Dell® Auto-Discovery Network Setup Specification

Document Number: DCIM2003
Document Type: Specification
Document Status: Published
Document Language: E
Date: 2012-09-05

Version: 2.0.0

THIS SPECIFICATION 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. ABSENT A SEPARATE AGREEMENT BETWEEN YOU AND DELL™ WITH REGARD TO FEEDBACK TO DELL ON THIS SPECIFICATION, YOU AGREE ANY FEEDBACK YOU PROVIDE TO DELL REGARDING THIS SPECIFICATION WILL BE OWNED AND CAN BE FREELY USED BY DELL.

Table of Contents

Table of Figures

Auto-Discovery Network Setup Specification

1 Purpose

The Dell Auto-Discovery Network Setup Specification (DCIM2003) was prepared by Dell Enterprise Product Group Engineering. The Auto-Discovery feature enables the remote provisioning of servers out-of-the-box without the need for an individual setup of every server. The information in this specification is sufficient for a server administrator to prepare the network infrastructure for automated discovery and remote configuration. Specifically, this document describes a set of procedures that can be used for the Integrated Dell Remote Access Controller (iDRAC) service processor in the Dell server to receive an IP address of a trusted provisioning server. This IP address is used to establish communication to receive a username and password for subsequent configurations using WS-Management Web Services protocol (WS-Man) or iDRAC RACADM command line utility from a remote console. Therefore, the end goal of this set of procedures is the acquisition (discovery) of an IP address by the iDRAC service processor of a management console that is hosting a provisioning server.

2 Scope

The procedures described in this document detail what occurs after the power and Ethernet cables are attached to the server until the time that a management console provisioning server IP address is discovered by the server service processor (iDRAC). The document does not cover the details of remote configuration, since it occurs after the discovery phase using WS-Man or the remote RACADM command-line utility for the iDRAC, for information on these topics consult the *iDRAC Web Services Interface Guide* or the iDRAC RACADM Users Guide. An alternative to Auto-Discovery is to set up a static IP address and user credentials at the server for every machine in the installation. The advantage this set of procedures provides is the ability to set up a specified remote provisioning user account *without* being present at *every* server. Using this procedure provides the added benefit of populating the management console inventory systems with service tags and iDRAC IP address of new servers that are ready to be provisioned as they are initially connected to the management network and plugged into AC power, although this is not the topic of this paper. This document specifies the first step: the discovery of a management console provisioning server IP address by a newly installed and powered Dell server.

3 Audience

The target audiences for this specification are the following groups:

1. Server administrators responsible for Dell server installations
2. Network administrators servicing Dell server installations

This is required information for the implementation of Auto-Discovery installations, as it describes the DHCP and DNS servers configuration requirements on either the management network or the network connected to the iDRAC service processor.

4 References

RFC 2782, *A DNS RR for specifying the location of services (DNS SRV)*

RFC 2131, *Dynamic Host Configuration Protocol*

RFC 1035, *Domain Names – Implementation and Specification*

RFC 2132*, DHCP Options and BOOTP Vendor Extensions*

5 Acronyms

CA – Certificate Authority

CN – Common Name

iDRAC – Integrated Dell Remote Access Controller

WS-Man – or WS-Management – Web Services for Management (DMTF Standard)

DMTF – Distributed Management Task Force, Inc.

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name Service

SOAP – Simple Object Access Protocol

SSL – Secure Sockets Layer

TLS – Transport Layer Security (successor to SSL)

6 Overview

6.1 Recent Enhancements to Auto-Discovery

The following enhancements have been made to Auto-Dicovery since its initial release:

- Manually setting the provisioning server addresses in the iDRAC Configuration Utility.
- WSMAN method to put a server back in factory default Auto-Discovery state (this is covered in the *Re-Initiate Auto-Discovery* whitepaper).
- Customer provided certificates can be used for both signing the iDRAC and authenticating the provisioning server.
- The status of Auto-Discovery can now be monitored on the server LCD.
- After Auto-Discovery is complete the provisioning server can request to be notified if the IP address of the iDRAC changes.

6.2 Supported Provisioing Servers

The following is a sample of some of the provisioning servers that support Auto-Discovery:

- Dell Lifecycle Controller Integration (DLCI) – http://en.community.dell.com/techcenter/os-applications/w/wiki/dell-lifecycle-controller-integration-for-configuration-manager.aspx
- Dell provided VCenter plugin - http://en.community.dell.com/techcenter/systems-management/w/wiki/1961.dell-management-plug-in-for-vmware-vcenter.aspx
- Dell Management Console (DMC) - http://en.community.dell.com/techcenter/systems-management/w/wiki/dell-management-console.aspx
- Several Others – contact your management console provider

6.3 Auto Discovery Workflow

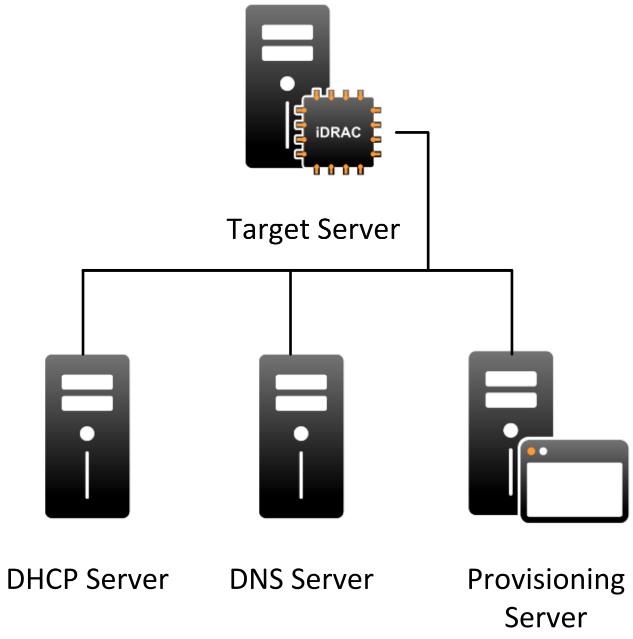


Figure 1 - Auto Discovery Network Diagram

6.4 Basic Setup

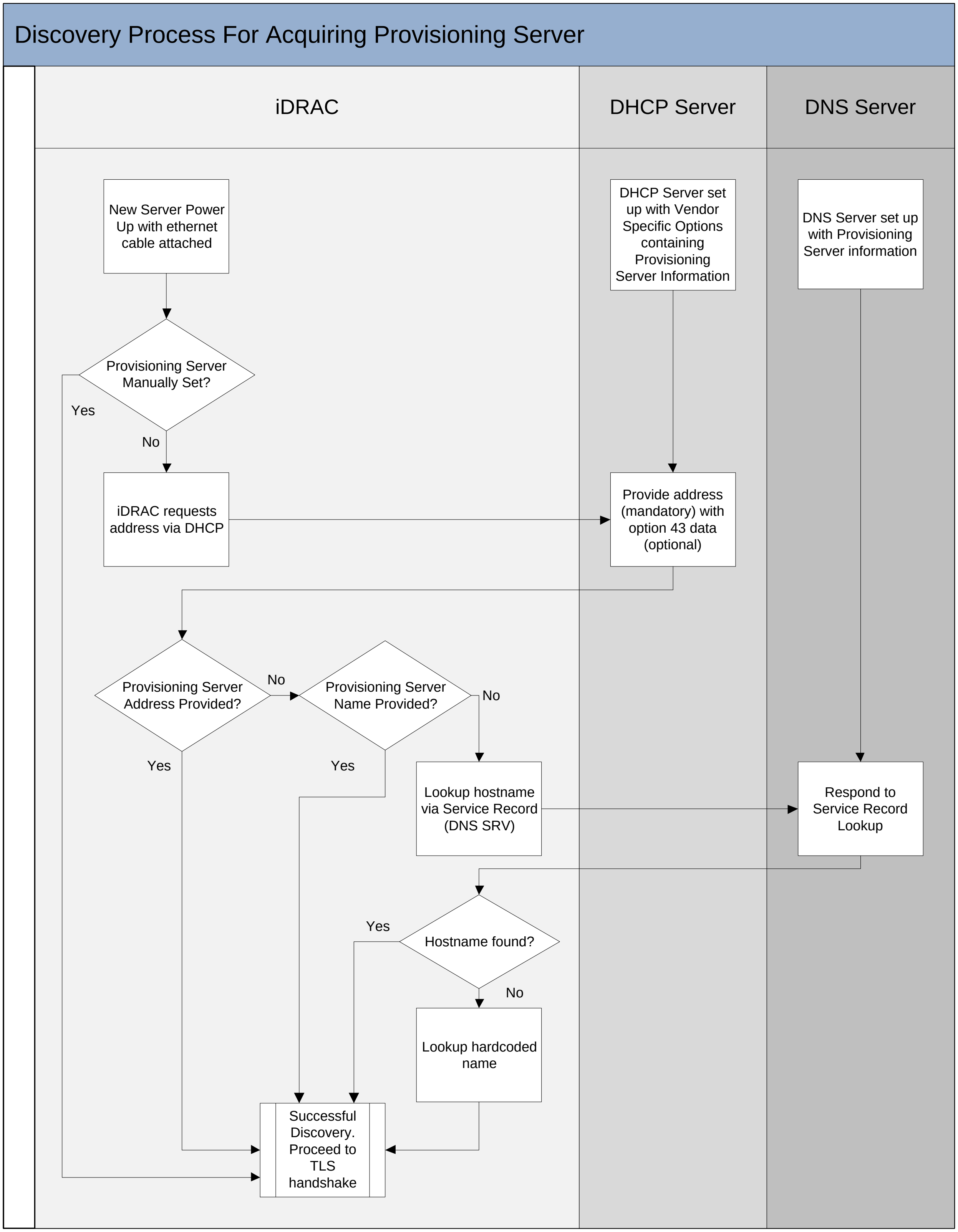
The discovery of a management console (with an Auto-Discovery provisioning server) by a newly installed server consists of several alternatives. One of the following must be implemented for this feature to work:

- Provisioning server address must manually be set in iDRAC settings.
- The DHCP server must specify a list of comma separated provisioning server addresses (and optionally ports) of the management console(s)[1] in a vendor specific option (option 43) data in response to the DHCP REQUEST sent out by iDRAC. This can be a full qualified domain name, hostname or IP.
- The DNS server must specify a service option *_dcimprovsrv* that specifies the hostnames and ports that resolves to IP addresses.
- The DNS server must specify an IP address for a server with the following known name: *DCIMCredentialServer*.

[1] NOTE: The IP address specified is the location of a service that will respond to an SSL connection setup, and provide server WS-Man login credentials; it is intended that the remote management console with an Auto-Discovery provisioning server performs this duty. However, it is possible that a completely independent service on a different machine could fill this role.

When a Dell® PowerEdge server is ordered with the Auto-Discovery option enabled, the iDRAC will come from the factory with DHCP enabled and no default credentials for a remote login. Following the acquisition of an provisioning server address for the management console \with one of the above alternatives, the iDRAC uses the discovered address to initiate a TLS connection (the handshake) that receives a new username and password. The receipt of this username and password is the end goal of the discovery and handshake process. These credentials are used by the remote console for subsequent configuration using WS-Man or remote RACADM. **Figure 2** illustrates the provisioning server address discovery process that iDRAC uses to acquire the provisioning server address prior to attempting to setup an TLS handshake with the provisioning server.

242


Discovery Process For Acquiring Provisioning Server
iDRAC
DHCP Server
DNS Server
New Server Power Up with ethernet cable attached
DHCP Server set up with Vendor Specific Options containing Provisioning Server Information
DNS Server set up with Provisioning Server information
Provisioning Server Manually Set?
Yes
No
iDRAC requests address via DHCP
Provide address (mandatory) with option 43 data (optional)
Provisioning Server Address Provided?
No
Provisioning Server Name Provided?
No
Yes
Yes
Lookup hostname via Service Record (DNS SRV)
Respond to Service Record Lookup
Yes
Hostname found?
No
Lookup hardcoded name
Successful Discovery. Proceed to TLS handshake

243

244 **Figure 2 - Discovery Process For Aquiring Provisioning Server**

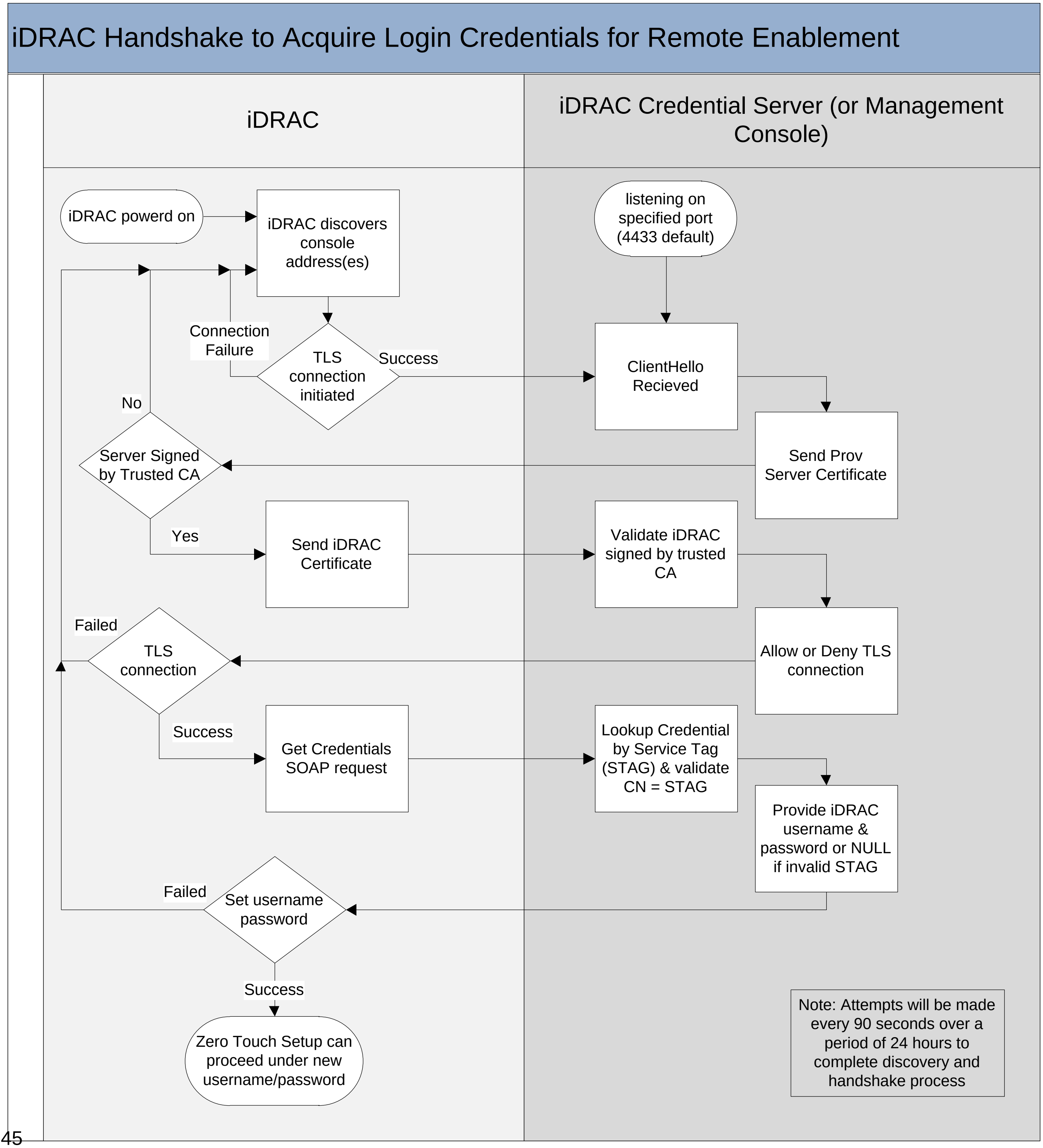

iDRAC Handshake to Acquire Login Credentials for Remote Enablement
iDRAC
iDRAC Credential Server (or Management Console)
iDRAC powerd on
iDRAC discovers console address(es)
TLS connection initiated
Connection Failure
Success
listening on specified port (4433 default)
ClientHello Recieved
Send Prov Server Certificate
No
Server Signed by Trusted CA
Yes
Send iDRAC Certificate
Validate iDRAC signed by trusted CA
Allow or Deny TLS connection
Failed
TLS connection
Success
Get Credentials SOAP request
Lookup Credential by Service Tag (STAG) & validate CN = STAG
Provide iDRAC username & password or NULL if invalid STAG
Failed
Set username password
Success
Zero Touch Setup can proceed under new username/password
Note: Attempts will be made every 90 seconds over a period of 24 hours to complete discovery and handshake process

Figure 3 - iDRAC Handshake to Acquire Login Credentials for Remote Enablement

7 Auto-Discovery Implementation Alternatives

If more than one discovery method is used simultaneously, the provisioning server address acquisition sequence is the following:

1. Provisioning Server Set in iDRAC settings
2. DHCP Vendor Scope Option
3. DNS SRV record
4. Default Host A record

7.1 Manually Setting the Provisioning Server

This is not zero touch but if DHCP and DNS services are not available, or if there is a desire to skip the discovery process, the iDRAC can have the provisioning server set manually. This can be done in either the iDRAC settings page (Cntrl E on 11th generation servers and F2 on 12th generation servers) or the System Services/Lifecycle Controller Page (F10) during boot. For more information on manually setting the provisioning server see Checking iDRAC Configuration Settings (11th generation servers)

7.2 Provide Provisioning Server information within DHCP scope options

To enable the Auto-Discovery feature, the default iDRAC NIC setting out of the box is required to be DHCP rather than statically assigned IP address. The iDRAC sets a vendor class identifier (option 60) in the DHCPREQUEST message to *LifecycleController*. This enables DHCP servers to optionally respond uniquely to the iDRAC.

There are three possible valid responses and outcomes to the DHCPREQUEST sent by the iDRAC:

- The request times out and an IP address is unobtainable. The iDRAC retains its DHCP setting indefinitely with no login credentials. To change this setting, you would have to be physically present at the server. [2]

- The DHCP server responds, but does not provide any option 43 data. In this case the iDRAC attempts to locate a server using DNS (see Figure 2).

- Option 43 data is present and includes an IP address and or hostname to use for the handshake. The data will have a format that can easily be set up on a Windows or Linux DHCP server. The sub option number for option 43 is “1” (see RFC2132) and has this format:

  (FQDN | Hostname | IP Address)[:port] [, (FQDN | Hostname | IP Address)[:port]] [, …]

  NOTE: If the iDRAC is using a custom trusted CA to validate the provisioning provisioning server, the value of sub option 1 for that provisioning server must match the CN value in the provisioning server certificate or the TLS connection will fail. For example if the CN=provserv1.dell.com the sub option 1 value must also be provserv1.dell.com

  Where either the hostname or the ipaddress are provided, followed optionally by a port number. Examples of string values are as follows (no spaces allowed) :

  - **Provisioning.dell.com:4433** (resolve using DNS, TCP port specified.)

[2] The iDRAC Configuration Utility using ctrl-E during boot up provides an opportunity for a static IP address and user credentials to be specified. Also, local RACADM commands can be used.

- **192.168.0.125:4433** (server IP address specified for DHCP with TCP port specified.)
- **192.168.0.126** (use specified server IP address, host name is ignored, no port specified, default TCP port will be used.)
- **Provisioning,Provisioning2:4433,Provisioning3** (resolve using DNS for all, 2nd server has TCP port specified.)
- **192.168.0.120,Provisioning2** (specified address resolved by DNS both with no TCP port specified)

The data returned by the DHCP server can be keyed off the vendor class identifier provided by iDRAC (*LifecycleController)*.

7.2.1 Linux DHCP Server Configuration

A dhcpd.conf file snippet for a Linux server, where the example hostname:port = “provisioning.dell.com:2800”, would look like this:

```
option space DELL;
option DELL.provsvr code 1 = string;
class “LifecycleController” {
                match if option vendor-class-identifier = “LifecycleController”;
                vendor-option-space DELL;
                option DELL.provsvr “provisioning.dell.com:2800”;
}
```

Figure 4 – Linux DHCP Server Configuration

7.2.2 Windows DHCP Server Configuration

The following figure illustrates an example DHCP Server configuration where the provisioning server is set to “provisioning.dell.com:2800”.

Windows Server 2003 Microsoft DHCP Version: 5.2.3790.3959 Configuration

1. Select the server name on left tree.
2. Click **Action->Define Vendor Classes:**
   a. Click **Add.**
   b. Display Name : LifecycleController
   c. Under ASCII: LifecycleController
   d. Click **OK.**
   e. Click **Close.**
3. Click **Action->Set Predefined Options:**
   a. Select **LifecycleController** in Option class dropdown.
   b. Click on **Add** for the following items:
      - Name : LifecycleController
      - Data type : String
      - Code : 1
      - Click **OK**
   c. Click on OK
4. Expand server tree and scope.
5. Select **Scope Options** on left tree.
6. Click **Action->Configure** Options:
   a. Click **Advanced** tab.
   b. Select **LifecycleController** in Vendor class dropdown.
   c. Under **Available Options**, check 001 LifecycleController.
   d. Under String value, enter provisioning server string: for example, **provisioning.dell.com:2800**

7.3 DNS SRV

Alternatively, if the DHCP scope option discovery methodology is not desired, the iDRAC can recognize a DNS service record that specifies a list of both the hostname and port. The iDRAC will lookup the _DCIMProvSrv record to determine the hostnames and ports of the Provisioning Servers. See the reference RFC 2782, *A DNS RR for specifying the location of services (DNS SRV)* for relevant specifications.

7.3.1 Linux DNS SRV Configuration

The following is an example of a DNS server configuration file entry in Linux (/etc/bind/pri/<primary.zone>):

Linux DNS SRV Configuration Example

```
_DCIMProvSrv._tcp.example.com 86400 IN SRV 1 100 4433 DellProvisioningServer1
_DCIMProvSrv._tcp.example.com 86400 IN SRV 2 100 4433 DellProvisioningServer2
```

Figure 6 **– Linux DNS SRV Configuration**

7.3.2 Windows DNS SRV Configuration

The following steps set up a service record on a Windows Server 2003 DNS Server Version:5.2.3790.3959 using the DNS snap-in to administer a DNS server:

Windows Server 2003 DNS Server Version:5.2.3790.3959 Configuration

1) Under **Server** expand the forward lookup zone.
2) Select the zone listed under the zone.
3) Go to **Actions** (or right click).
4) Select **Other new records**.
5) For **Select a resource record type:,** select a service location (SRV).
6) Click on **create record.**
7) Enter the Domain information (tcp.dell.com).
8) Service type, enter **_dcimprovsrv**.
9) For the protocol, leave the default of **_tcp**
10) Enter a priority value where the lower the number the higher the priority; enter **1**.
11) Enter the weight value; if this record should be used more than another enter **90.**
12) Enter a port number; the default is **4433.** To use a different port number, enter it here. To use another port, it would have to be configured on the provisioning server as well.
13) Enter the host offering this service; enter **provisioningserver**.

Figure 7 **- Windows DNS SRV Configuration**

7.4 DNS server resolution of hardcoded name DCIMCredentialServer

If the name (Host A record) DCIMCredentialServer is entered into the DNS tables, the iDRAC requests and recognize this name. This method of discovery will be iteratively attempted, along with the other provisioning server IP address discovery methodologies, every 90 seconds for 24 hours (see note in Figure 3 - iDRAC Handshake to Acquire Login Credentials for Remote Enablement) before timing out.

Note: The DCIMCredentialServer name is the last option used to locate a provisioning server. If the DHCP scope or DNS SRV records resolve then the DCIMCredentialServer will not be used.

8 Security

After the iDRAC determines the address of the Provisioning Service, it is ready to perform the handshake step in the Auto-Discovery process (see Figure 3 - iDRAC Handshake to Acquire Login Credentials for Remote Enablement). It will make a Web service call using SOAP (simple object access protocol) to the Provisioning Service. This call is made over a secure connection using TLS (Transport Layer Security). By using TLS, it is possible for the deployment console Provisioning Service to authenticate the iDRAC, and for the iDRAC to authenticate the Provisioning Service.

Following the successful TLS connection, a web service call is made from the Provisioning Service to the deployment console where the input parameter is the server service tag and the output parameters, returned to the iDRAC by the Provisioning Service, are an iDRAC admin username and password credentials. These iDRAC admin credentials are used for subsequent remote access and configuration using WS-Man Web service requests or remote IPMI, CLI, and iDRAC GUI interfaces. The deployment console can optionally check the service tag against a pre-approved list of service tags that are authorized to be provisioned. At this point in the process, the deployment console knows which service tags have come online.

Two certificates are used for the mutually authenticated encrypted TLS (Transport Layer Security) connection between the Lifecycle Controller and the Provisioning Service. The iDRAC handshake client encryption 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 Service. The handshake client encryption certificate 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 encryption certificate will be the service tag of the server.

A DellProvisioningServer certificate signed by *Dell Lifecycle Controller Provisioning Server Root CA* and private key is provided by Dell to console software partners. During the initial handshake connection, the iDRAC will verify that the certificate provided by the Provisioning Server is properly signed.

8.1 Authentication Options

Auto-Discovery uses full TLS mutual authentication. This means that the iDRAC must authenticate the provisioning server and the server must authenticate the iDRAC before any information is exchanged.

8.1.1 Dell Provisioning default server certificate

When Auto-Discovery is enabled with no additional configuration the iDRAC authenticates the provisioning server with the Dell Provisioning Server CA cert. In this mode, the iDRAC can not validate the CN of the provisioning server certificate against the hostname of the machine.

8.1.2 Dell iDRAC default CA

When Auto-discovery is enabled with no additional configuration the provisioning server authenticates the iDRAC using the default iDRAC CA cert and the service tag of iDRAC. Each iDRAC has a client certificate based on its service tag which is created in the factory. If the service tag of the machine does not match the certificate it will not authenticate. Additionally the provisioning server checks the service tag against a list of configured service tags before creating an admin account on the iDRAC.

8.1.3 Customer provided server CA certificate

A customer may optionally provide a provisioning server CA. If a provisioning server CA is provided, only servers with credentials signed by this CA are allowed by the iDRAC for the purposes of Auto-Discovery. The iDRAC addionally validates the CN of the server certificate against the hostname used to make the TLS connection.

8.1.4 Customer provided iDRAC CA

A customer may optionally provide an iDRAC CA certificate. If an iDRAC CA is provided, only iDRACs with credentials signed by this CA are allowed by provisioning server purposes of Auto-Discovery. See the *Web Services Interface Guide* for details on how to sign an iDRAC Auto-Discovery client certificate.

8.2 Factory Options

You can order Dell Servers with Auto-Discovery enabled out of the factory. When Auto-Discovery is enabled the default iDRAC admin account is disabled.

8.3 Provisioning Service Options

After TLS authentication, it is the provisioning servers responsibility to create an account on the iDRAC that can be used to perform future configuration. The provisioning server only creates an account if the server service tag matches its list of service tags to provision. Note that the account that the provisioning server creates can be unique for each server, and that this account can be deleted or disabled once Active Directory or LDAP is configured.

8.4 Auto-Discovery Re-Init

If a server is being moved to another provisioning service, then the user can use the current credentials to load new certificates (the iDRAC certificate and the provisioning server CA cert mentioned in the Authentication section). For more information refer to the *Re-Initiate Auto-Discovery Whitepaper (unreleased)*.

8.5 If Auto-Discovery fails

Auto-Discovery automatically retries up to 24 hours. After 24 hours if the issue is network related then power-cycling the server restarts Auto-Discovery and it should complete. If the problem is related to the TLS certificate, then you need to go into the BIOS and enable an admin account. Once this account is enabled, you can manually add the server to the provisioning service or you can add new certificates on the iDRAC using the Re-Initiate Auto-Discovery procedures detailed in the user guide.

8.6 Best Practices

It is recommended that the provisioning server validate the service tag sent in every request against the CN of the iDRAC certificate. Additionally the service tag should be validated against your inventory. The provisioning server should generate unique temporary credentials for each iDRAC and use them only long enough to setup a directory method of authentication. After that those credentials should be disabled and deleted. If customer provided certificates are used the certificates should be removed using LCWipe if the system is decommissioned or sold. After provisioning is complete the provisioning server can set a static IP on the iDRAC or enable IPChange notifications to make sure it always has management connectivity.

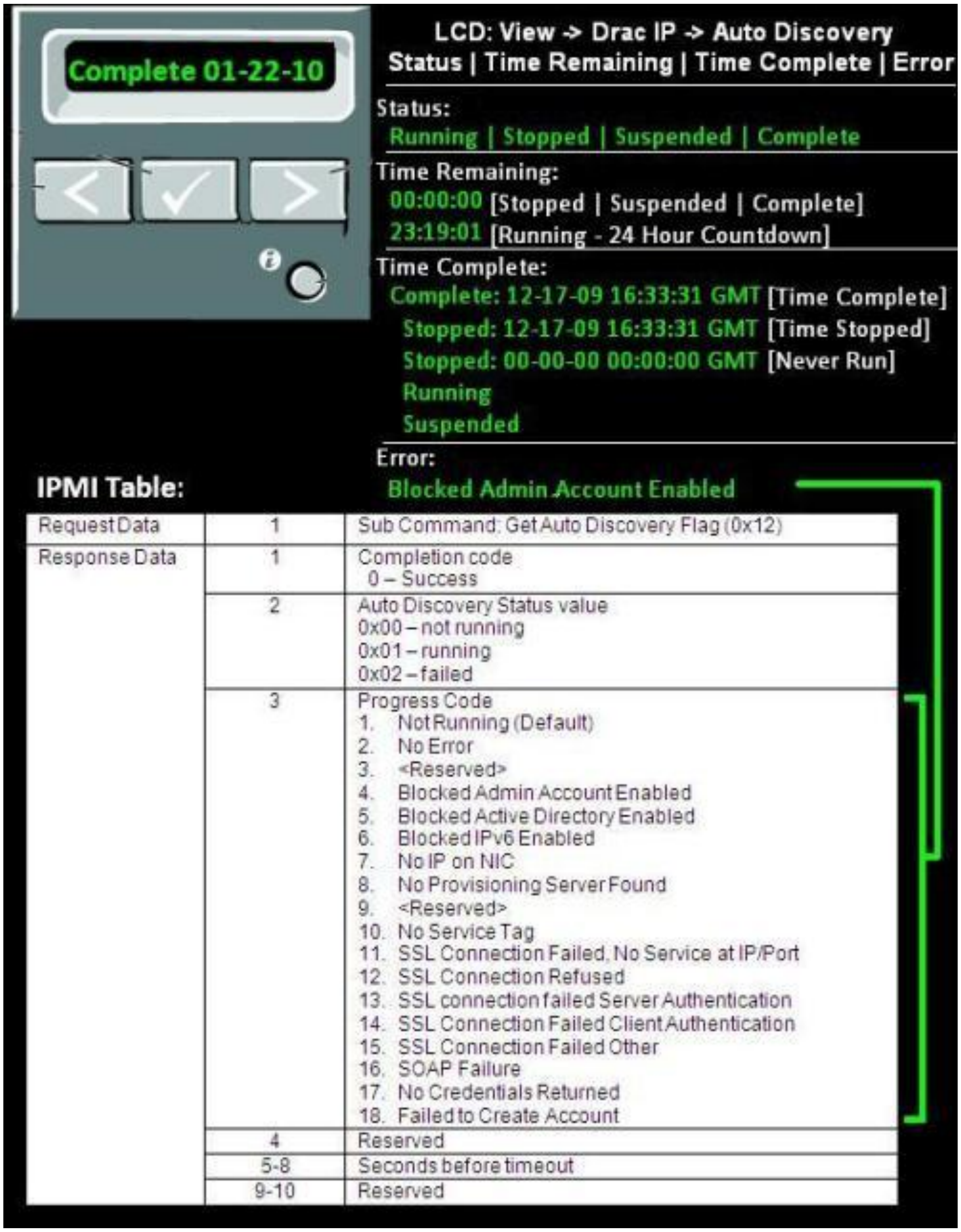
9 IP Change Notification

After Auto-Discovery completes and a user account is created it will be disabled. If the system is power cycled after that auto discovery will not run again. To handle a situation where a system would lose its DHCP lease and the IP address of the iDRAC would change the provisioning server can request that the iDRAC send IPChange Notification SOAP messages using the same mutually authenticated TLS method if the IP address of the iDRAC changes. This makes sure the console always knows the IP of the system’s iDRAC.

10 Trouble Shooting Auto-Discovery

10.1 Trouble Shoot With Physical Access to the System/iDRAC

10.1.1 Auto Discovery Status on the LCD



LCD: View -> Drac IP -> Auto Discovery
Status | Time Remaining | Time Complete | Error

Status:
Running | Stopped | Suspended | Complete

Time Remaining:
00:00:00 [Stopped | Suspended | Complete]
23:19:01 [Running - 24 Hour Countdown]

Time Complete:
Complete: 12-17-09 16:33:31 GMT [Time Complete]
Stopped: 12-17-09 16:33:31 GMT [Time Stopped]
Stopped: 00-00-00 00:00:00 GMT [Never Run]
Running
Suspended

Error:
Blocked Admin Account Enabled

IPMI Table:

Request Data	1	Sub Command: Get Auto Discovery Flag (0x12)
Response Data	1	Completion code 0 – Success
	2	Auto Discovery Status value 0x00 – not running 0x01 – running 0x02 – failed
	3	Progress Code 1. Not Running (Default) 2. No Error 3. <Reserved> 4. Blocked Admin Account Enabled 5. Blocked Active Directory Enabled 6. Blocked IPv6 Enabled 7. No IP on NIC 8. No Provisioning Server Found 9. <Reserved> 10. No Service Tag 11. SSL Connection Failed, No Service at IP/Port 12. SSL Connection Refused 13. SSL connection failed Server Authentication 14. SSL Connection Failed Client Authentication 15. SSL Connection Failed Other 16. SOAP Failure 17. No Credentials Returned 18. Failed to Create Account
	4	Reserved
	5-8	Seconds before timeout
	9-10	Reserved

Figure 8 **– Auto Discovery LCD Status**

Auto Discovery Progress Codes and Corrective Actions

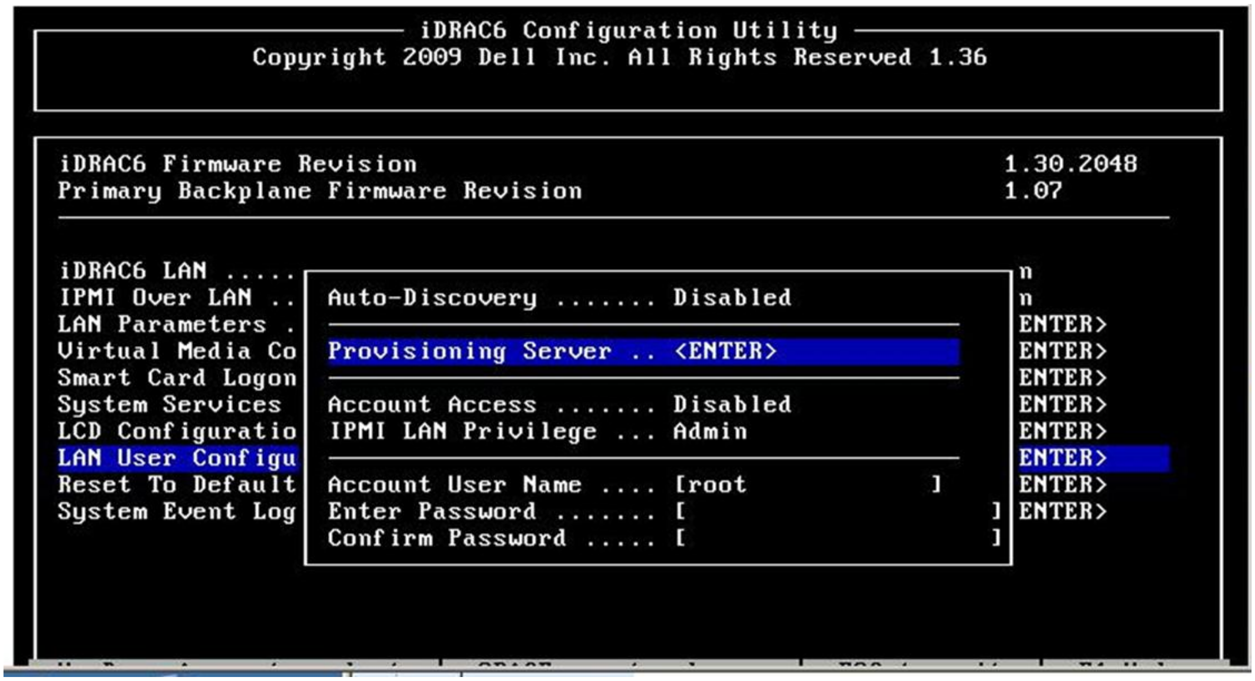
The following codes are displayed on the Server LCD and in the iDRAC RACLOG

Status	Description	Corrective action
0	stopped	N/A
1	running	see info
2	suspended	see info
3	complete	N/A
Info	**Description**	**Corrective action**
1	Stopped (default)	N/A
2	Started	N/A
3	Auto Discovery disabled	enable discovery
4	Blocked Admin Account Enabled	disable all admin accounts
5	Blocked Active Directory Enabled	disable active directory
6	Blocked IPv6 Enabled	disable IPv6
7	Blocked No IP on NIC	enable the NIC
8	No Provisioning Server Found	check the value of psinfo in the BIOS
9	Blocked Provisioning Server Unreachable/Invalid address	check the value of psinfo in the BIOS
10	No Service Tag	boot the server. If the problem remains contact tech support
11	TLS connection failed no service at IP/port	check the value of psinfo in the BIOS, or vendor option on DHCP server
12	TLS Connection refused	check the value of psinfo in the BIOS, or vendor option on DHCP server
13	TLS connection failed (server authentication)	server certificate is invalid or not signed by the trusted server CA cert installed on the idrac. Either replace the provisioning server certificate or upload a new server cert on the idrac
14	TLS connection failed (client authentication)	idrac client certificate was not signed by a CA trusted by the provisioning server. Either add the idrac CA to the trusted list or generate a new certificate on the iDRAC
15	TLS connection failed other	enable a root account through BIOS to retrieve the iDRAC tracelog. Contact tech support
16	SOAP failure	The provisioning server does not support the getCredentials() SOAP call. Verify that the provisioning server supports auto discovery and the provisioning server information is set correctly in the DHCP vendor option, DNS SRV record, or BIOS
17	No credentials returned	Check that the service tag is in the list of known servers on the provisioning server
18	Failed to create account	make sure that all 16 iDRAC account are not already used

Figure 9 - Auto Discovery Progress Codes Corective Actions Table

10.1.2 Checking Auto-Discovery Settings through iDRAC Configuration (11th Generation Servers)

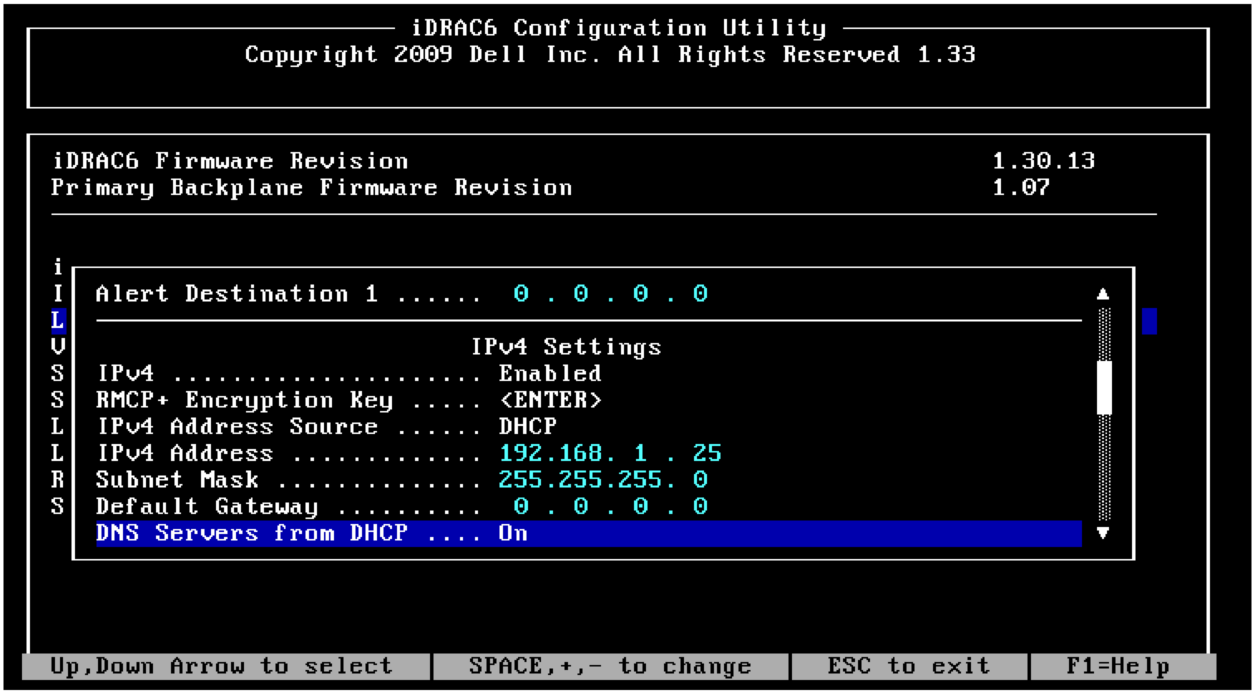
1) Reboot the system and enter CTRL-E during the system boot when the “Press CTRL-E for Remote Access Setup within 5 seconds….“ message appears to enter the iDRAC Configuration Utility.
2) Make sure the Auto-Discovery setting is Enabled and Account Access setting is Disabled. The following screenshot depicts the iDRAC Configuration settings needed.



```
                    iDRAC6 Configuration Utility
           Copyright 2009 Dell Inc. All Rights Reserved 1.36

 iDRAC6 Firmware Revision                                  1.30.2048
 Primary Backplane Firmware Revision                       1.07

 iDRAC6 LAN .....                                          n
 IPMI Over LAN .. | Auto-Discovery ....... Disabled       | n
 LAN Parameters . |                                       | ENTER>
 Virtual Media Co | Provisioning Server .. <ENTER>        | ENTER>
 Smart Card Logon |                                       | ENTER>
 System Services  | Account Access ....... Disabled       | ENTER>
 LCD Configuratio | IPMI LAN Privilege ... Admin          | ENTER>
 LAN User Configu |                                       | ENTER>
 Reset To Default | Account User Name .... [root        ] | ENTER>
 System Event Log | Enter Password ....... [             ]| ENTER>
                  | Confirm Password ..... [             ]|
```

Figure 10 **– 11G iDRAC Configuration Utility – Auto-Discovery & User**

3) Check that the iDRAC has an IP address leased from DHCP. The following screenshot depicts the iDRAC Configuration Utility settings needed.

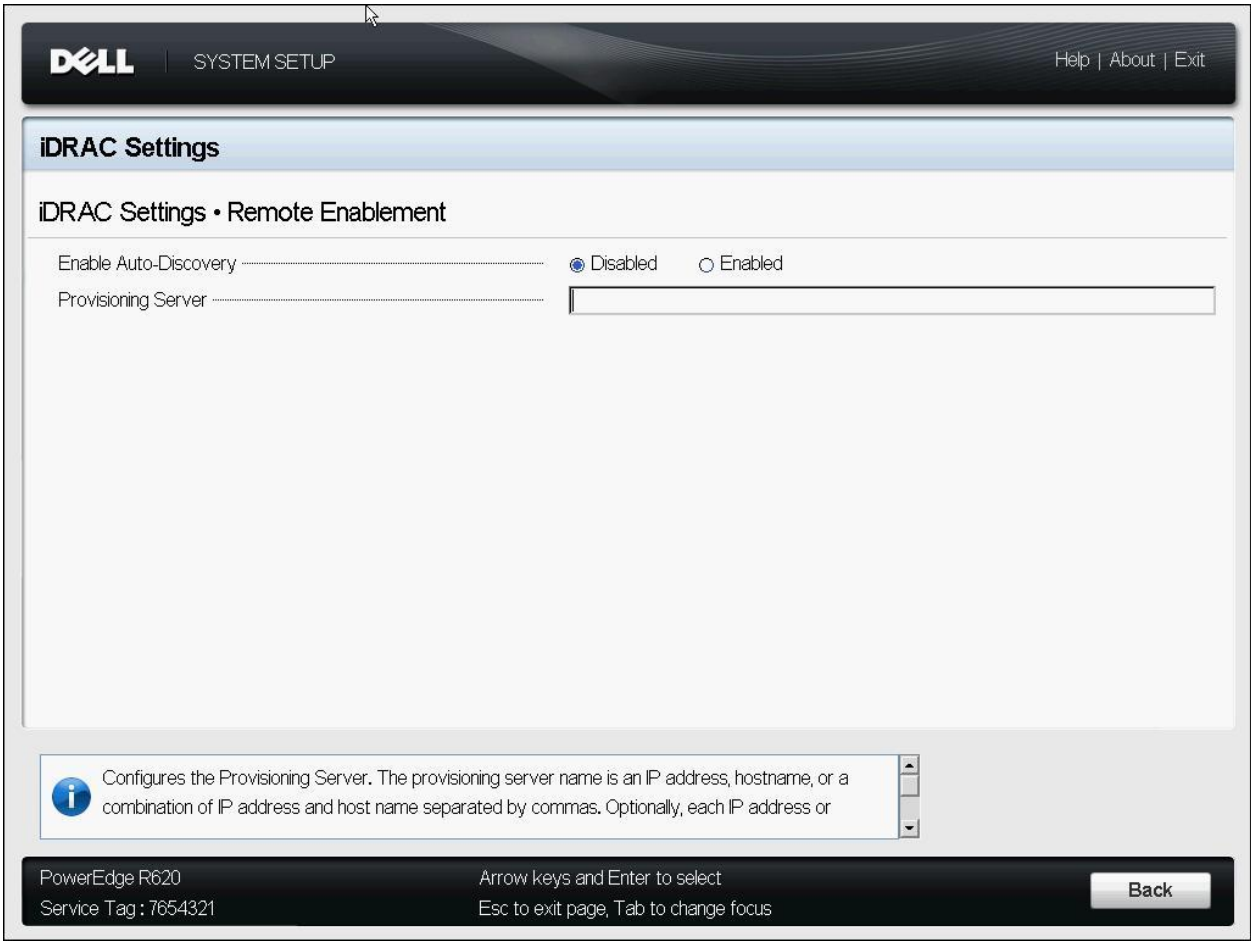


```
              iDRAC6 Configuration Utility
     Copyright 2009 Dell Inc. All Rights Reserved 1.33

iDRAC6 Firmware Revision                           1.30.13
Primary Backplane Firmware Revision                1.07

i
I  Alert Destination 1 ......  0 . 0 . 0 . 0
L
V                   IPv4 Settings
S  IPv4 ..................... Enabled
S  RMCP+ Encryption Key ..... <ENTER>
L  IPv4 Address Source ...... DHCP
L  IPv4 Address ............. 192.168. 1 . 25
R  Subnet Mask .............. 255.255.255. 0
S  Default Gateway ..........  0 . 0 . 0 . 0
   DNS Servers from DHCP .... On

Up,Down Arrow to select | SPACE,+,- to change | ESC to exit | F1=Help
```

Figure 11 - 11G iDRAC Configuration Utility – Lan Parameters

10.1.3 Checking Auto-Discovery Settings through system setup (12G)

1) Reboot the system and press F2.
2) Make sure the Auto-Discovery setting is Enabled



iDRAC Settings

iDRAC Settings • Remote Enablement

Enable Auto-Discovery ● Disabled ○ Enabled

Provisioning Server

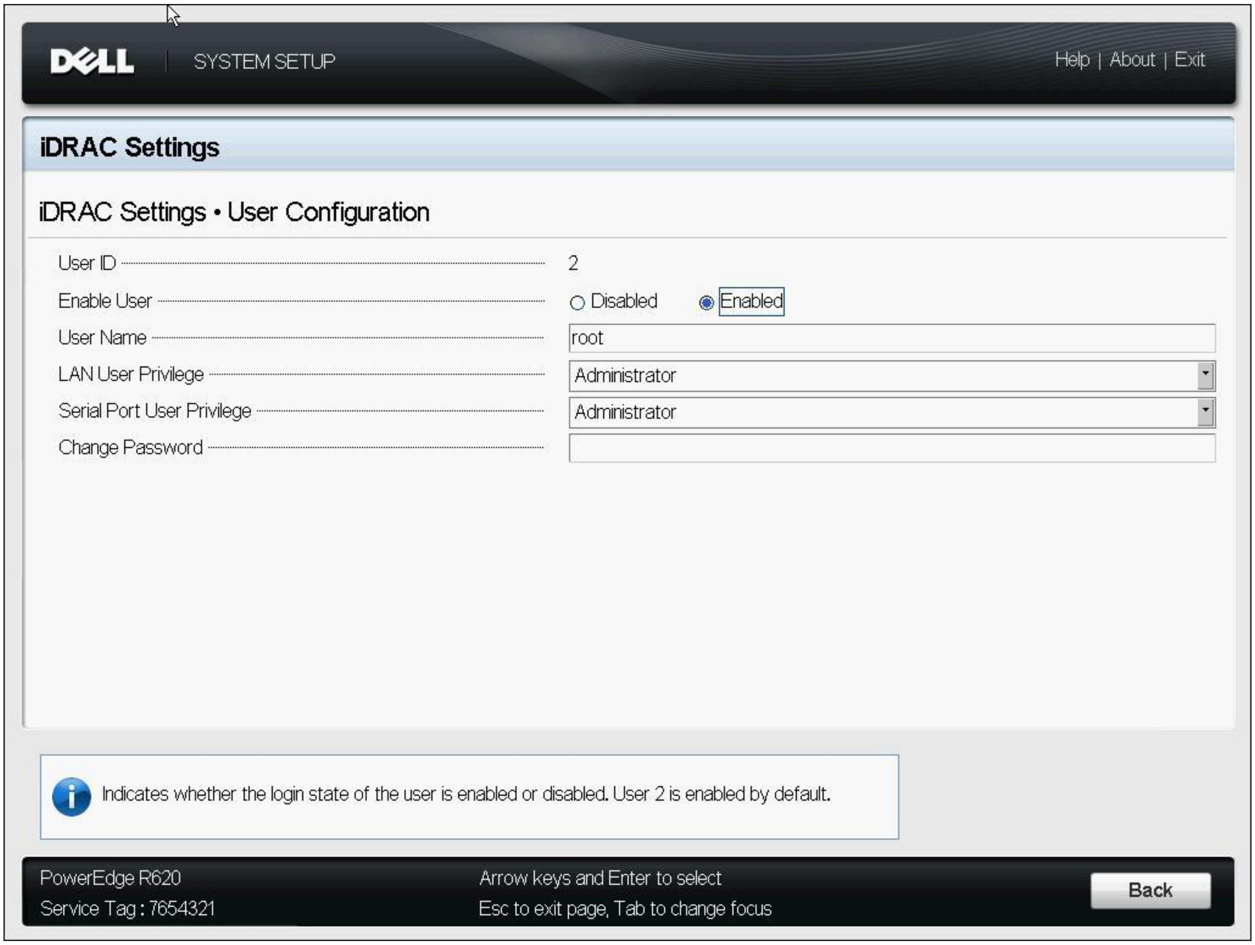
Configures the Provisioning Server. The provisioning server name is an IP address, hostname, or a combination of IP address and host name separated by commas. Optionally, each IP address or

PowerEdge R620
Service Tag : 7654321

Arrow keys and Enter to select
Esc to exit page, Tab to change focus

Figure 12 - 12G System Setup – iDRAC – Auto-Discovery

3) Make sure Account Access setting is Disabled



iDRAC Settings

iDRAC Settings • User Configuration

User ID: 2

Enable User: ○ Disabled ● Enabled

User Name: root

LAN User Privilege: Administrator

Serial Port User Privilege: Administrator

Change Password:

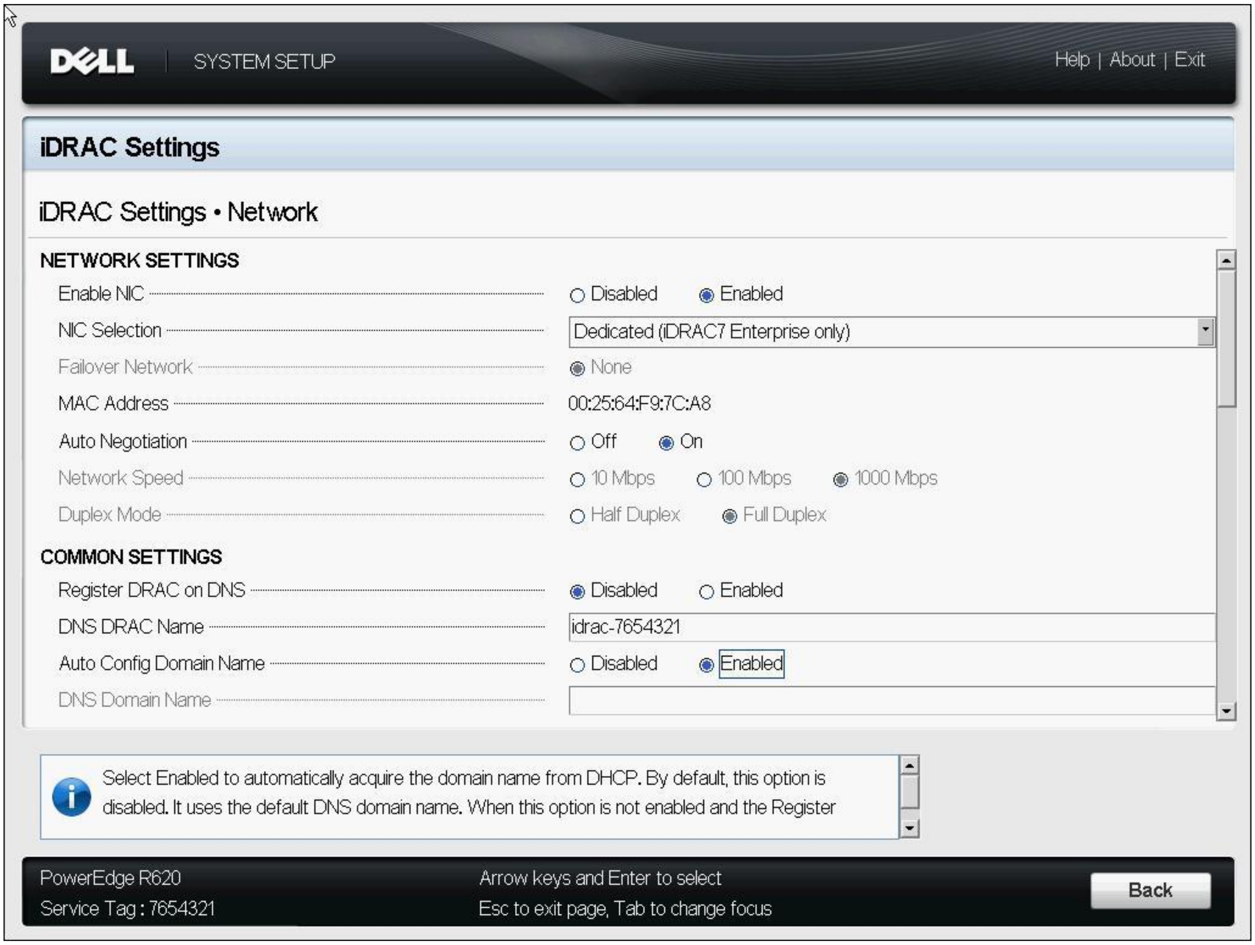
Indicates whether the login state of the user is enabled or disabled. User 2 is enabled by default.

PowerEdge R620
Service Tag : 7654321

Arrow keys and Enter to select
Esc to exit page, Tab to change focus

Figure 13 - 12G System Setup – iDRAC - User Config

4) Make sure iDRAC network settings are correct



iDRAC Settings

iDRAC Settings • Network

NETWORK SETTINGS

Enable NIC ○ Disabled ● Enabled

NIC Selection: Dedicated (iDRAC7 Enterprise only)

Failover Network ● None

MAC Address 00:25:64:F9:7C:A8

Auto Negotiation ○ Off ● On

Network Speed ○ 10 Mbps ○ 100 Mbps ● 1000 Mbps

Duplex Mode ○ Half Duplex ● Full Duplex

COMMON SETTINGS

Register DRAC on DNS ● Disabled ○ Enabled

DNS DRAC Name: idrac-7654321

Auto Config Domain Name ○ Disabled ● Enabled

DNS Domain Name:

Select Enabled to automatically acquire the domain name from DHCP. By default, this option is disabled. It uses the default DNS domain name. When this option is not enabled and the Register

PowerEdge R620
Service Tag : 7654321

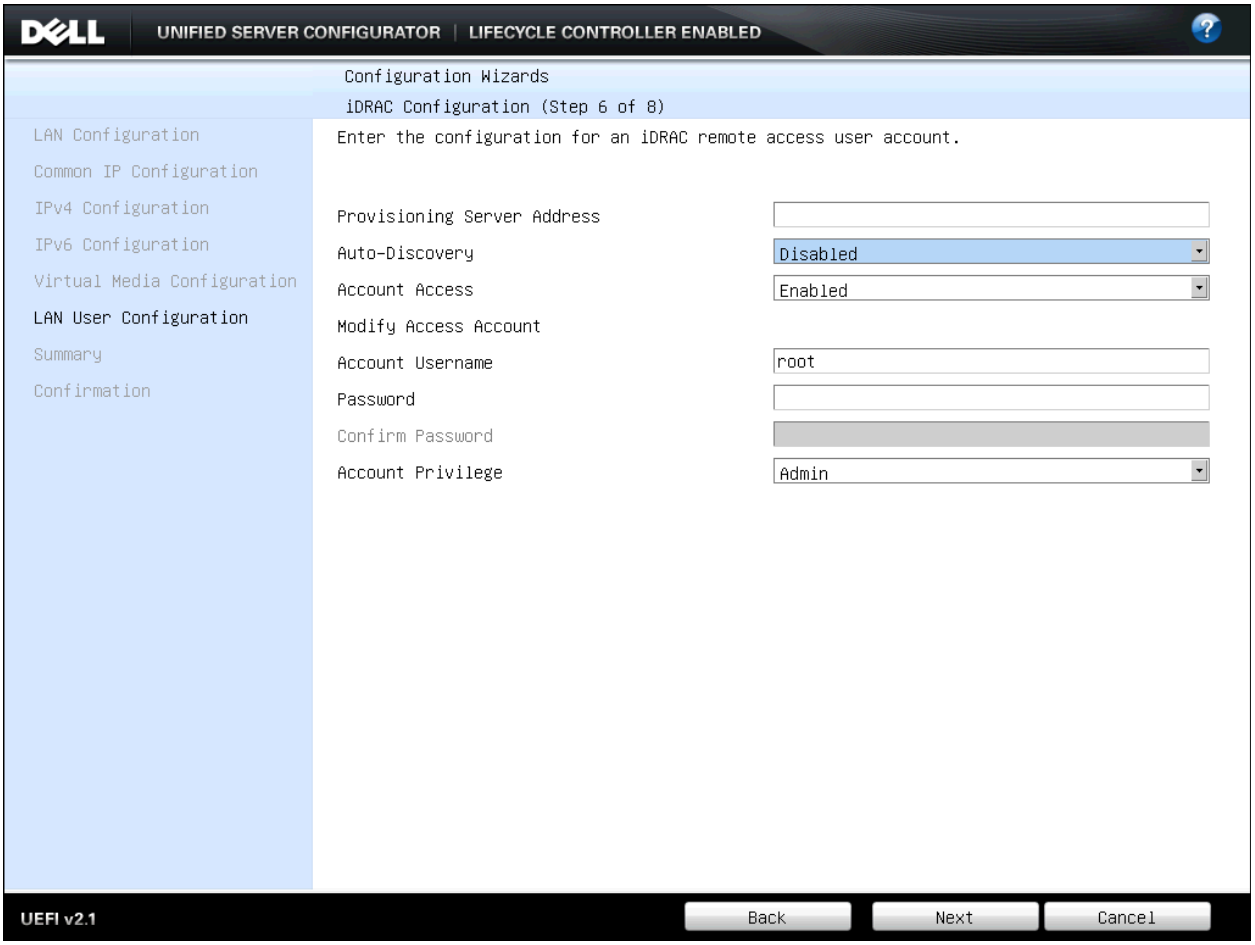
Arrow keys and Enter to select
Esc to exit page, Tab to change focus

Figure 14 - 12G System Setup - iDRAC - Network

10.1.4 Checking Auto-Discovery Settings through Lifecycle Controller

1) Reboot the system and press F10
2) Start the iDRAC configuration wizard
3) The Auto-Discovery settings are in step 6

This is a screen shot from the 11th generation server Lifecyle Controller.



Configuration Wizards

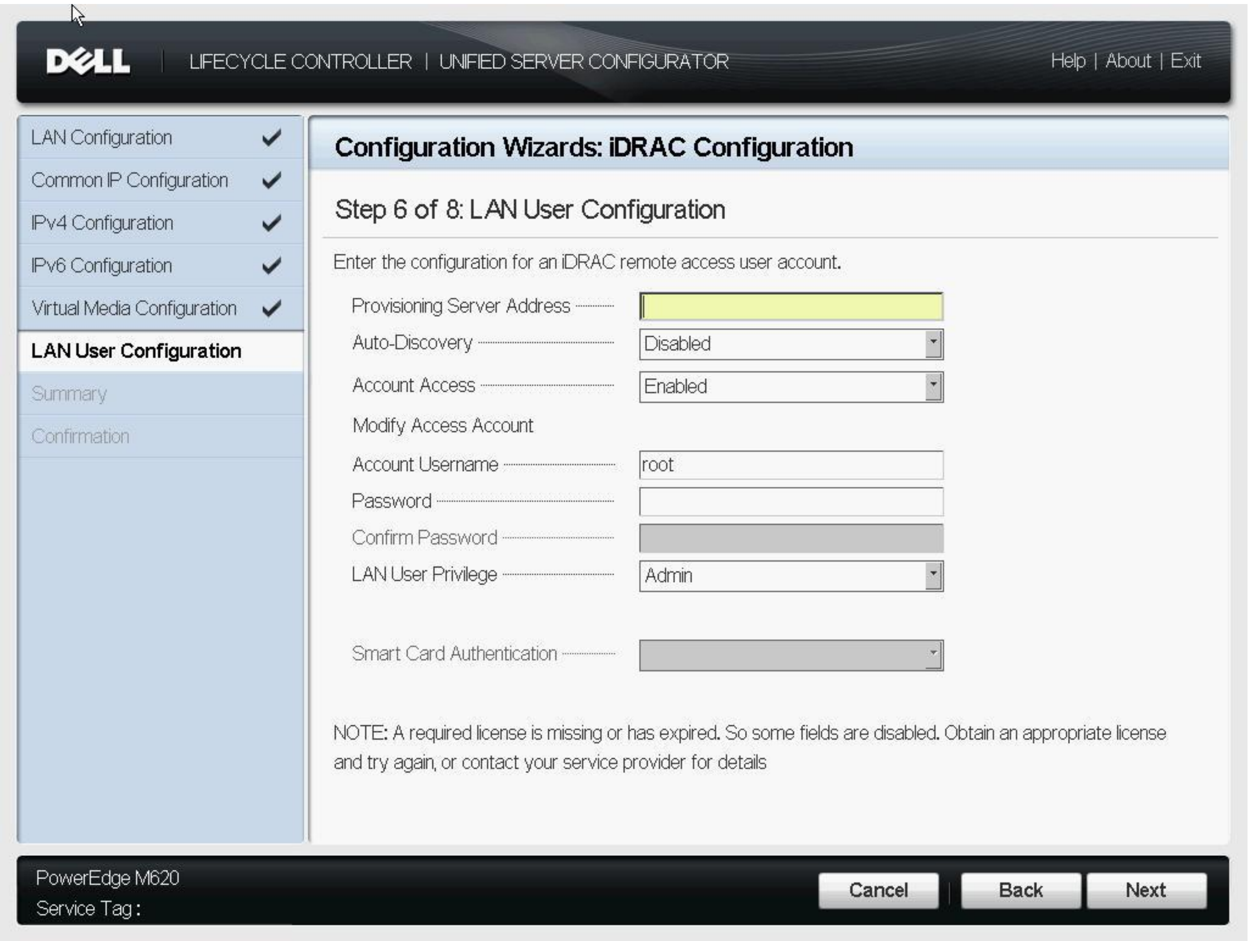
iDRAC Configuration (Step 6 of 8)

Enter the configuration for an iDRAC remote access user account.

Provisioning Server Address	
Auto-Discovery	Disabled
Account Access	Enabled
Modify Access Account	
Account Username	root
Password	
Confirm Password	
Account Privilege	Admin

Figure 15 - Lifecycle Controller - iDRAC – Auto-Discovery (11th Generaton Server)

This is a screen shot from the 12th generation server Lifecycle Controller.



Configuration Wizards: iDRAC Configuration

Step 6 of 8: LAN User Configuration

Enter the configuration for an iDRAC remote access user account.

Provisioning Server Address
Auto-Discovery: Disabled
Account Access: Enabled
Modify Access Account
Account Username: root
Password
Confirm Password
LAN User Privilege: Admin
Smart Card Authentication

NOTE: A required license is missing or has expired. So some fields are disabled. Obtain an appropriate license and try again, or contact your service provider for details

PowerEdge M620
Service Tag :

Figure 16 - Lifecycle Controller - iDRAC – Auto-Discovery (12th generation server)

10.2 Without Physical Access to the System/iDRAC

10.2.1 Verify DHCP Lease

Verify the iDRAC got a DHCP lease on the DCHP server. Refer to the documentation or Help information available for the DHCP server being used for the specific steps to check what IP addresses are leased out to which MAC addresses.

10.2.2 Verify DNS Entries

Verify the DNS entries on the DNS server. If DHCP is not being used and a hostname is specified in the SNS Serive Record, make sure the hostname is resolvable using ping or nslookup.

When using nslookup, if SRV is being used:

```
nslookup
>set type=srv
>_dcimprovsrv._tcp.<yourdomain>.com
```

If the default hostname “DCIMCredentialServer” is being used, make sure the DNS entry is resolvable.

```
nslookup DCIMCredentialServer.<yourdomain>.com
```

10.2.3 Checking the iDRAC RACLOG

If this is a modular system, enable the admin account from the CMC. The iDRAC RACLOG can be accessed using the iDRAC remote Graphical User Interface(GUI) or the remote racadm command line utility. See the *iDRAC6 User Guide* for instructions on how to view the RACLOG using the iDRAC GUI. To access the RACLOG using the remote racadm utility, invoke the “racadm getraclog” command (see the *iDRAC6 Users Guide* for details on invoking this command) and check the Auto-Discovery related messages. See the section *Auto Discovery Status on the LCD* for a complete listing of Auto-Discovery related messages, more detailed descriptions of the conditions that caused the messages to be generated, and recommended response actions.

11 Manual Configuration of iDRAC for Re-Initiating Auto-Discovery

For testing purposes, the iDRAC Auto-Discovery process can be re-initiated by physically visiting the server and manually configuring the iDRAC. The quickest way to manually configure a system to perform Auto-Discovery is to:

1. Enter the iDRAC6 Configuration Utility by pressing CTRL-E (11Gth generation server) or System Setup by pressing F2 (12th generation server) when the server is booting.
2. Reset the iDRAC to factory settings.
3. Set the iDRAC LAN Source Address to DHCP.
4. Enable Auto-Discovery.
5. Set Account Access to Disabled.

Note: see Trouble Shoot With Physical Access to the System/iDRAC for screen shots.

This matches the settings if the iDRAC was shipped from the factory with Auto-Discovery Enabled. The following are the iDRAC6 Configuration Utility settings from the factory:

1) Domain Name from DHCP: On
2) iDRAC Source Address: DCHP
3) DNS Server IP Address: On
4) Account Access (for default “root” account): Disabled
5) Auto-Discovery: Enabled

These settings support the following Auto-Discovery network environments: DHCP only and DHCP with DNS. Once the server main network port (that is shared with the iDRAC) is connected into in the network where DHCP, DNS, and the Provisioning Server are accessible and AC power is connected to the system, the Auto-Discovery process begins once the iDRAC completes its boot process. The server itself does not need to be turned on.

12 Advanced iDRAC Auto-Discovery Configuration

Most users do not need to configure these advanced settings for Auto-Discovery. These capabilities require one touch of the system to function properly.

12.1 Simultaneous Auto-Discovery Methodologies

If more than one discovery methodology is used simultaneously, the provisioning server address acquisition sequence is the following:

1) Vendor Scope Option

2) DNS SRV record

3) Default Host A record.

The method selected to provision the server determines the appropriate iDRAC6 configuration utility settings (accessible during boot using Ctrl-E).

Depending upon the desired environment, the settings can be filled out in a different ways. All settings must contain valid information; the domain name and IP addresses must be accurate for their environment. No setting can be left empty for Auto-Discovery to succeed, with one exception, *DCHP Only*.

If the discovery methodology is *DHCP Only* and is using the Vendor Scope option with a Specified IP address (port optional), the only setting in the iDRAC Configuration Utility that needs to be populated is the *IP4 address DCHP*. The Domain Name and Domain Server IP settings do not need to have any information or be enabled.

12.2 Using Static IP addresses

It is possible to configure iDRAC to use a static IP address and then proceed with Auto-Discovery to set up user credentials. In this case, the Auto-Discovery feature becomes “one-touch” provisioning for the environment. This method might be preferred if the you want to predetermine the locations and fixed IP addresses of their machines. If a static IP address is entered through the BIOS setup and iDRAC configuration screen (11th generation servers) or System Setup (12th generation servers), *and* there are no user accounts supplied, the discovery process attempts to locate the provisioning server through DNS. If a user account is supplied, the initial discovery and handshake becomes unnecessary, and the remote console may use these credentials for configuration using WS-Man or remote RACADM.

12.3 iDRAC Auto-Discovery Configuration Settings

This section covers the seven methods to configure a server based on the network environment using the four discovery implementation alternatives.

The iDRAC Configuration Utility(11th generation servers) or iDRAC System Settings (12th generation servers) settings are dependent on the provisioning method listed for the following items:

- Domain Name - On / off / manual
- iDRAC Source - DHCP / Specified
- DNS Server IP Address - On / off / manual

For the Domain Name and DNS Server IP address settings:

- On – the field Domain Name from the DHCP or DNS Server from DHCP is set to ON.
- Off – the field Domain Name from the DHCP or DNS Server from DHCP is set to OFF.
- Manual – the fields are set to OFF, and the user has entered information manually in the other fields.

The following settings listed here are only the LAN parameter settings. The iDRAC6 LAN must be enabled; select the Auto-Discovery field, and disable the Root account in the LAN User section in the iDRAC6 Configuration Utility for Auto-Discovery to begin running. This does not apply if the feature is included in the server when it was ordered.

12.3.1 Auto-Discovery option from the factory

The following are the iDRAC6 Configuration Utility settings from the factory:

1) Domain Name from DHCP: On
2) iDRAC Source: DCHP
3) DNS Server IP Address: On
4) Account Access (for default "root" account): Disabled
5) Auto-Discovery: Enabled

These settings allow for the widest range for the administrators. It supports the following network environments: DHCP only and DHCP with DNS. The server could be provisioned by any of the three methods. Once the server is plugged into in the network cable and the AC power cord, the Auto-Discovery process begins once the iDRAC completes its boot process. The server does not need to be powered on.

12.3.2 DHCP only, using Vendor scope option with Specified IP address

The iDRAC6 Configuration Utility settings have the following fields set:

1) Domain Name from DHCP: OFF
2) iDRAC Source: DCHP
3) DNS Server IP Address: OFF

These settings can be configured manually with IP4 address set to DHCP, no Domain Name and no DNS Server information set. The provisioning server Vendor Scope option would have a specified IP address. DNS services are not required for this method. It works with DNS services enabled; however, in a typical setup there would be no DNS.

12.3.3 DHCP w/ DNS using Vendor Scope option using Name resolution

The iDRAC6 Configuration Utility settings have the following fields set

1) Domain Name from DHCP: On
2) iDRAC Source: DCHP
3) DNS Server IP Address: On

All settings for the above fields would be set to DHCP, or could be manually configured; but all settings would need to be configured. The provisioning server Vendor Scope option would have a DNS Name, No SRV record, and no Default Host A record is set.

12.3.4 DHCP w/ DNS using SRV record

The iDRAC6 Configuration Utility settings have the following fields set:

1) Domain Name from DHCP: On
2) iDRAC Source: DCHP
3) DNS Server IP Address: On

All settings for the above fields would be set to DHCP, or could be manually configured; but all fields would need to be configured. The provisioning server DNS SRV record with a fully-qualified domain name needs to be present, but there is no Vendor Scope option and no default host A record is set.

12.3.5 DHCP w/ DNS using Default Host A record

The iDRAC6 Configuration Utility settings have the following fields set:

1) Domain Name from DHCP: On
2) iDRAC Source: DCHP
3) DNS Server IP Address: On

All settings for the above fields would be set to DHCP, or could be manually configured; but all fields would need to be configured. The provisioning server has a default host, but no Vendor Scope option. A record and DNS SRV are not set.

12.3.6 DNS only using SRV record

The iDRAC6 Configuration Utility settings have the following fields set:

1) Domain Name from DHCP: Manually set (ex. domainname.com)
2) iDRAC Source: 192.168.0.120
3) DNS Server IP Address: Manually set (ex. 192.168.0.2)

All settings for the above fields would need to be manually set to complete configuration for Auto-Discovery. The provisioning server has no DHCP services running, no Vendor Scope option, and no default host. A record is set.

12.3.7 DNS only using Default Host A record

The iDRAC6 Configuration Utility settings have the following fields set:

1) Domain Name from DHCP: Manually set (ex. domainname.com)
2) iDRAC Source: 192.168.0.120
3) DNS Server IP Address: Manually set (ex. 192.168.0.2)

All settings for the above fields would need to be manually set to complete configuration for Auto-Discovery. The provisioning server has no DHCP services running, no Vendor Scope option, and no SRV record are set up.

13 SOAP Messages

13.1 getCredentials

```
<?xml version="1.0" encoding="UTF-8" ?>

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:ns2="http://www.dell.com/HandshakeSoap" xmlns:ns3="http://www.dell.com/HandshakeSoap12"
xmlns:ns4="http://www.dell.com/IPChangeReportSoap" xmlns:ns1="http://www.dell.com/"
xmlns:ns5="http://www.dell.com/IPChangeReportSoap12">

    <SOAP-ENV:Body>

        <ns1:getCredentials>

            <ns1:clientIdentifier />

        </ns1:getCredentials>

    </SOAP-ENV:Body>

</SOAP-ENV:Envelope>
```

13.2 getCredentialsResponse

```
<?xml version="1.0" encoding="UTF-8" ?>

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:ns2="http://www.dell.com/HandshakeSoap" xmlns:ns3="http://www.dell.com/HandshakeSoap12"
xmlns:ns4="http://www.dell.com/IPChangeReportSoap" xmlns:ns1="http://www.dell.com/"
xmlns:ns5="http://www.dell.com/IPChangeReportSoap12">

    <SOAP-ENV:Body>

        <ns1:getCredentialsResponse>

            <ns1:getCredentialsResult>

                <ns1:UserID />

                <ns1:Password />

            </ns1:getCredentialsResult>

        </ns1:getCredentialsResponse>

    </SOAP-ENV:Body>

</SOAP-ENV:Envelope>
```

13.3 setIPChange

```
<?xml version="1.0" encoding="UTF-8" ?>

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:ns2="http://www.dell.com/HandshakeSoap" xmlns:ns3="http://www.dell.com/HandshakeSoap12"
xmlns:ns4="http://www.dell.com/IPChangeReportSoap" xmlns:ns1="http://www.dell.com/"
xmlns:ns5="http://www.dell.com/IPChangeReportSoap12">

    <SOAP-ENV:Body>

        <ns1:setIPChange>

            <ns1:clientIdentifier />

            <ns1:IpAddr />

        </ns1:setIPChange>

    </SOAP-ENV:Body>

</SOAP-ENV:Envelope>
```

13.4 setIPChangeResponse

```
<?xml version="1.0" encoding="UTF-8" ?>

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:ns2="http://www.dell.com/HandshakeSoap" xmlns:ns3="http://www.dell.com/HandshakeSoap12"
xmlns:ns4="http://www.dell.com/IPChangeReportSoap" xmlns:ns1="http://www.dell.com/"
xmlns:ns5="http://www.dell.com/IPChangeReportSoap12">

    <SOAP-ENV:Body>

        <ns1:setIPChangeResponse>

            <ns1:setIPChangeResult>

                <ns1:AckNak />

            </ns1:setIPChangeResult>

        </ns1:setIPChangeResponse>

    </SOAP-ENV:Body>

</SOAP-ENV:Envelope>
```