



Horizon DaaS Platform 6.1.4 Release Notes

VMware Horizon DaaS Platform | 07 APR 2015

Release notes last updated on 15 APR 2015

Check for additions and updates to these release notes.

What's in the Release Notes

The release notes cover the following topics:

- Patch Information
 - Patch Dependencies
 - Affected Horizon DaaS Versions
 - Patch Version
- New Feature: Integration With Access Point Gateway
- Resolved Issues
- Other Updates Included in Patch
- Known Issues
- Installing the Patch
 - Upload and Run the Pre-Patch Cleanup Script on Primary SP Appliance
 - Upload the Patch File
 - Install the Patch on All Service Provider Appliances
 - Install the Patch on All Tenant Appliances
- Uninstalling the Patch

Patch Information

Patch Dependencies

Horizon DaaS Platform 6.1.3 (Build 22807)

Affected Horizon DaaS Versions

Horizon DaaS Platform 6.1.0 (Build 22210)

Horizon DaaS Platform 6.1.1 (Build 22355)

Horizon DaaS Platform 6.1.2 (Build 22583)

Horizon DaaS Platform 6.1.3 (Build 22807)

Patch Version

New Feature: Integration With Access Point Gateway

Beginning in release 6.1.4, customers who no longer need RDP will have the option to upgrade their remote access gateway from the dtRAM appliance to Access Point. Customers who migrate to Access Point can reduce their firewall open ports to 443, 4172 and 8443. Also, Access Point will properly handle SSL certificates for Blast so that a certificate will no longer be required inside the virtual desktop. Migrating to Access Point deactivates RDP entirely on your system. For information on setting up Access Point, see the Horizon DaaS Platform Access Point Setup document.

Resolved Issues

This patch includes fixes for the following issues:

- DT-5685 – An error during a clone operation in vCenter could sometimes cause clone tasks to go into a loop and require a dtService restart before the clone task could be retried. This has been remedied so that errors do not cause the clone operation to get stuck in a loop.
- DT-6710 – On shared clusters, compute updates by users (for example, partition re-sizing) were being overwritten by the system. This has been remedied so that user changes are no longer lost.
- DT-6790 – Some logs (slony, heartbeat, and postgres) had not been rotating in the most recent appliance template. This has been remedied so the logs are operating as expected.
- DT-7052 – When a compute pool was added, the system was discovering it multiple times, so that duplicate compute pools would appear in the Service Center compute pool list. This has been remedied so that each compute pool is discovered once and duplicates do not appear in the Service Center.
- DT-7064 – In multi-data center configurations, resource manager appliances were sometimes pointing to service providers in remote data centers instead of local ones, which affected system performance. This issue has been remedied so that resource managers only use service provider nodes in the local data center.
- DT-7163 – In Enterprise Center, users have not been able to create new session pools with RDP or PCoIP if the Blast protocol was not also enabled. This has been remedied and session pools can now be created as expected.
- DT-7251 – Desktops have not been connecting to pools associated with gold patterns that have been deleted or moved, even though the current status of a gold pattern should not affect the availability of the pools based on it. This issue has been remedied so a pools remains available regardless of the status of the associated gold pattern.
- DT-7263 – Tenant inventory attempts were hanging for several days when the resource manager did not respond due to an outage. This has been remedied so that the inventory times out after four hours, and then can be attempted again when the resource manager is available.
- DT-7321 – Users have been unable to update or change their passwords when connecting via PCoIP using the View Client directly. A continuous prompting of user credentials would appear when this occurred. This is has been resolved. User connecting to their desktops via the View Client will be able to change their passwords. Users will not be able to change

their password via the Desktop Portal and must launch the View Client natively to trigger password change functionality. Blast connections do not support password change at this time.

- DT-7356 – Tenant inventory had been taking an unexpectedly long time, sometimes as long as 20-30 minutes, affecting desktop availability for users. This issue has now been remedied and inventories are executing as expected.
- DT-7562 – Virtual Storage Console (VSC) rapid cloning has sometimes failed with an InvalidLogin SOAP fault exception in the platform. This was happening because the platform was using inactive hypervisor manager (vCenter) resource credentials. This has been remedied by using active credentials from available resource credentials in VSC provisioning.
- DT-7940 – When remote application or desktop session is reconnected, the session was still being shown as disconnected in the Enterprise Center. This has been remedied so that the correct status for the session appears.

Note: This fix requires updating to DaaS Agent 6.1.2.

- DT-8262 – New Zealand time zone [(GMT+12:00) Auckland, Wellington] was not being shown as an option on the Pattern Management or Modify Gold Pattern and Reseal pages in Enterprise Center. This has been remedied so that the correct option now appears (in English only).
- DT-8272 – Tenant inventory was sometimes being returned empty because the Resource Manager could not communicate with the Service Provider appliance. This was due to either network issues or the Service Provider being offline. This has been remedied so that the inventory runs as expected.

Other Updates Included in Patch

- DaaS Agent is updated to version 6.1.2. This new version includes the fix for session status issue in Enterprise Center (DT-7940 above), as well as security updates.
- The Oracle (Sun) JDK package is updated to 1.6.0_91. The update addresses multiple security issues that exist in the earlier releases of Oracle (Sun) JDK. Oracle has documented the CVE identifiers that are addressed in JDK 1.6.0_91 in the Oracle Java SE Critical Patch Update Advisory for January 2015. The JDK update includes a fix for CVE-2014-6593.

Known Issues

- DT-7874 – The video card setting ‘auto-detect settings’ for a gold pattern VM is not supported. If this selection is made, it can cause pool creation with that gold pattern to fail.

Installing the Patch

Note: Confirm that all appliances have patch 6.1.3 installed before performing the 6.1.4 patch installation.

Pushing out software patches to all appliances in one or more Data Centers is a multi-step process:

- Upload and run the pre-patch cleanup script on the primary service provider appliance.

- Upload the patch. When you upload the patch file, it is automatically replicated to all appliances.
- Install the patch file on all Service Provider appliances.
- Install the patch file on all Tenant appliances.
- These steps are described below.

Upload and Run the Pre-Patch Cleanup Script on Primary SP Appliance

Perform the following steps on the primary SP appliance on the master data center only.

1. scp the prePatchCleanup-6.1.4.sh file to the /tmp directory.
2. Run the following commands:

```
chmod 755 prePatchCleanup-6.1.4.sh
/tmp/prePatchCleanup-6.1.4.sh
```

Note: This script restarts the DaaS service on the service provider appliances across all data centers. While the service is restarting, there may be errors reported by monitoring systems and in the resource manager and tenant appliance logs, and certain tenant administrative functionality may be briefly impacted. End user desktop sessions and the brokering of new desktop sessions will be unaffected.

Note: If any appliances still running 6.1.3 are restored (using the appliance restore functionality in the Service Center) after this script has been run, it is necessary to rerun the script prior to applying the 6.1.4 patch to that appliance.

Upload the Patch File

Note: The upload will fail if the Pre-Patch Cleanup Script has not been run first.

1. In the Service Center, select **appliances ► software updates**. The Software Updates screen displays.
2. Click **Browse** to browse for the patch file.
3. Click **Upload**.

The Service Center checks whether the file is the correct file type. The patch file is automatically replicated to all Service Provider appliances in each Data Center. The Replications column in the lower portion of the screen indicates the progress. For example, 2/2 means that the patch file has been replicated to both the primary and secondary Service Provider appliances in a single Data Center and 4/4 means that the patch file has been replicated to the primary and secondary Service Provider appliances in two Data Centers. It can take up to one minute for each appliance. You must wait until the patch file has been replicated to an appliance before installing the patch on that appliance.

Install the Patch on All Service Provider Appliances

Note: If you start the installation before the patch file has been replicated to all Service Provider appliances, you are warned that replication is not complete on specific appliances. However, you can begin installation on those appliances where replication is complete.

1. In the Service Center, select **appliances ► software updates**. The Software Updates screen lists the available patches. Each patch name is a link.
2. Click on the name of a patch. The Software Updates screen redisplay to show those organizations that have appliances that have not been patched.
3. Mark the checkbox for organization 1000.
4. To install the patch in a single Data Center, select a Data Center from the drop-down. To install the patch on all appliances in all Data Centers, accept the default value "All".
5. Click **Install**.

Install the Patch on All Tenant Appliances

1. In the Service Center, select **appliances ► software updates**. The Software Updates screen lists the available patches. Each patch name is a link.
2. Click on the name of a patch. The Software Updates screen redisplay to show those organizations that have appliances that have not been patched.
3. For each Tenant:
 - a. Mark the checkbox for the organizations you need to patch.
 - b. The Data Center drop-down default value is All, which installs the patch on all appliances in all Data Centers. To install in a single Data Center, select that Data Center from the drop-down.
4. Click **Install**.

Uninstalling the Patch

To revert to the previous version, uninstall the patch by executing these commands on all appliances as the root user:

```
sudo apt-get remove dt-platform-6-1-0-patch-4  
sudo service dtService restart
```

Copyright © 2021 VMware, Inc. All rights reserved.