

Update 1703b for Cloud Platform System (CPS) Standard

Dell Hybrid Cloud System for Microsoft

Dell Engineering
July 2017

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 |
| July 2017 | Release 1703b |

Copyright © 2017 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..... | 5 |
| 1.1 New functionality..... | 6 |
| 1.2 Additional update information..... | 6 |
| 1.3 How to check which update package is installed..... | 6 |
| 1.4 When to run the update package..... | 7 |
| 2 1703b Patch and Update Prerequisites..... | 8 |
| 2.1 Prepare the patching environment..... | 8 |
| 2.2 Step 1: Prepare user account for patching..... | 8 |
| 2.3 Step 2: Ensure that Group Policy does not block the mounting of USB virtual disks..... | 8 |
| 2.4 Step 3: Extract the Patch and Update package..... | 8 |
| 2.5 Step 4: Ensure that <code>LaJollaDeploymentService</code> is not running in the background on the Console VM .. | 9 |
| 2.6 Step 5: Clean up the WSUS server..... | 9 |
| 2.7 Step 6 (Optional): Exclude external SOFS storage clusters from P&U..... | 9 |
| 3 1703b Patch and Update Process..... | 11 |
| 3.1 Step 1: Run the 1703b DellEMC P&U package..... | 11 |
| 3.2 Step 2: Run the 1703b Microsoft P&U package..... | 14 |
| 3.3 Run an optional compliance scan..... | 18 |
| 4 Known Issues..... | 19 |
| 4.1 Patch and Update framework re-run is required after a subsystem encounters errors..... | 19 |
| 5 Microsoft payload for Update 1703b..... | 20 |
| 5.1 Updates for Windows Server 2012 R2..... | 20 |
| 5.2 Updates for Windows Server 2014..... | 20 |
| 5.3 Updates for Windows Azure Pack..... | 20 |
| 5.4 Updates for Windows Azure Site Recovery..... | 21 |
| 5.5 Updates for System Center 2012 R2—Data Protection Manager..... | 21 |
| 5.6 Updates for System Center 2012 R2—Operations Manager..... | 21 |
| 5.7 Updates for System Center 2012 R2—Virtual Machine Manager..... | 21 |
| 5.8 Other Microsoft updates (from previous updates)..... | 22 |
| 5.9 Troubleshooting the P&U process..... | 24 |
| 6 Dell EMC Payload for Update 1703b..... | 26 |

WARNING: You cannot run the 1703b Patch & Update framework—1.4—directly without first upgrading your environment to 1611 (1.3). You can directly upgrade to 1703b only after the DHCS stamp is at the 1.3 version, P&U 1611. 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.

1.1 New functionality

Update 1703b contains the following new features:

- Provides support for Windows Server 2016 as an operating system for tenant VMs. (This support is provided through Windows Azure Pack UR11 and VMM UR12.)
- Includes an updated compliance scan implementation. Previously, a compliance scan (to verify updates were installed through P&U) would show empty results if compliant.
- Provides additional logging during P&U for Hyper-V Network Virtualization (HNV) settings and VMM trace logs. This will help troubleshoot failures during P&U, as described below:
 - > You can find the HNV logs in the same 'temp' location as the **PUProgressDetails** log on the machine that is running P&U. For example, [\\<Prefix>-CON-01\c\\$\Users\CPS-Update-Admin\AppData\Local\Temp](#).
 - > You can find the VMM trace log files at the root of C: on the VMM servers.
 - > P&U deletes previous VMM trace logs each time a P&U run is started. If you encounter a failure in P&U that requires additional investigation, copy these logs before you restart P&U.

1.2 Additional update information

In addition to the features listed above, Update 1703b also includes the following:

- Prevents SQL Server accounts from lock-out while running `MCPasswordReset` in high-load scenarios.
- Updates to SQL Server components on DPM servers for greater resiliency in high-load scenarios.
- Updates all CPS hosts and infrastructure VMs to Windows Management Framework (WMF) 5.1.
- KB Article # [3000483](#) is a Windows Group Policy related security update (CVE-2015-0008). It requires both the binary files (delivered in P&U 1611 and 1703b), 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*".

Note: Review the KB article, and decide whether you want to implement these changes for the CPS domain. This procedure is optional.

1.3 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.

1.4 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 1703b contains three distinct phases:

- [Performing prerequisites](#)
- [Running the 1703b DellEMC P&U package](#)
- [Running the 1703b Microsoft P&U package](#)

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

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

2 1703b Patch and Update Prerequisites

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

2.1 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.

2.2 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*).

2.3 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
```

2.4 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.

2.5 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**.

2.6 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.

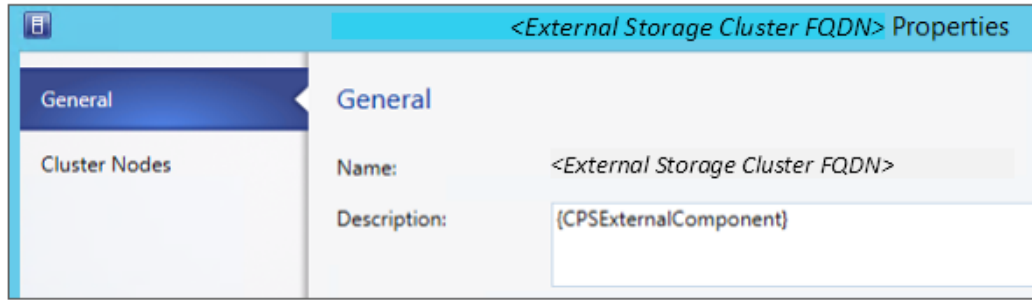
2.7 Step 6 (Optional): Exclude external SOFS storage clusters from P&U

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.

3 1703b Patch and Update Process

IMPORTANT: Be sure to follow the prerequisites listed in the previous section before you run the 1703b Patch and Update process.

3.1 Step 1: Run the 1703b DellEMC P&U package

IMPORTANT: You must run the 1703b DellEMC P&U package before you run the 1703b Microsoft P&U package.

Run the DellEMC P&U 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_DellEMC1703b
```

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_1703b_Run_First.exe** to extract the update. When prompted, select the **PU_DellEMC1703b** 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_DellEMC1703b\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:

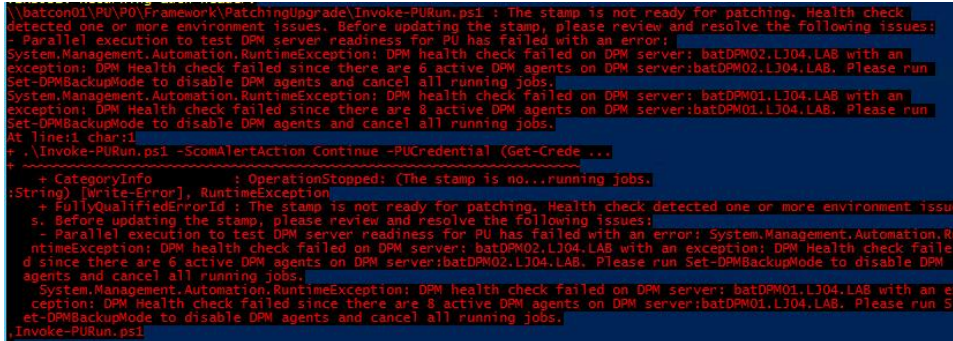
```
\\<Prefix>CON01\PUShare\PU_DellEMC1703b\PU\Framework\PatchingUpgrade\Invoke-  
PURun.ps1 -PUCredential (Get-Credential) -ScmAlertAction "Continue"
```

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 -ScmAlertAction 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.
 - In the navigation pane, right-click **Failover Cluster Manager**, and then click **Connect to Cluster**.
 - In the **Select Cluster** dialog box, click **Browse**.
 - 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.

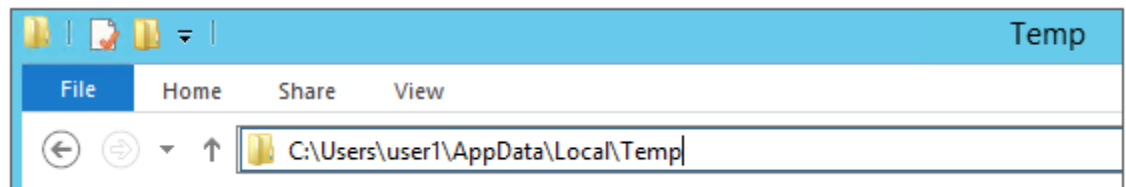
- If you have the VMM console open, and it reconnects, patching of the VMM server may be in progress. This is expected behavior.
2. To monitor the progress, you can use the following methods:
 - View the verbose output on the screen.
 - View the P&U events in Event Viewer. You can find P&U events under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

- 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**.

3.2 Step 2: Run the 1703b Microsoft P&U package

IMPORTANT: You must run the 1703b DellEMC P&U package before you run the 1703b Microsoft P&U package.

Run the 1703b 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 1703b Microsoft update package, such as **PU_MS#**, where # is the number or some other identifier of the specific update package. For example, where *1703b* represents the year/month:

```
\\<Prefix>CON01\PUShare\PU_MS1703b
```

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_1703b_Run_Second.exe** to extract the update. When prompted, select the **PU_MS1703b** 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_MS1703b\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"`

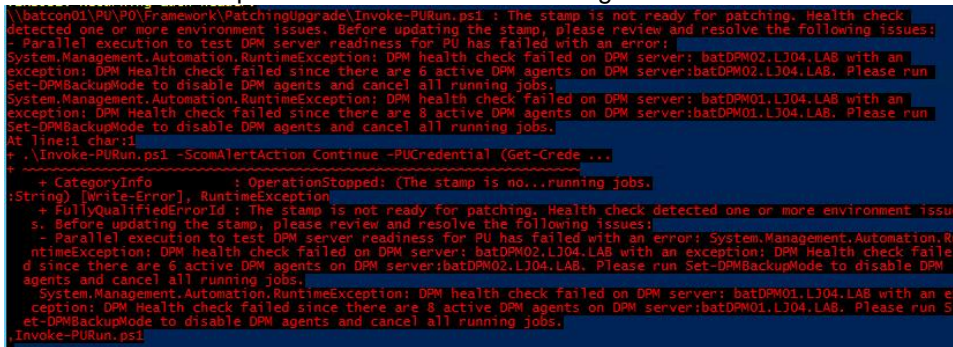
4. When prompted, enter the account credentials of the account that you used to log in.
5. The `Invoke-PURun` script performs a one-time environment setup and may prompt you to restart Windows PowerShell on its for invocation, for example:

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.
+ ~~~~~
+ 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-DPMBBackupMode -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.
 - Open Failover Cluster Manager.
 - Connect to the cluster.
 - In the navigation pane, right-click **Failover Cluster Manager**, and then click **Connect to Cluster**.
 - In the **Select Cluster** dialog box, click **Browse**.
 - Click the desired cluster, and then click **OK** two times.
 - In the navigation pane, right-click the cluster name, point to **More Actions**, and then click **Cluster-Aware Updating**.

- 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.

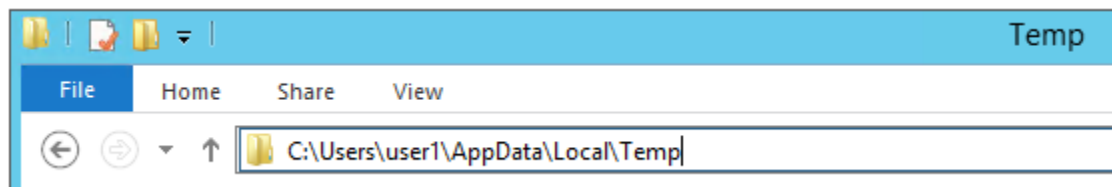
- If you have the VMM console open, and it reconnects, patching of the VMM server may be in progress. This is expected behavior.
2. To monitor the progress, you can use the following methods:
- View the verbose output on the screen.
 - View the P&U events in Event Viewer. You can find P&U events under **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 1703b 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 1703b 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.

3.3 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
```

4 Known Issues

The following issue has been identified in Update 1703b for CPS Standard.

4.1 Patch and Update framework re-run is required after a subsystem encounters errors

Description: Because of the complex nature of the Patch and Update and multiple operations of the framework, sometimes the subsystems encounter an error

Detection: The Patch and Update process will output an error in the PowerShell window similar to “**The following subsystems encountered errors during pass 'update' “sub-system-name” (such as SCL, CCL, WapAdmin etc.). Please see logs for exception details**”

Remediation:

1. Close the current PowerShell session running the Patch and Update process
2. Open a new PowerShell window (make sure to use “Run as Administrator”) and re-run the Patch and Update process as described in 1703b Patch and Update Process.

Note: If you run the 1703b Patch and Update multiple times and the same subsystem keeps failing, please contact your Dell Support Representative.

5 Microsoft payload for Update 1703b

5.1 Updates for Windows Server 2012 R2

| KB Article | Description | CVE |
|-------------------------|--|--|
| 4012216 | March, 2017 Security Monthly Quality Rollup for Windows Server 2012 R2 (KB4012216) | CVE-2016-7202, CVE-2016-7278, CVE-2016-7279, CVE-2016-7281, CVE-2016-7282, CVE-2016-7283, CVE-2016-7284, CVE-2016-7287 |
| 4014329 | Security Update for Adobe Flash Player for Windows Server 2012 R2 (KB4014329) | CVE-2017-2925, CVE-2017-2926, CVE-2017-2927, CVE-2017-2928, CVE-2017-2930, CVE-2017-2931, CVE-2017-2932, CVE-2017-2933, CVE-2017-2934, CVE-2017-2935, CVE-2017-2936, CVE-2017-2937 |
| 3191564 | Windows Management Framework 5.1 (for Windows Server 2012 R2) | N/A |

5.2 Updates for Windows Server 2014

| KB Article | Description | CVE |
|-------------------------|---|-----|
| 4010394 | Cumulative Update 4 for SQL Server 2014 SP2 | N/A |
| 3194724 | Microsoft SQL Server Native Client (from SQL CU) - Version 11.3.6567.0 | N/A |
| 4010394 | Microsoft ODBC Driver 11 for SQL Server (from SQL CU) - Version 12.2.5540.0 | N/A |

5.3 Updates for Windows Azure Pack

| KB Article | Description | CVE |
|-------------------------|---|-----|
| 3186207 | Update Rollup 11 for Windows Azure Pack | N/A |

5.4 Updates for Windows Azure Site Recovery

| KB Article | Description | CVE |
|-------------------------|---|-----|
| 4013824 | Update Rollup 16 for Microsoft Azure Site Recovery Provider | N/A |

5.5 Updates for System Center 2012 R2—Data Protection Manager

| KB Article | Description | CVE |
|-------------------------|--|-----|
| 3209592 | Update Rollup 12 for System Center 2012 R2 Data Protection Manager | N/A |

5.6 Updates for System Center 2012 R2—Operations Manager

| KB Article | Description | CVE |
|-------------------------|---|-----|
| 3209587 | Update Rollup 12 for Microsoft System Center 2012 R2 - Operations Manager (KB3209587) | N/A |

5.7 Updates for System Center 2012 R2—Virtual Machine Manager

| KB Article | Description | CVE |
|-------------------------|--|-----|
| 3209585 | Update Rollup 12 for System Center 2012 R2 Virtual Machine Manager | N/A |
| 4012720 | Hotfix for VMM 2012 R2- Test replica failover and cmdlet generated for VLAN isolation issues (Console) | N/A |
| 4014682 | Hotfix for VMM 2012 R2- Test replica failover and cmdlet generated for VLAN isolation issues (Server) | N/A |

5.8 Other Microsoft updates (from previous updates)

| KB Article | Description | CVE |
|-------------------------|--|---|
| 2538243 | Security Update for Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package (KB2538243) | CVE-2010-3190 |
| 3135985 | Security Update for Microsoft .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 for x64 (KB3135985) | CVE-2016-0132 |
| 3142026 | Security Update for Microsoft .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 for x64 (KB3142026) | CVE-2016-0149 |
| 3205404 | December, 2016 Security and Quality Rollup for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2 (KB3205404) | CVE-2016-7270 |
| 3000483 | Security Update for Windows Server 2012 R2 (KB3000483) | CVE-2015-0008 |
| 3032331 | Hotfix for Windows Server 2012 R2 x64 Edition (KB3032331) | N/A |
| 3045999 | Security Update for Windows Server 2012 R2 (KB3045999) | CVE-2015-1643, CVE-2015-1644 |
| 3071756 | Security Update for Windows Server 2012 R2 (KB3071756) | CVE-2015-1769 |
| 3080149 | Update for Windows Server 2012 R2 (KB3080149) | N/A |
| 3108381 | Security Update for Windows Server 2012 R2 (KB3108381) | CVE-2015-6128, CVE-2015-6132, CVE-2015-6133 |
| 3115224 | Update for Windows Server 2012 R2 (KB3115224) | N/A |
| 3126593 | Security Update for Windows Server 2012 R2 (KB3126593) | CVE-2016-0040, CVE-2016-0041, CVE-2016-0042, CVE-2016-0044, CVE-2016-0049 |
| 3128650 | Update for Windows Server 2012 R2 (KB3128650) | N/A |
| 3146723 | Security Update for Windows Server 2012 R2 (KB3146723) | CVE-2016-0151 |
| 3147071 | Update for Windows Server 2012 R2 (KB3147071) | N/A |
| 3172614 | Update for Windows Server 2012 R2 (KB3172614) | N/A |

| KB Article | Description | CVE |
|-------------------------|---|--|
| 3175024 | Security Update for Windows Server 2012 R2 (KB3175024) | CVE-2016-3305, CVE-2016-3306, CVE-2016-3371, CVE-2016-3372, CVE-2016-3373 |
| 3179574 | Update for Windows Server 2012 R2 (KB3179574) | N/A |
| 3192392 | October, 2016 Security Only Quality Update for Windows Server 2012 R2 (KB3192392) | CVE-2016-3237, CVE-2016-3300, CVE-2016-3267, CVE-2016-3298, CVE-2016-3331, CVE-2016-3382, CVE-2016-3383, CVE-2016-3384, CVE-2016-3385, CVE-2016-3387, CVE-2016-3388, CVE-2016-3390, CVE-2016-3391, CVE-2016-3209, CVE-2016-3262, CVE-2016-3263, CVE-2016-3270, CVE-2016-3393, CVE-2016-3396, CVE-2016-7182, CVE-2016-0142, CVE-2016-3266, CVE-2016-3341, CVE-2016-3376, CVE-2016-7185, CVE-2016-7211, CVE-2016-0070, CVE-2016-0073, CVE-2016-0075, CVE-2016-0079 |
| 3197873 | November, 2016 Security Only Quality Update for Windows Server 2012 R2 (KB3197873) | CVE-2016-7195, CVE-2016-7196, CVE-2016-7198, CVE-2016-7199, CVE-2016-7227, CVE-2016-7239, CVE-2016-7241, CVE-2016-7247, CVE-2016-7223, CVE-2016-7224, CVE-2016-7225, CVE-2016-7226, CVE-2016-7220, CVE-2016-7237, CVE-2016-7238, CVE-2016-7214, CVE-2016-7215, CVE-2016-7218, CVE-2016-7246, CVE-2016-7255, CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, CVE-2016-7184, CVE-2016-7210, CVE-2016-7205, CVE-2016-7217, CVE-2016-7256, CVE-2016-7248, CVE-2016-7221, CVE-2016-7222, CVE-2016-7212 |
| 3205410 | December, 2016 Security Only Update for .NET Framework 4.6.2 on Windows 8.1 and Windows Server 2012 R2 for x64 (KB3205410) | CVE-2016-7270 |
| 890830 | Windows Malicious Software Removal Tool for Windows 8, 8.1, 10 and Windows Server 2012, 2012 R2, 2016 x64 Edition - March 2017 (KB890830) | N/A |

5.9 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> |


```
<add key="TotalAllowedJobs" value="1000"/>
```

```
<add key="TotalAllowedJobs" value="1"/>
```

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.

6 Dell EMC Payload for Update 1703b

Dell Server BIOS R630/R730/R730XD Version 2.4.3 Fixes & Enhancements

Enhancements:

- > Updated the Intel Processor and Memory Reference Code to PLR8
- > Updated the Intel Xeon Processor E5-2600 v4 Product Family Processor Microcode to version 0x1F
- > Updated the Intel Xeon Processor E5-2600 v3 Product Family Processor Microcode to version 0x39

Fixes:

- > Export log issues in the Non-Volatile Memory Express (NVMe) Human Interface Infrastructure (HII)
- > The Intel Xeon Processor E5-2600 v4 based system may have CPU Internal error (iERR) and Machine Check error when idle.
- > Rarely, the system may stop responding because of a power failure during the boot process.
- > The feature to manually bifurcate slots is not functioning.

Dell Server BIOS PowerEdge C6320 Version 2.4.2 Fixes & Enhancements

Enhancements:

- > Updated the Intel Processor and Memory Reference Code to PLR8.
- > Updated the Intel Xeon Processor E5-2600 v4 Product Family Processor Microcode to version 0x1F.
- > Updated the Intel Xeon Processor E5-2600 v3 Product Family Processor Microcode to version 0x39.

Fixes:

- > Export log issues in the Non-Volatile Memory Express (NVMe) Human Interface Infrastructure (HII)
- > Rarely, the system may stop responding because of a power failure during the boot process.

Dell PERC H330 Mini/Adapter RAID Controllers firmware version 25.5.2.0001 Fixes & Enhancements

Enhancements:

- > None

Fixes:

- > Fixed an issue where not all drives might be discovered during server power-up in servers with 26 drives installed.
- > Disables ECRC at the PERC node to work around an issue where the server can PSOD due to a mal-formed TLP.

Dell PERC H730/H730P/H830/FD33xS/FD33xD Mini/Adapter RAID Controllers firmware version 25.5.2.0001 Fixes & Enhancements

Enhancements:

- > None

Fixes:

- > Fixed an issue where not all drives might be discovered during server power-up in servers with 26 drives installed.
- > Disables ECRC at the PERC node to work around an issue where the server can PSOD due to a mal-formed TLP.

Dell 13G PowerEdge Server Backplane Expander Firmware Version 3.32, A00-00 Fixes & Enhancements

Enhancements:

- > None

Fixes:

- > Addresses problems for medium to low severity issues related to SAS buffering issues.
- > Addresses a problem with Broadcom's SAS3xNN/3xNNR 12 Gb/s SAS expander SAS buffering (Broadcom DataBolt) for 3 or 6 Gb/s SAS drives due to a hardware limitation. SATA DataBolt is unaffected.

Dell 13G PowerEdge Server Non-expander Storage Backplane Firmware Version 2.25, A00-00 Fixes & Enhancements

Enhancements:

- > None

Fixes:

- > Addresses a problem detecting drive type for 1.8" drives.