The science behind the report:

Automate high-touch server lifecycle management tasks

This document describes what we tested, how we tested, and what we found. To learn how these facts translate into real-world benefits, read the report Automate high-touch server lifecycle management tasks.

We concluded our hands-on testing on February 28, 2021. During testing, we determined the appropriate hardware and software configurations and applied updates as they became available. The results in this report reflect configurations that we finalized on February 22, 2021 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

To learn more about how we have calculated the wins in this report, go to http://facts.pt/calculating-and-highlighting-wins. Unless we state otherwise, we have followed the rules and principles we outline in that document.

Table 1: The time and steps required to perform each common systems management task with Dell EMC™ OpenManage™ Enterprise (OME) 3.5 in conjunction with OpenManage Integration with ServiceNow® (OMISNOW), OpenManage Enterprise Power Manager, and the SupportAssist Enterprise (SAE) plugin compared to manual methods. Lower is better. Source: Principled Technologies.

	OME 3.5 Suite		Manual approaches		Difference			
	Time (sec.)	Steps	Time (sec.)	Steps	Time saved (sec.)	Percentage less time	Steps saved	Percentage fewer steps
Server-initiated discover per servery	14	5	28	5	14	50.0	0	0.0
Server profile deployment per server	42	8	183	12	141	77.0	4	33.3
Power policy creation	31	7	N/A	N/A	N/A	N/A	N/A	N/A
OMISNOW and Power Manager event monitoring, incident creation/ resolution per event	0	0	98	19	98	100.0	19	100.0
Updating server firmware on three servers	46	9	2,524	16	2,478	98.2	7	43.8
SupportAssist Enterprise server onboarding per server	0	0	235	8	235	100.0	8	100.0

System configuration information

Table 2: Detailed information on the system we tested.

System configuration information	Dell EMC PowerEdge™ R740 server
Operating system name and version/build number	ESXI 6.7.0 Update 3 Build-14320388
Power management policy	Performance
Processor	
Number of processors	2
Vendor and model	Intel® Xeon® Platinum 8168
Core count (per processor)	24
Core frequency (GHz)	2.70
Stepping	4
Memory module(s)	
Total memory in system (GB)	128
Number of memory modules	4
Vendor and model	Samsung® M386A4G40DM0-CPB
Size (GB)	32
Type	DDR4
Speed (MHz)	2,133
Speed running in the server (MHz)	2,133
Storage controller	
Vendor and model	Dell PERC H740P
Cache size (GB)	8
Driver version	7.710.07.00
Local storage	
Number of drives	2
Drive vendor and model	Toshiba® THNSF8120CCSE
Drive size (GB)	120
Drive information (speed, interface, type)	SATA SSD
Network adapter	
Vendor and model	Broadcom® Gigabit Ethernet BCM5720
Number and type of ports	4 x 1 Gigabit

System configuration information	Dell EMC PowerEdge™ R740 server
Cooling fans	
Vendor and model	Nidec UltraFlo 4VXP3-X30
Number of cooling fans	6
Power supplies	
Vendor and model	Delta - Dell PN: 0Y26KXA02
Number of power supplies	2
Wattage of each (W)	1,100

How we tested

Server-initiated discovery vs. discovery with network scanning

Configuring iDRAC

The following steps assume your management network is using DHCP for IP address allocation and DNS for name resolution.

1. Open a browser, and log into the iDRAC with administrator credentials (we used root/calvin).
2. Click Configuration→Licenses.
3. From the License Options drop-down menu, select Import.
4. To locate the OpenManage Enterprise Advance license, click Browse, and click Ok. Click Upload.
5. From the License Options drop-down menu, select Import.
6. To locate the Dell EMC OpenManage Integration for ServiceNow license, click browse, and click Ok. Click Upload.
7. Click iDRAC Settings→Connectivity.
8. Expand Network.
9. Expand iDRAC Auto Discovery, and confirm or enable AutoDiscovery. Click Apply.
10. Expand Common Settings, and set Auto Config Domain Name to Enabled. Click Apply.
11. Expand IPv4 settings. Confirm DHCP, enable Use DHCP to Obtain DNS Server Addresses, and click Apply.
12. Click Dashboard.
13. In the More Actions menu, select Reboot iDRAC. To reboot iDRAC, click OK, and click OK again.

Discovering servers with the OpenManage Enterprise server-initiated discovery feature

These steps assume that someone has configured a DNS to allow non-secure updates from OME, and that someone has enabled server-initiated discovery feature in the OME TUI (text-based user interface). See OME online help for details.

This process applies to all servers on the list for import.

1. From OME, click Monitor→Server Initiated Discovery.
2. Click Import.
3. Download the sample CSV file. Open the CSV file in a text editor, and replace the sample text with the Service Tag and admin credentials you want to import. Save the file.
4. Select the CSV file you edited, and click OK.
5. To import the CSV file, click Finish. Service Tags will appear in your console via automatic discovery when the server comes online and is configured to target the OME Server.

Discovering servers in the OpenManage Enterprise console using network scanning

This process applies to servers that are connected to the network, have IP addresses and are available for discovery, and which all use the same credentials. Failed discovery means the someone must repeat this process. For servers without the same credentials, someone must discover them in a separate job.

1. From OME, click Devices.
2. In the upper-right, click Discover Devices.
3. To select the type of device you want to add, use the drop-down menu.
4. In the pop-up window, select Dell iDRAC, and click OK.
5. In the text box, enter the IP address (or range of IP addresses) to discover. Change the Service API Credentials to the credentials of the servers to be discovered. Click the checkboxes for Enable trap reception… and Set Community String…, and click Finish.

Creating and deploying a Server Profile with OpenManage Enterprise

Creating a server template

1. In the OME console, select Configuration→Templates.
2. Click Create Template→From Reference Device.
3. Provide the template with a name, select Clone reference server, and click Next.
4. To choose the reference device, click Select Device. Check the box beside the reference server, and click OK.
5. Accept all defaults for import, and click Finish.
6. After the status shows Completed, click the newly created template, and click Edit.
7. Click Next.
8. Under Edit Components, in the BIOS section, select Optimize based on workload, and use the drop-down menu to select Virtualization Optimized Performance Profile. In the Boot section, accept the defaults. In Networking, select an identity pool to use with this template. Click Next.
9. Review the changes, and click Finish.

Creating a server profile

1. In the OME console, select Configuration→Profiles.
2. Click Create.
3. Select the template you want to assign to this profile, and click Next.
4. Provide a name prefix, and click Next.
5. To accept the Boot to Network ISO defaults (unchecked), click Next.
6. Click Finish.

Deploying a server profile

1. In the OME console, select Configuration→Profiles.
2. Check the box for the profile, and click Assign→Deploy.
3. Click Next.
4. To choose which target to deploy the profile, click Select. Click OK, and click Next.
5. To accept the default for Boot to Network ISO (unchecked), click Next.
6. To accept the default for iDRAC Management IP (Don't change IP settings), click Next.
7. To accept the defaults from the Policy, click Next.
8. Click Reserve Identities. Click Next.
9. Click Finish.
10. To confirm deployment, click Yes.

Creating and deploying a Server Profile without OpenManage Enterprise

Creating a server profile

1. Open a browser, and enter the IP address of the iDRAC you want to capture in a profile.
2. Log in with administrator credentials (we used root/calvin).
3. Click Configuration→Server Configuration Profile.
4. Expand Export.
    a. From the drop-down menu, for Location Type, select Network Share.
    b. Enter the file name. We used example.xml.
    c. For Protocol, select CIFS.
    d. Enter the IP Address.
    e. Enter the Share name.
    f. Enter the username and password for a user with access to the remote file share.
    g. Export All components.
    h. For Export type, select Clone.
5. Click Export.
6. To monitor the status, click Job Queue.

Deploying a server profile

1. Open a File Manager window on your local workstation, and browse to the share that contains the file name of the profile you want to import.
2. Open a browser, and enter the IP address of the iDRAC you want to capture in a profile.
3. Log in with administrator credentials (we used root/calvin).
4. Click Configuration→Server Configuration Profile.
5. Expand Import.
    a. From the drop-down menu, for Location Type, select Network Share
    b. Enter the file name. We used example.xml.
    c. For Protocol, select CIFS.
    d. Enter the IP Address.
    e. Enter the Share name.
    f. Enter the username and password for a user with access to the remote file share.
    g. Import All components.
6. Click Preview.
7. To monitor the status, click Job Queue.
8. Once the job completes with no errors, click Configuration→Server Configuration Profile.
9. Expand Import.
    a. From the drop-down menu, for Location Type, select Network Share.
    b. Enter the file name. We used example.xml.
    c. For Protocol, select CIFS.
    d. Enter the IP Address.
    e. Enter the Share name.
    f. Enter the username and password for a user with access to the remote file share.
    g. Import All components.
10. Click Import.
11. To confirm import, click OK.
12. To monitor the status, click Job Queue.

Creating a temperature-triggered power management policy

1. In OpenManage Enterprise, click Plugins→Power Management→Policies.
2. Click Create.
3. From the Type drop-down menu, select Temperature Triggered. Provide a name for the new policy, and click Next.
4. Click Select Group, and choose a static group containing your target servers. Click Add Selected, and click Next.
5. Enter the Temperature threshold at which the policy will apply Emergency Power reduction, or use the drop-down menu to select a pre-populated standard threshold. Click Next.
6. To accept the default schedule, click Next.
7. Click Finish.

Creating and resolving an incident with ServiceNow (manually)

1. Log into the ServiceNow console.
2. In the navigation filter, type incidents
3. From the Service Desk menu, click Incidents.
4. In the Incidents page, click New.
5. Open a new browser tab, and log into the OME console.
6. Select Alerts.
7. Select an active alert. On the right, select and copy the text in the detailed description for that alert.
8. Return to the ServiceNow console.
9. Fill out the information, and paste the copied text into the short description. We filled out the following:
    a. Caller
    b. Configuration item
    c. Contact type
    d. Short description
10. Click Submit.
11. To resolve the incident once the critical alert has resolved, log into the ServiceNow console. In the navigation filter, type incidents
12. From the Service Desk menu, click Incidents.
13. Locate the open alert you created in the previous steps, and click on it to open it.
14. Switch to the OME console.
15. Refresh the page, and copy the current status.
16. Return to the ServiceNow console.
17. On the Incident page, in the Notes tab, paste the current status into the Work notes field. Click the Resolution information tab.
18. Select a Resolution code, and for Resolution notes, type solved
19. Click Resolved.

Updating server firmware

The procedure below assumes a catalog and baseline have already been created for updating servers.

Updating server firmware one-to-many with OME

1. Click Configuration→Firmware/Driver Compliance.
2. Click Catalog Management.
3. Check the box beside the Catalog, and on the far right, click Check for update.
4. When the update completes, in the upper-left, click Return to Firmware/Driver Compliance.
5. Check the box beside the baseline you want to target. Target servers must be part of this baseline to be affected. Above the list of baselines, click Check Compliance.
6. When the job status is marked Completed, click View Report.
7. Check the boxes for all the entries you want to update, and click Make Compliant.
8. Accept the defaults, and check the boxes for Reset iDRAC and Clear Job Queue. Click Update.
9. To confirm the update, click Yes.

Updating a single Dell EMC PowerEdge R740 manually through Lifecycle Controller

1. Open a web browser and enter the IP address of the iDRAC.
2. Log into iDRAC with management credentials (we used root/calvin).
3. Click Launch Virtual Console.
4. Click Boot Control, and select Lifecycle Controller.
5. To confirm the next boot action, click Yes.
6. Click Power control, and power on the system.
7. To confirm, click Yes.
8. In the Lifecycle Controller window, click Firmware Update, and Launch Firmware Update.
9. Select Dell Website, and click Next.
10. To verify connectivity, click Test Network Connection. Click OK, and click Next.
11. To verify, click Yes.
12. To continue when prompted about HTTPS certificates, click Yes.
13. Select the available updates you want to download, and click Apply. (We excluded the OS drivers updates package due to its size.) Updates will begin to download. Time will vary based on number and sizes of the updates to download and download speed. We downloaded eight update packages in 3 minutes, 22 seconds.

14. The updates will apply in sequence before rebooting. iDRAC will update last and disconnect all sessions. Log back into iDRAC when available.
15. Launch the Virtual Console.
16. After reboot, the system re-enters Lifecycle Controller. Click Exit. To confirm exiting, click Yes. Do not remove power from the system until you have cleanly exited from Lifecycle Controller.

Onboarding a SupportAssist Enterprise server

OpenManage Enterprise and the SupportAssist Enterprise plugin

When using OpenManage Enterprise with the SupportAssist Enterprise plugin, the initial OME discovery of a device will check for SupportAssist entitlements for that server. If it is entitled, it is automatically added to the Plugin Group entitled SupportAssist. Hardware failure alerts will automatically create a case with Dell in SupportAssist. As such, no additional time or steps are required to monitor your servers for hardware failure and open cases with Dell for replacement.

SupportAssist Enterprise (full version)

To add a managed server to the full version of SupportAssist Enterprise, complete the following steps:

1. Open a browser, and navigate to the SupportAssist Enterprise web page. Enter the administrator credentials, and click Login.
2. Click Devices→View Devices.
3. Click Add Device.
4. Use the drop-down menu to select iDRAC. Provide the target IP address, and use the same IP address for the name. Use the Account Credentials drop-down to select Create New Account, and click Create.
5. Give the account credential a name (we used iDRAC Root). Leave the device type as iDRAC, enter the administrative credentials used to discover this server (We used root / calvin), and click Save.
6. Click Next. You will experience about a 3-minute wait while the device is discovered.
7. To assign the server to a different group, use the drop-down menu or leave the newly discovered server in the default group, and click Finish.
8. Click OK.

Read the report at http://facts.pt/v9fIV4J ▶

This project was commissioned by Dell EMC.