Technical Research Report

PROWESS

Reduce Server Downtime with Dell™ Rebootless Firmware Update for Single or Multiple Drives in Parallel

Prowess Consulting evaluated the Integrated Dell™ Remote Access Controller 9 (iDRAC9) sideband direct rebootless and parallel firmware update capabilities on Dell™ PowerEdge™ servers and analyzed their effects on server maintenance cycles and IT staff productivity.

Executive Summary

Server components like NVM Express® (NVMe®) drives require updates to firmware in the same way that the server operating systems require updates. Traditional firmware updates require a server to be rebooted, which means that the server must be taken out of service for a period of time. Organizations that rely heavily on their on-premises server environments cannot afford downtime for their critical business operations. To achieve higher uptime, maintenance windows must be smaller, which can make scheduling downtime for server firmware updates difficult.

Rebootless and parallel firmware updates help organizations avoid server downtime. Rebootless firmware updates to components such as NVMe drives and backplanes allow a server and its workloads to continue to run while the updates are applied and completed. Parallel firmware updates allow identical components, such as multiple NVMe drives, to be updated simultaneously instead of one at a time.

When servers do not need to be pulled from service to apply firmware updates, or when multiple NVMe drives can be updated in parallel, time and cost savings across large server deployments can quickly add up. Prowess Consulting conducted benchmarking tests to determine the potential time savings that can result from conducting a rebootless firmware update on a single NVMe drive and conducting rebootless firmware updates on multiple NVMe drives in parallel using Integrated Dell™ Remote Access Controller 9 (iDRAC9).

This technical research report details the findings of our testing and provides an analysis of how rebootless firmware updates and parallel firmware updates can benefit server deployments of any size.

Introduction

Organizations require higher uptime service-level agreements (SLAs) and more flexibility from their on-premises server deployments than ever before. These SLAs require servers to run for extended periods of time with shorter scheduled maintenance windows for critical operating system (OS) and hardware firmware updates. For example, an uptime of 99.99 percent for an individual server allows only 52 minutes of downtime per year. Shorter maintenance windows mean that IT infrastructure and operations teams have fewer opportunities to pull server hardware out of service for time-consuming and sometimes complex firmware updates that require reboots. This pressure to shrink maintenance windows makes it harder to apply critical firmware updates, including those related to security.

Keeping firmware up to date is an important part of any security and maintenance strategy. Firmware updates can enhance feature functionality and provide bug fixes, but more importantly, they can address security issues. Firmware attacks are one of the stealthiest methods by which an attacker can compromise devices at scale. But firmware security is often overlooked because of the downtime required for a reboot, the time required for IT staff to stay on top of firmware updates, and a fear that firmware updates could break business applications.

iDRAC9, an out-of-band management platform for Dell™ servers, provides the ability to apply firmware updates to multiple server components without having to reboot the server, and to apply updates to identical components in parallel. This approach, which uses the iDRAC9 sideband update capability, by which iDRAC9 communicates directly with hardware components, has the potential to drastically reduce both downtime and the amount of time required for IT staff to perform firmware updates.

Research Overview

To determine the potential savings from rebootless firmware updates, Prowess Consulting engineers ran firmware update tests on NVMe drives and a Dell Technologies universal backplane using the iDRAC9 rebootless firmware update method. We measured the amount of time and effort required for the rebootless firmware update to complete and then measured the time required for a server reboot. We used these values to determine the effect that rebootless firmware updates can have on server downtime and IT staff productivity.

To measure the impact of parallel firmware updates, our engineers also measured the time and effort required to update a single NVMe drive on a previous-generation Dell server using the reboot-required firmware update method, and we then measured the time and effort required to update 10 NVMe drives in parallel using the same reboot-required firmware update method. We used these values to measure the time savings generated by updating components in parallel.

iDRAC9 Overview

iDRAC9 is a baseboard management controller (BMC) built into all Dell™ PowerEdge™ servers. This controller allows administrators to monitor, manage, update, troubleshoot, and remediate Dell servers out-of-band over a network from any location, and without the use of agents. iDRAC9 uses sideband direct communication to directly interact with server components without the need to involve agents or the server's OS. iDRAC9 consists of both hardware and software that provide extensive features compared to a basic BMC.

By giving administrators the ability to manage servers remotely, iDRAC9 provides a number of benefits:

- **Increased availability:** Administrators can receive early alerts of failures that can help prevent server downtime. Early alerts can also help administrators pinpoint problem areas that require repair, which can reduce recovery time.
- **Lower total cost of ownership (TCO):** Simplified remote management of larger numbers of servers means that IT staff can be more efficient, which reduces operational costs and travel time.
- **Security:** iDRAC9 provides a secure environment in which administrators can manage server functions, which helps maintain a stronger overall network and server security model.
- **Enhanced embedded management through iDRAC9:** iDRAC9 provides a user interface (UI) for performing management tasks such as server configuration, deployment, update management, maintenance, and diagnosis.

Dell Technologies has tools that help identify and gather update packages for deployment. If you are using Dell™ OpenManage™ Enterprise, you can use the free Update Manager plugin to automate the identification, gathering, and staging of update packages. If you are not using OpenManage Enterprise, Dell Technologies provides Dell™ Repository Manager (DRM), which is a free application that assists with the identification, gathering, and notification of update packages. DRM has an option for reading the inventory of most Dell tools, such as OpenManage Integration with VMware, Microsoft® System Center, Windows® Admin Center, and iDRAC9, so that only the updates that are relevant to your environment are identified and gathered.

Rebootless firmware updates for additional NVMe drives and parallel firmware update capabilities of NVMe drives with the same Dell™ Update Package (DUP) are available in iDRAC9 release 6.10.00.00 and later. With reboot-required, rebootless, and parallel firmware updates, iDRAC9 uses sideband direct communication, in which it communicates directly with the server components instead of communicating with components using agents or the server's OS.

Firmware Update Process Overview

A typical PowerEdge server contains multiple components, each with its own firmware, including backplane, BIOS/Unified Extensible Firmware Interface (UEFI), network adapters, and storage devices. A typical firmware update can provide enhanced functionality, new features and capabilities, security patches, and bug fixes. With rebootless firmware updates, organizations can continue to use these devices during a firmware update without rebooting the server.

Dell server components support various update methods:

- **True rebootless:** iDRAC9 can update the component without requiring a server reboot. The server OS and all server workloads continue to run.
- **True rebootless with parallel NVMe firmware updates:** This method entails performing rebootless firmware updates to multiple NVMe drives in the server simultaneously.
- **Parallel NVMe updates with reboot:** This method is similar to true rebootless with parallel NVMe firmware updates, but it requires a reboot.
- **Sideband direct with reboot:** iDRAC9 communicates directly with server components during the update without the use of agents or the server's OS, but the update requires the server and all workloads to be rebooted.
- **Traditional update method with reboot:** The update requires the server and all workloads to be rebooted. The server must be rebooted into a pre-OS update environment using media such as a bootable USB device.

Table 1 lists the components that can be updated and their supported update methods.

Table 1 | Component firmware update options for typical Dell™ PowerEdge™ server configurations

Component	True Rebootless	True Rebootless with Parallel NVMe® Updates	Sideband Direct with Reboot	Traditional Update Method with Reboot
BIOS/UEFI				X
NVMe® (for some manufacturer models)	X	X		
iDRAC9	X			
Onboard diagnostics	X			
Driver packs	X			
SEP (passive) backplane	X			
Network interface controller (NIC)			X	
Power supply unit (PSU)			X (requires one reboot versus two reboots)	

Prior to the introduction of iDRAC9 rebootless firmware updates, when Dell Technologies released a new firmware patch, IT staff had multiple update options to choose from. All of these update options required a reboot. The first option is an online update method that uses a platform-specific bootable ISO image and iDRAC9. With this method, IT staff can update all of the firmware for PowerEdge servers in a single step. The updates occur automatically after IT staff reboot the server from a bootable ISO that launches an update environment. This method uses iDRAC9 and a network connection, and it can take up to one hour to complete.

Reboots are no longer required to update rebootless-compatible components.

The second option is an offline method—meant for systems without iDRAC9 or without an external network connection—that uses a bootable USB storage device. Like the online method, this method uses a bootable ISO image that is copied to a USB storage device. IT staff must manually boot the server from the USB device to launch the update environment and perform the firmware update.

IT staff can also use management tools such as OpenManage Enterprise, VMware vCenter® for VMware deployments, System Center for servers running Microsoft products, and Ansible® for servers running Linux® and Windows Server®. Like both the online and offline update methods, these tools often require the server to be rebooted so that a pre-OS environment can run for updating firmware.

When a server is rebooted into a pre-OS environment, the server's workloads are unavailable. Depending on the number of firmware updates and the number of deployed servers, this process can take a considerable amount of time and require constant monitoring from IT staff.

For this paper, Prowess Consulting tested the rebootless firmware update, parallel firmware update with reboot, and sideband direct with reboot methods.

iDRAC9 Rebootless and Parallel Firmware Updates Overview

iDRAC9 rebootless firmware updates are different than both online and offline update methods. System administrators can perform firmware updates using iDRAC9 without having to reboot the server or launch a pre-OS update environment. iDRAC9 inventories hardware components at runtime and determines whether components support new rebootless direct sideband firmware update methods or legacy methods that require a reboot. The ability for iDRAC9 to copy firmware to a device, and its ability to support rebootless firmware updates, will vary among manufacturers and components, although more components will eventually support rebootless firmware updates as manufacturers continue to broaden their support for this technology.

In a typical rebootless firmware update scenario, IT staff sign in to iDRAC9 using a web browser and upload a rebootless DUP to the server. iDRAC9 stores this package on the iDRAC9 storage, which is separate from the server's workload storage. Once the DUP has been uploaded, IT staff submit it to the iDRAC9 job queue. Figure 1 shows the iDRAC9 System Update UI with an iDRAC9 firmware update that has been uploaded and is ready to be submitted to the job queue. Note that in the example shown in Figure 1, IT staff have uploaded an iDRAC9 firmware update that can be installed without rebooting the server.

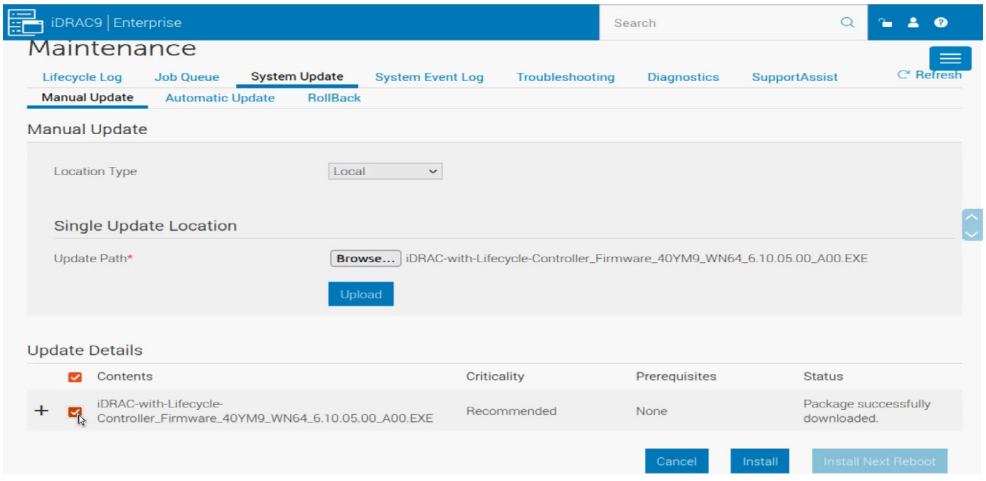

Figure 1 | IT staff can update firmware using the iDRAC9 UI without having to reboot the server

The job queue lets IT staff monitor the status of rebootless-capable firmware updates, all while the server and its workloads continue to run. In Figure 2, IT staff have successfully applied an NVMe drive firmware update to a running server.

iDRAC9 can also support parallel firmware updates for devices that support such updates and that use the same DUP. In a parallel firmware update, iDRAC9 determines which devices can support firmware updates simultaneously. Note that devices must have the same DUPs for parallel firmware updates to occur. For example, if a server contains 10 NVMe storage devices that support parallel firmware updates and use the same DUP, iDRAC9 will automatically update all 10 devices simultaneously instead of one at a time, which can result in significant time savings.

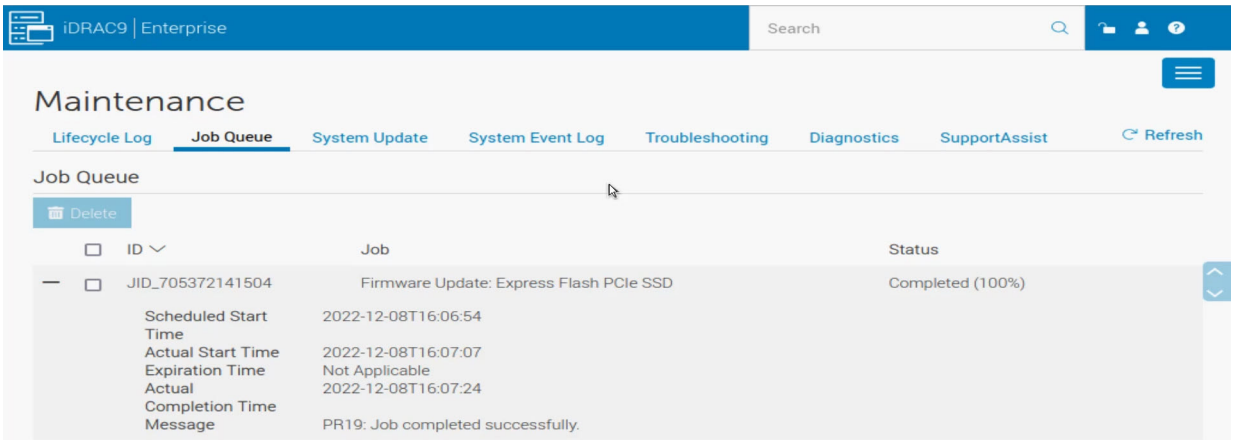

Figure 2 | The iDRAC9 job queue displays the status of an NVMe® drive rebootless firmware update

Rebootless Testing Methodology Overview

For the rebootless series of tests, we measured the time required to update rebootless-compatible firmware and reboot-required firmware. Since the iDRAC9 version 6.10.0.05 firmware does not allow reboot-required firmware updates for rebootless-compatible firmware updates, we also measured the time required to complete a full reboot cycle. This was done to determine the time difference between a server with older iDRAC firmware that supports only reboot-required firmware updates, and the newer iDRAC9 firmware that supports rebootless firmware updates. The goal of these tests was to determine how a rebootless firmware update can reduce server maintenance windows and operational expenses.

To determine the differences between rebootless and reboot-required firmware updates, we tested updating the firmware on three components:

- Dell™ NVMe v2 AGN MU.2 3.2 TB drive
- Dell universal backplane
- Broadcom® ADV dual 25 gigabit Ethernet (GbE) NIC

The Dell NVMe drive and Dell universal backplane both support the rebootless firmware update method, whereas the Broadcom NIC requires a reboot. Testing the Broadcom NIC gave us a picture of a reboot-required firmware update cycle, since the Dell NVMe drive and Dell universal backplane required rebootless firmware updates. Rebootless firmware updates are not currently supported for NVMe drives attached to a Dell™ PowerEdge™ RAID Controller (PERC) due to the NVMe drives not being exposed as PCIe® devices to iDRAC9.

Our first step was to update the server's iDRAC9 firmware to version 6.10.05.00, which supports rebootless firmware updates. Because iDRAC9 operates independently from the server and its OS, iDRAC9 rebooted itself after the firmware update, while the server and its workloads continued running. Once the iDRAC9 update completed, we performed the following steps for each of the three firmware updates:

1. Sign in to the iDRAC9 UI using a web browser on a remote computer.
2. Navigate to **Maintenance > System Update > Manual Update** in the iDRAC9 UI.

3. Select and upload a firmware update package from the remote computer's SSD to iDRAC9.
   Note: iDRAC9 provides several methods for transferring firmware update packages, including local file upload, network share, FTP, TFTP, HTTP, and HTTPS.
4. For the rebootless firmware update packages for the Dell NVMe drive and Dell universal backplane, select **Install** Install to submit the update package to the job queue where iDRAC9 installs the package.
   Note: For rebootless firmware update packages, the **Install on Next Reboot** option is not available.
5. For Broadcom NIC firmware update package that requires a reboot, select **Install and Reboot** to submit the update package to the job queue.
   Note: For firmware update packages that require a reboot, both the **Install and Reboot** and **Install Next Reboot** options are available. For this test, we selected **Install and Reboot**.
6. Once an update has been submitted to the job queue, measure the amount of time required to complete the update.

When the DUP for the Dell NVMe drive and Dell universal backplane are submitted to the job queue, iDRAC9 installs each update without requiring a reboot. In the case of the Broadcom NIC firmware update, which requires a reboot, iDRAC9 gracefully shuts down the OS, reboots the server, updates the firmware, and then reboots the server back to the OS. Once a firmware update has completed, iDRAC9 displays that the update job finished successfully.

To measure the server reboot time, we performed the following steps three times and took the average of the three runs:

1. At the Red Hat® Enterprise Linux 8.6 login screen, click the power icon in the upper right corner, and then click the power button on the drop-down menu.
2. In the **Power Off** dialog box, click **Restart** while simultaneously starting the stopwatch.
3. At the Dell Technologies logo screen, record the time when the power-on self-test (POST) completes. This is the hardware reboot time.
4. When the Red Hat login screen appears, record the time. This is the software reboot time.

Test Results

The test results for the components tested are summarized in Table 2.

Table 2 | Components tested and the test results

Component Tested	Reboot-Required Firmware Update Time (Seconds)	Rebootless Firmware Update Time (Seconds)	Hardware Reboot Time (Seconds)	Software Reboot Time (Seconds)	Approximate Reboot-Required Time (Seconds)[1]
Dell™ NVMe® v2 AGN MU.2 3.2 TB storage device	–	34	–	–	328
Dell universal backplane	–	529	–	–	708
Broadcom® ADV dual 25 GbE NIC	561	–	–	–	–
Server reboot	–	–	115	179	–

As shown in Table 2, after we submitted the firmware update to the iDRAC9 job queue, the Dell NVMe drive required only 34 seconds to complete the update, with no reboot required. The Dell universal backplane required 529 seconds to complete the update, with no reboot required. The server's OS continued to run, and no workloads were affected. The Broadcom NIC required 561 seconds to complete the firmware update, but it required the firmware update to be copied to iDRAC9, the OS and workloads to be shut down, the firmware update to be applied, and the OS and workloads to be restarted. While iDRAC9 makes the update process simple and quick for IT staff to do remotely and out of band, any workloads running on the server are affected by the reboot.

A reboot-required firmware update typically involves rebooting the server to a pre-OS environment, updating the firmware, and then rebooting the server to the OS. To approximate the time required for a reboot-required firmware update of rebootless firmware, we summed the times required for a hardware reboot, a rebootless firmware update, and a software reboot to arrive at a cumulative update time.

Using these cumulative values, the Dell NVMe drive required approximately 213 seconds for a reboot-required firmware update, versus 34 seconds for the rebootless firmware update. The Dell universal backplane required approximately 708 seconds for the reboot-required firmware update, versus 529 seconds for the rebootless firmware update.

The number of steps required in the iDRAC9 UI for both rebootless and reboot-required firmware updates are the same, but additional steps might be required in a reboot-required firmware update scenario, depending on the workloads that are running on the server. For example, if the server is part of a VMware vSphere® cluster, the server would need to be put into maintenance mode, all running virtual machines (VMs) would need to be moved to other servers in the cluster, and then the reboot-required firmware update would need to be applied. After the update, the server would then need to be taken out of maintenance mode and repopulated with running VMs.

Analysis

We found that the rebootless firmware updates can save a significant amount of IT staff time and eliminate system downtime:

- For the Dell NVMe drive, the rebootless firmware update decreased the update time by 90 percent from the approximate reboot-required firmware update time and did not require downtime.
- For the Dell universal backplane, the rebootless firmware update decreased the update time by 25 percent from the approximate reboot-required firmware update time and did not require downtime.[2]
- For the Broadcom NIC, a reboot was required, resulting in system downtime.

In the rebootless firmware update scenarios, no reboot was required and the server workloads continued to run. Contrast these results with the Broadcom NIC reboot-required firmware update, which required all workloads and the OS be shut down during the update.

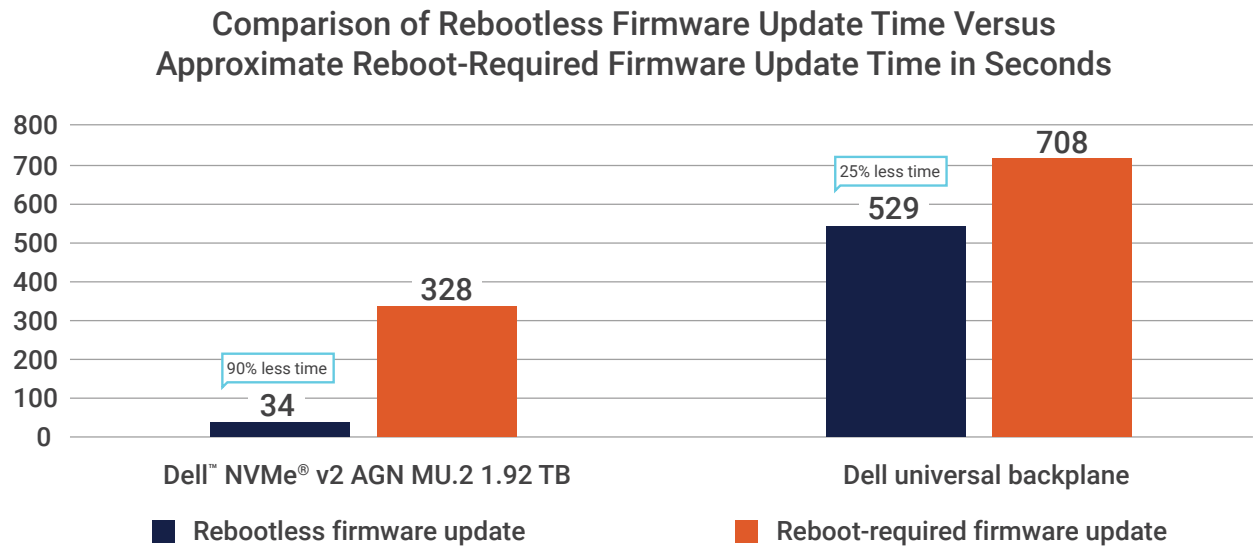

Figure 3 | Comparison of the rebootless firmware update time and the approximate reboot-required firmware update time for the Dell™ NVMe® and Dell universal backplane

Our results reflect testing on a single server with small workloads. In environments where dozens, hundreds, or even thousands of servers require firmware updates, the cumulative time savings from using rebootless firmware updates across the deployment can be significant. For example, in a moderately sized IT environment with 100 physical servers that are updated consecutively, an NVMe drive update could take more than nine hours to complete versus less than one hour using the rebootless firmware update option. For the Dell universal backplane, an update could take more than 19 hours versus less than 15 hours. Additionally, all operating systems and workloads continue to run during a rebootless firmware update, whereas workloads and operating systems must be shut down and restarted in a reboot-required firmware update, which results in service interruptions.

In a larger, more complex environment, such as a large VMware vSphere deployment, IT staff must put servers into maintenance mode for updates that require a reboot. When putting a server into maintenance mode, all running VMs must be moved to other active servers within the VMware vSphere cluster using VMware vSphere® vMotion™. This can take a considerable amount of time per server, and it increases the load on the storage infrastructure, storage network, and other servers within the cluster. Once the update completes, the server must then be taken out of maintenance mode, and running VMs must be restored to it. This process must be repeated for each server within the cluster.

Using rebootless firmware updates, IT staff can update each VMware vSphere server without putting the server into maintenance mode and moving VMs to other servers within the cluster. All VM workloads can continue to run, and no extra load is put on the storage infrastructure, storage network, and other servers within the cluster. Significantly reducing the time required to update each server in large deployments represents a considerable savings in both IT staff productivity and cost.

Parallel Firmware Update Testing Methodology Overview

For the parallel firmware update series of tests, we used a previous-generation Dell server configured with current-generation NVMe drives and iDRAC version 6.10.00 firmware. We measured the time and number of steps required to update a single NVMe drive. We then measured the time and number of steps required to update 10 NVMe drives in parallel. To determine the approximate amount of time required to serially update each of the 10 drives, we multiplied the time required to update a single drive by 10. For the number of steps, we multiplied the number of steps required to update a single drive by 10.[3]

Note that the single NVMe drive firmware update required significantly more time in this test than with the calculated reboot-required firmware update described in the rebootless firmware update section of this paper. This series of tests used a previous-generation Dell server, while the rebootless firmware update series of tests used a current-generation Dell server. Dell Technologies has optimized the boot process on current-generation Dell servers, which significantly reduces reboot times.

Test Results

The parallel firmware-update test results are summarized in Table 3.

Table 3 | Parallel firmware-update test results

Component	Update Time (Seconds)	Number of Steps
Single NVMe® drive	493	21
Parallel firmware update of 10 NVMe drives	622	21
Serial update of 10 NVMe drives	4,930 (approximate)	210 (approximate)

As shown in Table 3, updating a single NVMe drive required 493 seconds and 21 steps. Updating 10 NVMe drives in parallel required 622 seconds and the same number of steps. The approximate time required to update 10 drives serially is 4,930 seconds, while the approximate number of steps balloons to 210.

Analysis

We found that parallel firmware updates can help increase IT staff efficiency and reduce server downtime:

- Updating 10 NVMe drives in parallel increased the update time by 26 percent over updating a single NVMe drive.
- Updating 10 NVMe drives in parallel versus updating each of the drives serially resulted in an 87 percent decrease in the amount of time required from IT staff and a 90 percent decrease in the number of steps required.[4]

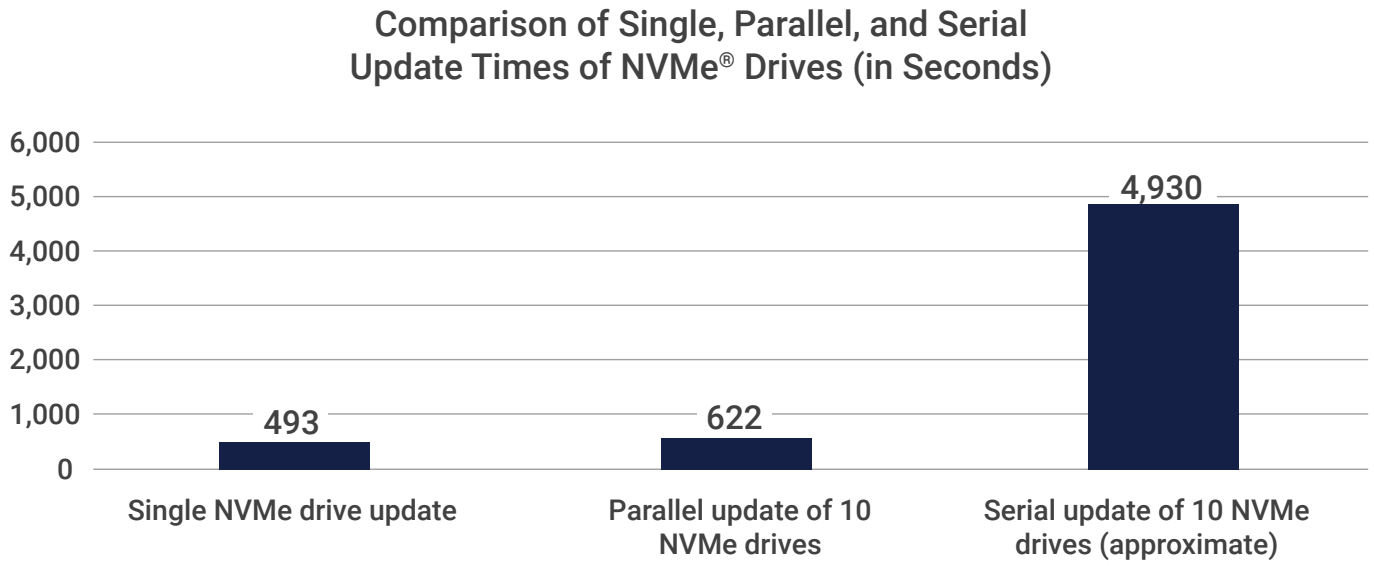

Figure 4 | Comparison of the time required (in seconds) to update a single NVMe® drive, update 10 NVMe drives in parallel, and update 10 NVMe drives serially

In our previous example of a moderately-sized server environment of 100 servers, with each server containing 10 NVMe drives, the time savings from using parallel firmware updates is significant. Manually updating each NVMe drive in each of the 100 servers would require nearly 140 hours to complete, but it takes only 16 hours to update those same drives in parallel. This time savings represents a significant increase in IT staff productivity and a substantial decrease in operational costs.

Conclusion

iDRAC9 rebootless firmware updates can reduce server downtime while increasing IT staff productivity by substantially shortening update windows and eliminating server reboots. Organizations are likely to address firmware-related security and interoperability issues quicker if update processes are more seamless and downtime is minimized. Organizations can also benefit from increased IT staff productivity, as staff can dedicate more time to important initiatives rather than to server firmware updates.

Appendix

At the time of this writing, and with the release of iDRAC9 version 6.10.00, the following NVMe drives support rebootless firmware updates.

Table A1 | NVMe® drives that support rebootless firmware updates

Brand	Model
KIOXIA	CM6 RI/MU
	CM7 RI/MU
	CM7 RI/MU (E3)
	CD7
	CD7 (E3)
Samsung	PM1733a/PM1735a
	PM1743/PM1745
	PM1743/PM1745 (E3)
SK hynix	PE8010
Solidigm	D7-P5520/D7-P5620

Table A2 | Dell™ PowerEdge™ R760 configuration used for testing both reboot-required and rebootless firmware updates

Dell™ PowerEdge™ R760 Server	
Processor(s)	2 x Intel® Xeon® Gold 6430 processor, 1,900 megatransfers per second (MT/s), 32 cores
BIOS version	0.2.29
iDRAC9 version	6.10.0.05.A00_01
Memory	16 x DDR5 64 GB 4,400 MT/s (1,024 GB total)
Storage	2 x Dell™ EC NVMe® ISE 7400 RI M.2 480 GB 2 x Dell NVMe CM6 RI 1.92 TB 2 x Dell NVMe v2 AGN MU.2 3.2 TB
Backplane	Dell universal backplane/Dell™ PERC H965i
NIC	Broadcom® ADV dual 25 GbE—22.21.20.00
OS	Red Hat® Enterprise Linux® 8.6

Table A3 | Dell™ PowerEdge™ R7525 configuration used for testing single and parallel NVMe® drive firmware updates

Dell™ PowerEdge™ R7525 Server	
Processor(s)	2 x AMD EPYC™ 7552 processor, 48 cores, 2,200 MT/s
BIOS version	2.6.6
iDRAC9 version	6.10.00.0
Memory	4 x DDR4 64 GB 3,200 MT/s (256 GB total)
Storage	11 x Dell™ NVMe® CD5 3.5 TB

Table A4 | Steps required for rebootless and reboot-required firmware updates

Rebootless Firmware Update Step	Action	Reboot-Required Firmware Update Step	Action*
1	Sign in to the iDRAC9 UI.	1	Sign in to the iDRAC9 UI.
2	Navigate to **Maintenance > System Update > Manual Update**.	2	Navigate to **Maintenance > System Update > Manual Update.**
3	Select and upload a firmware package.	3	Select and upload a firmware package.
4	Click **Install**.	4	Click **Install and Reboot**.

*** Though the reboots and firmware updates don't require any interaction, additional actions/steps might vary depending on server workloads.**

Table A5 | Single NVMe® drive update steps

Single NVMe® Drive Update Step	Action	Time (Seconds)
1	Sign in to the iDRAC9 UI.	20
2	Click the **Maintenance** drop-down menu.	3
3	Click the **System Update** tab.	3
4	Click **Choose File**.	1
5	In the **Open File** dialog box, double-click the firmware file.	2
6	Click **Upload**.	1
7	Wait for the firmware to upload.	9
8	Under **Update Details**, click the plus symbol.	2
9	Confirm the details of the update.	1
10	Select the checkbox next to the updated drive.	1
11	Click **Install and Reboot**.	5
12	Click **Job Queue**.	2
13	On the **Job Queue** page, click the plus symbol next to the job labeled **Firmware Update: PCIe SSD**.	2
14	Wait until the status changes from "Downloading" to "Scheduled."	11
15	Wait until the **RID Job Status** changes from "RebootPending" to "RebootCompleted."	14
16	Wait until the **JID Job Status** changes from "Scheduled" to "Running."	135
17	Wait until the **JID Job Status** changes from "Running" to "Completed."	270
18	Click the **Storage** tab.	5
19	Click **Physical Disks**.	2
20	Click the plus symbol next to the updated disk.	1
21	Scroll down to verify the firmware version for the NVMe drive.	3

Table A6 | Parallel firmware update steps for 10 NVMe® drives

Parallel Firmware Update Steps for 10 NVMe® Drives	Action	Time (Seconds)
1	Sign in to the iDRAC9 UI.	20
2	Click the **Maintenance** drop-down menu.	3
3	Click the **System Update** tab.	3
4	Click **Choose File**.	1
5	In the **Open File** dialog box, double-click the firmware file.	2
6	Click **Upload**.	1
7	Wait for the firmware to upload.	11
8	Under **Update Details**, click the plus symbol.	2
9	Confirm the details of the update.	3
10	Select the checkbox next to the updated drive.	1
11	Click **Install and Reboot**.	5
12	Click **Job Queue**.	2
13	On the **Job Queue** page, click the plus symbol next to the job labeled **Firmware Update: PCIe SSD**.	2
14	Wait until the status changes from "Downloading" to "Scheduled."	11
15	Wait until the **RID Job Status** changes from "RebootPending" to "RebootCompleted."	12
16	Wait until the **JID Job Status** changes from "Scheduled" to "Running."	155
17	Wait until the **JID Job Status** changes from "Running" to "Completed."	285
18	Click the **Storage** tab.	5
19	Click **Physical Disks**.	2
20	Click the plus symbol next to the updated disk.	1
21	Scroll down to verify the firmware version for the 10 NVMe drives.	36

[1] Because iDRAC version 6.10.0.05.A00_01 does not have a reboot-required firmware update option for rebootless firmware, we approximated the time required for a reboot-required firmware update by summing the hardware reboot time, rebootless firmware update time, and software reboot time. This value approximates the time required to boot the server into a pre-OS environment, update the firmware, and then reboot the server to the OS.
[2] The percentage changes were calculated using the following formula: (V2–V1)/V1*100, where V1 is the approximated reboot-required firmware update value in seconds, and V2 is the rebootless firmware update value in seconds.
[3] The number of steps required to update 10 NVM Express® (NVMe®) drives might vary slightly. For example, the first step in our test was to sign in to the iDRAC UI. This step might not be required for every drive update, assuming that the current session does not time out.
[4] The percentage changes were calculated using the following formula: (V2–V1)/V1*100. For the single NVM Express® (NVMe®) drive update versus the parallel firmware update of 10 NVMe drives, V1 is the time required to update the single NVMe drive, and V2 is the time required to update the 10 NVMe drives in parallel. For the comparison of updating 10 NVMe drives in parallel versus serially, V1 is the total time required to update each of the 10 drives serially, and V2 is the time required to update the 10 drives in parallel. For the comparison of the number of steps required to update 10 NVMe drives in parallel versus serially, V1 is the number of steps required to update each of the 10 drives serially, and V2 is the number of steps required to update the 10 drives in parallel.

The analysis in this document was done by Prowess Consulting and commissioned by Dell Technologies.

Results have been simulated and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance.

Prowess Consulting and the Prowess logo are trademarks of Prowess Consulting, LLC.

Copyright © 2023 Prowess Consulting, LLC. All rights reserved.

Other trademarks are the property of their respective owners.

0323/220198