

Update 1611 for Cloud Platform System (CPS) Standard

Dell Hybrid Cloud System for Microsoft

Dell Engineering
February 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 |

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 How to check which update package is installed..... | 6 |
| 1.2 When to run the update package..... | 6 |
| 2 1611 Patch and Update Prerequisites..... | 7 |
| 2.1 Prepare the patching environment..... | 7 |
| 2.2 Step 1: Prepare user account for patching..... | 7 |
| 2.3 Step 2: Ensure that Group Policy does not block the mounting of USB virtual disks..... | 7 |
| 2.4 Step 3: Extract the Patch and Update package..... | 7 |
| 2.5 Step 4: Copy the manifest file to the SMA server..... | 8 |
| 2.6 Step 5: Ensure that LaJollaDeploymentService is not running in the background..... | 8 |
| 2.7 Step 6: Install the VMM Hyper-V Network Virtualization policy hotfix..... | 8 |
| 2.8 Step 7: Clean up the WSUS server..... | 9 |
| 3 1611 Patch and Update Process..... | 11 |
| 3.1 Step 1: Run the 1611 P&U update package PUDellEMC..... | 11 |
| 3.2 Step 2: Run the 1611 P&U update package Microsoft P0..... | 14 |
| 3.3 Step 3: Run the 1611 P&U update package Microsoft P1..... | 18 |
| 3.4 Run an optional compliance scan..... | 21 |
| 4 Known Issues..... | 22 |
| 4.1 Issue: PURunstatus.json file reports failed state after console reboot..... | 22 |
| 4.2 Patch and Update framework re-run is required after a subsystem encounters errors..... | 22 |
| 5 Microsoft payload for Update P0 package..... | 23 |
| 5.1 Configuration changes from previous updates..... | 23 |
| 5.2 Updates for Windows Server 2012 R2, from previous updates..... | 24 |
| 6 Microsoft payload for Update P1 package..... | 25 |
| 6.1 New updates for Windows Server 2012 R2..... | 25 |
| 6.2 Updates for SQL Server 2014 SP1..... | 25 |
| 6.3 System Center and Windows Azure Pack updates, from previous updates..... | 25 |
| 6.4 Updates for Windows Server 2012 R2, from previous updates..... | 26 |
| 6.5 Troubleshooting the P&U process..... | 47 |
| 7 DELL payload for Update 1611..... | 51 |

WARNING: If you are running 1.0.2 or an earlier version of the Dell Hybrid Cloud System for Microsoft, you cannot run the 1611 Patch & Update framework directly without first upgrading your environment to 1.1 or later. You can directly upgrade to 1.3 only after the DHCS stamp is at the 1.1 version. Also be advised that the addition of any non-DHCS hardware to your system will cause the Patch & Update process to fail.

WARNING: The Patch and Update process will fail if you have custom Physical and or Virtual servers, not part of DHCS, being managed by the DHCS SCVMM. In order to exclude these servers, please see [Troubleshooting the P&U process](#), and follow the procedures detailed in **Issue 3**.

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 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.

1.2 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 1611 contains four distinct phases:

[Performing prerequisites](#)

[Running the 1611 P&U update package PUDellEMC](#)

[Running the 1611 Microsoft P0 Patch and Update package](#)

[Running the 1611 Microsoft P1 Patch and Update package](#)

CAUTION:

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

1. Prerequisites
2. PUDellEMC package
3. Microsoft P0 package
4. Microsoft P1 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 1611 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: Copy the manifest file to the SMA server

The manifest information has to be present on the SMA server in order for the Patch and Update framework to run successfully. To ensure that the manifest file content is copied over to the SMA server:

1. Open a PowerShell window, making sure you “Run as Administrator”.
2. Browse to the location where you unzipped the Patch and Update Package (C:\PUShare).
3. Run the script called `Save-CPSSDeploymentManifest.ps1`. You can find this script at
C:\PUShare> .\Save-CPSSDeploymentManifest.ps1.

2.6 Step 5: Ensure that `LaJollaDeploymentService` is not running in the background

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

1. 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**.

2.7 Step 6: Install the VMM Hyper-V Network Virtualization policy hotfix

Please install the following required hotfixes if you are updating your stamp to 1611 from 1603 or 1605. If you are updating your stamp from 1606, you do NOT need to install it again.

1. To install the HNV hotfix:
 - a. From the specified location where the Patch and Update package was unzipped, double click the “**System Center 2012 R2 VMM UR HotFix 6095474.exe**” file, review the EULA, and then click **Yes** to accept.
 - b. Choose the folder to store the extracted files, and then click **OK**.
2. For the new VMM placement hotfix:
 - a. From the specified location where the Patch and Update package was unzipped, double-click “`Placement_HF_UR9.EXE`”.
 - b. Choose the **PUShare** folder to store the extracted files, and then click **OK**.
3. In File Explorer, browse to the following folder on the VMM node:

```
\\<Prefix>VMM01>\c$\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager\bin
```
4. Make a backup copy of the following files in the `\bin` folder:

ImgLibEngine.dll (if installing the HNV hotfix)

Engine.Placement.ResourceModel.dll

5. On the VMM node, type **powershell** to open an elevated Windows PowerShell session, and then run the following commands:

```
Stop-Service SCVMMService  
Stop-Service SCVMMAgent
```

6. Verify that the services have stopped. To do this, run the following command:

```
Get-Service SCVMMService  
Get-Service SCVMMAgent
```

Verify that the status is **Stopped**. If you are prompted to close the System Center Management Service Host process, click **Ignore**.

7. In the \\<Prefix>VMM01>\c\$\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager\bin folder, replace the following files with the new version of the files that you extracted from the hotfix package:

ImgLibEngine.dll (if installing the HNV hotfix)

Engine.Placement.ResourceModel.dll

8. On the VMM node, run the following command to start the VMM Agent service:

```
Start-Service SCVMMService  
Start-Service SCVMMAgent
```

If you need to revert the patch, do the following:

1. On the VMM node, stop the *SCVMMService* service, and then stop the *SCVMMAgent* service.
2. Replace the files under your Virtual Machine Manager \Bin directory with your backup files.
3. Start the *SCVMMAgent* service.
4. Start the *SCVMMService* service.

2.8 Step 7: 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**.

Setting: **All Removable Storage classes: Deny all access**

\Computer Configuration\Policies\Administrative Templates\System\Device Installation\Device Installation Restrictions

Setting: **Prevent installation of removable devices**

If either of these policy settings are enabled for the nodes, you must disable the policy setting and wait for three (3) hours before you install firmware and driver updates through the P&U framework.

3 1611 Patch and Update Process

IMPORTANT: Be sure to follow the prerequisites listed in the previous section before you run the 1611 Patch and Update process.

3.1 Step 1: Run the 1611 P&U update package PUDellEMC

IMPORTANT: You must run the 1611 PUDellEMC package before you run the 1611 Microsoft P0 and Microsoft P1 packages.

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 PUDellEMC update package, such as **PU_#**, where # is the number or some other identifier of the specific update package. For example:

```
\\<Prefix>CON01\PUShare\PU_DellEMC
```

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_1611_Run_First.exe** to extract the update. When prompted, select the **PU_DellEMC** 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_DellEMC\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_DellEMC\PU\Framework\PatchingUpgrade\Invoke-PURun.ps1 -PUCredential (Get-Credential) -ScomAlertAction "Continue"
```

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

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

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

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

```

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

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

```

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

Import-Module .\PatchingUpgrade\DPM.psm1

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

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

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

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

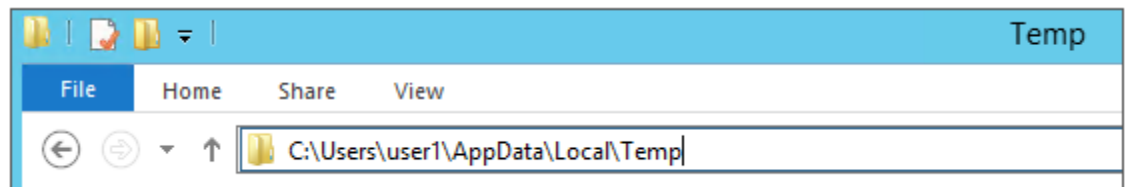
- If you have the VMM console open, and it reconnects, patching of the VMM server may be in progress. This is expected behavior.
2. To monitor the progress, you can use the following methods:
 - View the verbose output on the screen.
 - View the P&U events in Event Viewer. You can find P&U events under **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 1611 P&U update package Microsoft P0

IMPORTANT: You must run the 1611 PUDellEMC package before you run the 1611 P0 and P1 packages.

Run the 1611 Microsoft P0 update package by doing the following:

1. Browse to the shared folder **PUShare** on the console VM, and create a folder to store the 1611-0 update package, such as **PU_#**, where # is the number or some other identifier of the specific update package. For example, where *1611* represents the year/month:

```
\\<Prefix>CON01\PUShare\PU_1611_0
```

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_1611_Run_Second.exe** to extract the update. When prompted, select the **PU_1611_0** 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_1611_0\PU\Framework\PatchingUpgrade\Invoke-PURun.ps1 -  
PUCredential (Get-Credential)
```

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

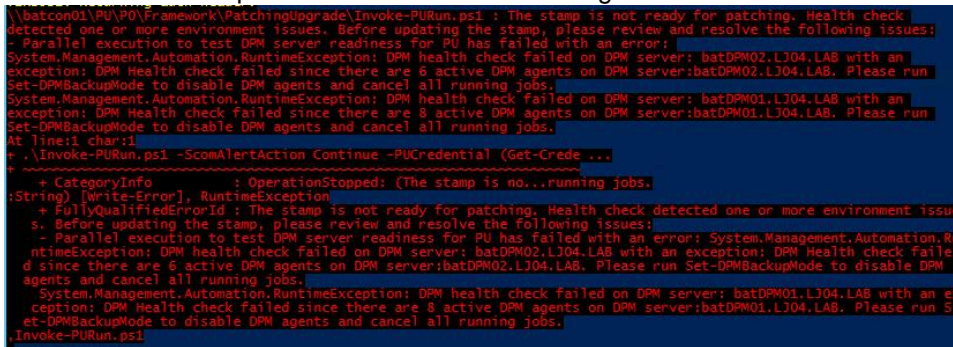
4. When prompted, enter the account credentials of the account that you used to log in.
5. The `Invoke-PURun` script performs a one-time environment setup and may prompt you to restart Windows PowerShell on its for invocation, for example:

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

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

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

The PowerShell output looks similar to the following screenshot:



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

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

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

Import-Module .\PatchingUpgrade\DPM.psm1

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

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

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

1. During the patching process note the following:
 - If you click inside the Windows PowerShell window during the patching process, the screen output will freeze, although the update process is still running. Press **Enter** to continue the scrolling of output.
 - Some component updates do not output status to the Windows PowerShell console. See the next step (6) 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.

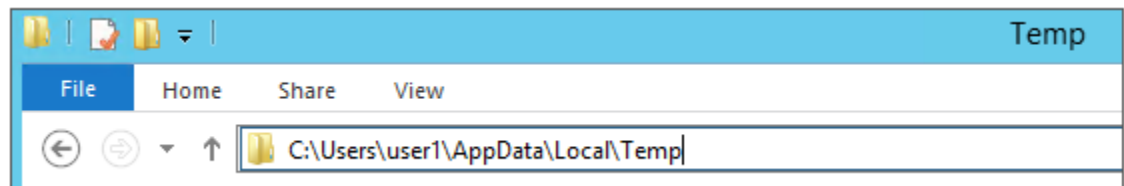
- If you have the VMM console open, and it reconnects, patching of the VMM server may be in progress. This is expected behavior.
2. To monitor the progress, you can use the following methods:
- View the verbose output on the screen.
 - View the P&U events in Event Viewer. You can find P&U events under **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 **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 1611 Microsoft P0 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 1611 Microsoft P0 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 Step 3: Run the 1611 P&U update package Microsoft P1

IMPORTANT: You must run the 1611 PUDellEMC package and the 1611 P0 package before you run the 1611 P1 package.

Run the 1611 Microsoft P1 update package by doing the following:

1. Browse to the shared folder **PUShare** on the console VM, and create a folder to store the 1611-1 update package, such as **PU_#**, where # is the number or some other identifier of the specific update package. For example, where 1611 represents the year/month:

```
\\<Prefix>CON01\PUShare\PU_1611_1
```

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 and execute the file with the format **DHCS_Update_1611_Run_Third.exe** file to extract the update. When prompted, select the **PU_1611_1** 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_1611_1\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"`

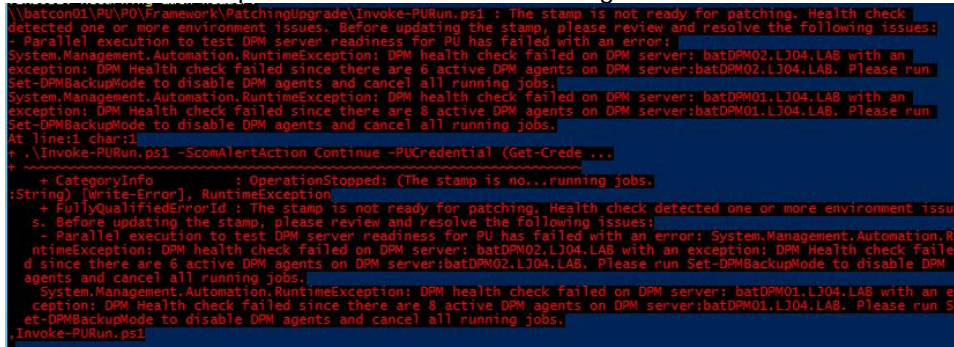
4. When prompted, enter the account credentials of the account that you are logged on as.
5. The `Invoke-PURun` script performs a one-time environment setup and may prompt you to restart Windows PowerShell on its first invocation, for example:

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
r .\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.
8. The Patch and Update process should begin, with verbose output of the progress. 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 (9) 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.

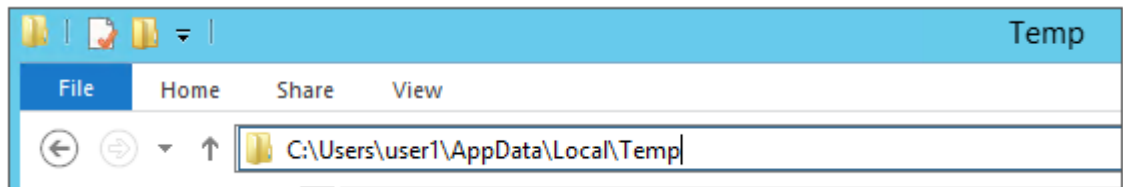
Note: After Cluster-Aware Updating (CAU) completes, you can click **Generate a report on past Updating Runs** to view details about what was installed through CAU.

- If you have the VMM console open, and it reconnects, patching of the VMM server may be in progress. This is expected behavior.
9. 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).

10. 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.

| Event Viewer (Local) | | Operational Number of events: 6,314 | | | |
|--------------------------------|-------------|-------------------------------------|------------------------|------------|---------------|
| | | Level | Date and Time | Source | Task Category |
| Applications and Services Logs | Operational | 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 |

11. 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 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 1611 Microsoft P1 immediately, remember to enable DPM agents if you disabled them earlier (as described in the *Dell Hybrid Cloud System for Microsoft Cloud Platform System (CPS) Standard Administrators Guide*). Note that this applies only if your solution includes Data Protection Manager (DPM) for backup.

3.4 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 1611 for CPS Standard.

4.1 Issue: `PURunstatus.json` file reports failed state after console reboot

Description: Servicing is set to automatically restart after rebooting the console from which servicing is run. This ensures that the console is fully updated. Occasionally, there are failures in servicing due to this reboot happening before actions are complete.

Detection: `PURunStatus.json` file has an entry near the end of the file indicating the state is in error.

```
State:      Error
```

Remediation: Run the scheduled task called `ConsoleRestartTask` by doing the following:

1. Open **Task Scheduler**.
2. Navigate to **Task Scheduler Library > Microsoft > PU**.
3. Select **Console Restart Task**.
4. Select **Run** from the right-click menu, or from the **Action** pane to the right of the window.

4.2 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 1611 Patch and Update Process.

Note: If you run 1611 Patch and Update multiple times and the same subsystem keeps failing, please contact your Dell Support Representative.

5 Microsoft payload for Update P0 package

5.1 Configuration changes from previous updates

| Computers | Update |
|-----------|---|
| All | <code>Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client" -Name DisabledByDefault -Type DWord -Value 1</code> |
| All | <code>Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client" -Name Enabled -Type DWord -Value 0</code> |
| All | <code>Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server" -Name DisabledByDefault -Type DWord -Value 1</code> |
| All | <code>Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server" -Name Enabled -Type DWord -Value 0</code> |
| All | <code>Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client" -Name DisabledByDefault -Type DWord -Value 1</code> |
| All | <code>Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client" -Name Enabled -Type DWord -Value 0</code> |
| All | <code>Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server" -Name DisabledByDefault -Type DWord -Value 1</code> |
| All | <code>Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server" -Name Enabled -Type DWord -Value 0</code> |

5.2 Updates for Windows Server 2012 R2, from previous updates

| KB Article | Description |
|-------------------------|--|
| 3138615 | Update for Windows Server 2012 R2 (KB3138615) |
| 3173424 | Servicing stack update for Windows 8.1 and Windows Server 2012 R2: July 12, 2016 |

6 Microsoft payload for Update P1 package

6.1 New updates for Windows Server 2012 R2

| KB Article | Description |
|-------------------------|--|
| 3062960 | Hotfix for Windows Server 2012 R2 x64 Edition (KB3062960) |
| 3163291 | Security Update for Microsoft .NET Framework 4.5.2 on Windows 8.1 and Windows Server 2012 R2 for x64 (KB3163291) |
| 3197874 | November, 2016 Security Monthly Quality Rollup for Windows Server 2012 R2 (KB3197874) |
| 3202790 | Security Update for Adobe Flash Player for Windows Server 2012 R2 (KB3202790) |

6.2 Updates for SQL Server 2014 SP1

| KB Article | Description |
|-------------------------|---|
| 3171021 | Microsoft SQL Server 2014 Service Pack 2 |
| 3188778 | Cumulative update 2 for SQL Server 2014 SP2 |
| 3194718 | Security Update for SQL Server 2014 Service Pack 2 CU (KB3194718) |

6.3 System Center and Windows Azure Pack updates, from previous updates

| KB Article | Description |
|-------------------------|--|
| 3147172 | This update fixes the problems described in KB article 3147172 |
| 3147191 | This update fixes the problems described in KB article 3147167 |

| KB Article | Description |
|-------------------------|--|
| 3147167 | This update fixes the problems described in KB article 3147167 |
| 3158609 | This update fixes the problems described in KB article 3158609 |
| 3158139 | This update fixes the problems described in KB article 3147167 |

6.4 Updates for Windows Server 2012 R2, from previous updates

| KB Article | Description |
|--------------------------|--|
| 3185331 | October 2016 security monthly quality rollup for Windows 8.1 and Windows Server 2012 R2 |
| 3188743 | MS16-120: Description of the Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1 and Windows Server 2012 R2: October 11, 2016 |
| 3192392 | October 2016 security only quality update for Windows 8.1 and Windows Server 2012 R2 |
| 3200006 | System Center Operations Manager Management Console crashes after you install MS16-118 and MS16-126 |
| +3063109 | Update for Windows Server 2012 R2 (KB3063109) |
| 3153224 | Update for System Center Endpoint Protection 2012 Client - 4.9.219.0 (KB3153224) |
| 3174644 | Security Update for Windows Server 2012 R2 (KB3174644) |
| 3175024 | Security Update for Windows Server 2012 R2 (KB3175024) |
| 3177186 | Security Update for Windows Server 2012 R2 (KB3177186) |

| KB Article | Description |
|-------------------------|---|
| 3178539 | Security Update for Windows Server 2012 R2 (KB3178539) |
| 3179574 | Update for Windows Server 2012 R2 (KB3179574) |
| 3184122 | Security Update for Windows Server 2012 R2 (KB3184122) |
| 3184471 | Security Update for Windows Server 2012 R2 (KB3184471) |
| 3184943 | Security Update for Windows Server 2012 R2 (KB3184943) |
| 3185319 | Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 (KB3185319) |
| 3185911 | Security Update for Windows Server 2012 R2 (KB3185911) |
| 3187022 | Update for Windows Server 2012 R2 (KB3187022) |
| 3188128 | Security Update for Adobe Flash Player for Windows Server 2012 R2 (KB3188128) |
| 3172729 | MS16-100: Description of the security update for Secure Boot: August 9, 2016 |
| 3175443 | MS16-095: Security update for Internet Explorer: August 9, 2016 |
| 3175887 | MS16-102: Description of the security update for Microsoft Windows PDF library: August 9, 2016 |
| 3177108 | MS16-101: Description of the security update for Windows authentication methods: August 9, 2016 |
| 3177725 | MS16-098: Description of the security update for Windows kernel-mode drivers: August 9, 2016 |
| 3178034 | MS16-097: Description of the security update for Microsoft Graphics Component: August 9, 2016 |

| KB Article | Description |
|-------------------------|--|
| 3170455 | MS16-087: Description of the security update for Windows print spooler components: July 12, 2016 |
| 3172727 | MS16-094: Description of the security update for Secure Boot: July 12, 2016 |
| 3164294 | MS16-073: Description of the security update for kernel mode drivers: June 14, 2016 |
| 3164035 | MS16-074: Description of the security update for Microsoft Graphics Component: June 14, 2016 |
| 3164033 | MS16-074: Description of the security update for Microsoft Graphics Component: June 14, 2016 |
| 3162835 | June 2016 DST and time zone update for Windows |
| 3162343 | MS16-076: Description of the security update for Netlogon: June 14, 2016 |
| 3161958 | MS16-082: Description of the security update for Windows Structured Query: June 14, 2016 |
| 3161951 | MS16-071: Description of the security update for DNS Server: June 14, 2016 |
| 3161949 | MS16-077: Description of the security update for WPAD: June 14, 2016 |
| 3161664 | MS16-073: Description of the security update for kernel mode drivers: June 14, 2016 |
| 3161561 | MS16-075 and MS16-076: Description of the security update for Windows Netlogon and SMB Server: June 14, 2016 |
| 3160352 | MS16-081: Security Update for Active Directory: June 14, 2016 |
| 3160005 | MS16-063: Security update for Internet Explorer: June 14, 2016 |
| 3159398 | MS16-072: Description of the security update for Group Policy: June 14, 2016 |

| KB Article | Description |
|-------------------------|---|
| 3157569 | MS16-080: Description of the security update for Windows PDF: June 14, 2016 |
| 3156418 | May 2016 update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 |
| 3149157 | Reliability and scalability improvements in TCP/IP for Windows 8.1 and Windows Server 2012 R2 |
| 3147071 | Connection to Oracle database fails when you use Microsoft ODBC or OLE DB Driver for Oracle or Microsoft DTC in Windows |
| 3146978 | RDS redirected resources showing degraded performance in Windows 8.1 or Windows Server 2012 R2 |
| 3146751 | "Logon is not possible" error or a temporary file is created when you log on App-V in Windows Server 2012 R2 |
| 3146604 | WMI service crashes randomly in Windows Server 2012 R2 or Windows Server 2012 |
| 3145432 | Cluster nodes or VMs go offline when they are using VMQ capable NICs on a Windows Server 2012 R2 host |
| 3145384 | MinDiffAreaFileSize registry value limit is increased from 3 GB to 50 GB in Windows 8.1 or Windows Server 2012 R2 |
| 3144850 | Update enables downgrade rights between Windows 10 IoT and Windows Embedded 8.1 Industry |
| 3141074 | "0x00000001" Stop error when a shared VHDX file is accessed in Windows Server 2012 R2-based Hyper-V guest |
| 3140234 | "0x0000009F" Stop error when a Windows VPN client computer is shutdown with an active L2TP VPN connection |
| 3140219 | "0x00000133" Stop error after you install hotfix 3061460 in Windows Server 2012 R2 |

| KB Article | Description |
|-------------------------|--|
| 3139923 | Windows installer (MSI) repair doesn't work when MSI package is installed on an HTTP share in Windows |
| 3139921 | "No computer account for trust" error when you change domain account password in Windows |
| 3139896 | Hyper-V guest may freeze when it is running failover cluster service together with shared VHDX in Windows Server 2012 R2 |
| 3139649 | Print job fails if Creator Owner is removed from Windows Server 2012 R2 or Windows Server 2012 |
| 3139219 | 0x1E Stop error when you restart or shut down a computer running Windows 8.1 or Windows Server 2012 R2 |
| 3139165 | High CPU load on a Windows Server 2012 R2-based server because NAT keep-alive timer isn't cleaned up |
| 3139164 | Tracert command doesn't receive responses when you trace resources on Internet through Windows Server 2012 R2 HNV GW |
| 3139162 | DirectAccess client receives incorrect response to reverse lookup query from a Windows Server 2012 R2-based DNS64 server |
| 3138602 | "File contents" option is always selectable, Start screen becomes blank, or computer freezes when startup in Windows 8.1 |
| 3137728 | VSS restore fails when you use ResyncLuns VSS API in Windows Server 2012 R2-based failover cluster |
| 3137725 | Get-StorageReliabilityCounter doesn't report correct values of temperature in Windows Server 2012 R2 |
| 3137061 | Windows Azure VMs don't recover from a network outage and data corruption issues occur |
| 3134815 | CryptDuplicateKey function doesn't save state for an RC2 40-Bit key in Windows 8.1 or Windows Server 2012 R2 |

| KB Article | Description |
|-------------------------|--|
| 3134785 | Memory leak in RPCSS and DcomLaunch services in Windows 8.1 or Windows Server 2012 R2 |
| 3134242 | DNS client API call fails and could lead to service restart freeze in Windows Server 2012 R2 or Windows Server 2012 |
| 3134179 | Update adds performance counters for Remote Desktop Connection Broker in Windows Server 2012 R2 |
| 3133924 | "Code 10 Device Cannot Start" error for EHCI USB Controller devices in Device Manager in Windows Server 2012 R2 |
| 3133690 | Update to add Discrete Device Assignment support for Azure that runs on Windows Server 2012 R2-based guest VMs |
| 3132080 | The logon process hangs at the "Welcome" screen or the "Please wait for the User Profile Service" error message window |
| 3130939 | Nonpaged pool memory leak occurs in a Windows Server 2012 R2-based failover cluster |
| 3128650 | Access to COM+ role-based security is denied in Windows Server 2012 R2 |
| 3126041 | MS16-014: Description of the security update for Windows: February 9, 2016 |
| 3126033 | Error occurs when you use Remote Desktop in Restricted Admin mode in Windows 8.1 or Windows Server 2012 R2 |
| 3125424 | LSASS deadlocks cause Windows Server 2012 R2 or Windows Server 2012 not to respond |
| 3125210 | Badpwdcount on PDC isn't reset when you use NTLM authentication to log on to Windows Server 2012 R2 |
| 3123245 | Update improves port exhaustion identification in Windows Server 2012 R2 |
| 3123242 | Reassociated WFP context in same flow doesn't work in Windows |

| KB Article | Description |
|-------------------------|--|
| 3121255 | "0x00000024" Stop error in FsRtlNotifyFilterReportChange and copy file may fail in Windows |
| 3118401 | Update for Universal C Runtime in Windows |
| 3115224 | Reliability improvements for VMs that are running on a Windows Server 2012 R2 or Windows Server 2012 host |
| 3109976 | Texas Instruments xHCI USB controllers may encounter a hardware issue on large data transfers in Windows 8.1 |
| 3103709 | Windows Server 2012 R2-based or Windows Server 2012-based domain controller update, April 2016 |
| 3103696 | Update for USB Type-C billboard support and Kingston thumb drive is enumerated incorrectly in Windows |
| 3103616 | WMI query doesn't work in Windows Server 2012 R2 or Windows Server 2012 |
| 3102467 | The .NET Framework 4.6.1 for Windows Server 2012 R2 on Windows Update |
| 3100956 | You may experience slow logon when services are in start-pending state in Windows Server 2012 R2 |
| 3100919 | Virtual memory size of Explorer increases when you open programs continuously in Windows 8.1 or Windows Server 2012 R2 |
| 3100473 | DNS records get deleted when you delete the scope on a Windows Server 2012 R2-based DHCP server |
| 3099834 | "Access violation" error and application that uses private keys crashes in Windows 8.1 or Windows Server 2012 R2 |
| 3096433 | Chkdsk command freezes when it's running in Windows |
| 3095701 | TPM 2.0 device can't be recognized in Windows Server 2012 R2 |

| KB Article | Description |
|-------------------------|--|
| 3094486 | KDS doesn't start or KDS root key isn't created in Windows Server 2012 R2 |
| 3092627 | September 2015 update to fix Windows or application freezes after you install security update 3076895 |
| 3091297 | You can't logon to an AD FS server from a Windows Store app on a Windows 8.1 or Windows RT 8.1 device |
| 3088195 | MS15-111: Description of the security update for Windows Kernel: October 13, 2015 |
| 3087137 | Gradient rendering issue when an application has nested transformed geometries in Windows 8.1 |
| 3087041 | You can't select the first item in a list by touching in Windows 8.1 |
| 3086255 | MS15-097: Description of the security update for the graphics component in Windows: September 8, 2015 |
| 3084135 | MS15-102: Description of the security update for Windows Task Management: September 8, 2015 |
| 3083992 | Microsoft security advisory: Update to improve AppLocker certificate handling: September 8, 2015 |
| 3082089 | MS15-102: Description of the security update for Windows Task Management: September 8, 2015 |
| 3080149 | Update for customer experience and diagnostic telemetry |
| 3080042 | CHM file freezes when you enter characters in Search box on the Index tab in Windows 8.1 or Windows Server 2012 R2 |
| 3078676 | Event 1530 is logged and ProfSvc leaks paged pool memory and handles in Windows 8.1 or Windows Server 2012 R2 |
| 3078405 | "0x0000004A" or "0x0000009F" Stop error occurs in Windows 8.1 |

| KB Article | Description |
|-------------------------|--|
| 3077715 | August 2015 cumulative time zone update for Windows operating systems |
| 3071663 | Microsoft applications might crash in Windows |
| 3067505 | MS15-076: Vulnerability in Windows Remote Procedure Call could allow elevation of privilege: July 14, 2015 |
| 3063843 | Registry bloat causes slow logons or insufficient system resources error 0x800705AA in Windows 8.1 |
| 3061512 | MS15-069: Description of the security update for Windows: July 14, 2015 |
| 3060793 | "0x0000001E" or "0x00000133" Stop error when you transfer data through a USB-based RNDIS device on Windows |
| 3060383 | Decimal symbol and digit grouping symbol are incorrect for the Swiss language locale in Windows |
| 3059316 | You cannot move the scrollbar on Windows by dragging the mouse |
| 3055343 | Stop error code 0xD1, 0x139, or 0x3B and cluster nodes go down in Windows Server 2012 R2 or Windows Server 2012 |
| 3055323 | Update to enable a security feature in Windows 8.1 or Windows Server 2012 R2 |
| 3054464 | Applications that use the AddEntry method may crash in Windows |
| 3054256 | Reliability improvements for Windows 8.1: June 2015 |
| 3054203 | Update for SIP to enable WinVerifyTrust function in Windows Server 2012 R2 to work with a later version of Windows |
| 3054169 | Update to add more information to minidump files that helps OCA servers categorize failures correctly in Windows |

| KB Article | Description |
|-------------------------|---|
| 3052480 | Unexpected ASP.Net application shutdown after many App_Data file changes occur on a server that is running Windows Server 2012 R2 |
| 3048043 | Screen flickers or becomes blank when you drag tiles on the Start screen in Windows |
| 3047234 | MS15-042: Vulnerability in Windows Hyper-V could allow denial of service: April 14, 2015 |
| 3046737 | "Paired" text is not translated correctly in Korean when you disconnect a paired Bluetooth device in Windows |
| 3046359 | MS15-068: Description of the security update for Windows Hyper-V: July 14, 2015 |
| 3046339 | MS15-068: Description of the security update for Windows Hyper-V: July 14, 2015 |
| 3045999 | MS15-038: Description of the security update for Windows: April 14, 2015 |
| 3045992 | "Description cannot be found" error in event logs in Event Viewer in Windows Server 2012 R2 or Windows Server 2012 |
| 3045746 | Single string is drawn by multiple fonts in the TextBox control of Windows Store application in Windows |
| 3045719 | Microsoft Project Siena crashes when you use galleries in the application in Windows |
| 3045717 | Narrator does not stop reading when you press Ctrl key in Windows |
| 3045634 | You cannot make a PPP connection after you reconnect a PLC device in Windows 8.1 or Windows 8 |
| 3044673 | Photos taken by certain Android devices show blank value in Date taken field in Windows Explorer |

| KB Article | Description |
|-------------------------|--|
| 3044374 | Update that enables you to upgrade from Windows 8.1 to Windows 10 |
| 3043812 | Layout of Cambria font is different in Word documents when the text metric changes in Windows 8.1 or Windows 8 |
| 3042085 | Device does not respond during shutdown after you have installed November 2014 update in Windows |
| 3042058 | Microsoft security advisory: Update to default cipher suite priority order: May 12, 2015 |
| 3041857 | "Code 0x80070057 The parameter is incorrect" error when you try to display a user's "effective access" to a file |
| 3038002 | UHS-3 cards cannot be detected in Windows on Surface devices |
| 3037924 | You cannot do System Image Backup to Blu-ray media in Windows |
| 3037579 | MS15-041: Description of the security update for the .NET Framework 4.5.1 and 4.5.2 on Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: April 14, 2015 |
| 3036612 | Windows Store apps may crash in Windows 8.1 or Windows RT 8.1 |
| 3034348 | "Access denied" error when you use a Windows Store app to configure printer property settings in Windows |
| 3033446 | Wi-Fi connectivity issues or poor performance on CHT platform computers in Windows 8.1 |
| 3031044 | Embedded Lockdown Manager is installed unexpectedly in Windows 8.1 or Windows Server 2012 R2 |
| 3030947 | Compatibility issues for applications that rely on a certain code layout for memory in Windows |

| KB Article | Description |
|-------------------------|---|
| 3029603 | xHCI driver crashes after you resume computer from sleep mode in Windows 8.1 or Windows Server 2012 R2 |
| 3027209 | Reliability improvements for Windows 8.1: March 2015 |
| 3024755 | Multi-touch gesture does not work after you exit the Calculator in Windows |
| 3024751 | The TAB key does not switch the cursor to the next input box when you enter Wi-Fi credentials on a Surface Pro 3 |
| 3021910 | April 2015 servicing stack update for Windows 8.1 and Windows Server 2012 R2 |
| 3016074 | Windows activation does not work when the sppsvc.exe process is not started automatically for a long time |
| 3013791 | "DPC_WATCHDOG_VIOLATION (0x133)" Stop error when there's faulty hardware in Windows 8.1 or Windows Server 2012 R2 |
| 3013538 | Automatic brightness option is disabled unexpectedly after you switch between PC settings pages in Windows |
| 3013410 | December 2014 cumulative time zone update for Windows operating systems |
| 3013172 | Individual memory devices cannot be ejected through the Safely Remove Hardware UI in Windows 8.1 |
| 3012702 | Some default program associations for a roamed user may be lost when you log on to an RDS server in Windows |
| 3006137 | Update changes the currency symbol of Lithuania from the Lithuanian litas (Lt) to the euro (€) in Windows |
| 3004394 | Support for urgent Trusted Root updates for Windows Root Certificate Program in Windows |

| KB Article | Description |
|-------------------------|---|
| 2989930 | "Not Connected" status for a paired Surface Pen in Bluetooth settings on Surface Pro 3 |
| 2894852 | Description of the security update for the .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2: December 10, 2013 |
| 890830 | The Microsoft Windows Malicious Software Removal Tool helps remove specific, prevalent malicious software from computers that are running supported versions of Windows |
| 3156059 | MS16-057: Description of the security update for Windows shell: May 10, 2016 |
| 3156019 | MS16-055: Description of the security update for Microsoft graphics component: May 10, 2016 |
| 3156017 | MS16-062: Description of the security update for Windows Kernel-Mode Drivers: May 10, 2016 |
| 3156016 | MS16-055: Description of the security update for Microsoft graphics component: May 10, 2016 |
| 3156013 | MS16-055: Description of the security update for Microsoft graphics component: May 10, 2016 |
| 3155784 | MS16-067: Security update for volume manager driver: May 10, 2016 |
| 3154070 | MS16-051: Security update for Internet Explorer: May 10, 2016 |
| 3153704 | MS16-061: Description of the security update for RPC: May 10, 2016 |
| 3153199 | MS16-062: Description of the security update for Windows Kernel-Mode Drivers: May 10, 2016 |
| 3153171 | MS16-060 and MS16-061: Description of the security update for RPC and for Windows kernel: May 10, 2016 |
| 3151058 | MS16-064: Description of the security update for Schannel: May 10, 2016 |

| KB Article | Description |
|-------------------------|---|
| 3149090 | MS16-047: Description of the security update for SAM and LSAD remote protocols: April 12, 2016 |
| 3146963 | MS16-040: Description of the security update for Microsoft XML core services: April 12, 2016 |
| 3146723 | MS16-048: Description of the security update for CSRSS: April 12, 2016 |
| 3146706 | MS16-044: Security update for Windows OLE: April 12, 2016 |
| 3142045 | MS16-039: Description of the security update for the .NET Framework 3.5 in Windows 8.1 and Windows Server 2012 R2: April 12, 2016 |
| 3142036 | MS16-065: Description of the security update for the .NET Framework 4.6 and 4.6.1 in Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: May 10, 2016 |
| 3142030 | MS16-065: Description of the security update for the .NET Framework 4.5.2 in Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: May 10, 2016 |
| 3142026 | MS16-065: Description of the security update for the .NET Framework 3.5 in Windows 8.1 and Windows Server 2012 R2: May 10, 2016 |
| 3135998 | MS16-035: Description of the security update for the .NET Framework 4.6 and 4.6.1 in Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: March 8, 2016 |
| 3135994 | MS16-035: Description of the security update for the .NET Framework 4.5.2 in Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: March 8, 2016 |
| 3135991 | MS16-035: Description of the security update for the .NET Framework 3.5 in Windows 8.1 and Windows Server 2012 R2: March 8, 2016 |
| 3135985 | MS16-035: Description of the security update for the .NET Framework 3.5 in Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: March 8, 2016 |
| 3135456 | MS16-045: Description of the security update for Windows Hyper-V: April 12, 2016 |

| KB Article | Description |
|-------------------------|--|
| 3130944 | March 2016 update for Windows Server 2012 R2 clusters to fix several issues |
| 3127231 | MS16-019: Description of the security update for the .NET Framework 4.6 and 4.6.1 in Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: February 9, 2016 |
| 3127226 | MS16-019: Description of the security update for the .NET Framework 4.5.2 in Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: February 9, 2016 |
| 3127222 | MS16-019: Description of the security update for the .NET Framework 3.5 in Windows 8.1 and Windows Server 2012 R2: February 9, 2016 |
| 3123479 | Microsoft security advisory: Deprecation of SHA-1 hashing algorithm for Microsoft root certificate program: January 12, 2016 |
| 3122660 | MS16-019: Description of the security update for the .NET Framework 4.6 and 4.6.1 in Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: February 9, 2016 |
| 3122654 | MS16-019: Description of the security update for the .NET Framework 4.5.2 in Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: February 9, 2016 |
| 3122651 | MS16-019: Description of the security update for the .NET Framework 3.5 in Windows 8.1 and Windows Server 2012 R2: February 9, 2016 |
| 3121918 | MS16-007: Description of the security update for Windows: January 12, 2016 |
| 3121461 | MS16-007: Description of the security update for Windows: January 12, 2016 |
| 3110329 | MS16-007: Description of the security update for Windows: January 12, 2016 |
| 3109560 | MS16-007: Description of the security update for Windows: January 12, 2016 |
| 3109094 | MS15-128 and MS15-135: Description of the security update for Windows kernel-mode drivers: December 8, 2015 |

| KB Article | Description |
|-------------------------|---|
| 3108604 | Microsoft security advisory: Description of the security update for Windows Hyper-V: November 10, 2015 |
| 3102939 | MS15-120: Security update for IPsec to address denial of service: November 10, 2015 |
| 3101246 | MS15-122: Description of the security update for Windows Kerberos: November 10, 2015 |
| 3098785 | MS15-118: Description of the security update for the .NET Framework 4.6 and 4.6.1 on Windows 8.1 and Windows Server 2012 R2: November 10, 2015 |
| 3098779 | MS15-118: Description of the security update for the .NET Framework 4.5.1 and 4.5.2 on Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: November 10, 2015 |
| 3098000 | MS15-118: Description of the security update for the .NET Framework 4.6 and 4.6 RC on Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: November 10, 2015 |
| 3097997 | MS15-118: Description of the security update for the .NET Framework 4.5.1 and 4.5.2 on Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: November 10, 2015 |
| 3097992 | MS15-118: Description of the security update for the .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2: November 10, 2015 |
| 3097966 | Microsoft security advisory: Inadvertently disclosed digital certificates could allow spoofing: October 13, 2015 |
| 3092601 | MS15-119: Description of the security update for Windows Winsock: November 10, 2015 |
| 3081320 | MS15-121: Security update for Schannel to address spoofing: November 10, 2015 |
| 3080446 | MS15-109: Description of the security update for Windows Shell: October 13, 2015 |

| KB Article | Description |
|-------------------------|---|
| 3078601 | MS15-080: Description of the security update for Windows: August 11, 2015 |
| 3076895 | MS15-084: Description of the security update for Windows XML core services: August 11, 2015 |
| 3075220 | MS15-082: Description of the security update for RDP in Windows: August 11, 2015 |
| 3074553 | MS15-101: Description of the security update for the .NET Framework 4.6 and 4.6 RC on Windows 8.1 and Windows Server 2012 R2: September 8, 2015 |
| 3074548 | MS15-101: Description of the security update for the .NET Framework 4.5.1 and 4.5.2 on Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: September 8, 2015 |
| 3074545 | MS15-101: Description of the security update for the .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2: September 8, 2015 |
| 3074232 | MS15-101: Description of the security update for the .NET Framework 4.6 and 4.6 RC on Windows 8.1 and Windows Server 2012 R2: September 8, 2015 |
| 3074228 | MS15-101: Description of the security update for the .NET Framework 4.5.1 and 4.5.2 on Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: September 8, 2015 |
| 3072630 | MS15-074: Vulnerability in Windows Installer service could allow elevation of privilege: July 14, 2015 |
| 3072307 | MS15-080: Description of the security update for the .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2: August 11, 2015 |
| 3071756 | MS15-085: Description of the security update for Windows Mount Manager: August 11, 2015 |
| 3068457 | MS15-071: Vulnerability in Netlogon could allow elevation of privilege: July 14, 2015 |

| KB Article | Description |
|-------------------------|---|
| 3060716 | MS15-090: Vulnerabilities in Windows could allow elevation of privilege: August 11, 2015 |
| 3059317 | MS15-060: Vulnerability in Microsoft common controls could allow remote code execution: June 9, 2015 |
| 3055642 | MS15-050: Vulnerability in Service Control Manager could allow elevation of privilege: May 12, 2015 |
| 3048072 | MS15-044: Description of the security update for the .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2: May 12, 2015 |
| 3046017 | MS15-088 Description of the security update for Windows, Internet Explorer, and Office: August 11, 2015 |
| 3045755 | Microsoft Security Advisory 3045755: Update to improve PKU2U authentication |
| 3045685 | MS15-038: Description of the security update for Windows: April 14, 2015 |
| 3042553 | MS15-034: Vulnerability in HTTP.sys could allow remote code execution: April 14, 2015 |
| 3037576 | MS15-041: Description of the security update for the .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2: April 14, 2015 |
| 3035126 | MS15-029: Vulnerability in Windows Photo Decoder component could allow information disclosure: March 10, 2015 |
| 3033889 | MS15-020: Description of the security update for Windows text services: March 10, 2015 |
| 3030377 | MS15-028: Vulnerability in Windows Task Scheduler could allow security feature bypass: March 10, 2015 |
| 3023266 | MS15-001: Vulnerability in Windows Application Compatibility cache could allow elevation of privilege: January 13, 2015 |

| KB Article | Description |
|-------------------------|--|
| 3023222 | MS15-048: Description of the security update for the .NET Framework 4.5.1 and 4.5.2 on Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: May 12, 2015 |
| 3023219 | MS15-048: Description of the security update for the .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2: May 12, 2015 |
| 3022777 | MS15-005: Vulnerability in Network Location Awareness service could allow security feature bypass: January 13, 2015 |
| 3021674 | MS15-003: Vulnerability in Windows User Profile service could allow elevation of privilege: January 13, 2015 |
| 3019978 | MS15-004: Description of the security update for Windows: January 13, 2015 |
| 3010788 | MS14-064: Description of the security update for Windows OLE: November 11, 2014 |
| 3006226 | MS14-064: Description of the security update for Windows OLE: November 11, 2014 |
| 3004365 | MS15-006: Vulnerability in Windows Error Reporting could allow security feature bypass: January 13, 2015 |
| 3004361 | MS15-014: Vulnerability in Group Policy could allow security feature bypass: February 10, 2015 |
| 3000483 | MS15-011: Vulnerability in Group Policy could allow remote code execution: February 10, 2015 |
| 2994397 | MS14-059: Description of the security update for ASP.NET MVC 5.1: October 14, 2014 |
| 2993939 | MS14-059: Description of the security update for ASP.NET MVC 2.0: October 14, 2014 |
| 2993937 | MS14-059: Description of the security update for ASP.NET MVC 3.0: October 14, 2014 |

| KB Article | Description |
|-------------------------|---|
| 2993928 | MS14-059: Description of the security update for ASP.NET MVC 4.0: October 14, 2014 |
| 2992080 | MS14-059: Description of the security update for ASP.NET MVC 5.0: October 14, 2014 |
| 2979576 | MS14-057: Description of the security update for the .NET Framework 4.5.1 and the .NET Framework 4.5.2 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: October 14, 2014 |
| 2979573 | MS14-057: Description of the security update for the .NET Framework 3.5 for Windows 8.1 and Windows Server 2012 R2: October 14, 2014 |
| 2978126 | MS14-072: Description of the security update for the .NET Framework 4.5.1 and 4.5.2 on Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: November 11, 2014 |
| 2978122 | MS14-072: Description of the security update for the .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2: November 11, 2014 |
| 2977765 | MS14-053: Description of the security update for the .NET Framework 4.5.1 and the .NET Framework 4.5.2 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: September 9, 2014 |
| 2977292 | Microsoft security advisory: Update for Microsoft EAP implementation that enables the use of TLS: October 14, 2014 |
| 2973114 | MS14-053: Description of the security update for the .NET Framework 3.5 for Windows 8.1 and Windows Server 2012 R2: September 9, 2014 |
| 2972213 | MS14-053: Description of the security update for the .NET Framework 3.5 for Windows 8.1 and Windows Server 2012 R2: September 9, 2014 |
| 2972103 | MS14-057: Description of the security update for the .NET Framework 3.5 for Windows 8.1 and Windows Server 2012 R2: October 14, 2014 |
| 2968296 | MS14-057: Description of the security update for the .NET Framework 3.5 for Windows 8.1 and Windows Server 2012 R2: October 14, 2014 |

| KB Article | Description |
|-------------------------|---|
| 2966828 | MS14-046: Description of the security update for the .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2: August 12, 2014 |
| 2966826 | MS14-046: Description of the security update for the .NET Framework 3.5 in Windows 8.1 and Windows Server 2012 R2: August 12, 2014 |
| 2934520 | The Microsoft .NET Framework 4.5.2 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 |
| 2898850 | Description of the security update for the .NET Framework 4.5.1 and the .NET Framework 4.5.2 on Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: May 13, 2014 |
| 2898847 | Description of the security update for the .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2: May 13, 2014 |
| 2565063 | MS11-025: Description of the security update for Visual C++ 2010 Service Pack 1: August 9, 2011 |
| 2565057 | MS11-025: Description of the security update for Visual Studio 2010 Service Pack 1: August 9, 2011 |
| 2542054 | MS11-025: Description of the security update for Visual Studio 2010: June 14, 2011 |
| 2538243 | MS11-025: Description of the security update for Visual C++ 2008 SP1 Redistributable Package: June 14, 2011 |
| 2538241 | MS11-025: Description of the security update for Visual Studio 2008 SP1: June 14, 2011 |
| 2467173 | MS11-025: Description of the security update for Visual C++ 2010 Redistributable Package: April 12, 2011 |

6.5 Troubleshooting the P&U process

Issue 1

Symptoms:

The **"SQLProductUpdates"** subsystem fails and returns the following error message:

The WS-Management service cannot complete the operation within the time specified in OperationTimeout.

Description:

There seems to be a timing issue in the service. Microsoft is currently researching this issue. This can cause **SQLProductUpdates** to fail and return an error message that resembles the following:

```
The Microsoft.HotfixPlugin plug-in reported a failure while attempting to
install updates on node "". Additional information reported by the plug-in:
(ClusterUpdateException) There was a failure in a Common Information Model (CIM)
operation, that is, an operation performed by software that Cluster-Aware
Updating depends on. The computer was "", and the operation was
"RunUpdateInstaller[,CauNodeWCD[]]". The failure was: (CimException) The WS-
Management service cannot complete the operation within the time specified in
OperationTimeout. HRESULT 0x80338029 ==> (CimException) The WS-Management
service cannot complete the operation within the time specified in
OperationTimeout. HRESULT 0x80338029
```

Although the P&U process fails while waiting for the action to finish, the underlying Cluster-Aware Updating (CAU) process succeeds.

Detection:

Verify that the CAU process has succeeded. You can do so by following these steps:

1. On the Console VM, open **Cluster-Aware Updating**.
2. In the **Connect to a failover cluster** list, click the **SQL Server cluster** (<Prefix>-HA-SQL), and then click **Connect**.
3. The **Last Run** status should show a **Succeeded** value for all four SQL Server nodes.

Verify the SQL Server version. To do so, follow these steps:

1. Open **SQL Server Management Studio**.
2. Connect to the <Prefix>SQLIN01\SQLIN01 instance.
3. Click **New Query**.
4. Run the following command: `SELECT @@VERSION`

The result should begin as follows:

```
Microsoft SQL Server 2014 (SP1-CU8) (KB3174038) - 12.0.4468.0 (X64)
```

Repeat steps 1 through 4 for the following SQL Server instances: <Prefix>SQLIN02\SQLIN02

Resolution:

If the CAU status shows a **Succeeded** value for all nodes, and if version information for all instances is correct, restart the P&U process, and add “SQLProductUpdates” to the -ExcludeSubsystems parameter array.

If the CAU status does not show **Succeeded** for all nodes, or if version information for all instances is correct, restart the P&U process, and make no change in parameters.

If the process fails again, escalate the case through your usual support channels.

Issue 2

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'."
```

Description:

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

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

Detection:

Looking at running SMA jobs in the WAP Administrator’s Service Management Portal, 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, which is not recommended, has performance impacts to SMA, 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 |
|--|---|
| <add key="MaxRunningJobs" value="30"/> | <add key="MaxRunningJobs" value="1"/> |
| <add key="TotalAllowedJobs" value="1000"/> | <add key="TotalAllowedJobs" value="1"/> |

2. After changing these two settings, reboot the SMA VM (<Prefix>APA01).

Issue 3

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 **External**, 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.

7 DELL payload for Update 1611

Dell Server BIOS R630/R730/R730XD Version 2.3.4 Fixes & Enhancements

Enhancements

- Updated the Intel Processor and Memory Reference Code to PLR5.
- Added the I/O Snoop HoldOff Response BIOS setup option in the Integrated Devices menu.

Fixes

- Removed BIOS power capping when in performance mode. This prevents the Node Manager power capping SCI from triggering.
- A PCI resource handling issue on the PowerEdge R630 server.
- Applied Intel Xeon Processor E5-2600 v3 memory CLK/RCD MRC workaround on Intel Xeon Processor E5-2600 v4

Dell Server BIOS PowerEdge C6320 Version 2.3.4 Fixes & Enhancements

Enhancements

- Updated the Intel Xeon Processor and Memory Reference Code to PLR5
- Added the I/O Snoop hold-off Response BIOS Setup option in the Integrated Devices menu

Fixes

- Removed the BIOS Power Capping when in Performance mode. This prevents the Node Manager power capping SCI from triggering.
- Applied Intel Xeon Processor E5-2600 v3 memory CLK/RCD MRC workaround on Intel Xeon Processor E5-2600 v4.

iDRAC with Lifecycle Controller Version 2.4140.40 Fixes & Enhancements

Enhancements

- Security - SSL library upgrade

Fixes

- Fixed occasional driver pack update failures when performed through iDRAC GUI, WS-MAN API, or remote RACADM command.
- NTLMv2 policy support for CIFS share while using SCP feature over all out of band iDRAC interfaces.
- Fix for occasional iDRAC unresponsiveness caused by upgrades via Firmware RACADM or have an active SOL or SSH sessions while firmware upgrade is in progress.
- Allow libwebsocket headers of up to 8192 characters.
- License self-service portal link on iDRAC license page in GUI updated with Digitallocker URL.
- Fixed the Import Buffer size limit for Server Configuration Profile (SCP) import operations via Redfish interface.
- Fixed incorrect URL within the Redfish Server Configuration Profile (SCP) schema.

Intel C600/C610/C220/C230/C2000 Series Chipset Drivers Fixes & Enhancements

Enhancements

- Certified for Windows Server 2016

Fixes

- None

Intel NIC Family Version 17.5.0 Firmware for I350, I354, X520, X540, and X550 adapters Fixes & Enhancements

Enhancements

- Added support for Intel(R) Ethernet 10G 2P X550-t Adapter
- Added support for Red Hat Enterprise Linux 7.2 x86_64
- Added support for Novell SUSE Linux Enterprise Server 12 SP1

Fixes

- Systems with five or more Intel(R) Gigabit 4P I350-t Adapters no longer hang during POST
- When running the firmware update on an Intel(R) Ethernet Server Adapter X520-T2, the installed version of firmware may have incorrectly shown 0.0.0.

Dell Storage MD14XX Enclosure Firmware Version 1.07 Fixes & Enhancements

Enhancements

- Increased the SSPT queue depth to 32

Fixes

- Fix a possible issue where enclosure overall status can possibly get out of sync with elements
- Implements Broadcom's recommendation to remove SAS buffering (Broadcom DataBolt) for 3 or 6Gb/s SAS drives due to a hardware
- Fix for thermal algorithms and thermal data reporting

Dell PERC H330 Mini/Adapter RAID Controllers firmware version 25.4.1.0004 Fixes & Enhancements

Enhancements

- Added support for SAS/SATA ISE drives.
- Added support for SATA 4k sector drives.
- Added support for Turbo Cache drives.
- Improved boot time for some specific failed SATA drives.

Fixes

- Disabled T10 Rebuild Assist (Rapid Rebuild).
- Corrected an issue where a specific cache flush condition could cause the controller to hang.
- Fixed an issue where after converting PERC personality mode to HBA, PDs still display as Ready state instead of Non-Raid.
- Resolved an issue that could lead the RAID controller to hang during multiple DC reboots.
- Resolved an issue where the PERC9 Windows drivers log each boot event which could eventually cause extended boot time.
- Changed memory reservation method to prevent serious issues when enabling Host Guardian Hyper V on Windows 2016 data center.

Dell H730/H730P/H830/FD33xS/FD33xD Mini/Adapter RAID Controllers firmware version 25.5.0.0018 Fixes & Enhancements

Enhancements

- Added support for SAS/SATA ISE drives.
- Added support for SATA 4k sector drives.
- Added support for Turbo Cache drives.
- Improved boot time for some specific failed SATA drives.
- Added 1MB IO support for H730, H730P and H830 controllers

Fixes

- Disabled T10 Rebuild Assist (Rapid Rebuild).
- Corrected an issue where a specific cache flush condition could cause the controller to hang.
- Fixed an issue where after converting PERC personality mode to HBA, PDs still display as Ready state instead of Non-Raid.
- Resolved an issue that could lead the RAID controller to hang during multiple DC reboots.
- Resolved an issue where the PERC9 Windows drivers log each boot event which could eventually cause extended boot time.

Windows 2012 R2 Driver 6.604.06.00 for PERC H330/H730/H730P/H830/FD33xD/FD33xS Controllers Fixes & Enhancements

Enhancements

- Added 1MB I/O support for H730, H730P and H830 controllers.

Fixes

- None

Dell 12Gbps HBA firmware version 13.17.03.00 Fixes & Enhancements

Enhancements

- None.

Fixes

- Fixed issue where tape drive is unintentionally loaded during boot.
- Fixed issue where unmap command is sent to the last LBA of an SSD.

Windows Server 2012 R2 Driver version 2.51.15.00 for Dell 12Gbps HBA and HBA330 Fixes & Enhancements

Enhancements

- None.

Fixes

- Fixed issue where array path is lost when the SAS end device has a LUN that cannot respond successfully to TUR.