

Update 1803 for Cloud Platform System (CPS) Standard

Dell Hybrid Cloud System for Microsoft

Dell Engineering
April 2018

Revisions

Date	Description
July 2016	Initial release 1605
August 2016	Release 1606
August 2016	Release 1607
October 2016	Release 1608
November 2016	Release 1609
December 2016	Release 1610
January 2017	Revision of instructions for running PUDellEMC
February 2017	Release 1611
March 2017	Release 1701
May 2017	Release 1703
May 2017	Release 1703a
June 2017	Release 1705
August 2017	Release 1706
September 2017	Release 1707
October 2017	Release 1708
November 2017	Release 1709
January 2018	Release 1710
January 2018	Release 1712
March 2018	Release 1802
April 2018	Release 1803

Table of contents

Revisions.....	2
1 Overview of the Patch and Update framework.....	5
2 Update 1803—Summary.....	6
2.1 Additional update information.....	6
2.2 How to check which update package is installed.....	7
2.3 When to run the update package.....	7
3 1803 Patch and Update Prerequisites.....	8
3.1 Prepare the patching environment.....	8
3.2 Step 1: Prepare user account for patching.....	8
3.3 Step 2: Ensure that Group Policy does not block the mounting of USB virtual disks.....	8
3.4 Step 3: Extract the Patch and Update package.....	9
3.5 Step 4: Ensure that <code>LaJollaDeploymentService</code> is not running in the background on the Console VM ..	9
3.6 Step 5: Clean up the WSUS server.....	9
3.7 Step 6: (Optional): Exclude external SOFS storage clusters from P&U.....	10
4 1803 Patch and Update Process.....	12
4.1 Step 1: Run the <code>DHCS_Run_First</code> package.....	13
4.2 Step 2: Run the 1803 Microsoft P&U package.....	16
4.2.1 Run an optional compliance scan.....	20
4.3 Step 3: Run the 1803 DellEMC P&U package.....	22
5 Microsoft payload for Update 1803.....	25
Payload for Update 1803.....	25
5.1 Troubleshooting the P&U process.....	26
6 Dell EMC Payload for Update 1803.....	33

WARNING: You cannot run the 1803 Patch & Update framework—1.5—directly without first upgrading your environment to 1703b Patch & Update framework—1.4. You can directly upgrade to 1803 only after the DHCS stamp is at the 1.4 version, P&U 1703b. Also be advised that the addition of any non-DHCS hardware to your system will cause the Patch & Update process to fail. For a workaround to this problem, see [Troubleshooting the P&U process](#), and follow the procedures detailed in **Issue 2**.

1 Overview of the Patch and Update framework

The Dell Hybrid Cloud System for Microsoft includes the Patch and Update (P&U) framework. This framework enables you to easily update the infrastructure components of the Dell Hybrid Cloud System for Microsoft stamp with minimal or no disruption to tenant workloads. The framework automates the installation of software, driver, and firmware updates on the physical hosts and the infrastructure VMs.

Note: The P&U framework does not update tenant VMs.

When the P&U framework runs, it does the following:

- Orchestrates the updates so that they are performed in the correct order.
- Automatically puts servers in and out of maintenance mode during servicing.
- Validates components when servicing is complete.

The P&U framework installs approved software updates on infrastructure hosts and VMs for various combinations of the following products:

Note: Any given package may or may not contain updates from all the categories listed. For the specific contents of any particular package, see the package Release Notes, which you can obtain from the same download location as the package itself.

- Windows Server
- Windows Azure Pack
- System Center
- SQL Server
- Dell software
- Dell Deployment UI
- Drivers and firmware updates for Dell Hardware.

If the package also includes firmware and driver updates, the framework installs the approved firmware and driver updates on the physical cluster nodes.

IMPORTANT: Do NOT install Windows Server, Windows Azure Pack, System Center, and SQL Server updates by using any method other than the P&U framework. Install only update packages that Microsoft and Dell have tested and approved for the Dell Hybrid Cloud System for Microsoft.

2 Update 1803—Summary

Update 1803 for CPS Standard includes updates for Windows Server and other software components. This update includes the following components:

- **1803 update.** This is the main package. It contains Windows Server, System Center, and SQL Server updates.

IMPORTANT: Update 1703 is a prerequisite for installing update 1803.

IMPORTANT: New installations of Data Protection Manager (DPM) or Azure Onboarding for Azure Site Recovery (ASR) requires the install of update 1803 before install/expansion. Once the install/expansion are complete, re-run update 1803 to update the newly installed servers.

IMPORTANT: Update 1712 (and higher) contains 3 updated SMA Management Packs for SCOM. These need to be installed manually after the P&U run is complete.

IMPORTANT: The OEM OOB (Out-of-Band Management) web interface may not work correctly after applying P&U 1706 (or higher). See the troubleshooting section at the end of this document for workarounds/resolution.

IMPORTANT: Update 1803 contains manual steps post-install to ensure protection from vulnerabilities. See “Step 5: Post-update manual steps” in the “Update the computers” section of “Apply P&U updates”

IMPORTANT: Update 1712 (and higher) contains the Windows binary and registry changes to mitigate “speculative execution side-channel attacks” in Security Advisory [ADV180002](#).

For detailed update payload information, see [Payload information](#).

2.1 Additional update information

This update includes new functionality to enforce Transport Layer Security (TLS) 1.2 communications across the stamp. Details and impacts include:

- Microsoft Support KB# [3117336](#) – Recommendation to migrate all Windows computers to TLS 1.2.
- TLS 1.0/1.1 are disabled across all hosts and VMs.
- Update 1606 (minor release) and 1611 (major release) for CPS disabled SSL 2.0/3.0 communications to protect against POODLE SSL vulnerabilities.
- Windows XP, Windows Vista, Windows Server 2003, and Windows Server 2008 will no longer be able to access stamp resources. Examples include the WAP Admin Portal, WAP Tenant Portal, and RDP access to the Console VMs.
- Configuration changes force Windows SChannel communications, Internet Explorer Security, and .NET Framework 4.0 to all use TLS 1.2 only.
- <https://requirements.azurewebsites.net/Requirements/Details/6417#guide> – Details of registry key changes to force TLS 1.2 communication cipher suites (“Opportunity for Excellence, < Windows 10” section)

2.2 How to check which update package is installed

To check the version of the update package that is currently installed on the stamp, do the following:

1. On the Console VM, open the **DeploymentManifest.xml** file at the path:
C:\Program Files\Microsoft Cloud Solutions\DeployDriver\Manifests.
2. At the top of the file, look for the following entries:
 - “**Version=**”: This is the version of the Dell-provided update package.
 - “**MicrosoftVersion=**”: This is the version of the Microsoft-specific updates that were incorporated in the Dell-provided update package, for example:

```
"MicrosoftVersion": "1.0.1603.21000"
```

The third value (1603 in the example) indicates the year and month of the Microsoft update package.

2.3 When to run the update package

Dell recommends that the package be running during a scheduled maintenance window, or when there is low activity. There is associated downtime for the infrastructure VMs if the package installs updates that require a server restart on the VMs.

The patch and update mechanism does not target tenant workloads for software updates, so tenant VMs should not typically experience downtime. However, if an update package contains driver and firmware updates, there may be associated downtime. Check the information that is provided with the update package.

Update 1803 contains three distinct phases:

- [Performing prerequisites](#)
- [DHCS_Run_First](#)
- [Running the 1803 Microsoft P&U package](#)
- [Running the 1803 DellEMC P&U package](#)

CAUTION: The only supported sequence for running the packages is as follows:

1. Prerequisites
2. DHCS_Run_First
3. Microsoft P&U package
4. DellEMC P&U package

If you deviate from this sequence, the P&U process will fail.

If you receive an error when running one package, rerun that same package again. Do not run an earlier package.

Run these phases sequentially in the same maintenance window, or in separate time blocks if needed. Each of these procedures is described in the sections that follow.

3 1803 Patch and Update Prerequisites

You must do the following in order to run the P&U successfully.

3.1 Prepare the patching environment

You must first prepare the environment. To do this, you verify that you have an account that has the required permissions to run the framework, extract the P&U package to the correct share on the stamp, and verify that Group Policy settings will not block any driver updates by blocking the mounting of USB virtual disks (if the package contains firmware/driver updates). Detailed steps are provided below.

3.2 Step 1: Prepare user account for patching

To prepare the user account:

1. On a computer that has the Active Directory Users and Computers snap-in installed, log on as a domain administrator or as a user who has delegated permissions to the organizational unit (OU) for the CPS Standard stamp.
2. Add the user account that you want to use for patching to the **<Prefix>-Setup-Admins** group in the OU for the stamp (*Parent OU\StampPrefix OU*).

3.3 Step 2: Ensure that Group Policy does not block the mounting of USB virtual disks

If there are firmware and driver updates in the P&U package, make sure that there are no Group Policy settings in place that block the mounting of a USB virtual disk on any of the physical nodes. These settings can block the installation of some drivers.

As a domain administrator, on a computer that has the Group Policy Management Console (GPMC) installed, check the specified Group Policy settings at the following path:

```
\Computer Configuration\Policies\Administrative Templates\System\Removable  
Storage Access
```


3.4 Step 3: Extract the Patch and Update package

To extract the P&U package:

1. Download the zip file for the Patch and Update and unzip it to a location that you can access from the Console VM. This location can be locally on the console VM or a remote location accessible via console VM.
2. Log on to the Console VM using the account that is a member of **<Prefix>Setup-Admins**.
3. Create a share for the P&U package.
 - a. On the Console VM, create a folder, such as **PUShare**.
 - b. Right-click the folder, and then click **Properties**.
 - c. On the **Sharing** tab, click **Share**.
 - d. Add the **<Prefix>Setup-Admins** group with **Read/Write** permissions.

3.5 Step 4: Ensure that `LaJollaDeploymentService` is not running in the background on the Console VM

You can ensure that the service `LaJollaDeploymentService` is stopped by doing the following:

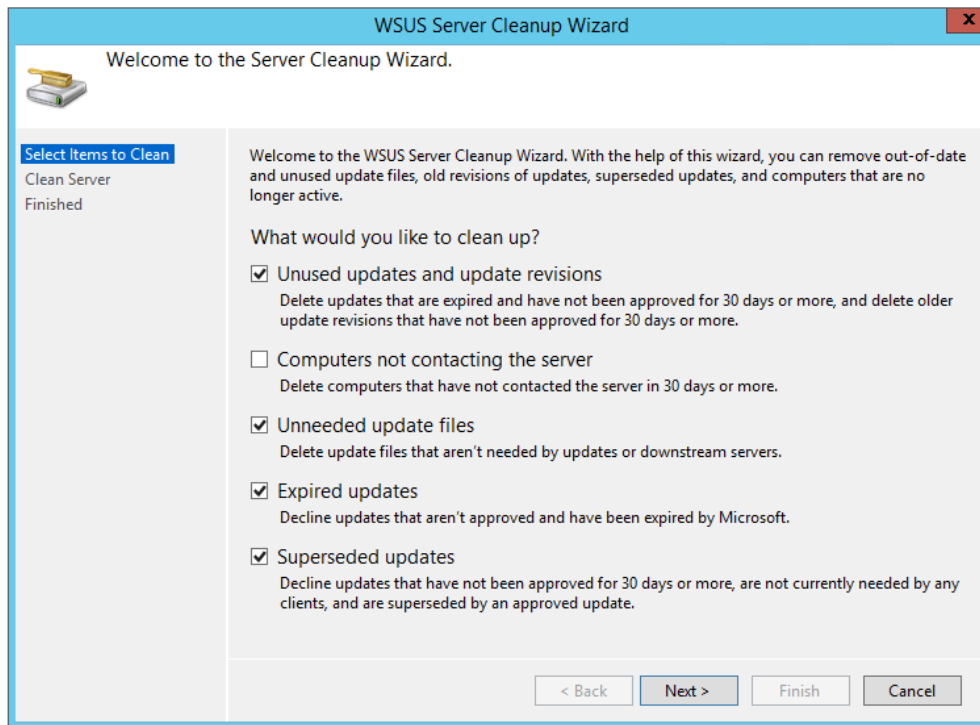
1. On the Console VM, open up the services MMC console that is located under **Control Panel->System and Security->Administrative Tools->Services**.
2. Look for **LaJollaDeploymentService**.
3. Ensure that **Status** is **Stopped**.

3.6 Step 5: Clean up the WSUS server

To clean up the server:

1. On the Console VM, open the **Windows Server Update Services** console.
2. Right-click **Update Services**, click **Connect to Server**, and then connect to the WSUS VM (**<Prefix>VMM01**).
3. In the left pane, expand **Update Services > [WSUS Server]> Updates**, and then click **All Updates**.
4. In the **All Updates** pane, in the **Approval** list, click **Any except declined**. In the **Status** list, click **Any**. Then, click **Refresh**.
5. Select all updates.
6. Right-click the selection, and then click **Decline**.
7. In the left pane, expand the server name, and then click **Options**.
8. In the **Options** pane, click **Server Cleanup Wizard**.

9. Select all check boxes *except* for **Computers not contacting the server**.



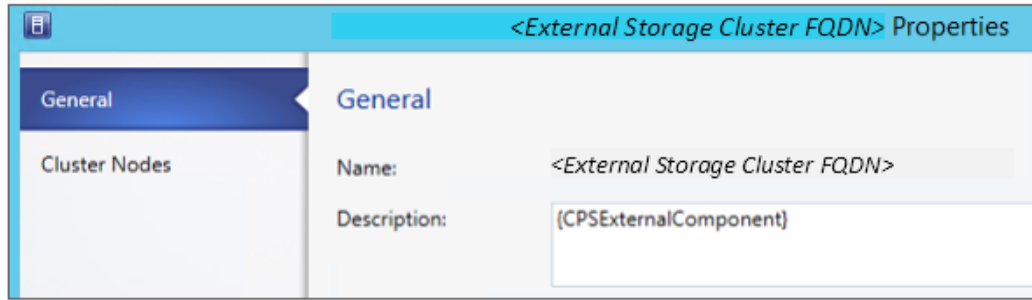
10. Click **Next**.
11. Restart the Console VM.

3.7 Step 6: (Optional): Exclude external SOFS storage clusters from P&U

IMPORTANT: This procedure applies only if you attached external Scale-Out File Server (SOFS) storage clusters to the CPS Standard stamp.
If you attached external Scale-Out-File-Server (SOFS) storage clusters to the CPS Standard stamp (for additional workload capacity), you must exclude them from P&U. If you do not, P&U will fail.

To exclude external storage clusters, do the following:

1. Open the VMM console.
2. In the **Fabric** workspace, under **Storage**, click **File Servers**.
3. In the **File Servers, File Shares** pane, right-click the external storage cluster, and then click **Properties**.
4. On the **General** tab, in the **Description** box, enter `{CPSExternalComponent}`, and then click **OK**.



With this entry, P&U will skip the external SOFS and corresponding file server nodes. You are responsible for updating these servers outside of P&U.

4 1803 Patch and Update Process

IMPORTANT: Be sure to follow the prerequisites listed in the previous section before you run the 1803 Patch and Update process.

You must first prepare the environment. This section covers the preparation steps.

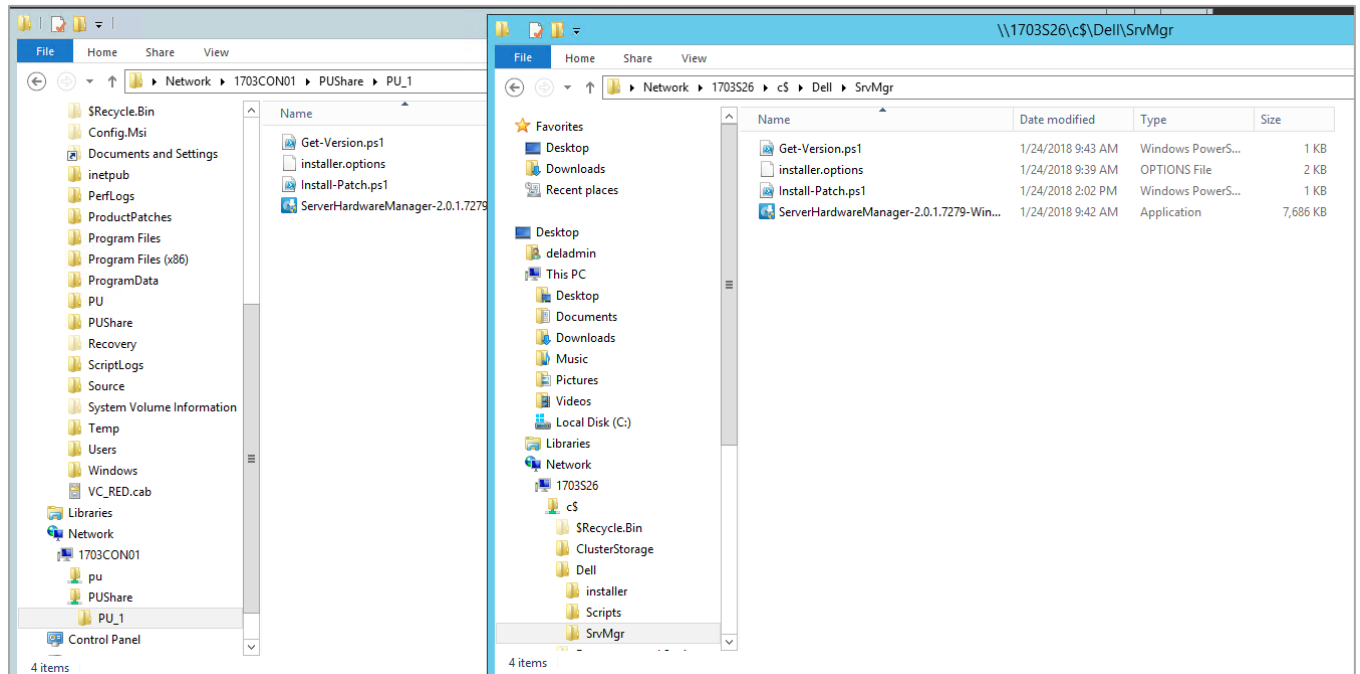
In the "Update the computers" section of the CPS Standard Administrators Guide, complete "**Step 1: Restart the Console VM**" and "**Step 2: Run a health check and fix any discovered issues.**" This includes functionality to check for and disable any running backup jobs.

Important: Do not start the update process. Instead, run the Health Check, fix any discovered issues, and stop any running backup jobs.

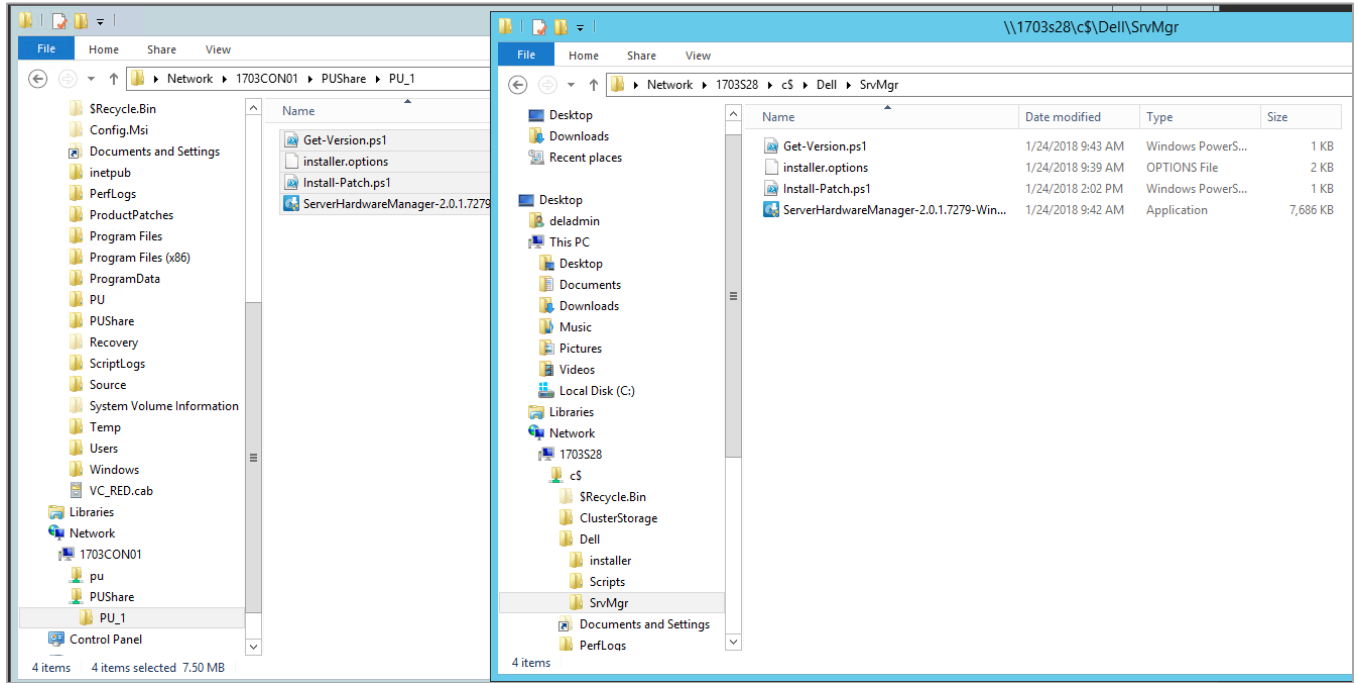
4.1 Step 1: Run the DHCS_Run_First package

Run the following instructions from the console server.

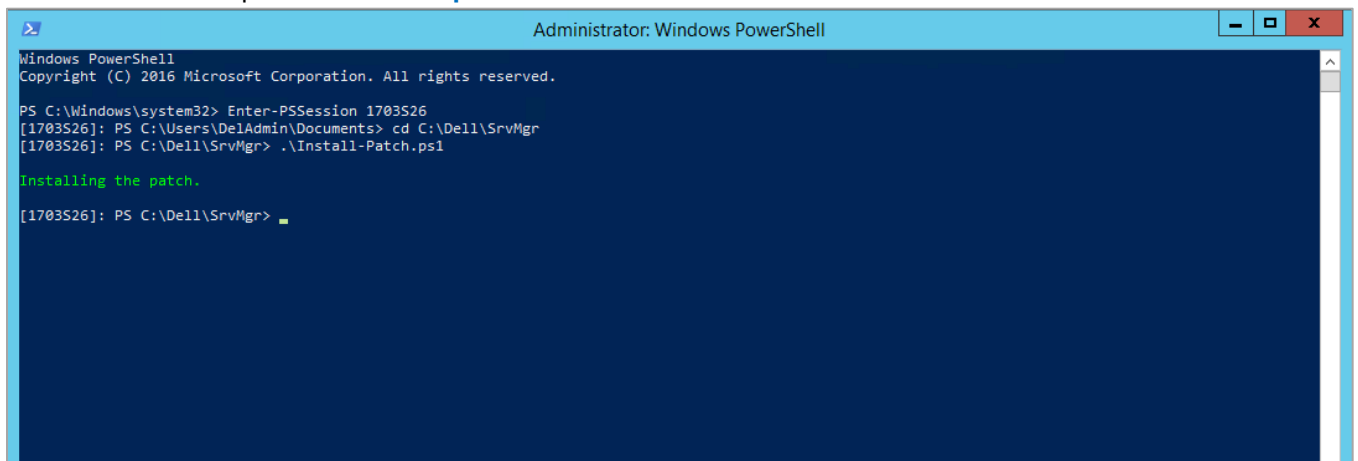
1. Execute the **DHCS_Update_1803_Run_First.exe** file to extract the files from the package.
2. Prepare the first file server.
 - i. Open windows explorer and navigate to **\\SoFS-1 Name\C\$\Dell**
 - ii. Create a subfolder called **SrvMgr**
 - iii. Copy the contents of **\\ConsoleServerName\PUShare\CPSPU FolderName** to **\\SoFS-1 Name\C\$\Dell\SrvMgr**



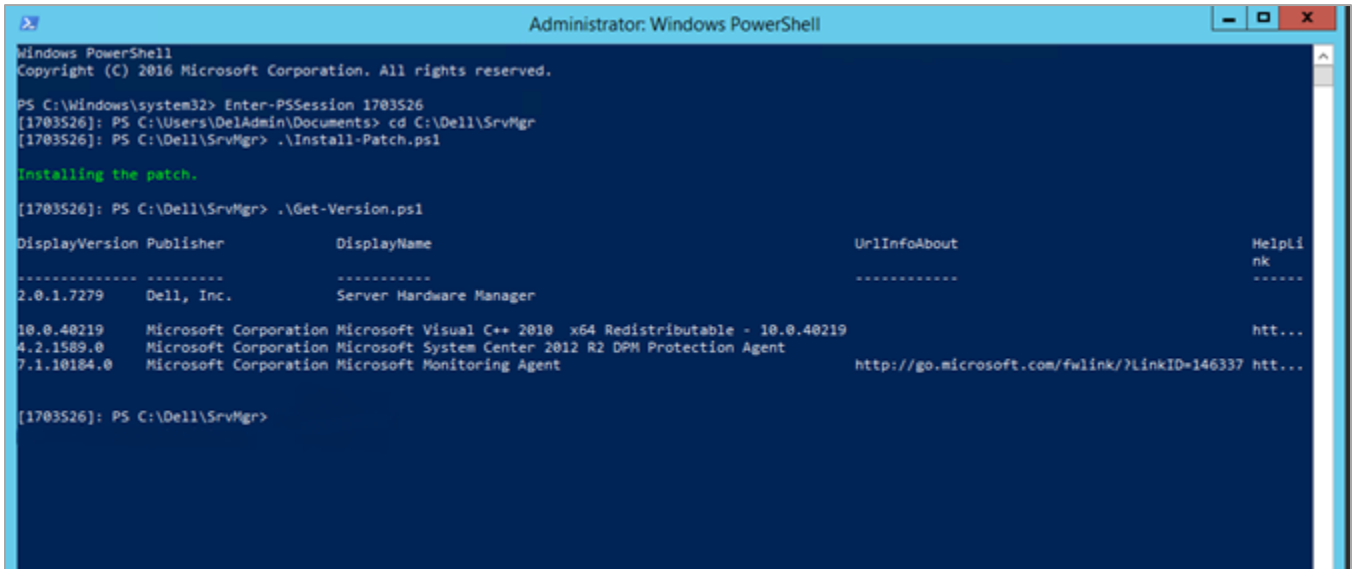
3. Prepare the second file server.
 - i. Open windows explorer and navigate to **\\SoFS-2_Name\C\$\Dell**
 - ii. Create a subfolder called **SrvMgr**
 - iii. Copy the contents of **\\ConsoleServerName\PUShare\CPSPU FolderName** to **\\SoFS-2_Name\C\$\Dell\SrvMgr**



4. Open up a PowerShell window in administrator mode
 - i. Run the command: **Enter-PSSession SoFS-1_Name**
 - ii. Navigate to **C:\Dell\SrvMgr**
 - iii. Run the script **.\Install-Patch.ps1**



- iv. Verify that the patch was installed by running the script `.\Get-Version.ps1`



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

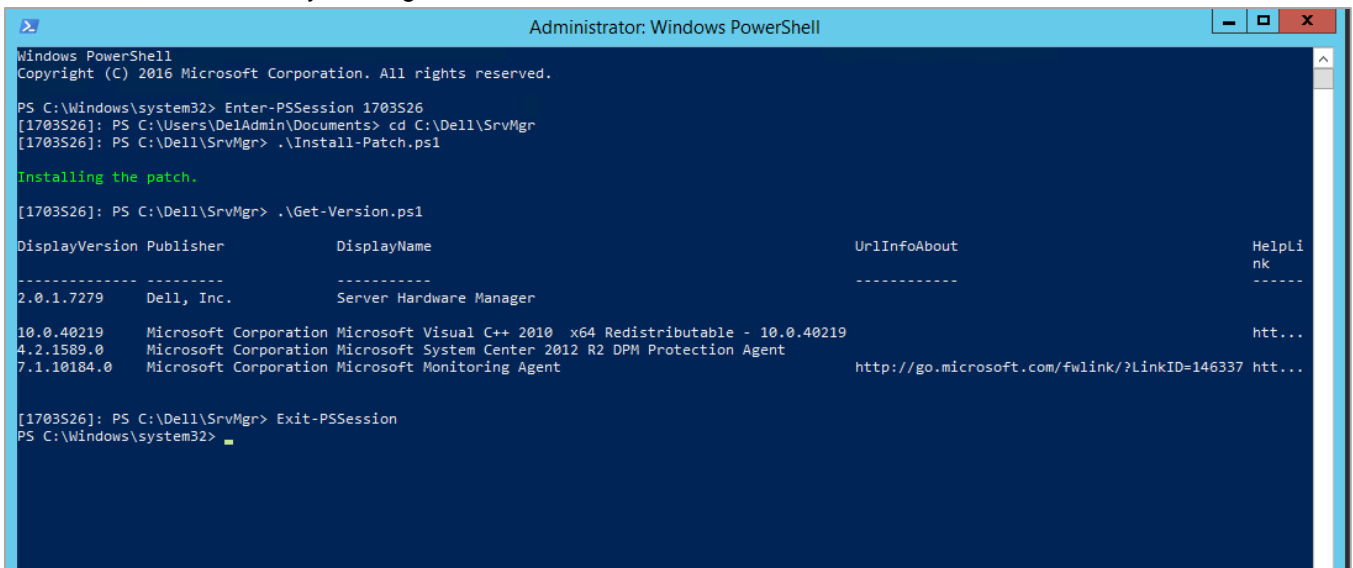
PS C:\Windows\system32> Enter-PSSession 1703526
[1703526]: PS C:\Users\DelAdmin\Documents> cd C:\Dell\SrvMgr
[1703526]: PS C:\Dell\SrvMgr> .\Install-Patch.ps1

Installing the patch.

[1703526]: PS C:\Dell\SrvMgr> .\Get-Version.ps1

DisplayVersion Publisher          DisplayName                                UrlInfoAbout                                HelpLi
-----
2.0.1.7279      Dell, Inc.          Server Hardware Manager
10.0.40219      Microsoft Corpora Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219  htt...
4.2.1589.0      Microsoft Corpora Microsoft System Center 2012 R2 DPM Protection Agent
7.1.10184.0     Microsoft Corpora Microsoft Monitoring Agent                                http://go.microsoft.com/fwlink/?LinkID=146337 htt...
```

- v. Exit the session by running the command: `Exit-PSSession`.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Enter-PSSession 1703526
[1703526]: PS C:\Users\DelAdmin\Documents> cd C:\Dell\SrvMgr
[1703526]: PS C:\Dell\SrvMgr> .\Install-Patch.ps1

Installing the patch.

[1703526]: PS C:\Dell\SrvMgr> .\Get-Version.ps1

DisplayVersion Publisher          DisplayName                                UrlInfoAbout                                HelpLi
-----
2.0.1.7279      Dell, Inc.          Server Hardware Manager
10.0.40219      Microsoft Corpora Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219  htt...
4.2.1589.0      Microsoft Corpora Microsoft System Center 2012 R2 DPM Protection Agent
7.1.10184.0     Microsoft Corpora Microsoft Monitoring Agent                                http://go.microsoft.com/fwlink/?LinkID=146337 htt...

[1703526]: PS C:\Dell\SrvMgr> Exit-PSSession
PS C:\Windows\system32>
```

5. Repeat Step 4 on the second file server.
6. You have now completed the first section of the 1803 patch.

4.2 Step 2: Run the 1803 Microsoft P&U package

IMPORTANT: You must run the DHCS_Run_First package before you run the 1803 Microsoft P&U package.

Because of the size of this package, estimates for deployment duration are 12 to 18 hours. Run the 1803 Microsoft P&U update package by doing the following:

1. Browse to the shared folder **PUShare** on the console VM, and create a folder to store the 1803 Microsoft update package, such as **PU_MS#**, where # is the number or some other identifier of the specific update package. For example, where *1803* represents the year/month:

```
\\<Prefix>CON01\PUShare\PU_MS1803
```

IMPORTANT: Do not use the same folder name as an existing folder because you want to maintain a history of each patching update.

Note: If the update package is larger than 2 GB, and the copy and paste operation fails, see <https://support.microsoft.com/en-us/kb/2258090>.

2. While logged into the console VM, browse to location where you unzipped the Patch and Update package and execute the file with the format **DHCS_Update_1803_Run_Second.exe** to extract the update. When prompted, select the **PU_MS1803** folder to store the extracted files.
3. Now that the patching environment is set up, you can start the patching process by running a Windows PowerShell script. Run the following command:

```
\\<Prefix>CON01\PUShare\PU_MS1803\PU\Framework\PatchingUpgrade\Invoke-PURun.ps1 - PUCredential (Get-Credential)
```

Note: The P&U (Patch and Update) engine automatically runs a health check as part of the update process. You can control what happens if critical Operations Manager alerts are discovered. To do this, change the value of the `-ScmAlertAction` parameter. For example, `-ScmAlertAction "Continue"`

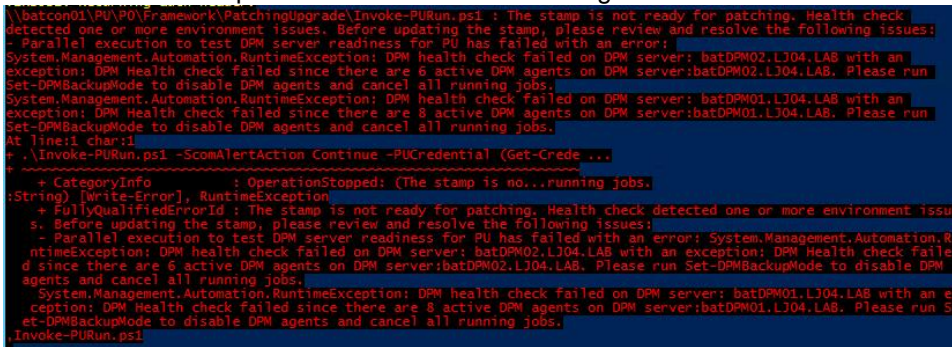
4. When prompted, enter the account credentials of the account that you used to log in.
5. The `Invoke-PURun` script performs a one-time environment setup and may prompt you to restart Windows PowerShell on its for invocation, for example:

PowerShell environment settings have changed. Please restart the PowerShell console before proceeding.

If you see this message, close the current Windows PowerShell session, open a new elevated Windows PowerShell session, and repeat steps 2 through 4 to start the health check process.

6. DPM agents on the DPM servers are in an enabled state. If this is the case, the health check output indicates that you must run the **Set-DPMBackupMode** script to cancel the jobs and disable the agents.

The PowerShell output looks similar to the following screenshot:



```
\\batcon01\PU\PO\framework\PatchingUpgrade\Invoke-PURun.ps1 : The stamp is not ready for patching. Health check
detected one or more environment issues. Before updating the stamp, please review and resolve the following issues:
- Parallel execution to test DPM server readiness for PU has failed with an error:
System.Management.Automation.RuntimeException: DPM health check failed on DPM server: batDPM02.LJ04.LAB with an
exception: DPM Health check failed since there are 6 active DPM agents on DPM server:batDPM02.LJ04.LAB. Please run
Set-DPMBackupMode to disable DPM agents and cancel all running jobs.
System.Management.Automation.RuntimeException: DPM health check failed on DPM server: batDPM01.LJ04.LAB with an
exception: DPM Health check failed since there are 8 active DPM agents on DPM server:batDPM01.LJ04.LAB. Please run
Set-DPMBackupMode to disable DPM agents and cancel all running jobs.
At line:1 char:1
+ .Invoke-PURun.ps1 -ScomAlertAction Continue -PUCredential (Get-Crede...
+ ~~~~~
+ CategoryInfo          : OperationStopped: (The stamp is no...running jobs.
:String) [Write-Error], RuntimeException
+ FullyQualifiedErrorId : The stamp is not ready for patching. Health check detected one or more environment issue
s. Before updating the stamp, please review and resolve the following issues:
- Parallel execution to test DPM server readiness for PU has failed with an error: System.Management.Automation.Ru
ntimeException: DPM health check failed on DPM server: batDPM02.LJ04.LAB with an exception: DPM Health check fail
ed since there are 6 active DPM agents on DPM server:batDPM02.LJ04.LAB. Please run Set-DPMBackupMode to disable DPM
agents and cancel all running jobs.
System.Management.Automation.RuntimeException: DPM health check failed on DPM server: batDPM01.LJ04.LAB with an ex
ception: DPM Health check failed since there are 8 active DPM agents on DPM server:batDPM01.LJ04.LAB. Please run S
et-DPMBackupMode to disable DPM agents and cancel all running jobs.
Invoke-PURun.ps1
```

7. To cancel the jobs and disable the agents, do the following:
 - a. From an elevated Windows PowerShell session, run the following commands. Press **Enter** after each command:

```
cd \\<Prefix>CON01\PUshare\<CPSPU Folder
Name>\PU\Framework\PatchingUpgrade"
Import-Module .\PatchingUpgrade\DPM.psm1
Set-DPMBackupMode -BackupMode Disable -Credential (Get-Credential)
```

- b. When prompted, enter the account credentials of the account that you are logged on as.

At this point the patch and update process should begin, with verbose output of the progress.

1. During the patching process note the following:
 - If you click inside the Windows PowerShell window during the patching process, the screen output will freeze, although the update process is still running. Press **Enter** to continue the scrolling of output.
 - Some component updates do not output status to the Windows PowerShell console. See the next step for other ways to monitor progress.
 - Updates of the physical cluster nodes may take a while. For example, a task that involves the compute cluster (CCL) or storage cluster (SCL) may take some time, and the output may not update for a while. You can use the following steps to view the progress of cluster updates in Failover Cluster Manager:
 - i. Open Failover Cluster Manager.
 - ii. Connect to the cluster.
 - a. In the navigation pane, right-click **Failover Cluster Manager**, and then click **Connect to Cluster**.
 - b. In the **Select Cluster** dialog box, click **Browse**.
 - c. Click the desired cluster, and then click **OK** two times.
 - iii. In the navigation pane, right-click the cluster name, point to **More Actions**, and then click **Cluster-Aware Updating**.
 - iv. In the **ClusterName – Cluster-Aware Updating** dialog box, click the **Log of Updates in Progress** tab to monitor what is happening.

Note: After Cluster-Aware Updating (CAU) completes, you can click **Generate a report on past Updating Runs** to view details about what was installed through CAU.

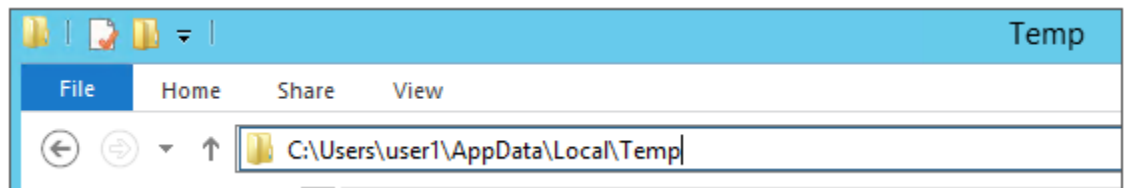
- If you have the VMM console open, and it reconnects, patching of the VMM server may be in progress. This is expected behavior.
2. To monitor the progress, you can use the following methods:
 - View the verbose output on the screen.
 - View the P&U events in Event Viewer. You can find P&U events under **Applications and Services Logs -> PUEventLog -> Operational**.
 - View the temp folder to retrieve logs with more details. To determine the temp folder, run the following command in Windows PowerShell:

```
[System.IO.Path]::GetTempPath()
```

The temp folder path will be something similar to this:

```
C:\Users\username\AppData\Local\Temp\2\
```

If the temp folder path includes a numbered folder, such as 2, 3, or 4, you will need to go up one folder level to the **\Temp** folder. If you browse in File Explorer, note that AppData is a hidden folder. You can type the folder path to get to it, for example:



In the **Temp** folder, look for the file that is named **PUPProgressDetails.txt**.

- View running jobs in the VMM console (in the **Jobs** workspace).
3. At the very end of the patching process, the Console VM will automatically restart (which closes the Windows PowerShell session). To verify that P&U successfully completed, look for the following event in Event Viewer (under **Applications and Services Logs -> PUEventLog -> Operational**) on the Console VM. You can search for **CompletePU**.

Note: Some Patch and Update processes run post Console VM reboot. Once you log in, the Patch and Update will run processes in the background and generate the event for a successful completion after a few

minutes. After the Console VM reboots and you log into the machine, please allow a few minutes for the background processes to complete and run the next package.

Level	Date and Time	Source	E...	Task Category
Information	11/20/2015 10:31:40 AM	PUEventLog	9	Progress
Information	11/20/2015 10:31:40 AM	PUEventLog	5	Start
Information	11/20/2015 10:31:40 AM	PUEventLog	9	Progress
Information	11/20/2015 10:31:40 AM	PUEventLog	2	CompletePU
Information	11/20/2015 10:31:40 AM	PUEventLog	6	Complete
Information	11/20/2015 10:31:40 AM	PUEventLog	9	Progress
Information	11/20/2015 10:31:40 AM	PUEventLog	6	Complete
Information	11/20/2015 10:31:40 AM	PUEventLog	6	Complete
Information	11/20/2015 10:31:40 AM	PUEventLog	6	Complete

4. If you disabled DPM agents on the DPM servers earlier, do the following to restart any canceled jobs and enable the DPM agents:

- a. On the Console VM, make sure that you are logged on as the account that is a member of **<Prefix>Setup-Admins**.
- b. Open an elevated Windows PowerShell session, and run the following commands. Press **Enter** after each command.

```
cd "\\<Prefix>CON01\PUshare\<CPSPU Folder Name>\PU\Framework\PatchingUpgrade"
```

```
Import-Module .\PatchingUpgrade\DPM.psm1
```

```
Set-DPMBackupMode -BackupMode Enable -Credential (Get-Credential)
```

- c. When prompted, enter the account credentials of the account that you are logged on as.

When the updates complete, compliance reports are generated at the following location:

```
\\<Prefix>CON01\PUshare\<CPSPU Folder Name>\PU\AggregatedLogs
```

This folder contains all logs and compliance reports. The top-level folder is named with a GUID. Sort by date modified to see the latest. You can open each subfolder to review the compliance report to verify what was installed.

Note: If you open the Windows Server Update Services (WSUS) console to view update status, understand that the P&U process does not apply Endpoint Protection definition updates. Therefore, you may see definition updates with a status of **Needed** or **No Status**. Antimalware updates are applied automatically by WSUS. By default, Endpoint Protection checks for updated antimalware definitions every eight hours.

If you do not intend to apply the 1803 Microsoft package immediately, remember to enable DPM agents if you disabled them earlier (as described in the *Dell Hybrid Cloud System for Microsoft CPS Standard Administrators Guide*). Note that this applies only if your solution includes Data Protection Manager (DPM) for backup.

Also, if you do not intend to apply the 1803 Microsoft package immediately, follow the steps in the "Post-update clean up" section of the *Dell Hybrid Cloud System for Microsoft CPS Standard Administrators Guide* after you have completed the update.

4.2.1 Run an optional compliance scan

If you want to run a compliance scan, pass the following flag:

```
\\SU1_InfrastructureShare1<CPSPU FolderName>\Framework\PatchingUpgrade\Invoke-  
PURun.ps1 -PUCredential $cred -ComplianceScanOnly
```

The compliance scan output is written to the following location, the place where the update package was extracted. For example, the following shows output written to:

```
"PURoot"\MissingUpdates.json
```

Post-update manual steps

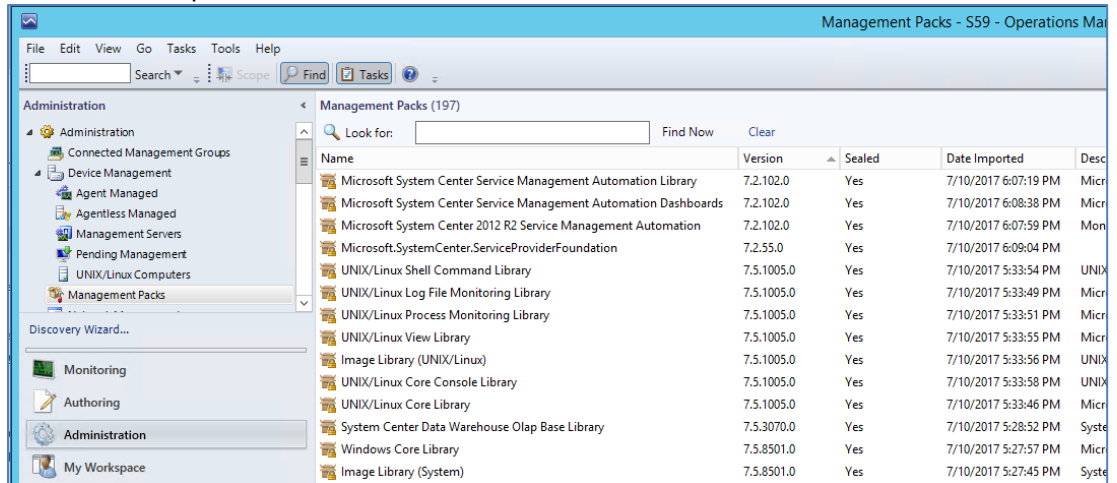
1. [KB#3000483](#) is a Windows Group Policy related security update (CVE-2015-0008). It requires both the binary files (delivered in P&U 1611 and 1703), and a Group Policy update. See the KB article for details on the Group Policy changes, including a section titled "Minimum recommended configuration for domain-joined computers". (Review the KB article, and decide how to implement for your organization and CPS domain.)
2. [KB#4038792](#) (Released in P&U 1803) includes a fix for security vulnerability [CVE-2017-8529](#). Two additional registry changes needs to be implemented through an Active Directory Group Policy Object (AD GPO). See the CVE article for the 2 registry keys that need to be implemented for 64-bit systems.
3. [KB#3170005](#) (Released in P&U 1803) will prevent the installation of some printers (non-package aware Version 3 printer drivers). If these older pre-Windows Vista printer drivers are being used with CPS, follow the steps in the KB article for creation of Active Directory Group Policy Object (AD GPO) to allow these older drivers. This change is not required if these older printer drivers are not in use.

Manually update the SMA Management Packs (MPs) for SCOM

Apply the updated SMA MPs into the SCOM Operations Console.

1. On the Console VM, open the SCOM Operations Console to import the MPs:
 - a. Navigate to: Administration | Management Packs.
 - b. In the right pane of the SCOM Operations Console, click on "Import Management Packs..."
 - c. In the Import Management Packs window, click on Add | Add from Disk...
 - d. Select "No" on the question of whether to search online for dependencies.
 - e. In the Import selection window, browse to the P&U share on the Console VM. Path similar to this (local to the Console VM):
C:\PU_Share\1706\PU\Payload\MgmtAssets\ManagementPacks.
 - f. Select the three files beginning with
"Microsoft.SystemCenter.ServiceManagementAutomation" in the 1803 P&U package.
 - g. Click on Open to select these three files into the import screen.
 - h. Click on "Install" to install these updated MP files for SMA.

2. Verify that the SMA MPs are updated in the SCOM Operations Console
 - a. In the Management Pack list (Administration | Management Packs) verify the version of these files has been updated to 7.2.102.0



- b. The updated MPs should show with the names of “Microsoft System Center Service Management Automation Library”, “Microsoft System Center Service Management Automation Dashboards”, and “Microsoft System Center 2012 R2 Service Management Automation”. The version should be 7.2.102.0 if they have been imported correctly.

Post-update clean up

After you have verified that patching has completed successfully, do the following to clean up the environment.

1. If you disabled DPM agents on the DPM servers earlier, do the following to restart any canceled jobs and enable the DPM agents:

- On the Console VM, make sure that you are logged on as the account that you created for patching, such as **CPS-Update-Admin**.
- Open an elevated Windows PowerShell session, and then run the following command:

```
$cred = Get-Credential (whoami)
```

- When prompted, enter the account password.
- Run the following commands. Press **Enter** after each command.

```
cd "\\VM Name\PUShare\<CPSPU Folder Name>\>\Framework\PatchingUpgrade"
```

```
Import-Module .\PatchingUpgrade\DPM.psml
```

```
Set-DPMBackupMode -BackupMode Enable -Credential $cred
```

2. If disk space is a concern, you can delete the VMM trace logs on each VMM server. These files are located at the root of C: on each VMM server, and will have names like: C:\VMMLog_*<Prefix>*-VMM-01_03301505.etl.

IMPORTANT: We recommend that you leave the latest update package in the PUShare in case diagnostics or debugging is needed. Also, do not remove the artifacts that were created during patching; for example, the VMM artifacts such as custom resources, and any associated log files, Windows Installer packages (.msi files), or patch files (.msp files).

4.3 Step 3: Run the 1803 DellEMC P&U package

IMPORTANT: You must run DHCS_Run_First and the 1803 Microsoft P&U package before you run the 1803 DellEMC P&U package.

Because of the size of this package, estimates for deployment duration are 12 to 18 hours. Run the PUDellEMC update package by doing the following:

1. Browse to the shared folder **PUShare** on the console VM, and create a folder to store the DELLEMC P&U package, such as **PU_DellEMC#**, where # is the number or some other identifier of the specific update package. For example:

```
\\<Prefix>CON01\PUShare\PU_DellEMC1803
```

IMPORTANT: Do not use the same folder name as an existing folder because you want to maintain a history of each patching update.

Note: If the update package is larger than 2 GB, and the copy and paste operation fails, see <https://support.microsoft.com/en-us/kb/2258090>.

2. While logged into the console VM, browse to the location where you unzipped the Patch and Update package you downloaded from the website, and execute the file with the format **DHCS_Update_1803_Run_Third.exe** to extract the update. When prompted, select the **PU_DellEMC1803** folder to store the extracted files.
3. Now that the patching environment is set up, you can start the patching process by running a Windows PowerShell script. Run the following command:

```
\\<Prefix>CON01\PUShare\PU_DellEMC1803\PU\Framework\PatchingUpgrade\Invoke-PURun.ps1 -PUCredential (Get-Credential)
```

Note: The P&U (Patch and Update) will stop if you have alerts in your SCOM. Please fix any issues reported by SCOM. If the alerts are not critical you can use:

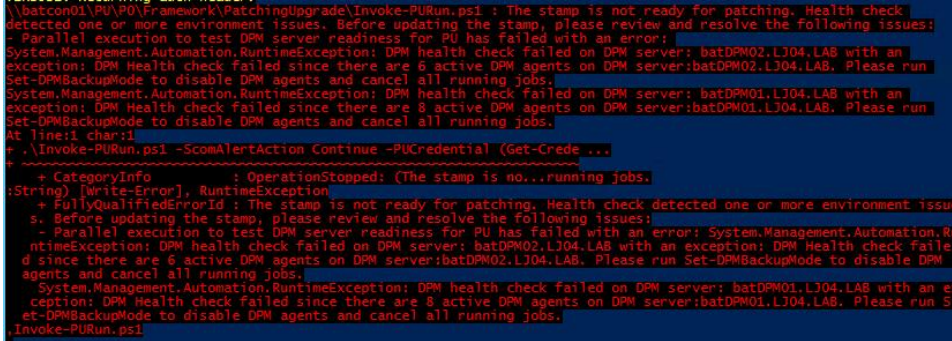
```
\\<Prefix>CON01\PUShare\PU_DellEMC1803\PU\Framework\PatchingUpgrade\Invoke-PURun.ps1 -PUCredential (Get-Credential) -ScomAlertAction "Continue"
```

4. When prompted, enter the account credentials of the account that you used to log into the ConsoleVM.
5. The **Invoke-PURun** script performs a one-time environment setup and may prompt you to restart Windows PowerShell on its for invocation, for example:

PowerShell environment settings have changed. Please restart the PowerShell console before proceeding.

If you see this message, close the current Windows PowerShell session, open a new elevated Windows PowerShell session, and repeat steps 2 through 4 to start the health check process.

6. DPM agents on the DPM servers are in an Enabled state. If this is the case, the health check output indicates that you must run the **Set-DPMBackupMode** script to cancel the jobs and disable the agents. The PowerShell output looks similar to the following screenshot:



```
\\batcon01\PU\PO\Framework\PatchingUpgrade\Invoke-PUrun.ps1 : The stamp is not ready for patching, Health check
detected one or more environment issues. Before updating the stamp, please review and resolve the following issues:
- Parallel execution to test DPM server readiness for PU has failed with an error:
System.Management.Automation.RuntimeException: DPM health check failed on DPM server: batDPM02.LJ04.LAB with an
exception: DPM Health check failed since there are 6 active DPM agents on DPM server:batDPM02.LJ04.LAB. Please run
Set-DPMBackupMode to disable DPM agents and cancel all running jobs.
System.Management.Automation.RuntimeException: DPM health check failed on DPM server: batDPM01.LJ04.LAB with an
exception: DPM Health check failed since there are 8 active DPM agents on DPM server:batDPM01.LJ04.LAB. Please run
Set-DPMBackupMode to disable DPM agents and cancel all running jobs.
At line:1 char:1
+ .\Invoke-PUrun.ps1 -ScomAlertAction Continue -PUCredential (Get-Crede...
+ ~~~~~
+ CategoryInfo          : OperationStopped: (The stamp is no...running jobs,
:String) [Write-Error], RuntimeException
+ FullyQualifiedErrorId : The stamp is not ready for patching, Health check detected one or more environment issue
s. Before updating the stamp, please review and resolve the following issues:
- Parallel execution to test DPM server readiness for PU has failed with an error: System.Management.Automation.Ru
ntimeException: DPM health check failed on DPM server: batDPM02.LJ04.LAB with an exception: DPM Health check fail
ed since there are 6 active DPM agents on DPM server:batDPM02.LJ04.LAB. Please run Set-DPMBackupMode to disable DPM
agents and cancel all running jobs.
System.Management.Automation.RuntimeException: DPM health check failed on DPM server: batDPM01.LJ04.LAB with an ex
ception: DPM Health check failed since there are 8 active DPM agents on DPM server:batDPM01.LJ04.LAB. Please run S
et-DPMBackupMode to disable DPM agents and cancel all running jobs.
.\Invoke-PUrun.ps1
```

7. To cancel the jobs and disable the agents, do the following:
 - a. From an elevated Windows PowerShell session, run the following commands. Press **Enter** after each command:

```
cd "\\<Prefix>CON01\PUshare\<CPSPU Folder
Name>\PU\Framework\PatchingUpgrade"

Import-Module .\PatchingUpgrade\DPM.psm1

Set-DPMBackupMode -BackupMode Disable -Credential (Get-Credential)
```

- b. When prompted, enter the account credentials of the account that you are logged on as.

At this point, the Patch and Update process should begin, with verbose output of the progress.

1. During the patching process note the following:
 - If you click inside the Windows PowerShell window during the patching process, the screen output will freeze, although the update process is still running. Press **Enter** to continue the scrolling of output.
 - Some component updates do not output status to the Windows PowerShell console. See the next step for other ways to monitor progress.
 - Updates of the physical cluster nodes may take a while. For example, a task that involves the compute cluster (CCL) or storage cluster (SCL) may take some time, and the output may not update for a while. You can use the following steps to view the progress of cluster updates in Failover Cluster Manager.
 - i. Open Failover Cluster Manager.
 - ii. Connect to the cluster.
 - a. In the navigation pane, right-click **Failover Cluster Manager**, and then click **Connect to Cluster**.
 - b. In the **Select Cluster** dialog box, click **Browse**.
 - c. Click the desired cluster, and then click **OK** two times.

- iii. In the navigation pane, right-click the cluster name, point to **More Actions**, and then click **Cluster-Aware Updating**.
- iv. In the **ClusterName – Cluster-Aware Updating** dialog box, click the **Log of Updates in Progress** tab to monitor what is happening.

Note: After Cluster-Aware Updating (CAU) completes, you can click **Generate a report on past Updating Runs** to view details about what was installed through CAU.

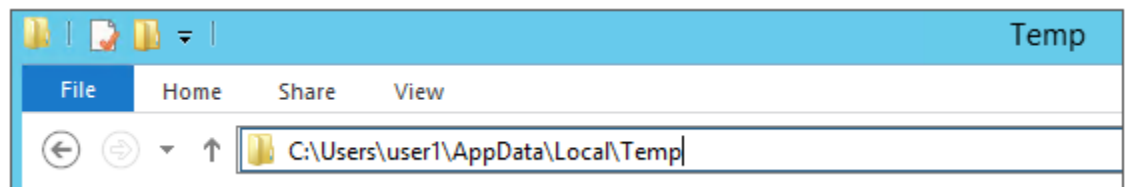
- If you have the VMM console open, and it reconnects, patching of the VMM server may be in progress. This is expected behavior.
2. To monitor the progress, you can use the following methods:
 - View the verbose output on the screen.
 - View the P&U events in Event Viewer. You can find P&U events under **Applications and Services Logs -> PUEventLog -> Operational**.
 - View the temp folder to retrieve logs with more details. To determine the temp folder, run the following command in Windows PowerShell:

```
[System.IO.Path]::GetTempPath()
```

The temp folder path will be something similar to this:

C:\Users\username\AppData\Local\Temp\2

If the temp folder path includes a numbered folder, such as 2, 3, or 4, you will need to go up one folder level to the **\Temp** folder. If you browse in File Explorer, note that **AppData** is a hidden folder. You can type the folder path to get to it, for example:



In the **Temp** folder, look for the file that is named **PUPProgressDetails.txt**.

- a. View running jobs in the VMM console (in the **Jobs** workspace).

At the very end of the patching process, the Console VM will automatically restart (which closes the Windows PowerShell session). To verify that P&U successfully completed, look for the following event in Event Viewer (under **Applications and Services Logs -> PUEventLog -> Operational**) on the Console VM. You can search for **CompletePU**.

5 Microsoft payload for Update 1803

Payload for Update 1803

Update Details

KB Number	Title	CVE / ADV
890830	Windows Malicious Software Removal Tool x64 - March 2018	N/A
4055266	2018-01 Security and Quality Rollup for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1 on Windows 8.1 and Server 2012 R2 for x64	CVE-2018-0786, CVE-2018-0764
4088876	2018-03 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0816, CVE-2018-0817, CVE-2018-0868, CVE-2018-0878, CVE-2018-0881, CVE-2018-0883, CVE-2018-0885, CVE-2018-0886, CVE-2018-0888, CVE-2018-0889, CVE-2018-0891, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, CVE-2018-0901, CVE-2018-0904, CVE-2018-0927, CVE-2018-0929, CVE-2018-0932, CVE-2018-0935, CVE-2018-0942
4088785	2018-03 Security Update for Adobe Flash Player for Windows Server 2012 R2 for x64-based Systems	ADV180006
N/A	Azure Site Recovery - MARS Agent v.2.0.9106.0	N/A
N/A	Azure Site Recovery - ASR Provider v.5.1.2948.0	N/A
4041077	Update Rollup 14 for Microsoft System Center 2012 R2 - Virtual Machine Manager	N/A
4043909	Update Rollup 12 for Windows Azure Pack	N/A
N/A	SQL Native Client - v.11.4.7462.6	N/A
N/A	SQL ODBC 11 Client - v.12.2.5571.0	N/A
N/A	Azure PowerShell Module – v.5.3.0	N/A
4052725	Cumulative Update 10 for SQL Server 2014 SP2	N/A
4056898	2018-01 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	ADV180002, CVE-2018-0744, CVE-2018-0746, CVE-2018-0747, CVE-2018-0748, CVE-2018-0749, CVE-2018-0751, CVE-2018-0752, CVE-2018-0753, CVE-2018-0754, CVE-2018-0788
N/A	System Center Management Pack for System Center 2012 R2 Orchestrator - Service Management Automation (Version 7.2.102.0)	N/A

5.1 Troubleshooting the P&U process

Issue 1

Symptoms:

The P&U install process fails with an SMA MAX Timeout Error:

```
Exception calling "InvokeRunbook" with "2" argument(s): "Max Timeout reached for SMA runbook 'Import-OmManagementPack'."
```

P&U fails after a two-hour timeout waiting for the Runbook to complete.

Description:

SMA Service is hanging when processing runbooks for P&U, specifically the **"Import-OmManagementPack"** Runbook.

Detection:

Looking at running SMA jobs in the Windows Azure Pack management portal for administrators, under **Automation | Runbooks** you see jobs stuck with the **Job Status** showing **"Queued"**.

Resolution:

There are two potential fixes for this issue, one temporary, and one more permanent.

- The temporary fix resolves the problem immediately, but does not prevent it from happening again. This fix involves rebooting the SMA VM (<Prefix>APA01). This restarts any queued jobs in SMA.
- The more permanent fix has performance impacts to SMA (<Prefix>APA01), but will prevent the issue from happening again.

To apply the more permanent fix, do the following:

1. On the SMA VM (<Prefix>APA01), modify the following values in the Program Files\Microsoft System Center 2012 R2\Service Management Automation\Orchestrator.Settings.config file:

Old Values	New Values
<code><add key="MaxRunningJobs" value="30"/></code>	<code><add key="MaxRunningJobs" value="1"/></code>
<code><add key="TotalAllowedJobs" value="1000"/></code>	<code><add key="TotalAllowedJobs" value="1"/></code>

2. After changing these two settings, reboot the SMA VM (xxxAPA01).

Issue 2

Symptoms:

Exclude external host from P&U.

Description:

If you have added a physical host to VMM that is not part of the CPS Standard stamp—in this case the stamp includes backup infrastructure—you must exclude the host from P&U. If you do not, P&U will fail.

Detection:

The P&U process fails after adding a physical host to VMM that is not part of the CPS Standard stamp.

Resolution:

To exclude an external host from P&U:

1. In the VMM Console, open the **Fabric** workspace.
2. Under **Servers**, click **All Hosts**.
3. In the **Hosts** pane, right-click the external host, and then click **Properties**.
4. Click the **Custom Properties** tab.
5. In the PU custom property box, type **External1**, and then click **OK**.

With this entry, P&U will skip the external host. You are responsible for updating any external servers outside of P&U.

Issue 3

Symptoms:

The P&U process updates the console, including reboots, but does not finish final P&U processing.

Description:

This can include examining the Deployment Manifest and running compliance checks.

Detection:

Run the following script (updating the `$prefix` variable before running with the prefix of your stamp):

```
$prefix = "<Prefix>"  
(Get-SmaVariable -WebServiceEndpoint ("https://{0}APA01" -f $prefix) -Name  
PUSubsystemVersions).Value
```

If any of the values for "MicrosoftVersion" is not "1.0.1803.18000", you have run into this issue.

Resolution:

Restart P&U.

Issue 4

Symptoms:

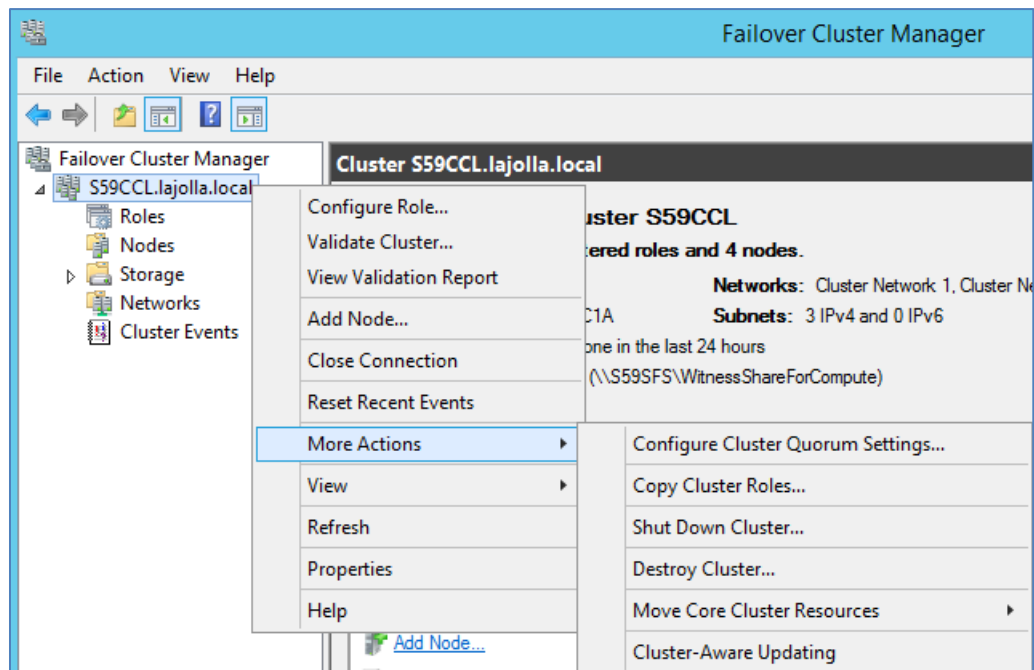
Failure in P&U during the "CCL" subsystem.

Description:

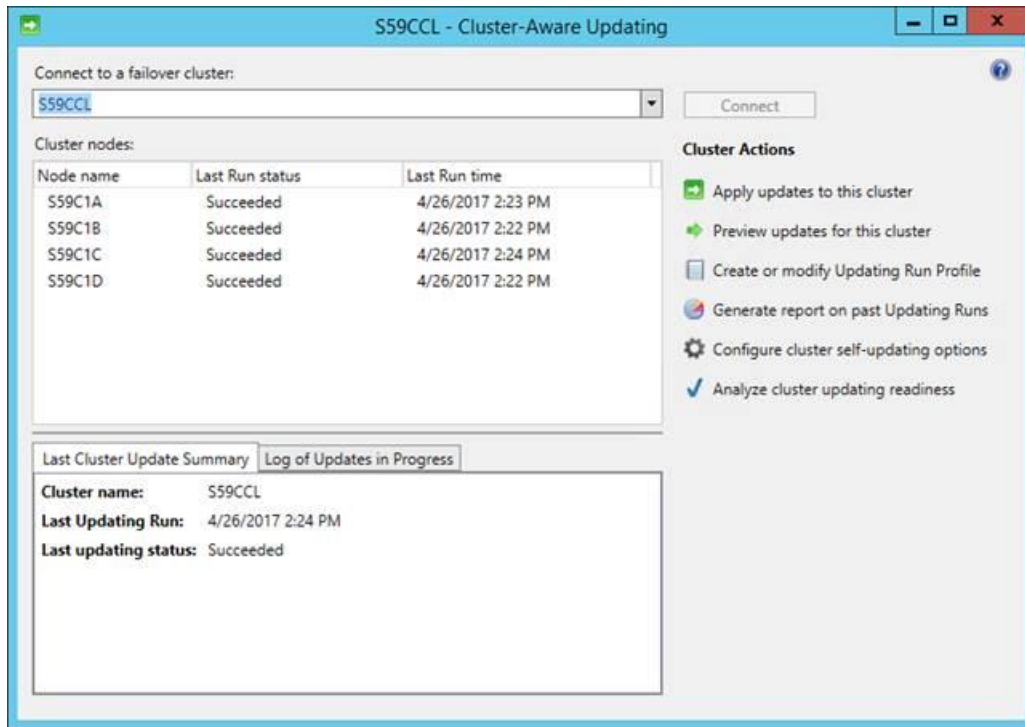
This can include updating the Deployment Manifest and running compliance checks.

Detection:

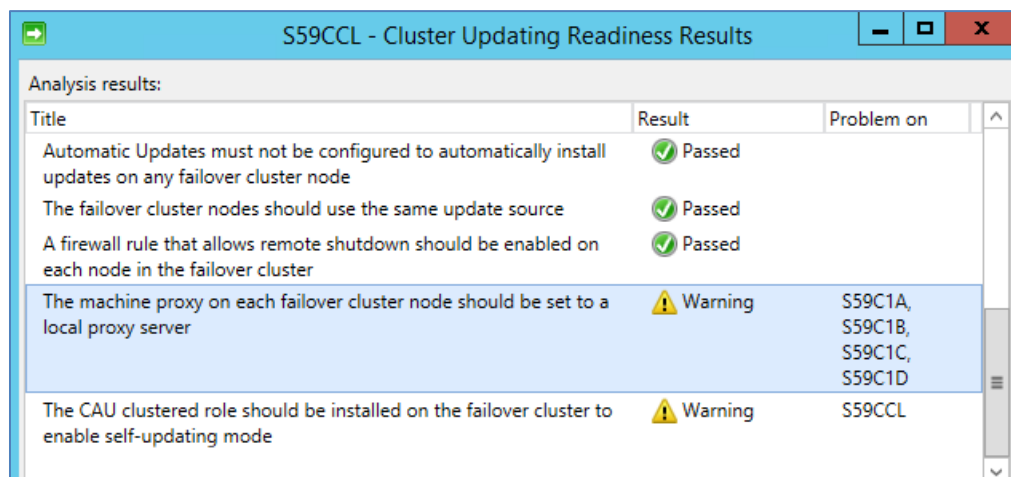
1. Open **Failover Cluster Manager**.
2. Right-click on the CCL cluster and choose **More Actions**, and then choose **Cluster-Aware Updating**.



- Once the **Cluster-Aware Updating** dialog opens, select **Analyze cluster updating readiness**.



- The analyzer runs for a minute or two, and then shows you the results, as illustrated by the following graphic:



Under the Title **“A firewall rule that allows remote shutdown should be enabled on each node in the failover cluster”** you should see a green **‘Passed’** result. If there are any compute nodes that are members of this CCL cluster listed as having failed this test, you have run into this issue.

Resolution:

Reboot the affected nodes. After you have rebooted the affected nodes, run **Analyze cluster updating readiness** again. Once it is in a **Passed** state, you can rerun the P&U.

Issue 5

Symptoms:

NVGRE issue. The DellEMC Patch and Update framework does not bypass the "External" custom property of any non-DHCS hardware in the stamp.

Description:

If you add non-DHCS hardware external servers to your stamp, or have a different custom property setup on any of the existing servers, you need to set the custom property as "External" for the framework to bypass it.

The Microsoft P&U framework bypasses anything with custom property set to "External", but the DellEMC framework does not. The DellEMC P&U framework runs on a variation of Microsoft's P&U framework, and is a different package.

Resolution:

Browse to the location where the DellEMC Patch and Update package has been extracted. Under `C:\PUShare\PU_DellEMC1803\ Subsystems\PU` you can find the `Test-PUHealth.ps1` script, and in the following snippet, add the highlighted workaround:

```
Write-HealthLog -TelemetryInfo $TelemetryInfo -EventType
"Progress" -Message "Checking PU custom property for
'$($server.ComputerName) '."

    $PUCustomPropertyValue = Get-SCCustomPropertyValue -VMMServer
$VMMServerName -CustomProperty $PUCustomProperty -InputObject $server

    if($PUCustomPropertyValue -ne $null)
    {
        if($PUCustomPropertyValue.Value -eq "External")
        {
            continue
        }
    }
}
```

```
    }

    if($ObjectType -eq "Host")
    {
        $expectedCustomValue =
if($PUCustomPropertyValue.Value -eq "BackupHost")
{$customValues["DPMHost"]} else {$customValues[$ObjectType]}
    }

    else
    {
```

Now re-run the DellEMC patch and update framework, and this will bypass the server with the "External" custom property.

Issue 6

Symptoms:

From the Console VM, the CPS Administrator cannot access the OEM OOB (Out-of-Band Management) webpage through Internet Explorer. The error will be similar to the following:

This page can't be displayed

Turn on TLS 1.0, TLS 1.1, and TLS 1.2 in **Advanced settings** and try connecting to <https://URL> again. If this error persists, it is possible that this site uses an unsupported protocol or cipher site such as RC4 (link for details), which is not considered secure. Please contact your administrator.

Cause:

TLS 1.2 ciphers were strengthened in P&U 1706 (and higher) on all hosts and VMs in the CPS stamp. The Dell iDRAC cannot communicate using these enhanced cryptography ciphers.

Workaround:

1. To temporarily unblock the issue, delete this registry key value on the Console VM trying to access the F5 Configuration:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002]
"Functions"="TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256"
```

2. Reboot the console VM after deleting the "Functions" value, which will return the Console VM to the default Windows cipher suites.

6 Dell EMC Payload for Update 1803

- **Dell Server PowerEdge BIOS R630/R730/R730XD Version 2.7.1 Fixes & Enhancements:**
 - **Fixes**
 - None
 - **Enhancements**
 - Updated the Intel Xeon Processor Microcode to address CVE-2017-5715 (<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5715>)
 - Updated the Intel Xeon Processor E5-2600 v4 Product Family Processor Microcode to version 0x0b00002A.
 - Updated the Xeon Processor E5-2600 v3 Product Family Processor Microcode to version 0x3C.
 - CVE-2017-5753 and CVE-2017-5754 are addressed by Operating System & Hypervisor updates.
 - Please see more information at <http://www.dell.com/support/article/SLN308588>
- **Dell Server BIOS PowerEdge C6320 Version 2.7.1 Fixes & Enhancements**
 - **Fixes**
 - None
 - **Enhancements**
 - Updated the Intel Xeon Processor Microcode to address CVE-2017-5715 (<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5715>)
 - Updated the Intel Xeon Processor E5-2600 v4 Product Family Processor Microcode to version 0x0b00002A.
 - Updated the Xeon Processor E5-2600 v3 Product Family Processor Microcode to version 0x3C.
 - CVE-2017-5753 and CVE-2017-5754 are addressed by Operating System & Hypervisor updates.
 - Please see more information at <http://www.dell.com/support/article/SLN308588>
- **iDRAC with Lifecycle Controller V.,2.52.52.52 for C6320/R630 Fixes & Enhancements**
 - **Fixes:**
 - iDRAC and LC firmware
 - Fixed code to correct intermittent PCIe SSDs not reporting in iDRAC GUI issue.
 - Fixed the issue of iDRAC intermittently not populating inventory details.
 - Improved the JffS2 file system recovery logic to avoid iDRAC boot hang.
 - Fixed the issue of HBA330 card not being displayed in BIOS and iDRAC.
 - **Security**
 - Fixed CVE-2018-1207, CVE-2018-1208, CVE-2018-1209, CVE-2018-1210, and CVE-2018-1211.
 - **Enhancements:**
 - Networking and IO
 - Removed support for SMBv1 protocol. All iDRAC features now support SMBv2/SMBv3 protocols. For information on enabling SMBv2/SMBv3 protocols, see the Operating System documentation.
- **Dell PERC H330 Mini/Adapter RAID Controllers firmware version 25.5.4.0006 Fixes & Enhancements**
<http://www.dell.com/support/home/us/en/04/drivers/driversdetails?driverId=V4G60>
 - **Fixes**
 - Changes default value of drive cache for 6 Gbps SATA drives to disabled. This is to align with the industry for SATA drives. This may result in a performance degradation especially in non-Raid mode. You must perform an AC reboot to see existing configurations change.

- Fixes an issue where a random corner case firmware FMU fault can lead to controller hangs for approximately 15 seconds. Search controller logs for the string "fusionMUErrors: FMU Error Status 00040000."
- Fixes an issue where SATA drives could randomly return 04/44/00 check condition in a VSAN environment. Search the controller log for the string "Sense: 4/44/00". For example: "07/24/17 11:00:55: C0:EVT#8446014-07/24/17 11:00:55: 113=Unexpected sense: PD 02(e0x20/s2) Path 500056b3fafedac2, CDB: 9e 10 00 00 00 00 00 00 00 00 00 00 20 00 00, Sense: 4/44/00"
- Fixes an issue where you can see false multiple SRAM correctable errors that could result in performance problems or even in a server crash. Search tty log for the string "SRAM errAddr" or "Correctable err, continuing...". For example: "C0:SRAM errAddr c0023010 errAttrib 00000003" followed by "C0:Correctable err, continuing..."
- Fixes an issue where a random RSOD could occur during boot only if there are multiple PERC controllers in the config.
- Fixes an issue where VD deletion and VD creation events are not seen in iDRAC LC log.
- Fixes an issue where sometimes controller fails to unlock and import multiple secure foreign configurations only if foreign VDs have different secured pass phrases.
- **Enhancements**
- None
- **Dell PERC H730/H730P/H830/FD33xS/FD33xD Mini/Adapter RAID Controllers firmware version 25.5.4.0006 Fixes & Enhancements**
 - **Fixes**
 - Changes default value of drive cache for 6 Gbps SATA drive to disabled. This is to align with the industry for SATA drives. This may result in a performance degradation especially in non-Raid mode. You must perform an AC reboot to see existing configurations change.
 - Fixes an issue where a specific firmware FMU fault can lead to controller hangs for approximately 15 seconds. Search controller logs for the string "fusionMUErrors: FMU Error Status 00040000".
 - Fixes an issue where SATA drives could randomly return 04/44/00 check condition in a VSAN environment. Search the controller log for the string "Sense: 4/44/00". For example: "07/24/17 11:00:55: C0:EVT#8446014-07/24/17 11:00:55: 113=Unexpected sense: PD 02(e0x20/s2) Path 500056b3fafedac2, CDB: 9e 10 00 00 00 00 00 00 00 00 00 00 20 00 00, Sense: 4/44/00"
 - Fixes an issue where you can see false multiple SRAM correctable errors that could result in performance problems or even in a server crash. Search tty log for the string "SRAM errAddr" or "Correctable err, continuing...". For example: "C0:SRAM errAddr c0023010 errAttrib 00000003" followed by "C0:Correctable err, continuing..."
 - Fixes an issue where external enclosures sometimes lose time sync.
 - Fixes an issue where a random RSOD could occur during boot only if there are multiple PERC controllers in the configuration.
 - Fixes an issue where the battery could inadvertently change to WT during a transparent learn cycle.
 - Fixes an issue where VD deletion and VD creation events are not seen in iDRAC LC log.
 - Fixes an issue where sometimes controller fails to unlock and import multiple secure foreign configurations only if foreign VDs have different secured pass phrases.
 - **Enhancements**
 - None
- **Dell HBA330 Mini firmware version 15.17.08.01 Fixes & Enhancements**
 - **Fixes:**
 - Miscellaneous SATA fixes including::
 - SMART Passthrough Commands might fail in some circumstances
 - Passthrough commands issued PIO Mode might receive incorrect status values
 - Inquiry to page 0xB0 returned truncated data
 - Inquiry to VPD page 0x89 returned extra, invalid data
 - Unmap command translation for SATA drives might fail if Number of Logical Blocks or Parameter List Length was set to zero

- Inquiry comments to Non-Zero LUNs (which are not supported by SATL) would improperly succeed if a FORMAT UNIT was in progress
- WRITE SAME command had several issues in which a single command failure could result in subsequent commands being improperly failed
- **Enhancements**
 - NA
- Windows Server 2012 R2 Driver version 2.51.15.00 for Dell 12Gbps HBA and HBA330 Fixes & Enhancements
 - Fixes
 - Fixed issue where array path is lost when the SAS end device has a LUN that cannot respond successfully to TUR
 - Enhancements
 - N/A
- **Intel NIC Family Version 18.3.0 Firmware for I350, I354, X520, X540, and X550 adapters Fixes & Enhancements**
 - **Fixes**
 - Fixed a problem affecting Intel(R) Ethernet 10G 2P X550-t Adapter where 'Virtual World Wide Node Name' and 'Virtual World Wide Port Name' are non-zero by default, displayed as having values of "20:00:" and "20:01:", respectively. To apply the fix, do the following:
 1. Update the firmware via the operating system (not the Lifecycle Controller or iDRAC)
 2. Reboot the system
 - Fixed issue with rollback functionality in iDRAC9 with Lifecycle Controller not working for the Intel devices supported by this package.
 - Fixed issue with Intel(R) X550 adapters not allowing use of special characters for iSCSI Boot "Chap ID" and "Chap Secret" settings.
 - Fixed issue with Lifecycle Controller that may cause fatal OS error if diagnostics are run twice after firmware update.
 - Resolved issue with PXE boot failure in UEFI mode at 1Gb link speed on Intel(R) X550 adapters.
 - **Enhancements**
 - Added support for Red Hat Enterprise Linux 7.4
 - Added support for Red Hat Enterprise Linux 6.9
 - Added support for SUSE Linux Enterprise Server 12 SP3
- **Intel C600/C610/C220/C230/C2000 Series Chipset Drivers Version 10.1.2.85 Fixes & Enhancements**
 - **Fixes:**
 - Resolves an issue where the DUP is not executing under Windows Server Core OS installations.
 - Enhancements:
 - None
- **Dell 13G PowerEdge Server Backplane Expander Firmware Version 3.35, A00-00 Fixes & Enhancements**
 - **Fixes:**
 - Addresses problems for medium to low severity issues related to SAS enumeration issues when connected to a Broadcom HBA.
 - **Enhancements:**
 - None

- **Non-expander Storage Backplane Firmware Version 2.25, A00-00 Fixes & Enhancements**
 - **Fixes:**
 - Addresses a problem detecting drive type for 1.8" drives.
 - **Enhancements:**
 - None