an Auto-Discovery Provisioning Server. It is generated during the factory build of the server and is unique to every system. The default hostname (Common Name) embedded in the handshake client certificate is the service tag of the server. The console software can optionally check that the certificate hostname (Common Name) provided matches the service tag provided in the initial handshake request payload.

You can also install a customized client certificate using WS-MAN. The DownloadClientCerts() method on the DCIM_LCService class is called to cause a custom signed Auto-Discovery client encryption certificate to generate. The method takes as input a Certificate Authority generated key certificate and related hash and password parameters. It uses the provided key certificate to sign a certificate containing the system service tag as the Certificate Name(CN). The method returns a job ID that is used to check the success of the download, generation, and installation of the Auto-Discovery client private certificate. For examples of command-line invocations using WinRM and WSMANCLI, see the Lifecycle Controller Web Services Interface Guide.

Private server certificate

A private certificate signed by the Dell certificate authority for the console software provisioning server is provided by Dell to console software partners. During the initial handshake connection, the iDRAC handshake client verifies that the certificate provided by the provisioning server during the initial SSL exchange is properly signed by the Dell certificate authority.

You can install a customized server certificate using WS-MAN. The DownloadServerPublicKey() method on the DCIM_LCService class is called to transfer a provisioning server public key certificate. The provisioning server public key is used as part of strict mutual authentication between the Auto-Discovery client and the provisioning server. The method takes as input a provisioning server public key certificate and related hash and hash type parameters. The method returns a job ID that checks the success of the processing and installation of the provisioning server public key. For examples of command-line invocations using WinRM and WSMANCLI, see the Lifecycle Controller Web Services Interface Guide. DCIM Profile specification and related MOF files are available at Dell TechCenter wiki in the DCIM Extension Library area (www.DellTechCenter.com).