



Horizon DaaS Platform 6.1.3 Release Notes

VMware Horizon DaaS Platform | 08 JAN 2015

Release notes last updated on 05 AUG 2020

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
- Resolved Issues
- Installing the Patch
 - 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 6.1.2 (Build 22583)

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)

Patch Version

Horizon DaaS Platform 6.1.3 (Build 22807)

New Features

This patch includes the following new features:

- Horizon DaaS has been updated to support HTML Access (Blast) for RDSH desktops. This includes integration with the View Agent 6.0.2 and View Client 3.2 releases.

Note: Before attempting to create an RDS session pool with Blast, you must install View Agent 6.0.2. See Product Support Notices below for more information.

To use the HTML Access (Blast) protocol for a new session pool:

1. In the Enterprise Center, select pool management ► create pool
2. Select Session Based.
3. On the Pool Composition Input page, select the HTML Access check box.
4. Proceed with the pool creation process as usual.

Note: Although you are allowed to select remote applications for these session pools, the use of remote applications with an HTML Access connection is NOT supported.

For more information on HTML Access configuration, refer to the Desktop Protocols Technical Note.

- It is now possible to associate multiple datastores with a single Desktop Manager. Previously the destination datastore for desktop VMs was determined by the datastore the gold pattern resided on. Service Providers can now specify multiple datastores using a regular expression. The platform will deploy new VMs based on which matching datastore has the most free space at the time the desktop VMs are created.

Before you begin, note the following:

- In order for a datastore to be added, it must first be configured on a Compute Resource.
- It is highly recommended that you use a standard naming convention for datastores, for example: datastore1, datastore2, etc. This will be helpful if you want to add a large number of datastores to a Desktop Manager (see step 3 below).

To add datastores to a Desktop Manager:

1. In the Service Center, select **Service Grid ► Desktop Managers**.
 2. Verify that you have the correct Compute Resource assigned on the Compute Resources tab.
 3. Select the Datastores tab.
 4. Enter names of datastores using a regular expression. The field for this expression is limited to 128 characters, so it is recommended that you use a compact expression that allows you to add a larger number of datastores without exceeding that limit. For this to be effective, you must be using a standard naming convention for datastores as recommended above. For example, if you named your datastores datastore1, datastore2, etc., you could use the expression `datastore.*` to capture the whole list.
- French localizations have been updated for both Desktop Portal and Enterprise Center.

Resolved Issues

- DT-1910 – Race condition resulted in one or more desktops failing to get properly

initialized when creating a pool of several desktops. This issue has been remedied so the error no longer occurs.

- DT-5890 - Portal authentication had been failing when the password entered contained the special character for the UK pound (£). Passwords containing this character are now accepted.
- DT-5930 – The following issues were occurring in the Horizon DaaS user interfaces:
 - When users were logged into Desktop Portal or Service Center and tried to switch to Enterprise Center by entering <IP Address>/admin in the browser address bar, the system would prompt them to log in again.
 - When users were logged into Desktop Portal or Enterprise Center and tried to switch to Service Center by entering <IP Address>/service in the browser address bar, the system would prompt them to log in again.
 - Users would get redirected to the login screen in the Desktop Portal after launching desktops via PCoIP.

These issues have now been remedied.

- DT-5938 - If a full inventory ran on a tenant while one of the service provider appliances was down, all desktops were being marked as deleted until the impacted appliance recovered and the next full inventory reconciliation ran (every 12 hours by default). This issue no longer occurs when an inventory is run while a service provider is down.
- DT-5989 – When launching a PCoIP session using the Mac OS version of the View 3.1 client, users were being forced to re-authenticate with the client. This issue has now been resolved.
- DT-6039 – When trying to log into Desktop Portal using a default desktop setting, some users were receiving an HTTP 404 error. This issue has been remedied so the error no longer occurs.
- DT-6196 – When a tenant appliance was extended to multiple datacenters, users were not being given the option to select PCoIP as a protocol for a session or RDS pool even when PCoIP quota was available. This issue has been fixed so that PCoIP is available for selection when creating a session pool on an extended tenant.
- DT-6324 – The status of the host manager had sometimes been changing to Unknown even though it is still Online (or changing back and forth several times between Unknown and Online). When the host manager (and consequently the compute pools) are marked as unknown, pool expansion tasks fail to get created since no compute pools are available. This was caused by idle connections in the connection pool, which became invalid after an extended period of not being used. When validation failed for an idle connection, the status of the host manager was being set to unknown. In this release, these idle connections are no longer left in the pool, which prevents this from occurring.
- DT-6352 – Some VMs had been failing to complete the provisioning process when there was a race condition and then a state change coming during post-clone customization. The system now updates the life state after the resource manager has been called so the lock will not persist and cause this issue.

- DT-6390 – Some pool expansion tasks have sometimes been failing because of sequence table locking issues. When a pool was being expanded to a larger number of desktops, some of the pool manager tasks failed to be submitted to the desktop manager. The system relies on database row locking, but during times of heavy concurrency the lock would sometimes not be available to one or more transactions, causing them to cancel after quickly retrying three times. The transactions now wait for the lock until the transaction itself times out, and the locking has also been improved to avoid two transactions getting the same sequence value by refreshing the value at the time the lock is acquired. As a result of these improvements, pool expansion tasks are no longer being interrupted.
- DT-6423 – On vCenter implementations, gold patterns that had been backed up had been appearing in the Imported Desktops pool after inventory runs. This had been occurring when the following were true:
 - System is using Netapp storage with the VSC plug-in.
 - Storage is configured on the desktop resource manager.These gold patterns are now filtered out as they had been in earlier releases.

Product Support Notices

Microsoft Internet Explorer: Microsoft Internet Explorer 9 is no longer supported for HTML Access (Blast) connections.

View Agent: It is recommended that you update to View Agent 6.0.2. Failure to do so can cause problems with creating RDS pools. In this case, when you create a new RDS session pool, the system can allow you to select HTML Access (Blast) as a protocol, but this selection will not be applied to the pool even though it appears to have been applied successfully.

Known Issues

- DT-6528 – If a HTML Access (Blast) desktop connection is left open and inactive for periods longer than the configured Enterprise Center values for User Idle Timeout or Broker Session Timeout, the client connection may not be ended as expected.
- DT-6659 - The first login attempt with the HTML Access (Blast) client may display an agent protocol error message or unauthorized message and need to be retried.
- DT-6831 – Although HTML Access (Blast) is now selectable as an option when creating a session pool of RDSH desktops, it should not be available when the user has remote applications mapped. Currently HTML Access is selectable when applications are mapped, even though remote applications are not supported for these pools.

Installing the Patch

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

- 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 the Patch File

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.

Procedure

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-3  
sudo service dtService restart
```

Copyright © 2021 VMware, Inc. All rights reserved.