

The science behind the report:

# Reduce hands-on deployment times to near zero with iDRAC9 automation

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 [Reduce hands-on deployment times to near zero with iDRAC9 automation](#).

We concluded our hands-on testing on November 27, 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 November 18, 2019 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

## Our results

The table below presents our findings in detail. Please note that organizations can order new Dell EMC PowerEdge servers with Zero-Touch provisioning already enabled, which would eliminate all steps and time to complete these tasks.

Time to provision	One-time setup (mm:ss)	Single server (mm:ss)	10 servers (hh:mm:ss)	50 servers (d:hh:mm:ss)
Manual attended	N/A	30:50	05:08:20	1:01:41:40
Manual unattended	N/A	21:54	-	-
Manual total	N/A	52:44	-	-
Automated with iDRAC9 v4.00.00.00 attended	25:44	00:16	00:02:40	0:00:13:20
Automated with iDRAC9 v4.00.00.00 unattended	00:00	31:17	-	-
Automated with iDRAC9 v4.00.00.00 total	25:44	31:33	-	-

Note: We did not extrapolate the unattended times because the times would not scale linearly as the attended times do. An admin would configure each system and allow the OS to install automatically, so many OS installations would happen in parallel.

Number of steps to provision	Single server	10 servers	50 servers
Provision a server manually	40	400	2,000
One-time setup for automated provisioning	47	N/A	N/A
Automated provisioning with iDRAC9 v4.00.00.00	4	40	200

## System configuration information

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

Server configuration information	Dell EMC™ PowerEdge™ R640
BIOS name and version	Dell 2.3.10
Non-default BIOS settings	N/A
Operating system name and version/build number	N/A
Date of last OS updates/patches applied	November 22, 2019
Power management policy	Default
Processor	
Number of processors	2
Vendor and model	Intel® Xeon® Silver 4114
Core count (per processor)	10
Core frequency (GHz)	2.20
Stepping	U0
Memory module(s)	
Total memory in system (GB)	64
Number of memory modules	4
Vendor and model	Hynix® HMA82GR7CJR8N-VK
Size (GB)	16
Type	DDR4
Speed (MHz)	2,400
Speed running in the server (MHz)	2,400
Storage controller	
Vendor and model	Dell PERC H740P Mini
Cache size (GB)	2
Firmware version	50.5.1.-2818
Local storage	
Number of drives	2
Drive vendor and model	Dell AL15SEB060NY (KIOXIA)
Drive size (GB)	600
Drive information (speed, interface, type)	10k SAS 12.0 HDD
Network adapter	
Vendor and model	Broadcom® Adv Dual 10GBASE-T Ethernet
Number and type of ports	4 x 10GbE
Firmware version	21.40.25.31

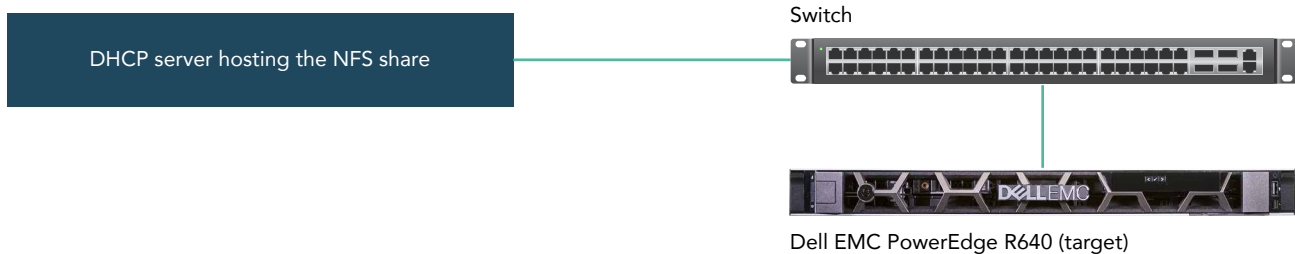
Server configuration information	Dell EMC™ PowerEdge™ R640
Cooling fans	
Vendor and model	Nidec® UltraFlo 4VXP3-X30
Number of cooling fans	8
Power supplies	
Vendor and model	Dell 0PJMDNA01
Number of power supplies	2
Wattage of each (W)	750

## How we tested

Here, we provide the steps required to enable and execute Zero-Touch provisioning of Dell EMC PowerEdge servers with iDRAC9 v4.00.00.00. (Note that Zero-Touch provisioning requires that you have either the Enterprise or Datacenter license for iDRAC9.) We compare the time it takes to change some BIOS settings, create a RAID, and deploy Microsoft Windows Server 2019 manually to the time it takes to do those tasks automatically via iDRAC.

Zero-Touch provisioning via Server Configuration Profile (SCP) requires an environment that includes a DHCP server, a network file share, and a Windows Server 2019 ISO with the \boot\bootfix.bin file removed to prevent the “press any key to boot” option. For this study, we assumed this environment already exists in an organization’s IT infrastructure, so we did not include the time and steps to create or obtain them. We did, however, include time and steps for any modifications to the DHCP and file share necessary for the automation task.

We used NFS for our network file share and outlined the steps and time required to modify the DHCP, create the SCP, and run the automated installation. Admins must perform these one-time tasks to enable one-touch provisioning. After completing these tasks, admins can quickly and easily provision additional servers as needed. To perform the OS deployment, the automation process requires an unattend.xml or answer file for the SCP to call. Many companies will already have this file, and there is more than one way to create one. Because of this, we included the steps to create the file for reference but did not include the time or number of steps for the iDRAC automation. We recorded time and steps for completing these tasks manually.



## Manual configuration and OS deployment steps

### Configuring the manually installed server

We configured a Dell EMC PowerEdge R640 with the following settings to build a manually installed server:

1. Log into the iDRAC console.
2. Open the Virtual Console.
3. Power on the server.
4. To enter the Lifecycle Controller when the prompt appears, press F10.
5. In the Lifecycle Controller, select System Setup.
6. Navigate to Advanced Hardware Configuration → Device Settings → Integrated RAID Controller.
7. Navigate to Main Menu → Configuration management → Create Virtual disk, and configure the following:
  - Select RAID Level: RAID1
  - Select Physical Disks From: Unconfigured Capacity
  - Select Physical Disks: (Select 2 disks, click Apply Changes, and click OK.)
  - Virtual Disk Name: OS
  - Virtual Disk Size: (Use maximum.)
  - Strip Element Size: 256
  - Read Policy: Read Ahead
  - Write Policy: Write Back
  - Disk Cache: Default
  - Default Initialization: No
8. Click Create Virtual Disk.
9. Check Confirm, and click Yes.
10. Click OK, and click Back until you return to the RAID controller’s Main Menu.
11. Click Controller Management, and to reflect the newly created RAID1 Drive, change Select Boot Device.
12. Click Back twice, and click Finish.

13. Click Finish until you return to the LC main menu, and click Exit.
14. To enter the Lifecycle Controller when the prompt appears, press F10.
15. In the iDRAC menu, click Configuration, and click BIOS Settings. Change the following settings, clicking Apply after each change:
  - Memory Settings→Memory Operating Mode
    - Change to Mirror Mode
  - Boot Settings→Hard -Disk Drive Placeholder
    - Change to Enabled
  - Boot Settings→Set Boot Order Enable
    - Change to RAID.Integrated.1-1
  - Integrated Devices→Internal USB Port
    - Change to Off
  - Integrated Devices→iDRAC Direct USB Port
    - Change to Off
  - System Profile Settings→System Profile
    - Change to Performance
16. From the Virtual Console, power off the system.
17. In the iDRAC, at the bottom of the BIOS Setup page, click Apply and Reboot.
18. The system will reboot multiple times. To view the progress, click Job Queue or view the Virtual Console.
19. At the top of the window in the Virtual Console, click Virtual Media.
20. Under Map CD/DVD, click Choose File browse to your ISO, and click Open.
21. Click Map Device, click Close, and reboot the system.
22. To enter the Lifecycle Controller when the prompt appears, press F10.
23. Click OS Deployment.
24. Select Go Directly to OS Deployment, and click Next.
25. Select the following, and click Next:
  - **Boot Mode:** UEFI
  - **Secure Boot:** Disabled
  - **Secure Boot Policy:** Standard
  - **Available Operating Systems:** Microsoft Windows Server 2019
26. Check Manual Install, and click Next.
27. In the Select Media drop-down, select your ISO File, and click Next.
28. To reboot the system, click Finish.
29. In the Windows Setup window, select your Language, Time and Keyboard, and click Next.
30. Click Install Now.
31. Enter the license key, and click Next.
32. Select Windows Server 2019 Datacenter (Desktop Experience), and click Next.
33. Accept the license terms, and click Next.
34. Select Custom: Install Windows only (advanced).
35. Select the drive to install the OS on, and click Next.
36. Use the maximum size, and click Apply.
37. In the popup window, click OK.
38. To begin OS installation, click Next.
39. Allow the OS to complete installation, and boot to the initial login screen.

## One-time configuration for automated process with iDRAC9

### Configuring the initial server

We configured a Dell EMC PowerEdge R640 with the following settings to use as the template for the SCP XML file that iDRAC uses to provision additional servers:

1. Log into the iDRAC console.
2. Open the Virtual Console.
3. Power on the server.
4. To enter the Lifecycle Controller when the prompt appears, press F10.
5. In the Lifecycle Controller, select System Setup.
6. Navigate to Advanced Hardware Configuration→Device Settings→Integrated RAID Controller.
7. Navigate to Main Menu→Configuration management→Create Virtual disk, and configure the following:
  - Select RAID Level: RAID1
  - Select Physical Disks From: Unconfigured Capacity
  - Select Physical Disks: (Select 2 disks, click Apply Changes, and click OK.)
  - Virtual Disk Name: OS
  - Virtual Disk Size: (Use maximum)
  - Strip Element Size: 256
  - Read Policy: Read Ahead
  - Write Policy: Write Back
  - Disk Cache: Default
  - Default Initialization: No
8. Click Create Virtual Disk.
9. Check Confirm, and click Yes.
10. Click OK, and click Back until you return to the RAID controller's Main Menu.
11. Click Controller Management, and to reflect the newly created RAID1 drive, change Select Boot Device.
12. Click Back twice, and click Finish.
13. Click Finish until you return to the LC main menu, and click Exit.
14. To enter the Lifecycle Controller when the prompt appears, press F10.
15. In the iDRAC menu, click Configuration, and click BIOS Settings.
16. Change the following settings, clicking Apply after each change:
  - Memory Settings→Memory Operating Mode
    - Change to Mirror Mode
  - Boot Settings→Hard -Disk Drive Placeholder
    - Change to Enabled
  - Boot Settings→Set Boot Order Enable
    - Change to RAID.Integrated.1-1
  - Integrated Devices→Internal USB Port
    - Change to Off
  - Integrated Devices→iDRAC Direct USB Port
    - Change to Off
  - System Profile Settings→System Profile
    - Change to Performance
17. From the Virtual Console, power off the system.
18. In the iDRAC, at the bottom of the BIOS Setup page, click Apply and Reboot.
19. The system will reboot multiple times. To view the progress, click Job Queue or view the Virtual Console.

## Creating the SCP configuration file

According to a representative from Dell Technologies, the Server Configuration Profile (SCP) is an iDRAC feature that allows you to configure server hardware, install firmware updates using a network repository and provision an OS image using a simple XML or JSON formatted file. Users can import and export an SCP from a local management station or from a Network Share via CIFS, NFS, HTTP or HTTPS. Zero-Touch provisioning leverages DHCP to not only provide an iDRAC IP address but also the location of an SCP file to use in bare-metal provisioning of a server. iDRAC uses the SCP information to automatically apply detected server configurations changes (iDRAC, BIOS, NICs, RAID, etc), then uses a network repository to locate, apply Dell firmware update packages (DUPs), and lastly, perform OS installation if necessary. Using SCP in this way enables automated, plug-and-play provisioning of servers without complex scripting or PXE booting.

You can learn more about SCP by reading the following Dell documentation: [https://downloads.dell.com/solutions/dell-management-solution-resources/Server%20Cloning%20with%20Server%20Configuration%20Profiles%201\\_1%20Final.pdf](https://downloads.dell.com/solutions/dell-management-solution-resources/Server%20Cloning%20with%20Server%20Configuration%20Profiles%201_1%20Final.pdf).

We created the configuration file by performing the following steps on a Dell EMC PowerEdge R640:

1. Log into the iDRAC console.
2. Click Configuration.
3. Click Server Configuration Profile.
4. Expand Export.
5. Select the following:
  - Location Type: Network Share
  - File Name: system\_config.xml
  - Protocol: NFS
  - IP Address: 192.168.0.10
  - Share Name: NFS\_Share
  - Export Components: All
  - Export Type: Clone
  - Export File Format: XML
6. Click Export.
7. A pop-up window shows that the job has started. To monitor the job, click Job Queue.
8. Log into the file server and edit the system-config.xml file with the following changes and additions:

- Change the following under the Component FQDD="Disk.Virtual.0:RAID.Integrated.1-1" section:

```
<Attribute Name="Size">0</Attribute>
```

- Change or verify the following under the Component FQDD="BIOS.Setup.1-1" section:

```
<Attribute Name="UefiBootSeq">RAID.Integrated.1-1</Attribute>  
<Attribute Name="HddPlaceholder">Enabled</Attribute>
```

- To set up the OS installation information, add the following to the system-config.xml file:

```
<Component FQDD="LifecycleController.Embedded.1">  
<!-- <Attribute Name="OSD.1#SupportedOSList">Microsoft Windows Server 2016, Microsoft Windows Server  
2012 R2, Microsoft Windows Server 2019, Red Hat Enterprise Linux 8.0 x64, Red Hat Enterprise Linux  
7.6 x64, SuSE Enterprise Linux 15 x64</Attribute> -->  
<Attribute Name="OSD.1#OSName">Microsoft Windows Server 2019</Attribute>  
<Attribute Name="OSD.1#OSMediaShareIP">192.168.0.10</Attribute>  
<Attribute Name="OSD.1#OSMediaShareName">NFS_Share</Attribute>  
<Attribute Name="OSD.1#OSMediaShareUsername"></Attribute>  
<Attribute Name="OSD.1#OSMediaSharePassword"></Attribute>  
<Attribute Name="OSD.1#OSMediaShareDomainName"></Attribute>  
<Attribute Name="OSD.1#OSMediaShareType">NFS</Attribute>  
<Attribute Name="OSD.1#OSMediaName">Win2019DC.iso</Attribute>  
<Attribute Name="OSD.1#AnswerFileName">autounattend.xml</Attribute>  
<Attribute Name="OSD.1#ExposeDuration">3600</Attribute>  
<Attribute Name="OSD.1#OSMediaHashType"></Attribute>  
<Attribute Name="OSD.1#OSMediaHashValue"></Attribute>  
</Component>
```

9. Save the file, and power off the server.

## Configuring options 43 and 60 on the DHCP server

1. Log into the DHCP server.
2. Click Start→Administrative Tools→DHCP.
3. Navigate to <server>→IPv4→Scope <ip> General Scope→Scope Options.
4. Right-click Scope Options, and select Configure Options.
5. In the popup, check the box for 043 Vendor Specific Info.
6. Inside the Data Entry location, enter the IP address of your DHCP server in the ASCII column, and click OK.
7. Navigate to <server>→IPv4.
8. Right-click IPv4, and select Define Vendor Classes.
9. In the popup window, click Add, and edit the following information:
  - **Display name:** iDRAC
  - **Description:** Vendor Class
  - **ASCII:** iDRAC
10. Click OK, and click Close.
11. Right-click IPv4, and select Set Predefined Options.
12. In the popup, use the Option Class drop-down to select iDRAC, and click Add.
13. In the Option Type popup, enter the following, and click OK:
  - **Name:** iDRAC
  - **Data Type:** String
  - **Code:** 60
14. Navigate to <server>→IPv4→Scope <ip> General Scope→Scope Options.
15. Right-click Scope Options, and select Configure Options.
16. Click the Advanced Tab, and from the Vendor Class drop-down menu, select iDRAC.
17. Under the Available Options column, select -060 iDRAC.
18. Under the Data Entry section, enter the String Value to be used. This must include the Answer file name, file server IP, and share name. Click apply, and click OK. For our testing, we used the following:

```
-f system_config.xml -i 192.168.0.10 -n /nfs_share -s 0 -d 1
```
19. Click OK, exit DHCP, and log out of the DHCP server.

## Installing the configuration and OS via auto config with DHCP provisioning

To automatically provision the BIOS and RAID settings and deploy the OS via iDRAC, we performed the following on a Dell EMC PowerEdge R640 server:

1. Log into iDRAC.
2. Click iDRAC Settings.
3. Click Connectivity.
4. Expand Network→Auto Config, and select Enable Once in the DHCP Provisioning drop-down menu. Click Apply.

To monitor the job's progress, click Maintenance , and click Job Queue, or watch progress via the Virtual Console. The system will boot into the Lifecycle Controller and reboot several times while running tasks from the Automated Task Application screen.



## Non-timed steps for assumed existing infrastructure

### Creating the Windows autounattend.xml file

We did not include this segment in our time and steps to create the environment for the automated provisioning because we assumed organizations already have this infrastructure in place. These steps are supplied for reference only.

1. Log into the Windows 10 VM.
2. At the following location, download the Windows ADK for Windows 10, version 1903:
  - <https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install>
  - Click Download the Windows ADK for Windows 10, version 1903.
3. Double-click adksetup.exe, and click Run.
4. Select Install the Windows Assessment and Development Kit - Windows 10 to this computer, using the default path "C:\Program Files (x86)\Windows Kits\10\". Click Next.
5. On the Windows Kits Privacy screen, select No, and click Next.
6. Accept the License Agreement.
7. On Select the features you want to install, keep the default selections, click Install, and click Close.
8. At the following location, download the Windows PE add-on for the ADK:
  - <https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install>
  - Click Download the Windows PE add-on for the ADK.
9. Double-click adkwipesetup.exe.
10. Select Install the Windows Assessment and Development Kit Preinstallation Environment Add-ons - Windows 10 to this computer, using the default path "C:\Program Files (x86)\Windows Kits\10\". Click Next.
11. On the Windows Kits Privacy screen, select No, and click Next.
12. Accept the License Agreement, and click Next.
13. On Select the features you want to install, keep the default selections, and click Install.
14. At the following location, download the Windows System Image Manager (WSIM) patch for 64-bit systems:
  - <https://go.microsoft.com/fwlink/?linkid=2095334>
15. Unzip WSIM1903.zip.
16. To install the WSIM patch from an elevated command line shell, browse to the unzipped contents folder, and execute UpdateSIM.bat.
17. Reboot the VM.
18. Create the folder C:\IOS\_Build\ISO\_Extracted.
19. Mount and extract Windows Server installation ISO, and copy contents to C:\IOS\_Build\ISO\_Extracted.
20. From the Start Menu, Launch Windows System Image Manager.
21. Click File, and click Select Windows Image.
22. Browse to C:\IOS\_Build\ISO\_Extracted\sources, select install.wim, and click Open.
23. Select Windows Server 2019 SERVERDATACENTER, and click OK.
24. To create a catalog file, click Yes. This will take several minutes.
25. Click File, and click New Answer File.
26. In the Windows Image section, perform the following:
  - Right-click amd64\_Microsoft-Windows-International-Core-WinPE\_\_neutral, and select Add Setting to Pass 1 windowsPE.
  - Right-click amd64\_Microsoft-Windows-Setup\_\_neutral, and select Add Setting to Pass 1 windowsPE.
27. In the Answer File section, modify the following:
  - amd64\_Microsoft-Windows-International-Core-WinPE\_\_neutral→SetUILanguage
    - Change WillShowUI to Never.
  - amd64\_Microsoft-Windows-Setup\_\_neutral→Disk Configuration
    - Expand amd64\_Microsoft-Windows-Setup\_\_neutral→Disk Configuration.
    - Click Disk Configuration, and change WillShowUI to Never.
    - In the Disk Properties section, modify the Disk ID to 0 and WillWipeDisk to true.
    - Expand Disk, right-click CreatePartitions, and click Insert new CreatePartition.
    - Repeat twice more.
    - Modify the three new CreatePartition entries as follows:

- ◆ Order = 1, Size = 260, Type = EFI
- ◆ Order = 2, Size = 16, Type = MSR
- ◆ Order = 3, Size = 20000, Type = Primary
- Expand Disk, right-click ModifyPartitions, and click Insert new ModifyPartition.
- Repeat once more.
- Modify the two new ModifyPartition entries as follows:
  - ◆ Order = 1, PartitionID = 1, Format = FAT32, Label = System
  - ◆ Order = 2, PartitionID = 3, Format = NTFS, Label = OS, Letter = C, Extend = true
- amd64\_Microsoft-Windows-Setup\_\_neutral→ImageInstall
  - Navigate to OSImage→Install From.
  - Right-click Install From, and select Insert New Metadata.
  - Click MetaData.
  - In the MetaData Properties section, modify the following:
    - ◆ Key = /IMAGE/NAME , Value = Windows Server 2019 SERVERDATACENTER
    - ◆ Navigate to Install To, and change the following in the InstallTo Properties section:
      - ◆ Disk ID = 0 , PartitionID = 3
- amd64\_Microsoft-Windows-Setup\_\_neutral→Userdata
  - Change AcceptEULA to true.
  - Select ProductKey, add your key, and change WillShowUI to Never.

28. In the Answer File, remove residual stale entries.
29. Click Tools, and to make sure there are no errors, click Validate Answer File.
30. Save Answer file as autounattend.xml.
31. Copy autounattend.xml to your NFS Share.
32. Copy the Windows Server ISO to your NFS Share.

Read the report at <http://facts.pt/j9tim6z> ▶

This project was commissioned by Dell EMC.



Facts matter.®

Principled Technologies is a registered trademark of Principled Technologies, Inc.  
All other product names are the trademarks of their respective owners.

**DISCLAIMER OF WARRANTIES; LIMITATION OF LIABILITY:**

Principled Technologies, Inc. has made reasonable efforts to ensure the accuracy and validity of its testing, however, Principled Technologies, Inc. specifically disclaims any warranty, expressed or implied, relating to the test results and analysis, their accuracy, completeness or quality, including any implied warranty of fitness for any particular purpose. All persons or entities relying on the results of any testing do so at their own risk, and agree that Principled Technologies, Inc., its employees and its subcontractors shall have no liability whatsoever from any claim of loss or damage on account of any alleged error or defect in any testing procedure or result.

In no event shall Principled Technologies, Inc. be liable for indirect, special, incidental, or consequential damages in connection with its testing, even if advised of the possibility of such damages. In no event shall Principled Technologies, Inc.'s liability, including for direct damages, exceed the amounts paid in connection with Principled Technologies, Inc.'s testing. Customer's sole and exclusive remedies are as set forth herein.