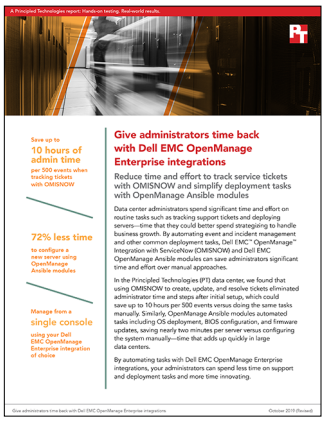

The science behind the report:

Give administrators time back with Dell EMC OpenManage Enterprise integrations

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 Give administrators time back with Dell EMC OpenManage Enterprise integrations.

We concluded our hands-on testing on September 30, 2019. 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 September 30, 2019 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

The tables below present our findings in detail. We consider differences of less than one second to be a tie. Numbers are rounded to their nearest integer, but calculations are based on the unrounded numbers. All tasks are admin time to complete the task after completing initial one-time setup tasks. The recorded time includes only the time for active user input and does not include time waiting for automated processes to complete.

Dell EMC OpenManage Integration with ServiceNow testing

Ticket creation, update, and resolution	Time (seconds)	Steps	Single pane?
OMISNOW	0	0	Yes
Manual (without OMISNOW)	72	21	No
Manual w/ SNMP server (without OMISNOW)	67	19	Yes

OpenManage Ansible modules testing

	Manually (via iDRAC)		Using Ansible modules		Difference		Difference (%)	
Task	Time (seconds)	Steps	Time (seconds)	Steps	Time saved (seconds)	Steps saved	Time saved	Steps saved
Configure iDRAC	9	4	8	2	0	2	3%	50%
Configure BIOS	13	5	9	2	4	3	32%	60%
Configure RAID	34	12	9	2	25	10	73%	83%
Deploy OS	69	15	9	2	60	13	87%	87%
Update firmware	33	7	9	2	25	5	75%	71%
Total per server	158	43	44	10	114	33	72%	77%

System configuration information

The table below presents detailed information on the systems we tested.

Server configuration information	Dell EMC™ PowerEdge™ R740xd (OMISNOW testing)	Dell EMC PowerEdge R740xd (manual testing)
BIOS name and version	Dell 2.3.10	Dell 2.3.10
Non-default BIOS settings	N/A	N/A
Operating system name and version/build number	ESXI 6.7.0 build- 14212230	ESXI 6.7.0 build- 14212230
Date of last OS updates/patches applied	9/30/19	9/30/19
Power management policy	Performance	Performance
Processor		
Number of processors	2	2
Vendor and model	Intel® Xeon® Gold 6130	Intel Xeon Platinum 8170
Core count (per processor)	16	26
Core frequency (GHz)	2.10	2.10
Stepping	4	4
Memory module(s)		
Total memory in system (GB)	64	64
Number of memory modules	4	4
Vendor and model	Hynix® HMA82GR7AFR8N-VK	Hynix HMA82GR7AFR8N-VK
Size (GB)	16	16
Type	DDR4	DDR4
Speed (MHz)	2,666	2,666
Speed running in the server (MHz)	2,666	2,666
Storage controller		
Vendor and model	Dell PERC H730P Mini	Dell PERC H740P
Cache size (GB)	2	2
Firmware version	25.5.5.0005	25.5.5.0005
Driver version	7.708.07.00	7.708.07.00
Local storage		
Number of drives	2	2
Drive vendor and model	Dell THNSF8960CCSE (Toshiba)	Dell THNSF8960CCSE (Toshiba)
Drive size (GB)	960	960
Drive information (interface, type)	SATA SSD	SATA SSD
Network adapter 1		
Vendor and model	QLogic® Corporation QLogic 57800 10 Gigabit Ethernet	QLogic Corporation QLogic 57800 10 Gigabit Ethernet
Number and type of ports	4 x 10GbE	2 x 10GbE

Server configuration information	Dell EMC™ PowerEdge™ R740xd (OMISNOW testing)	Dell EMC PowerEdge R740xd (manual testing)
Network adapter 2		
Vendor and model	Broadcom P225p NetXtreme dual port 10/25 Gigabit Ethernet	QLogic Corporation QLogic 57800 1 Gigabit Ethernet
Number and type of ports	2 x 10/25GbE	2 x 1GbE
Cooling fans		
Vendor and model	Nidec® UltraFlo 4VXP3-X30	Nidec UltraFlo 4VXP3-X30
Number of cooling fans	6	6
Power supplies		
Vendor and model	Dell 0PJMDN	Dell 0PJMDN
Number of power supplies	2	2
Wattage of each (W)	750	750

How we tested

We tested two different Dell EMC solutions:

- Dell EMC OpenManage Integration with ServiceNow
- Dell EMC OpenManage Ansible Modules

We compared each solution to traditional options commonly used by server administrators. We used the following infrastructure to test each solution:

- 2x Dell EMC PowerEdge R740xd servers
- A Dell EMC PowerEdge R730 as an infrastructure host for our VMware vCenter® instance with the following virtual machines:
  - A vCenter Appliance version 6.7.0 build 14070654
  - An Active Directory service hosted on Windows 2016 Datacenter edition
  - A CentOS 6.7 minimal installation for our Ansible installation
  - A Windows 2016 server to be used for the MID server
- A ServiceNow Developer's instance
- An NTP server

For our testing, we measured administrative effort to create, update, and close tickets. For ServiceNow, the MID server acts as a local agent that connects the cloud-hosted ServiceNow instance to your local network. This allows the server to monitor local systems. Managed systems require an OpenManage Integration for ServiceNow license, which we acquired and applied to the target server. We compared ticketing solutions using OpenManage Enterprise, ServiceNow, and OMISNOW, to performing the same tasks with only OpenManage Enterprise and Service Now.

For the second phase of our testing, we measured the administrative effort to complete a series of system configuration tasks versus performing the same tasks through the iDRAC menus. We installed Ansible on the CentOS 6.7 virtual machine along with the OpenManage Ansible Modules. We ran playbooks that completed each task through automated scripts.

Setting up Dell EMC OpenManage Enterprise

Deploying Dell EMC OpenManage Enterprise on VMware vSphere®

1. Download the openmanage_enterprise_ovf_format.zip file from the support site, and extract the file to a location accessible by VMware vSphere™ Client. We recommend using a local drive or CD/DVD, because installing from a network location can take up to 30 minutes.
2. In the vCenter Appliance, right-click the host computer, and select Deploy OVF Template.
3. On the Source page, click Browse, and select the OVF package by selecting the OVF, VMX, and VMDK files. Click Next.
4. On the OVF Template Details page, review the information. Click Next.
5. On the End User License Agreement page, read the license agreement, and click Accept. To continue, click Next.
6. On the Name and Location page, enter a name with up to 80 characters, and select an inventory location where the template will be stored. Click Next.
7. Depending on the vCenter configuration, one of the following options will display:
   - If resource pools are configured: On the Resource Pool page, select the pool of virtual servers to deploy the appliance VM.
   - If resource pools are NOT configured: On the Hosts/Clusters page, select the host or cluster on which you want to deploy the appliance VM.
8. If the host has more than one datastore available, the Datastore page will display them. Select the location to store VM files, and click Next.
9. On the Disk Format page, click Thin provision for storage space efficiency.
10. On the Ready to Complete page, review the options you selected on previous pages. To run the deployment job, click Finish. A completion status window displays where you can track job progress.
11. Start the VM and connect to the Text User Interface (TUI) using either the web console or VMware Remote Console™ (VMRC).
12. Before logging into the TUI, when prompted, accept the EULA. In the Choose keyboard layout screen, if needed, change the keyboard layout.
    - On the Change admin password screen, enter the new password and confirm it. (You must change the password when logging on for the first time.)
    - To select Apply, use the arrow keys or press Tab.
    - When prompted for a confirmation, select Yes, and press Enter.

13. Navigate to Set Networking Parameters, and enter and confirm the admin password.
14. Enable IPv4 and tab down to the static IP. Enter the proper IP, Gateway, Subnet, and DNS information.
15. To enable Register with DNS, press the space bar, and enter the DNS name and DNS Domain name.
16. Tab over, and select Apply.

Configuring OpenManage Enterprise

If you are logging into OpenManage Enterprise for the first time, the Welcome to OpenManage Enterprise page will display, allowing you to set the time (either manually or using NTP time synchronization) and proxy configurations.

1. Select the Use NTP check box.
2. For time synchronization, enter the IP address or hostname in Primary NTP Server Address and Secondary NTP Server Address (optional).
3. To save the settings, click Apply.

Configuring iDRAC SNMP

1. Log into iDRAC for monitored asset.
2. At the top, click Configuration→System Settings.
3. Under Alert Configuration, set Alerts to Enabled, and click Apply.
4. Under Alerts and Remote System Log Configuration, enable any events that need to be monitored, and click Apply.
5. Under SNMP Traps Configuration, enter the MID server address, check the State checkbox, and click Apply.
6. Scroll down to SNMP Settings, configure the following settings, and click Apply:

    - Set Community String to public.
    - Set SNMP Alert Port Number to 162.
    - Set SNMP Trap Format to SNMP v2.

Configuring OpenManage Enterprise Alert Policies

1. Log into the OME console.
2. At the top, click Application Settings→Alerts
3. Under SNMP Configuration, configure the following settings, and click Apply:

    - Check Enabled.
    - Destination Address set to MID server IP.
    - SNMP Version set to SNMP V2.
    - Community String set to public.
    - Port Number set to 162.

4. At the top, click Application Settings→Incoming Alerts.
5. For Community, enter public. For Port, enter 162. Click Apply.
6. At the top, click Alerts→Alert Policies.
7. Click Create.
8. Under Name and Description, configure a name, enter a description, and click Next.
9. Under Category, select iDRAC and any other alerts that need to be monitored, and click Next.
10. Under Target, click Select Devices, select all devices to be monitored, and click OK.
11. Click Next.
12. Under Date and Time, select all days, and click Next.
13. Under Severity, select desired alert severities, and click Next.
14. Under Actions, check SNMP Trap Forwarding, and click Next.
15. Under Summary, click Finish.

Configuring ServiceNow to receive SNMP Traps

1. Log into the ServiceNow console.
2. In the Filter Navigation, search for MID Server.
3. Under MID Server→Extensions, click MID SNMP Trap Listener.
4. At the top, click New.
5. Enter a Name for the listener.
6. Change the UDP port to 162.
7. Click the search icon next to the MID Server box, and select the MID Server.
8. Click Submit.
9. Click the Name of the newly created SNMP Trap Collector.
10. Under Related Links, click Start.

Integrating OMISNOW and OpenManage Enterprise

Installing the MID server

OMISNOW requires a MID server to connect to ServiceNow. We used a Windows 2016 VM.

1. In the ServiceNow console, under MID Server, click Downloads.
2. Select the Windows 64-bit download.
3. Under User Administration, select Users.
4. Click New.
5. Create a new user with a password.
6. Under the Roles list, click Edit.
7. Select the MID server from the list, add it, and save the role.
8. On the target MID server VM, copy the files to the server and extract them. Copy the agent folder to where you'd like to install the program. We used C:\Program Files\MID.
9. In the agent folder, double-click the installer.bat file.
10. For the ServiceNow MID Server Installer, enter the location of your ServiceNow server and the credentials for the created user. Click Test your connection.
11. When Connection tested successfully appears, click Next.
12. Fill out your information, and click Next. (We used OMISNOWmid for our MID server name.)
13. Click Next.
14. Click Start MID Server.
15. Click MID Servers List Page.
16. Click the record for your MID server, and click Validate.

Downloading OpenManage Integration with ServiceNow

1. Browse to dell.com/support.
2. Enter your service tag.
3. Under Drivers & Downloads, for Category, select Systems Management.
4. Download Dell EMC OpenManage Integration Version 1.0 With ServiceNow.
5. Unzip the files.

Activating the Enterprise Management Plugin

1. Sign into the servicenow.com Developer Site for ServiceNow.
2. For your instance, click Action, and click Activate Plugin.
3. Scroll down to Event Management, select Activate, and select Activate Plugin Only.

Adding the Update Set to ServiceNow

1. In the ServiceNow console, under System Update Sets, select Retrieved Update Sets.
2. Click Import Update Set from XML.
3. Click Choose File, and select the Dell_EMC_OpenManage_Integration_1_0_ServiceNow_UpdateSet.xml file.
4. Click Upload.
5. Click the Dell EMC OpenManage Integration Update Set, and click Preview Update Set.
6. Select all errors, and click Accept remote update.
7. Click Commit Update Set.

Adding the JAR file to ServiceNow

1. In the ServiceNow console, under MID server, select JAR files.
2. Click New.
3. Click the Manage Attachments clip icon.
4. Navigate and select Dell_EMC_OpenManage_Integration_1_0_ServiceNow_Connector.jar.
5. In the navigation panel, under MID Server, select Servers.
6. Select the MID server. Under related LINKs, select Restart MID.
7. Wait until the status shows it is working.

Connecting OpenManage and ServiceNow

Creating the OpenManage Enterprise Connection Profile

1. In navigation, under Connection Profiles, select OpenManage Enterprise Connection Profiles.
2. Click New.
3. Enter your information as requested. We used the following:
    - Name: OM Connect
    - OME IP/FQDN: [OME IP]
    - User Name: admin
    - Password: *********
    - MID Server: [Select your added MID server]
4. Click Test Connection.

Setting up SupportAssist Enterprise (SAE)

Deploying OpenManage Enterprise on VMware vSphere

1. Download the OVF file from the support site, and extract the file to a location accessible by the VMware vSphere Client.
2. On the right pane, click Create/Register VM.
3. On the Select creation type page, select Deploy a virtual machine from an OVF or an OVA file, and click Next.
4. On the Select OVF and VMDK files page, select the OVF and VMDK files, and click Next.
5. Enter a name for the virtual machine, and click Next.
6. Select the compute resource, and click Next.
7. Review template details, and click Next.
8. On the License agreements page, click I agree, and click Next.
9. For Disk provisioning, select Thin Provision.
10. Select the location to store the virtual machine, and click Next.
11. Select the correct VM network, and click Next.
12. On the Additional settings page, enter the following details, and click Next.
    - Domain name servers 1 and 2
    - Hostname
    - Default gateway
    - Network IPV4
    - Time zone
    - NTP Server
    - Root password
    - Web Administrator User Name
13. On the Ready to complete page, verify the details displayed, and click Finish.
14. Wait for 10 to 15 minutes before logging into the SupportAssist Enterprise user interface.

Configuring SupportAssist Enterprise

1. Go to https://<SAE IP>:5700/SupportAssist, where <SAE IP> is the IP address of the SupportAssist Enterprise appliance.
2. In the Username box, enter root.
3. Enter the password, and click Sign In.
4. On the License Agreement page, and click Accept.
5. Enter the password for the administrator account, and click Next.

6. Click Login as admin.
7. At Set Up and Configure SupportAssist Enterprise, and click Next.
8. Enter any Proxy settings, and click Next.
9. Enter the access key and PIN displayed when appliance downloaded, and click Next.
10. Update contact information, and click Next.
11. Leave default for Parts Replacement, and click Next.
12. On the Summary page, click Finish.
13. Under Settings, click Preferences.
14. Under SupportAssist Enterprise Application, enable API Interfaces for SupportAssist Enterprise, and click Apply.
15. Under Devices, click Manage Credentials→Credential Profiles.
16. Click Create Profile.
17. Click Add account credentials.
18. Enter a name, select iDRAC for device type, enter the username and password for iDRAC, and click Done.
19. Under Credential profile, check iDRAC, and select the profile.
20. Click Save.
21. Under Extensions, click Manage Adapters.
22. Click Set Up Adapter.
23. For Adapter Type, select OpenManage Enterprise.
24. Enter IP address, User Name, and Password for OME Appliance, and click OK.
25. Verify the adapter connects to and detects devices.

Connecting SupportAssist Enterprise to ServiceNow

1. In the navigation filter, enter Dell EMC OpenManage Integration. Under Connection Profiles, select SupportAssist Enterprise.
2. Click New.
3. Enter a name, IP, user name, and password for the SupportAssist Enterprise console.
4. Select the MID server.
5. Click Test Connection.
6. Click Submit.

Manually creating events in ServiceNow

1. Navigate to Event Management→All Events. To open a form for creating a new event, click New.
2. On the form, fill in the fields manually by copying information from an alert in OpenManage Enterprise.

Note: An IT admin will have to manually find the Alert information and the corresponding Alert Definition from the OpenManage Enterprise console and update the fields in the ServiceNow instance. An IT admin will have to do this for all the critical and warning alerts generated in OpenManage Enterprise.

Tracking tickets

Tracking tickets with OMISNOW

OMISNOW automated each of the following tasks. Because of this, we had no timings or steps to capture for tracking tickets after we set up and linked OMISNOW.

Manually creating and tracking a ticket in ServiceNow

1. Log into the ServiceNow console.
2. In the navigation filter, type New incident. From the Incident menu, select Create New.
3. In a new window, log into the Open Manage Enterprise Console.
4. Select Alerts.
5. Click the target device from the selected alert.
6. Under the device name, select Alerts.
7. Select the target alert, and copy the text from the alert output.
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:
    - Caller
    - Configuration item
    - Contact type
    - Short description

10. Click Submit.
11. To update the ticket, click the Incident Number.
12. Switch to the OME console.
13. Refresh the page, and copy the current status.
14. Switch back to the ServiceNow Console.
15. Under Additional comments, paste the current status, and click Submit.
16. Navigate to the ServiceNow Console.
17. Under Additional comments, paste the current status, and click Submit.
18. To resolve the ticket, click the Incident Number.
19. On the Incident screen, click Resolution information.
20. Select a Resolution note, and for Resolution notes, type `solved`
21. Click Resolved.

Manually creating and tracking a ticket in ServiceNow

After ServiceNow has received the TRAP alert from OME, complete the following steps to create a ticket:

1. Log into the ServiceNow console.
2. In the navigation filter, type `incident`. Right-click New Incident, and select New Window.
3. In the original window, in the navigation filter, type `Event`, and select All events.
4. Select the target event.
5. Copy the description.
6. Return to the ServiceNow New incident screen.
7. Fill out the information and paste the copied text into the short description. We filled out the following:
    - Caller
    - Configuration item
    - Contact type
    - Short description
8. Click Submit.
9. To update the ticket, click the Incident Number.
10. Switch to the OME console.
11. Refresh the page, and copy the current status.
12. Switch to the ServiceNow Console.
13. Under Additional comments, paste the current status, and click Submit.
14. Switch to the ServiceNow Console.
15. Under Additional comments, paste the current status, and click Submit.
16. To resolve the ticket, click the Incident Number.
17. On the Incident screen, click Resolution information.
18. Select a Resolution note, and for Resolution notes, type `solved`
19. Click Resolved.

Enabling the vCenter probe in

1. Log into the target vCenter.
2. Select the vCenter IP.
3. Select Permissions.
4. To add a new user, click the plus sign.
5. Name the user. We used snuser. For role, select read-only. Select Propagate to children, and click OK.
6. In the ServiceNow console, search for credentials.
7. Navigate to Discovery, and select Credentials.
8. Click New.
9. Select VMware Credentials.
10. For name, enter `snuser`. For username, enter `vsphere.local\snuser` and the appropriate password. Click submit.
11. Under Discovery, select Discovery Schedules.
12. Click Quick Discovery.
13. Enter the vCenter ID, and select the MID server. Click OK.

Discovery will run and begin logging events for vCenter.

Setting up the OpenManage Ansible modules

Installing the Dell EMC repository

We created a shared file to host a Dell EMC repository of firmware updates for our target Dell EMC PowerEdge R740xd.

1. On the Windows server used for the MID, create a Shared folder accessible to the CentOS VM's root user. We named ours \[fileserver]\share.
2. Install the Dell EMC Repository Manager v3.2, accepting all defaults from https://www.dell.com/support/driver/us/en/04/DriversDetails?driverid=57CX7.
3. Open the Dell EMC Repository Manager.
4. Click Add Repository.
5. In the Add Repository Window, name the repository R740xd. For Base Catalog, select the 19.09.01 catalog. Click Integration, and select iDRAC.
6. In the iDRAC menu, enter the hostname for the target server. Enter the appropriate username and password for the target server. Click Connect.
7. Select all DUP formats, and click Add.
8. Check the box next to the R740xd repository, and click Export.
9. For the Deployment Tool Type, leave the default (Share) selected. For the location, choose Browse, select the shared folder described above, and click Open.
10. Click Export.
11. Verify the access to the file at \[fileserver]\share\r740xd_1.00_Catalog.xml.
12. Place a customized ESXI installation file (.iso) in the share.

Configuring the Ansible virtual machine

We ran the following commands to install Ansible, the OpenManage SDK, and Open Manage Ansible modules.

To disable selinux and firewalld:

```
$ pip3 install ansible
$ systemctl disable firewalld
$ systemctl stop firewalld
$ setenforce 0
$ sed -i 's/SELINUX=enforcing/SELINUX=disabled/' /etc/selinux/config
```

To install Ansible:

```
$ pip3 install ansible
$ pip3 install wheel
```

To install omsdk:

```
$ git clone https://github.com/dell/omsdk.git
$ cd omsdk
$ sh build.sh 1.2 379
$ cd dist
$ pip install omsdk-1.2.379-py2.py3-none-any.wh
```

To install OpenManage Ansible modules:

```
$ git clone https://github.com/dell/dellemc-openmanage-ansible-modules.git
$ cd dellemc-openmanage-ansible-modules
$ python install.py
```

To mount the shared repository:

```
$  sudo mount -t cifs \\\\[fileserver]\\share -o username=user,password=Password,dir_mode=0777,file_
mode=0666 /mnt/dellshare/
```

Creating the inventory and playbook files

Create the following files on the ansible server under the directory/playbooks/Inventory.yml:

```
all:
  hosts:
  vars:
  children:
    PowerEdge:
      hosts:
        r740xd_host:
          idrac_ip: X.X.X.X
      vars:
        idrac_user: root
        idrac_password: Password
        idrac_port: 443
      children:
```

ConfigureiDRAC.yml

```
---
- hosts: PowerEdge
  connection: local
  gather_facts: false

  tasks:
  - name: Change NTP
    dellemc_configure_idrac_timezone:
      idrac_ip: "{{ idrac_ip }}"
      idrac_user: "{{ idrac_user }}"
      idrac_pwd: "{{ idrac_pwd }}"
      share_mnt: "/mnt/dellshare/"
      share_name: "\\\\[fileserver]\\share\\"
      setup_idrac_timezone: "America/New_York"
      enable_ntp: Enabled
      ntp_server_1: "[ntp_server]"
```

ConfigureBIOS.yml

```
---
- hosts: PowerEdge
  connection: local
  gather_facts: False

  tasks:
  - name: Configure Bios Generic Attributes
    dellemc_configure_bios:
      idrac_ip: "{{ idrac_ip }}"
      idrac_user: "{{ idrac_user }}"
      idrac_pwd: "{{ idrac_pwd }}"
      attributes:
        SysProfile : "PerfOptimized"
```

ConfigureRAID.yml

```
---
- hosts: PowerEdge
  connection: local
  name: iDRAC storage volume configuration.
  gather_facts: False

  tasks:
  - name: Create single volume.
    dellemc_idrac_storage_volume:
      idrac_ip:    "{{ idrac_ip }}"
      idrac_user:  "{{ idrac_user }}"
      idrac_pwd:   "{{ idrac_pwd }}"
      state: "create"
      # To determine the appropriate storage controller name, run the following command:
      # curl -k -s https://user:password@[R740xd]/redfish/v1/Systems/System.Embedded.1/Storage   |
python -m json.tool
      controller_id: "RAID.Slot.4-1"
      media_type: "SSD"
      protocol: "SATA"
      raid_reset_config: "False"
      volume_type: "RAID 0"
      capacity: 100
      volumes:
        - name: "Volume1"
          drives:
           location: [1]
```

DeployOS.yml

```
---
- hosts: PowerEdge
  connection: local
  gather_facts: False

  tasks:
  - name: "Boot to Network ISO"
    dellemc_boot_to_network_iso:
      idrac_ip:   "{{ idrac_ip }}"
      idrac_user: "{{ idrac_user }}"
      idrac_pwd:  "{{ idrac_pwd }}"
      share_name: "\\\\[fileserver]\\share\\"
      iso_image:  "esxi.iso"
    tags:
      - network_iso
```

FirmwareUpdate.yml

```
---
- hosts: PowerEdge
  connection: local
  gather_facts: False

  tasks:
  - name: Update firmware from repository on a Network Share
    idrac_firmware:
      idrac_ip: "{{ idrac_ip }}"
      idrac_user: "{{ idrac_user }}"
      idrac_password: "{{ idrac_password }}"
      share_mnt: "{{ local_share }}"
      #Target the Windows SMB (cifs) setup above.
      share_name: "\\\\[fileserver]\\share\\"
      reboot: "True"
      job_wait: "True"
      catalog_file_name: "r740xd_1.00_Catalog.xml"
      share_user: "user"
      share_password: "Password"
```

System configuration using OpenManage Ansible modules

We timed the following tasks.

Running the Ansible module to configure iDRAC

1. In the Ansible console, navigate to the Playbook folder:
   - $ cd /playbook/
2. Run the Playbook using the following command:
   - $ ansible-playbook -vvvv ConfigureiDRAC.yml -i inventory.yml

Running the Ansible module to configure the BIOS

1. In the Ansible console, navigate to the Playbook folder:
   - $ cd /playbook/
2. Run the Playbook using the following command:
   - $ ansible-playbook -vvvv ConfigureBIOS.yml -i inventory.yml

Running the Ansible module to configure the RAID

1. In the Ansible console, navigate to the Playbook folder:
   - $ cd /playbook/
2. Run the Playbook using the following command:
   - $ ansible-playbook -vvvv ConfigureRAID.yml -i inventory.yml

Running the Ansible module to deploy the OS

1. In the Ansible console, navigate to the Playbook folder:
   - $ cd /playbook/
2. Run the Playbook using the following command:
   - $ ansible-playbook -vvvv DeployOS.yml -i inventory.yml

Running the Ansible module to update the firmware

1. In the Ansible console, navigate to the Playbook folder:
    - $ cd /playbook/
2. Run the Playbook using the following command:
    - $ ansible-playbook -vvvv FirmwareUpdate.yml -i inventory.yml

System configuration manually using iDRAC

We timed the following tasks.

Configuring iDRAC

1. In the Integrated Dell Remote Access Controller, click iDRAC Settings.
2. Click Settings.
3. Under Time Zone and NTP Settings, in the NTP Server 1 text box, enter the NTP Server IP.
4. Click Apply.

Configuring the BIOS

1. In the Integrated Dell Remote Access Controller, click Configuration.
2. Under Configuration, click BIOS Settings. Click System Profile Settings.
3. In the System Profile drop-down box, select Performance.
4. Click Apply.

Configuring the RAID

1. In the Integrated Dell Remote Access Controller, click Configuration.
2. Under Configuration, click Storage Configuration.
3. In the Controller drop-down box, select the correct controller.
4. Select Virtual Disk Configuration.
5. Click Create Virtual Disk.
6. Input a name for the virtual disk.
7. Select RAID layout.
8. Input the capacity for the virtual disk.
9. Select physical disks you are using for the virtual disk.
10. Click Add to Pending Operations.
11. Click Close Now.
12. Click Apply Now.

Deploying the OS

1. In the Integrated Dell Remote Access Controller, to open the console, click Launch Virtual Console.
2. Click Virtual Media.
3. Click Choose File, and select the OS image that will be used.
4. Click Map Device.
5. Click Close.
6. Click Boot→Virtual CD/DVD/ISO.
7. To confirm Boot Action, click Yes.
8. Click Power→Reset System (warm boot).
9. On the Confirm Power Action screen, click Yes.
10. At the Installation starting screen, press Enter.
11. To accept and continue, press F11.
12. Select the drive that the OS will be installed to, and press Enter.
13. Select Keyboard layout, and press Enter.
14. Input Password, and press Enter.
15. To install, press F11.

Updating the firmware

1. In the Integrated Dell Remote Access Controller, click Maintenance.
2. Under Maintenance, click System Update.
3. Under Manual Update, click the drop-down box next to Location Type, and select FTP.
4. In the FTP Address text box, input `ftp.dell.com`
5. Click Check for Update.
6. Select all updates that you wish to install.
7. Click Install and Reboot.

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

This project was commissioned by Dell EMC.

Principled Technologies®

Facts matter.®