

Update 1909 for Cloud Platform System (CPS) Standard

Dell Hybrid Cloud System for Microsoft

Dell Engineering

January 2020

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
May 2018	Release 1804
June 2018	Release 1805
July 2018	Release 1806
August 2018	Release 1807
September 2018	Release 1808
October 2018	Release 1809
November 2018	Release 1810
December 2018	Release 1811
January 2019	Release 1812
March 2019	Release 1901. Added "Upgrade the Intel NIC Driver" section
April 2019	Release 1902
April 2019	Release 1903
June 2019	Release 1905
January 2020	Release 1909

Copyright © 2019 Dell Inc. All rights reserved. Dell and the Dell EMC logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Table of contents

- Revisions 2
- 1 Overview of the Patch and Update framework 6
- 2 Update 1909—Summary 7
 - 2.1 Additional update information..... 7
 - 2.2 How to check which update package is installed..... 8
 - 2.3 When to run the update package 8
- 3 1909 Patch and Update Prerequisites 9
 - 3.1 Prepare the patching environment..... 9
 - 3.2 Step 1: Prepare user account for patching 9
 - 3.3 Step 2: Ensure that Group Policy does not block the mounting of USB virtual disks 9
 - 3.4 Step 3: Extract the Patch and Update package 9
 - 3.5 Step 4: Ensure that `LaJollaDeploymentService` is not running in the background on the Console VM.. 10
 - 3.6 Step 5: Clean up the WSUS server..... 10
 - 3.7 Step 6: (Optional): Exclude external SOFS storage clusters from P&U 11
- 4 1909 Patch and Update Process 12
 - 4.1 Step 1: Run the 1909 DellEMC P&U package (`DHCS_Update_1909_Run_First`)..... 12
 - 4.2 Step 2: Upgrade the Intel NIC Driver 15
 - 4.3 Step 3: Run the 1909 Microsoft P&U package (`DHCS_Update_1909_Run_Second`) 17
 - 4.3.1 Run an optional compliance scan 21
- 5 Microsoft payload for Update 1909 24
 - Payload for Update 1909 24
 - 5.1 Troubleshooting the P&U process 25
- 6 Dell EMC Payload for Update 1909 32

WARNING: You cannot run the 1909 Patch & Update framework—1.5.14—directly without first upgrading your environment to 1803 Patch & Update framework—1.5. You can directly upgrade to 1909 only after the DHCS stamp is at the 1.5 version, P&U 1803. 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** in the Troubleshooting section.

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 1909—Summary

Update 1909 for CPS Standard includes updates for Windows Server. This update includes the following components:

1909 update. This is the main package. It can contain Windows Server, System Center, and SQL Server updates. (See payload details in [Chapter 5](#).)

IMPORTANT: Update 1803 is a prerequisite for installing update 1909.

IMPORTANT: Update 1812 contains a security related WAP update ([See CVE-2018-8652](#)). It is advised that this update be applied promptly due to the vulnerability described in the CVE.

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.

For detailed update payload information, see [Chapter 5](#).

2.1 Additional update information

- **Update 1804** (and higher) includes configuration changes to support [KB# 4093492](#), which impacts CredSSP authentication protocol and RDP functions. All servers in a CPS environment are now forcing the registry key “HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\CredSSP\Parameters\AllowEncryptionOracle” to a value of “1”. See [KB# 4093492](#) for any impacts to your environment
- **Update 1808** (and higher) includes configuration changes to support [KB# 4072698](#), the FeatureSettingsOverride registry setting is set to “8”. This setting enables mitigations around Speculative Store Bypass (CVE-2018-3639) together with mitigations around Spectre Variant 2 (CVE-2017-5715 "Branch Target Injection") and Meltdown (CVE-2017-5754) through the following registry settings (because they are not enabled by default).
- Update 1909 (and higher) includes configuration changes to support [KB# 4072698](#), the FeatureSettingsOverride registry setting is set to “72”. This setting enables mitigations for microarchitectural Data Sampling (CVE-2018-11091, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130) along with Spectre [CVE-2017-5753 & CVE-2017-5715] and Meltdown [CVE-2017-5754] variants, including Speculative Store Bypass Disable (SSBD) [CVE-2018-3639] as well as L1 Terminal Fault (L1TF) [CVE-2018-3615, CVE-2018-3620, and CVE-2018-3646]

All instructions on installing this update are included in this guide.

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": "1.0.1803.21000"
```

The third value (1803 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 1909 contains three distinct phases:

- [1909 Patch and Update Prerequisites](#)
- [Step 1: Run the 1909 DellEMC P&U package \(DHCS_Update_1909_Run_First\)](#)
- [Step 2: Upgrade the Intel NIC Driver](#)
- [Step 3: Run the 1909 Microsoft P&U package \(DHCS_Update_1909_Run_Second\)](#)

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

1. Prerequisites
2. DellEMC P&U package (DHCS_Update_1909_Run_First)
3. Apply New NIC Driver
4. Microsoft P&U package (DHCS_Update_1909_Run_Second)

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 1909 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

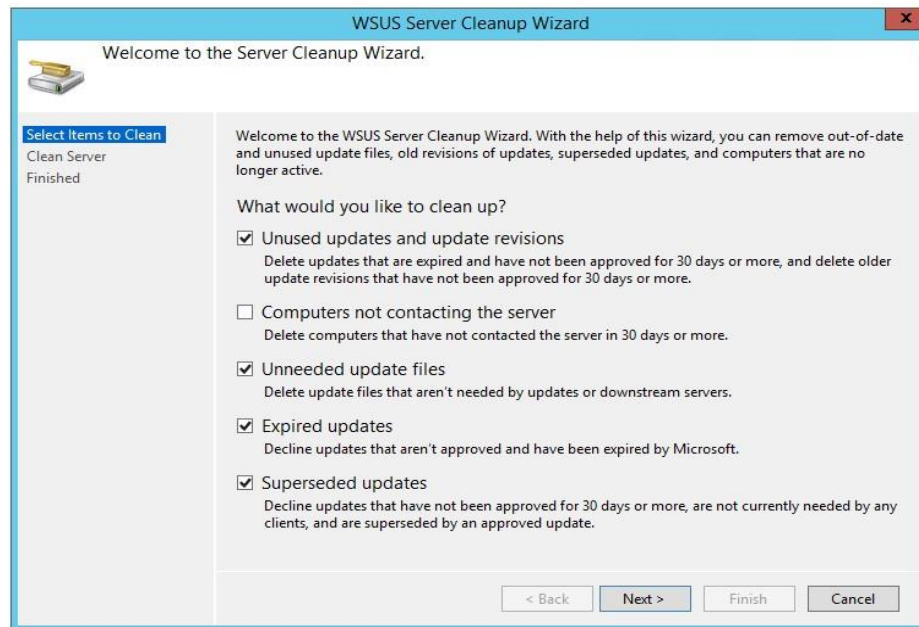
You can ensure that the service `LaJollaDeploymentService` is stopped by doing the following:

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

Before you run P&U, run the WSUS Server Cleanup Wizard to remove old files.

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**.
5. In the **Status** list, click **Any**. Then, click **Refresh**.
6. Select all updates.
7. Right-click the selection, and then click **Decline**.
8. In the left pane, expand the server name, and then click **Options**.
9. In the **Options** pane, click **Server Cleanup Wizard**.
10. Make sure that all check boxes are selected *except* for the **Computers not contacting the server** check box.



11. Click **Next** to start the cleanup process.
12. Restart the Console VM.

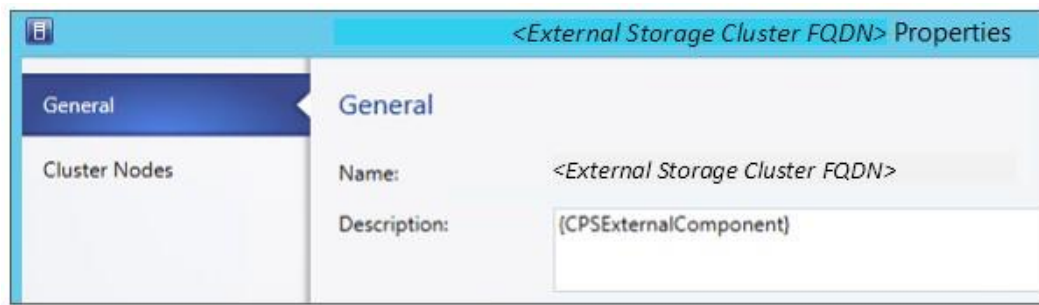
3.7 Step 6: (Optional): Exclude external SOFS storage clusters from P&U

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 1909 Patch and Update Process

IMPORTANT: Be sure to follow the prerequisites listed in the previous section before you run the 1909 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 1909 DellEMC P&U package (DHCS_Update_1909_Run_First)

IMPORTANT: You must run this package (DHCS_Update_1909_Run_First) before you run the 1909 Microsoft P&U package (DHCS_Update_1909_Run_Second).

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 DELL EMC 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_DellEMC1909
```

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_1909_Run_First.exe** to extract the update. When prompted, select the **PU_DellEMC1909** 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_DellEMC1909\PU\Framework\PatchingUpgrade\InvokePURun.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_DellEMC1909\PU\Framework\PatchingUpgrade\InvokePURun.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.

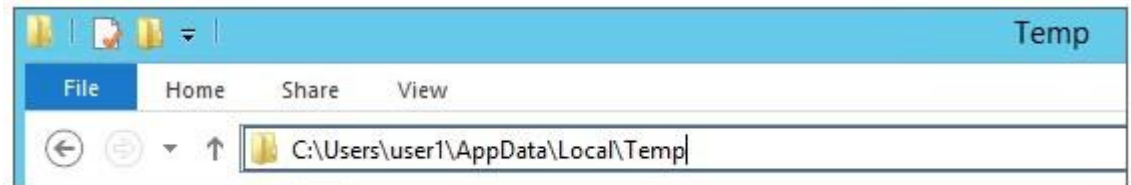
- If you have the VMM console open, and it reconnects, patching of the VMM server may be in progress. This is expected behavior.
2. To monitor the progress, you can use the following methods:
- View the verbose output on the screen.
 - View the P&U events in Event Viewer. You can find P&U events under **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**.

4.2 Step 2: Upgrade the Intel NIC Driver

IMPORTANT: You must manually upgrade the NIC driver on all your physical servers. Failure to do so could result in Blue Screen of Death Errors.

1. **Extract the NIC driver from the zip package**
 - a. Unzip the NIC drivers from the file [Network_Driver_M1P35_WN64_18.8.0_A00_01.zip](#) which is located in the folder [C:\PUShare\DellEMC1909\Payload\PatchingUpdates\DellUpdate\CAUHotfix_All\Binaries](#) to the folder [C:\PUShareNIC](#)
2. **Replicate the Intel NIC drivers to all the servers**
 - a. Open a PowerShell window with Administrative Privileges
 - b. Copy the Intel NIC driver to all the Compute Nodes
 - i. Run the command: `Robocopy "C:\NIC" "\\<Prefix>C<xx><Node ID>\C$\DellNIC" /e /r:0 /w:0`

Example:
`Robocopy "C:\PUShareNIC" "\\1703C12A\C$\DellNIC" /e /r:0 /w:0`
 - ii. Repeat the above step for every File server node in your stamp
 - c. Copy the Intel NIC driver to all the File Servers
 - i. Run the command: `Robocopy "C:\NIC" "\\<Prefix>S<xx>\C$\DellNIC" /e /r:0 /w:0`

Example:
`Robocopy "C:\PUShareNIC" "\\1703S120\C$\DellNIC" /e /r:0 /w:0`
 - ii. Repeat the above step for every File server in your stamp
 - d. Copy the Intel NIC driver to all the DPM Servers
 - i. Run the command: `Robocopy "C:\NIC" "\\<Prefix>B<xx>\C$\DellNIC" /e /r:0 /w:0`

Example:
`Robocopy "C:\PUShareNIC" "\\1703B01\C$\DellNIC" /e /r:0 /w:0`
 - ii. Repeat the above step for every DPM server in your stamp
3. **Upgrade the Intel NIC Driver on the Compute Cluster Nodes**
 - a. Open the Failover Cluster Manager console
 - i. Expand the Compute Node Cluster **<Prefix>CCL**
 - ii. Click on Nodes
 - iii. Select one of the nodes in the cluster
 - iv. Right mouse click on it, select Pause, then on Drain Roles
 - v. You must now wait until the status of the node changes to Paused
 - b. Open a PowerShell window with Administrative Privileges and run the following commands:
 - i. `Enter-PSSession <Prefix>C<xx><Node ID>`
 - ii. `pnputil -i -a C:\DellNIC\Umb\Winx64\PRO1000\NDIS64*.inf`
 - iii. `pnputil -i -a C:\DellNIC\Umb\Winx64\PROXGB\NDIS64*.inf`
 - iv. `Restart-Computer`
 - v. `Exit`
 - c. Monitor the progress of the node
 - i. Go back to the Failover Cluster Manager console
 - ii. The status of the node will have changed to Down
 - iii. After the node has finished rebooting, the status will change to Paused
 - iv. Select the node and right mouse click on it, select Resume, then on Fail Roles Back
 - v. You must now wait until the status of the node changes to Up

- d. Verify that the driver was successfully updated
 - i. Go back to the PowerShell window and run the following commands:
 - ii. `Enter-PSSession <Prefix>C<xx><Node ID>`
 - iii. `Get-WmiObject Win32_PnPSignedDriver | Select-Object -Property devicename, driverversion | Where devicename -like 'Intel(R) Ethernet*'`

Note: The driver version should now be 3.14.78.0
 - e. Repeat steps a through d on every Compute cluster node in the stamp.
4. **Upgrade the Intel NIC Driver on the File Servers**
 - a. Open the Failover Cluster Manager console.
 - i. Expand the Compute Node Cluster `<Prefix>SCL`.
 - ii. Click on Nodes.
 - iii. Select one of the nodes in the cluster.
 - iv. Right mouse click on it, select Pause, then on Drain Roles.
 - v. You must now wait until the status of the node changes to Paused.
 - b. Open a PowerShell window with Administrative Privileges and run the following commands:
 - i. `Enter-PSSession <Prefix>S<xx>`
 - ii. `pnputil -i -a C:\Dell\NIC\Umb\Winx64\PRO1000\NDIS64*.inf`
 - iii. `pnputil -i -a C:\Dell\NIC\Umb\Winx64\PROXGB\NDIS64*.inf`
 - iv. `Restart-Computer`
 - v. `Exit`
 - c. Monitor the progress of the node:
 - i. Go back to the Failover Cluster Manager console.
 - ii. The status of the node will have changed to Down.
 - iii. After the node has finished rebooting, the status will change to Paused.
 - iv. Select the node and right mouse click on it, select Resume, then on Fail Roles Back.
 - v. You must now wait until the status of the node changes to Up.
 - d. Verify that the driver was successfully updated:
 - i. Go back to the PowerShell window and run the following commands:
 - ii. `Enter-PSSession <Prefix>C<xx><Node ID>`
 - iii. `Get-WmiObject Win32_PnPSignedDriver | Select-Object -Property devicename, driverversion | Where devicename -like 'Intel(R) Ethernet*'`

Note: The driver version should now be 3.14.78.0
 5. Upgrade the Intel NIC Driver on the DPM Servers:
 - a. Open a PowerShell window with Administrative Privileges and run the following commands:
 - i. `Enter-PSSession <Prefix>B<xx>`
 - ii. `pnputil -i -a C:\Dell\NIC\Umb\Winx64\PRO1000\NDIS64*.inf`
 - iii. `pnputil -i -a C:\Dell\NIC\Umb\Winx64\PROXGB\NDIS64*.inf`
 - iv. `Restart-Computer`
 - v. `Exit`
 - b. Verify that the driver was successfully updated:
 - i. Go back to the PowerShell window and run the following commands:
 - ii. `Enter-PSSession <Prefix>B<xx><Node ID>`
 - iii. `Get-WmiObject Win32_PnPSignedDriver | Select-Object -Property devicename, driverversion | Where devicename -like 'Intel(R) Ethernet*'`

Note: The driver version should now be 3.14.78.0

4.3 Step 3: Run the 1909 Microsoft P&U package (DHCS_Update_1909_Run_Second)

IMPORTANT: You must run the **DHCS_Update_1909_Run_First** package before you run the 1909 Microsoft P&U package (**DHCS_Update_1909_Run_Second**).

Because of the size of this package, estimates for deployment duration are 12 to 18 hours. Run the 1909 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 1909 Microsoft update package, such as **PU_MS#**, where # is the number or some other identifier of the specific update package. For example, where **1909** represents the year/month:

```
\\<Prefix>CON01\PUShare\PU_MS1909
```

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_1909_Run_Second.exe** to extract the update. When prompted, select the **PU_MS1909** 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_MS1909\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 **-ScomAlertAction** parameter. For example, **-ScomAlertAction "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\PU\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.)
+ FullyQualifiedErrorId : 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
untimeException: 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.

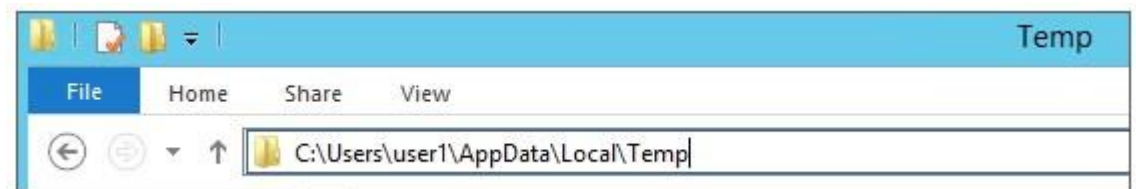
- If you have the VMM console open, and it reconnects, patching of the VMM server may be in progress. This is expected behavior.
2. To monitor the progress, you can use the following methods:
 - View the verbose output on the screen.
 - View the P&U events in Event Viewer. You can find P&U events under **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.psml

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 a 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 1909 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 1909 Microsoft package immediately, follow the steps in the "Postupdate clean up" section of the *Dell Hybrid Cloud System for Microsoft CPS Standard Administrators Guide* after you have completed the update.

4.3.1 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
```

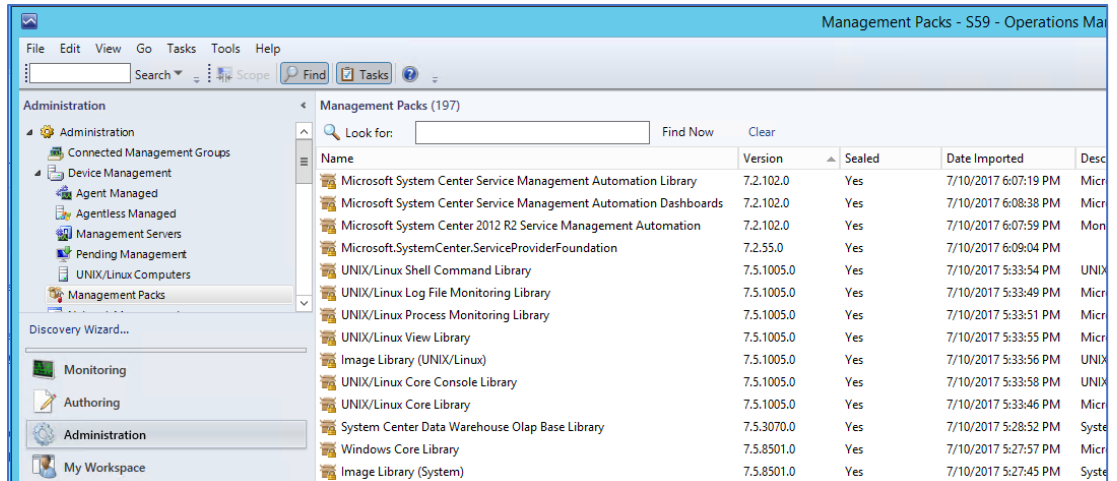
Post-update manual steps

[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 domainjoined computers”. (Review the KB article and decide how to implement for your organization and CPS domain.)

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 1909 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.psm1
```

```
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).

5 Microsoft payload for Update 1909

Payload for Update 1909

Update Details

KB Number	Title	CVE / ADV
890830	Windows Malicious Software Removal Tool x64 - August 2019	N/A
4514604	2019-09 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, 4.7.2, 4.8 for Windows 8.1 and Server 2012 R2 for x64	CVE-2019-1142
4516067	2019-09 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1252, CVE-2019-1256, CVE-2019-1250, CVE-2019-0787, CVE-2019-0788, CVE-2019-1267, CVE-2019-1268, CVE-2019-1208, CVE-2019-1269, CVE-2019-1271, CVE-2019-1214, CVE-2019-1215, CVE-2019-1216, CVE-2019-1274, CVE-2019-1219, CVE-2019-1220, CVE-2019-1280, CVE-2019-1282, CVE-2019-1221, CVE-2019-1235, CVE-2019-1285, CVE-2019-1236, CVE-2019-1240, CVE-2019-1286, CVE-2019-1287, CVE-2019-1290, CVE-2019-1241, CVE-2019-1242, CVE-2019-1291, CVE-2019-1293, CVE-2019-1243, CVE-2019-1244, CVE-2019-1245, CVE-2019-1246
4516115	2019-09 Security Update for Adobe Flash Player for Windows Server 2012 R2 for x64-based Systems	ADV190022

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:

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" are not "1.0.1909.12001", you have run into this issue

Resolution:

Restart P&U

Issue 3

Symptoms:

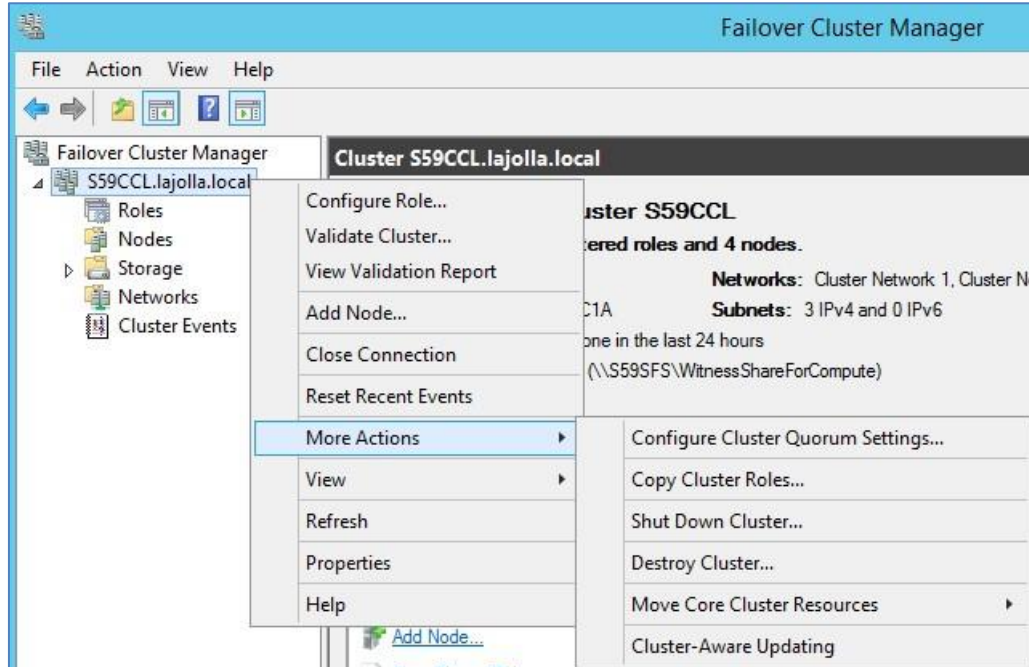
Failure in P&U during the "CCL" subsystem.

Description:

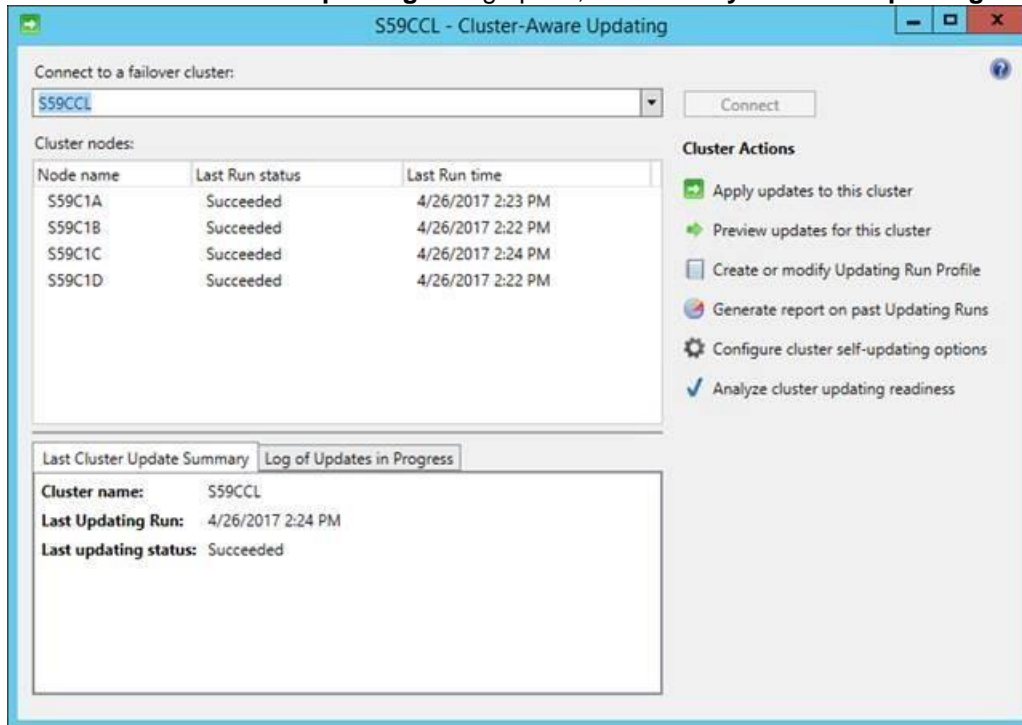
This can include updating the Deployment Manifest and running compliance checks.

Detection:

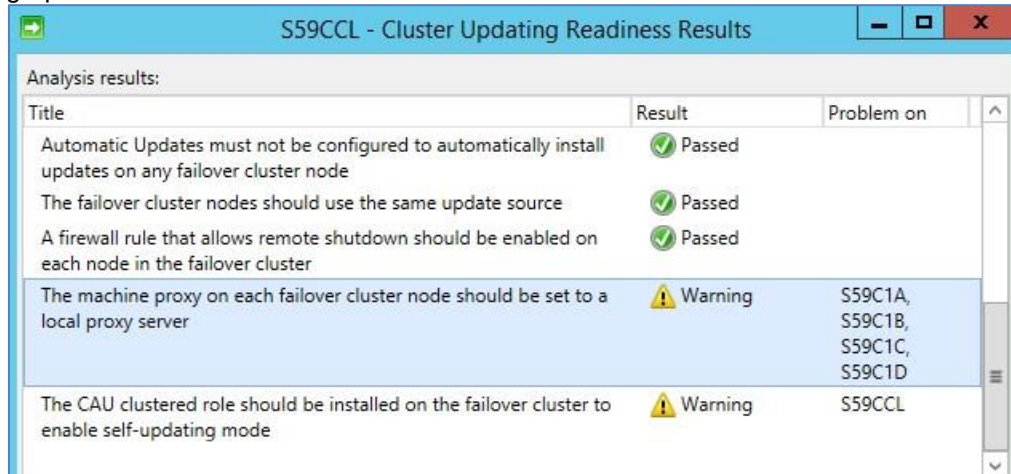
1. Open **Failover Cluster Manager**.
2. Right-click on the CCL cluster and choose **More Actions**, and then choose **Cluster-Aware Updating**.



3. 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:



Title	Result	Problem on	
Automatic Updates must not be configured to automatically install updates on any failover cluster node	Passed		^
The failover cluster nodes should use the same update source	Passed		
A firewall rule that allows remote shutdown should be enabled on each node in the failover cluster	Passed		
The machine proxy on each failover cluster node should be set to a local proxy server	Warning	S59C1A, S59C1B, S59C1C, S59C1D	
The CAU clustered role should be installed on the failover cluster to enable self-updating mode	Warning	S59CCL	

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 4

Symptoms:

NVGRE issue. The Dell EMC 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 Dell EMC framework does not. The Dell EMC 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 Dell EMC Patch and Update package has been extracted. Under C:\PUShare\PU_DellEMC1909\ 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 Dell EMC patch and update framework, and this will bypass the server with the "External" custom property.

Issue 5

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 EMC 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.

Issue 6

Symptoms:

The P&U install process fails with the following error:

"Connecting to remote server <ServerName> failed with the following error message: The request is not supported."

Cause:

Microsoft Update KB# 4093492, that impacts CredSSP authentication protocol and RDP functions. All servers in a CPS environment are now forcing the registry key “HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\CredSSP\Parameters\AllowEncryptionOracle” to a value of “1”.

Workaround #1:

Open a Microsoft Management Console and add the Group Policy Editor Snap for the WSUS server. Expand the Computer Configuration, then the Administrative Templates, then System, and then Credentials Delegation. Select the setting *Encryption Oracle Remediation*. In the properties for the setting and **Enable** it, then set the options to **Vulnerable**. Save the changes and then reboot the WSUS server so that the settings will take. After the update is complete set the *Encryption Oracle Remediation* back to not configured and reboot the server.

Workaround #2:

If the <ServerName> listed in the above error is for the backup server, you will need to perform the same step on the backup server and the console server. Open a Microsoft Management Console and add the Group Policy Editor Snap for the WSUS server. Expand the Computer Configuration, then the Administrative Templates, then System, and then Credentials Delegation. Select the setting *Encryption Oracle Remediation*. In the properties for the setting and **Enable** it, then set the options to **Vulnerable**. Save the changes and then reboot all three servers so that the settings will take. After the update is complete set the *Encryption Oracle Remediation* back to not configured on all three servers and reboot them.

6 Dell EMC Payload for Update 1909

Dell EMC Update 1909 for CPS Standard includes the following driver and firmware updates.

WARNING: *Once the Intel NIC firmware is updated to 18.8.x, do not downgrade to previous A-Rev versions below 18.8.x.*

- **Dell Server PowerEdge BIOS R630/R730/R730XD Version 2.10.5 Fixes & Enhancements**

This release contains new Intel Xeon Processor Scalable Family Processor Microcode Enhancement to address the security vulnerabilities (Common Vulnerabilities and Exposures-CVE) such as CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, and CVE-2019-0089. This release contains BIOS firmware version 2.10.5 for Dell PowerEdge R630/R730/R730XD

- **Enhancements**

- Enhancement to address the security vulnerabilities (Common Vulnerabilities and Exposures-CVE) such as CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, and CVE-2019-0089.
- Updated the Intel Xeon Processor E5-2600 v4 Product Family Processor Microcode to version 0x0b000038.
- Updated the Xeon Processor E5-2600 v3 Product Family Processor Microcode to version 0x43.
- Updated the Intel Management Engine firmware to version SPS_E5_03.01.03.072.0_GR_WBG_REL.
- Support for the iDRAC8 2.70.70.70 version.

- **Fixes**

- When booting to RHEL 8, the following message is displayed:
Kernel panic - not syncing: Fatal hardware error!

- **Dell Server BIOS PowerEdge C6320 Version 2.10.5 Fixes & Enhancements**

Enhanced BIOS security protection features. Updated the Intel Xeon Processor Microcode to version 0x0B000038 and Xeon Processor E5-2600 v3 Microcode to version 0x43. Updated the Intel Management Engine firmware to version SPS_E5_03.01.03.072.0_GR_WBG_REL. Enhanced protection for the DIMM Serial Presence Detect (SPD) data. For more information about specific items added and resolved in this BIOS version, see the Fixes and New and enhanced features sections.

- **Fixes**

- When booting to RHEL 8, the following message is displayed: Kernel panic - not syncing: Fatal hardware error!

- **Enhancements**

- Enhancement to address the security vulnerabilities (Common Vulnerabilities and Exposures--CVE) such as CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, and CVE-2019-0089.
- Updated the Intel Xeon Processor E5-2600 v4 Product Family Processor Microcode to version 0x0b000038.
- Updated the Intel Xeon Processor E5-2600 v3 Product Family Processor Microcode to version 0x43.
- Updated the Intel Management Engine firmware to version SPS_E5_03.01.03.072.0_GR_WBG_REL.
- Support for the iDRAC8 2.70.70.70 version.
- Added setup option Lower Memory Mapped I/O Base to 512 GB. Default is set to Disabled.
- Enhanced protection for the DIMM Serial Presence Detect (SPD) data.

- **iDRAC with Lifecycle Controller Version 2.63.60.61 Fixes & Enhancements**

- **Fixes:**
 - Added HTTPS support for Firmware Update feature
- **Enhancements:**
 - Security/IPS fixes
- **Dell PERC H330 Mini/Adapter RAID Controllers firmware version 25.5.6.0009 Fixes & Enhancements**
 - **Fixes**
 - Controller is less likely take a logical drive offline in VSAN
 - Controller now passes the proper drive group while creating a configuration using HII
 - Controller now retains HII device setting after a boot
 - Controller now gives status on all drives including failed drives with Perc CLI "show all" command
 - Controller now performs Patrol Read on SSD drives to better align with the industry
 - Reinserting a drive from a VD will no longer lead to a foreign state
 - Controller now handles crypto erase on Micron 5100 SSD drives
 - Controller reduces delay if there is a bad PHY condition at boot
 - Controller now reports smart trip condition on non-Raid drives
 - Reduces PL errors 0x3110e03 and 0x31110d01 after resetting a SATA target
 - Controller now gives correct messaging when a power supply is hot removed from an enclosure
 - Controller better handles poorly formed ATA passthrough CDBs.
 - Unsupported "Raid00" option in HII has been removed
 - Fixed an isolated issue where an exception error could occur during boot. The symptoms include a hang during system boot which displays "FW initializing" on screen for two hours or more, and iDRAC LC log reporting "PR8 Device not detected"
 - **Enhancements**
 - Controller reduces the bad block count print in the ttylog to once each boot
 - Removed "timeout > 3600" prints to the TTYlog
 - Controller has improved detection of a failed battery
- **Dell PERC H730/H730P/H830/FD33xS/FD33xD Mini/Adapter RAID Controllers firmware version 25.5.6.0009 Fixes & Enhancements**
 - **Fixes**
 - Controller is less likely take a logical drive offline in VSAN
 - Controller now passes the proper drive group while creating a configuration using HII
 - Controller now retains HII device setting after a boot
 - Controller now gives status on all drives including failed drives with Perc CLI "show all" command
 - Controller now performs Patrol Read on SSD drives to better align with the industry
 - Reinserting a drive from a VD will no longer lead to a foreign state
 - Controller now handles crypto erase on Micron 5100 SSD drives
 - Controller reduces delay if there is a bad PHY condition at boot
 - Controller now reports smart trip condition on non-Raid drives
 - Reduces PL errors 0x3110e03 and 0x31110d01 after resetting a SATA target
 - Controller now gives correct messaging when a power supply is hot removed from an enclosure
 - Controller better handles poorly formed ATA passthrough CDBs.
 - Unsupported "Raid00" option in HII has been removed
 - **Enhancements**
 - Controller reduces the bad block count print in the ttylog to once each boot
 - Removed "timeout > 3600" prints to the TTYlog
 - Controller has improved detection of a failed battery

- **Intel NIC Family Version 18.8.0 Firmware for I350, I354, X520, X540, and X550 adapters Fixes & Enhancements**
Note: Firmware downgrade from 18.8.x to 18.5.x or older versions is not supported.
 - **Fixes**
 - Resolved an issue that may cause the link to stay down with both port LEDs off on Intel(R) 10G X520 LOM, Intel(R) 10G X520 rNDC and Intel(R) 10G 4P X520/I350 rNDC when firmware is upgraded to version 18.5.17.
 - **Enhancements**
 - A reset is now enforced after UEFI iSCSI configuration parameters are updated to ensure previous iSCSI parameters are not used.
- **Windows Server 2012 R2 Driver version 2.51.21.2 for Dell 12Gbps HBA and HBA330 Fixes & Enhancements**
 - **Fixes**
 - NA
 - **Enhancements**
 - NA
- **Dell 12Gbps HBA firmware version 16.17.00.05 Fixes & Enhancements**
 - **Fixes**
 - Fixed an issue that was causing periodic diagnostic resets which could ultimately lead to a failed drive, particularly in VSAN/VXRail environments.
 - Fixed an issue where mal-formed ATA passthrough commands could lead to command timeouts.
 - Fixed an issue where SCSI pass-through command timeouts could occur at 18-20 minute intervals in a VSAN environment.
 - Fixed an issue where a SATA link reset could cause many IOP Log events (31110e03) to be sent to the kernel log.
 - Fixed an issue in which a drive reset could lead to a false check condition with error 4/44/00.
 - **Enhancements**
 - None