Reinitiate Auto-discovery

Lee Ballard
Sylvia Tien
Reinitiate Auto-discovery
Reinitiate Auto-discovery

Contents
Introduction ......................................................................................................................... 4
Environment requirements .................................................................................................... 4
Auto-discovery reinitialize workflow .................................................................................. 4
Setting, updating, or deleting custom auto-discovery certificates .................................... 6
  Use custom certificates ..................................................................................................... 6
  Use default certificate ...................................................................................................... 8
Specifying the provisioning server ...................................................................................... 8
  Setting the provisioning server attribute ......................................................................... 9
Reinitializing auto discovery ................................................................................................ 10
Getting the provisioning server ......................................................................................... 10
Clearing the provisioning server ......................................................................................... 11
Reinitializing now or when the system is plugged in ........................................................... 11
Summary ........................................................................................................................... 12

Figures
Figure 1. Reinitialize auto-discovery network diagram ....................................................... 5
Figure 2. Reinitialize auto-discovery sequence diagram ...................................................... 6
Figure 3. Auto-discovery process flow .................................................................................. 9
Introduction

The auto-discovery feature of Lifecycle Controller allows newly installed servers to automatically discover the remote management console that hosts the provisioning server. This also has the effect of notifying the management console there is a new server in the network that needs to be provisioned.

The easiest way to implement this feature is to request that auto-discovery be enabled when you order your servers from Dell. Then, provided your console supports Lifecycle Controller auto-discovery (plugins are available for vCenter, SCCM, and others), the discovered server will automatically be added to the management console when the server is powered on. However, what if a server was not ordered from the factory with auto-discovery enabled, or you need to repurpose a machine to a different network or put it under the control of a different management station? This paper shows you how to remotely return a server to factory auto-discovery default settings, and discusses in detail the options which are available to you when reinitializing auto-discovery:

- Setting, updating or deleting custom auto discovery certificates
- Reinitializing now or when the system is plugged in
- Specifying the provisioning server

Environment requirements

For information on the requirements needed to support Auto-discovery, see Lifecycle Controller Auto Discovery Network Setup Specification on the Dell Enterprise Technology Center at www.delltechcenter.com/page/Lifecycle+Controller

Auto-discovery reinitialize workflow

Reinitializing auto-discovery involves resetting the iDRAC configuration to factory default settings for auto-discovery. Once the server is in this mode it will perform the exact same auto-discovery operation as would a factory-ordered server that had been set up with auto-discovery enabled.

Reinitializing auto-discovery is a two-step process. First the user must configure any custom certificates on the iDRAC or if the default certificate will be used, delete any custom certificates that might already be on the iDRAC. Then the user must send the reinitialize request, optionally specifying the new provisioning server and setting the run time either to “time now” or to the next boot of the iDRAC (remove and reapply power). The figure below shows the high level sequence.
Figure 1. Reinitialize auto-discovery network diagram
Reinitialize auto-discovery sequence diagram

Figure 2. Reinitialize auto-discovery sequence diagram

Setting, updating, or deleting custom auto-discovery certificates

Reinitializing auto-discovery will undo all iDRAC custom configuration settings, and set the iDRAC back to auto-discovery factory defaults with the exception of auto-discovery certificates used for handshake and provisioning server. If the new network/provisioning server uses custom certificates, those must be set on the server before auto-discovery is reinitialized. If the new network/provisioning server uses default certificates, any custom certificates should be deleted.

Use custom certificates

Install provisioning server's CA certificate

The following WSMAN method sets the CA certificate on the iDRAC that it uses to validate the provisioning server. This must be the same CA that signed the provisioning server's certificate.

EXAMPLE:
Reinitiate Auto-discovery

```bash
winrm i DownloadServerPublicKey http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_LCService
?CreationClassName=DCIM_LCService
+Name=DCIM:LCService
+SystemCreationClassName=DCIM_ComputerSystem
+SystemName=DCIM:ComputerSystem
-u:[USER] -p:[PASSWORD]
-r:https://[IPADDRESS]/wsman:443
-SkipCNCheck -SkipCACheck -encoding:utf-8
-a:basic -file:DownloadServerPublicKey.xml
```

The input file `DownloadServerPublicKey.xml` is shown below:

```xml
  <p:KeyContent>
    -----BEGIN CERTIFICATE-----
    MIIEQjCCA6ugAwIBAgIBADANBgkqhkiG9w0BAQQFADCBzTELMAkGA1UEBhMCVVMx
    CzAJBgNVBAgTAlRYMRQwEgYDVQQH
    EwtNYWluIFN0cmVldEVz
    .
    qvoMCKtoqLnGBByj/H2vyN7Fe/zMKXD5pO6XwYydGfA66w3HGUAR0+fIKD40NDi9
    bKFEMxbRx2ysUuukZ9c+RA1Uilrjz3mfX3fn1Yp7k05KU9vHY=
    -----END CERTIFICATE-----
  </p:KeyContent>
</p:DownloadServerPublicKey_INPUT>

Installing client CA certificate and CA private key

The following WSMAN method will generate a new key pair on the iDRAC and then sign it using the provided CA certificate and CA private key.

```bash
EXAMPLE:

winrm i DownloadClientCerts http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_LCService
?CreationClassName=DCIM_LCService
+Name=DCIM:LCService
+SystemCreationClassName=DCIM_ComputerSystem
+SystemName=DCIM:ComputerSystem
-u:[USER] -p:[PASSWORD]
-r:https://[IPADDRESS]/wsman:443 -SkipCNCheck -SkipCACheck
-encoding:utf-8 -a:basic -file:DownloadClientCerts.xml
```

The input file `DownloadClientCerts.xml` is shown below:

```xml
  <p:KeyContent>
    -----BEGIN RSA PRIVATE KEY-----
    Proc-Type: 4,ENCRYPTED
    DEK-Info: DES-EDE3-CBC,5FD6D6131DFA5A86
    u1G9hRgOlkoJ3jXMB895ZL18H5KvZkNUMnqyHQIqNco9WtKyINR1FbcI1AU9ToUJOM
    SnuS1A8fRBtJXZZVBA+KAt+341vO/FEAijSOzKMWN1wA+CUuzCFM7t3P+3kmD+o6a
    .
    -----END RSA PRIVATE KEY-----
  </p:KeyContent>
</p:DownloadClientCerts_INPUT>
```
Reinitiate Auto-discovery

Use default certificate

Deleting custom auto-discovery keys
The following WSMAN methods will delete any custom auto-discovery keys that may exist on the iDRAC. Once the custom keys are deleted, the iDRAC will return to using factory signed keys.

EXAMPLES:

```bash
winrm i DeleteAutoDiscoveryServerPublicKey
http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_LCService
?SystemCreationClassName=DCIM_ComputerSystem
+CreationClassName=DCIM_LCService
+SystemName=DCIM:ComputerSystem
+Name=DCIM:LCService
-u:%USERNAME% -p:%PASSWORD%
-r:https://%IPADDRESS%/wsman
-encoding:utf-8 -a:basic -SkipCACheck -SkipCNCheck -skiprevocationcheck
```

```bash
winrm i DeleteAutoDiscoveryClientCerts
http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_LCService
?SystemCreationClassName=DCIM_ComputerSystem
+CreationClassName=DCIM_LCService
+SystemName=DCIM:ComputerSystem
+Name=DCIM:LCService
-u:%USERNAME% -p:%PASSWORD%
-r:https://%IPADDRESS%/wsman
-encoding:utf-8 -a:basic -SkipCACheck -SkipCNCheck -skiprevocationcheck
```

Specifying the provisioning server

There are two steps in auto-discovery (see Figure 2). In the first step the iDRAC discovers the provisioning server. In the second step the provisioning server learns there is a new server that needs to be configured, the iDRAC receives its initial credentials, and the secure SSL handshake takes place.
Reinitiate Auto-discovery

The iDRAC discovers the provisioning server in one of three ways: DHCP vendor options, DNS SRV lookup, or default DNS entry. There is also a fourth option—manually configuring the provisioning server. Configuring the provisioning server address in the reinitialize request will bypass the discovery step, and the iDRAC will proceed directly to handshake. Setting the provisioning server is very useful if there are multiple provisioning servers in the network and the user wants to move a server from the control of one provisioning server to another. It can also be used in situation where the user does not have control of the DHCP or DNS services.

Figure 3. Auto-discovery process flow

There are two ways to set the provisioning server: setting the provisioning server attribute, or reinitiating auto-discovery. You may choose either one to set the value of the provisioning server.

Setting the provisioning server attribute

The following WSMAN command will set the IP address or host name of the provisioning server on the iDRAC.

EXAMPLE:

```
winrm i SetAttribute cimv2/root/dcim/DCIM_LCService
```
Reinitiate Auto-discovery

?SystemCreationClassName=DCIM_ComputerSystem
+CreationClassName=DCIM_LCService
+SystemName=DCIM:ComputerSystem+Name=DCIM:LCService
-u:[USERNAME] -p:[PASSWORD] -r:https://[IPADDRESS]/wsman
-encoding:utf-8 -a:basic -file:SetAttribute.xml

The input file SetAttribute.xml containing the parameters for the SetAttribute method is shown below:

```xml
</p:SetAttribute_INPUT>
```

Reinitiating auto discovery

You may choose to set the provisioning server during reinitiating auto-discovery. Use the following WSMAN command to reinitialize auto-discovery.

EXAMPLE:

```cmd
winrm i ReInitiateDHS cimv2/root/dcim/DCIM_LCService
?SystemCreationClassName=DCIM_ComputerSystem
+CreationClassName=DCIM_LCService
+SystemName=DCIM:ComputerSystem+Name=DCIM:LCService
-u:[USERNAME] -p:[PASSWORD] -r:https://[IPADDRESS]/wsman
-encoding:utf-8 -a:basic -file:ReInitiateDHS.xml
```

The input file ReInitiateDHS.xml containing the parameters for the ReInitiateDHS method is shown below:

```xml
<p:ReInitiateDHS_INPUT xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_LCService">
  <p:ResetToFactoryDefaults>TRUE</p:ResetToFactoryDefaults>
  <p:PerformAutoDiscovery>3</p:PerformAutoDiscovery>
</p:ReInitiateDHS_INPUT>
```

The PerformAutoDiscovery attribute can have the following values:

1 = off (disables auto discovery)
2 = Now (enables and initiates auto discovery immediately)
3 = NextBoot (delay reconfiguration & auto discovery until next power cycle)

Getting the provisioning server

The following WSMAN command will display the provisioning server on the iDRAC.

EXAMPLES:
Reinitiate Auto-discovery

```
winrm g "http://schemas.dell.com/wbem/wscim/1/cim-schema/2/DCIM_LCSString?InstanceID=LifecycleController.Embedded.1#LCAttributes.1#ProvisioningServer+__cimnamespace=root/dcim"
-u:[USERNAME] -p:[PASSWORD] -r:https://[IPADDRESS]/wsman
-encoding:utf-8 -a:basic -SkipCNcheck -SkipCAcheck
```

Clearing the provisioning server

The following WSMAN command will clear the provisioning server on the iDRAC.

```
winrm i ClearProvisioningServer cimv2/root/dcim/DCIM_LCService
?SystemCreationClassName=DCIM_ComputerSystem
+CreationClassName=DCIM_LCService
+SystemName=DCIM:ComputerSystem+Name=DCIM:LCService
-u:[USERNAME] -p:[PASSWORD] -r:https://[IPADDRESS]/wsman
-encoding:utf-8 -a:basic
```

Reinitializing now or when the system is plugged in

The last thing to consider when reinitializing auto-discovery is when will the operation occur? If the system is being reallocated to a different provisioning server on the same network, time now would be appropriate. If the system will be unplugged, moved and powered on in a different location, selecting next boot (meaning next iDRAC boot, not server boot) would be the best option. Be aware that if you select time now the reinitialize process will begin immediately. This means all login credentials on the iDRAC will be disabled until auto discovery completes, so no remote access (ssh, web, wsman, or remote RACADM) will be possible until auto-discovery is complete. If you are moving a server from one provisioning server to another and you use time now, you should either specify the new provisioning server to the iDRAC, or tell the old provisioning server to ignore credential requests from the service tag associated with the server to prevent it from discovering the old provisioning server and then disabling auto discovery. If auto discovery is not working, the reason for the failure can be determined on the server LCD menu under View->iDRAC IP->Auto Discovery. If the 24-hour timeout has occurred, removing and reapplying power will restart the auto-discovery process. If you want to abort the auto-discovery process and regain remote access to the iDRAC, reboot the server and press <Ctrl-E> (or Press F2 on a 12G server) after the BIOS splash screen to configure the iDRAC and set the admin user name and password.

You may choose to set the provisioning server when reinitiating auto-discovery. Use the following WSMAN command to reinitiate auto-discovery.

**EXAMPLE:**

```
winrm i ReInitiateDHS cimv2/root/dcim/DCIM_LCService
?SystemCreationClassName=DCIM_ComputerSystem
+CreationClassName=DCIM_LCService
+SystemName=DCIM:ComputerSystem+Name=DCIM:LCService
-u:[USERNAME] -p:[PASSWORD] -r:https://[IPADDRESS]/wsman
-encoding:utf-8 -a:basic -file:ReInitiateDHS.xml
```
The input file `ReInitiateDHS.xml` containing the parameters for the `ReInitiateDHS` method is shown below:

```xml
<p:ReInitiateDHS_INPUT xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_LCService">
  <p:ResetToFactoryDefaults>TRUE</p:ResetToFactoryDefaults>
  <p:PerformAutoDiscovery>3</p:PerformAutoDiscovery>
</p:ReInitiateDHS_INPUT>
```

The `PerformAutoDiscovery` attribute can have the following values:

1 = off (disables auto discovery)
2 = Now (enables and initiates auto discovery immediately)
3 = NextBoot (delay reconfiguration & auto discovery until next power cycle)

**Summary**

This whitepaper has provided an overview of the auto-discovery reinitialize process and demonstrated how it can be used to reinitiate or repurpose a Dell Power Edge Server. For more information please refer to the following documents on the Dell Tech Center website and other Dell websites:

- Lifecycle Controller 1.5 Web Services Interface Guide for Windows
- Lifecycle Controller 1.5 Web Services Interface Guide for Linux
- Dell Auto-Discovery Network Setup Specification
- What is a White Paper?