



Horizon DaaS Platform 6.1.6 Release Notes

VMware Horizon DaaS Platform | 25 JUL 2016

Release notes last updated on 09 JAN 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
- WARNING: Restore process for HA tenants
- Prerequisites
- New Features
- Other Updates Included in Patch
- Resolved Issues
- Product Support Notices
- Known Issues
- Installing the Patch

Patch Information

Patch Dependencies

Horizon® DaaS™ Platform 6.1.5 (Build 5448_5d84044)

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)
Horizon DaaS Platform 6.1.4 (Build 23625)
Horizon DaaS Platform 6.1.5 (Build 5448_5d84044)

Patch Version

WARNING: Restore process for HA tenants

When you restore both appliances in an HA appliance pair, the database is not retained. To avoid data loss, you must restore each appliance separately.

Prerequisites

Prerequisites for upgrading to Horizon DaaS 6.1.6 are as follows:

- All DaaS appliances and domain controllers must be synchronized to an accurate time source using the NTP protocol. Ideally a common NTP time source should be used.
- All DaaS appliances must be able to perform forward and reverse DNS lookups for each domain controller's fully qualified hostname that is contactable from the appliance public network.

Note: DaaS 6.1.6 uses GSSAPI by default. To disable it, set `fabric.ad.disable.gssapi` policy to "true" in the Service Center.

New Features

Access Point Support

Beginning in Horizon DaaS Platform 6.1.6, dtRAM is no longer supported. All Service Providers now need to transition to using Access Point, the new Security gateway. For more information about configuring Access Point, see Access Point Support under *Product Support Notices* below.

Appliance Service Utility

An Appliance Service Utility has been created to facilitate a number of additional tasks that must be performed after the patch is installed. See *Post-Patch Tasks* below for more information.

Multi-Domain AD Forest Support

This new feature allows admins to create entitlements between VMs and Users in different domains so long as those domains are trusted and in a single forest. Previously, users and VMs had to be in the same domain for entitlements to work.

- All domains are registered in the Enterprise Center, as they have been in the past. The difference is that you are able to register more than one domain using the same domain bind account (see below for details).
- Note the limitations listed below.

Registering Child Domains in the Enterprise Center

You can now use the same bind account to register all child domains in the same forest.

- In order to do this, you need to enter the complete Domain Bind Account DN, instead of

the partial name that you would normally use. The best way to do this is to copy and paste the full account name from the domain where it has already been entered to the **Domain Bind Account DN** field on the Domain Bind tab.

Note: If you start typing the account name in the field, it will not auto-populate because it is from the other domain. This is why it is best to copy and paste the name instead.

- All the users in multi-domain must belong to a universal group, and for all users in the universal group to be able to launch the desktops you must add that universal group(s) to all registered child domains as well. The best way to do this is to copy and paste the complete group name from the domain where it exists to the appropriate field on the Group Info tab.

Multi-Domain Active Directory in Enterprise Center

In the Enterprise Center, child domain and users/group items are found in the Active Directory in the following locations: Login, Dashboard page, Mapping Page, Pool Management page.

Limitations

- You must register all child domains from which users will be logging in.
- The administrator or end user must select a login domain from the provided dropdown menu to successfully log into the Enterprise Center, the Desktop Portal, or the Horizon Client. This must be a domain to which that administrator or end user belongs.

Note: If authentication fails in the Horizon Client, you may not be able to select a domain. If this occurs, close the client and re-open it before attempting to log in again.

- At least one of the registered domains must have the global catalog enabled. For optimal performance, all registered domains should have the global catalog enabled.
- The use of domain local security groups is not recommended or supported when registering user/admin groups.

External and Forest Trust Support

Horizon DaaS Platform now supports traversing external (or forest) trusts between domains in different forests. This includes:

- Assignment/entitlement of users/groups in one forest to resources in a different forest.
- Support for one-way trusts.

For this functionality to work, you must do the following.

- Register all domains from all forests that contain accounts and desktops you wish to use.
- Register forest root domains from both sides of a forest trust.
This is required to allow the tenant to connect to the forest roots and decode the relevant TDO. This requirement holds even if there are no DaaS desktops or users in the forest root domains.
- Enable global catalog for at least one of the registered domains in each forest.
For optimal performance all registered domains should have global catalog enabled.

- To entitle groups from different forests to a desktop, register at least one universal group from each forest.
- Entitlement/assignment using domain local groups is not supported. As a result, the system filters out FSPs from 'member' attribute DNs and tokenGroups.
- Follow a hierarchical structure with regard to DNS name and root naming context for forest domains. For example, if the parent domain is called example.edu, a child domain could be called vpc.example.edu but not vpc.com.
- Avoid having a domain from an externally trusted forest with a clashing NETBIOS name, as such domains will be excluded. The registered NETBIOS name will always take precedence over a clashing NETBIOS name found during enumeration of a trusted forest's domains.

Resolved Issues

This patch includes fixes for the following issues:

- The Sessions tab under Browse Pools in the Enterprise Center was showing an error when there is a session for a user unknown to Active Directory. This has been remedied so that the error no longer occurs. (DT-8708/1542519)
- Clicking Cancel Notice under Maintenance in the Service Center was resulting in a system error. This issue has been fixed so that the error no longer occurs. (DT-9568/1501825)
- Attempts to disable tenants had been failing with "unexpected error occurred" in Internet Explorer. This has been fixed so that the disable task completes successfully. (DT-9803/1557612)
- On the Service Center > Service grid > Resources > Desktop Manager > Datastore tab, if the regular expression entered for the datastore name is more than 128 characters under, users received error 500. Now this is fixed and the character limit has been increased to 256. (1518721/1686261)
- Users accessing the Service Center via Microsoft Internet Explorer 11 had been unable to create Desktop Models or disable Tenant appliances. This has been remedied so that both of these functions work as expected. (1545412)
- When user activity logs are downloaded for non-existent pools/VMs, null values had been appearing for those non-existent items. This has been remedied so that instead of null values UNKNOWN-DELETED is now shown in the appropriate columns. (1617077)
- When users attempted to print or export lists of more than 100 mapped users in the Enterprise Center, the system skipped each 101st user in the output. For example, if there were 300 users in the list, the 101st and 201st were skipped, so that only 298 were included in the output. This has been remedied so that all users are included in the list as expected. (1554261)
- In Horizon DaaS Platform 6.1.5 some users had been unable to adjust desktop display settings on the Preferences tab in the Desktop Portal. This has been remedied in version 6.1.6 so that the settings work as expected. (1576697)
- Some users had been noticing high CPU utilization on Tenant appliances. The issue that was causing this behavior has been fixed. (1605066)

Product Support Notices

For complete information on interoperability among VMware products, see the VMware Product

Interoperability Matrixes on the VMware web site.

Access Point Support

- dtRAM to Access Point Transition

Beginning in Horizon DaaS Platform 6.1.6, dtRAM is no longer supported. All Service Providers now need to transition to using Access Point, the new Security gateway.

As part of this phasing out, RDP will no longer be supported as an external connection protocol through the Security Gateway. In order to transfer from dtRAM to Access Point, Service Providers must transition their customers from RDP to PCoIP and Blast/HTML5.

For more information about setting up Access Point, see the following documents: Horizon DaaS Platform 6.1 Access Point Setup (available for download on the Horizon DaaS 6.1 download site) and Deploying and Configuring Access Point (available online for Access Point 2.0.x and Access Point 2.5.x).

- Access Point Versions

- Access Point 2.0, 2.0.1, 2.0.2, 2.5, and 2.5.1 are supported.
- Access Point 2.5.1 is supported only with View 6.2.2 or higher.
- If you are using a version of View older than 6.2.2, it is recommended that you use Access Point 2.5 or 2.0.2.

Access Point OVA files are available on the Horizon DaaS 6.1 download site.

- Custom Certificates Required for Access Point 2.5.x

Default web portal certificates in tenant organizations, patched to Horizon DaaS 6.1.6, are supported only with VMware Horizon Access Point releases prior to 2.5. Tenants must upload custom certificates to use VMware Horizon Access Point 2.5 or 2.5.1.

Other Support Notices

- Horizon View

- Horizon View versions 6.2.1 and 6.2.2 are now supported.
- It is recommended that customers use Horizon View client 4.0.1 or 4.1.

- Horizon Agent

Horizon Agent 6.2.1 or 6.2.2 is required.

- DaaS Agent

DaaS Agent 6.1.6 version is recommended.

Known Issues

- HTML Access (Blast) sessions via Access Point failing

Desktop remote access using the HTML Access (Blast) protocol fails while connecting through an Access Point appliance configured with Certificate Authority (CA) signed SSL

certificates.

When you configure an Access Point certificate, the Privacy Enhanced Mail (PEM) file might contain additional text outside of the certificate text, such as a Bag Attributes section. The presence of such text causes the Blast Secure gateway to fail, effectively preventing remote desktop access using the Blast protocol.

Workaround: While configuring an Access Point 2.5.1 or lower version SSL certificate, manually edit the certificate files in PEM format, removing all the text before -----BEGIN CERTIFICATE----- and all the text after -----END CERTIFICATE-----. [1647130]

Installing the Patch

Note: Confirm that all appliances have patch 6.1.5 installed before performing the 6.1.6 patch installation.

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

- Take a snapshot of all appliances being patched.
- Back up database on all appliances being patched.
- 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.
- Perform required post-patch tasks.

WARNING: There is no automated process for rolling back (uninstalling) Horizon DaaS Platform 6.1.6. Failure to take snapshots before you begin could result in loss of data.

Take a Snapshot of All Appliances Being Patched

Before you begin the installation process, take a snapshot of each appliance that is going to be patched.

Back Up Database on all Appliances Being Patched

Note: It is recommended that you repeat this backup procedure periodically after upgrade as well.

Run the following command on each appliance:

```
/usr/local/desktopone/scripts/backup_db.sh -P '<postgres_db_password>'
```

This command extracts a PostgreSQL database into an archive file, creating a backup file of the form <hostname>.<timestamp>.tar.gz in the /usr/local/desktopone/backup folder.

Optional Commands

backup_db.sh accepts the following optional command line arguments.

Argument	Description
-P password	Password for database user admin
-V true	Enable verbose mode
-U username	PostgreSQL username (default is postgres)

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 prePatchScript-6.1.6.sh file to the /tmp directory.
2. Run the following commands:

```
sudo -i
```

```
chmod 755 prePatchScript-6.1.6.sh
```

```
/tmp/prePatchScript-6.1.6.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 6.1.5 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 6.1.6 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**.

Post-Patch Tasks

Run the post-patch script, `appliance_service.sh`, as described below after successfully patching organization 1000 and other target tenant organizations.

Note the following:

- Post-patch tasks must be executed only for existing appliances which have been patched to 6.1.6.

- Post-patch tasks must not be executed for staggered tenant organizations.
- It is not required to execute post-patch tasks for the following, once the organization 1000 has been patched successfully to 6.1.6 (including post-patch tasks):
 - Newly created/restored appliances
 - Newly created organization

It is recommended to restart above-mentioned appliances for the new glibc package version to take effect.

1. Download the appliance_service-6.1.6.tgz file from the Horizon DaaS 6.1 download site onto the SP1 of master datacenter.

Note: It is recommended that you not extract the appliance_service-6.1.6.tgz into the /tmp directory as the contents of the /tmp directory will be deleted during appliance reboot.

2. Execute the following commands:

cd <path> where “path” is the directory into which appliance_service-6.1.6.tgz is saved.

```
tar -xvzf ./appliance_service-6.1.6.tgz
```

```
chmod 755 ./appliance_service.sh
```

3. Edit ./appliance_service.properties file and set "orgid.upgrade" property to the comma-separated list of organization IDs of the Service Provider and target Tenant(s) as shown below.

Ex.: orgid.upgrade = 1000,1001,1002

4. Verify that all appliances in the organizations configured in the above step are up and running.
5. Execute the following:

```
./appliance_service.sh
```

6. Follow the Help Screen instructions:

1. Next
2. Do not show "Help Screen" again and go to next screen
3. Exit

When you enter option 1 or 2 (this option also disables repeating the “Help Screen”), the system displays the next screen with following options:

```
=====
Appliance Service Utility (6.1.6)
=====
*** OPTIONS 1 TO 5 MUST BE EXECUTED FOR ORGANIZATION 1000 ***
1. Generate RSA key from template key for complete platform
```

2. Generate SSH host key for complete platform
3. Generate SHA2 certificates for configured organizations
4. Upgrade database for configured organizations
5. Update glibc package for configured organizations

6. Regenerate RSA key for complete platform

7. Enable "Help Screen"
8. Display Executed Operations History
9. Exit

=====

Options 1 and 2 do not require any configuration. For options 3, 4 and 5, please configure "orgid.upgrade" key in the extracted file `appliance_service.properties`. [e.g `orgid.upgrade = 1000,1001`]

7. Select the option to carry out the required operation.

Note: Option 6 (Regenerate RSA key for complete platform) is not required and should be executed only if the administrator wants to regenerate RSA keys in the future.

Also note the following:

- Options 1 and 2 perform key upgrade tasks on all appliances in all data centers. They do not break any ongoing functionality or restart any appliance. The other options impact the services running on the target appliances and so must be performed in planned maintenance windows.
- Options 1 and 2 need to be executed only once after organization 1000 patching. For any other staggered organization patching these options should not be executed.
- Post-patch tasks should be executed only once on organization 1000 by specifying it in the `appliance_service.properties` file in the master DC.
- Post-patch tasks must not be executed on any tenant organizations before executing post-patch tasks on organization 1000. However, they can be executed together. For example, `orgid.upgrade = 1000,1001`
- Option 4 will upgrade database for organizations (configured in `appliance_service.properties` file) in the current datacenter. To upgrade appliances in other datacenters, copy `appliance_service-6.1.6.tgz` to the Service Provider appliance of that datacenter and perform the same operation. Make sure to update `appliance_service.properties` with regard to organizations in that datacenter.
- After successful execution, option 5 (Update glibc package for configured organizations) will reboot the appliances in the organizations configured in "orgid.upgrade" attribute in the `appliance_service.properties` file.
- During execution of any of the above options (1-6), `appliance_service-6.1.6.tgz` will generate following logs for progress monitoring:
 - Event logs (process execution status): `/var/log/deskone/appliance_service_edr.log`
 - Command execution logs: `/var/log/deskone/appliance_service_cmd.log`
 - Stack trace: `/var/log/deskone/appliance_service_stack.log`
- The following are the consolidated success and failure status messages for the respective operations which can be verified in the `/var/log/deskone/appliance_service_edr.log` file:

Sr. No.	Operation Type	Success Message	Failure Message
1	Generate RSA key from template key for complete platform	RSA KEY GENERATION FOR PLATFORM FROM TEMPLATE HAS COMPLETED SUCCESSFULLY	RSA KEY GENERATION FOR PLATFORM FROM TEMPLATE HAS FAILED
2	Generate SSH host key for complete platform	SSH HOST KEY GENERATION HAS COMPLETED SUCCESSFULLY	SSH HOST KEY GENERATION HAS FAILED
3	Generate SHA2 certificates for configured organizations	CERTIFICATE GENERATION HAS COMPLETED SUCCESSFULLY	CERTIFICATE GENERATION HAS FAILED
4	Upgrade database for configured organizations	DATABASE UPGRADE HAS COMPLETED SUCCESSFULLY	DATABASE UPGRADE HAS FAILED
5	Update glibc package for configured organizations	GLIBC UPGRADE HAS COMPLETED SUCCESSFULLY	GLIBC UPGRADE HAS FAILED
6	Regenerate RSA key for complete platform	RSA KEY GENERATION FOR PLATFORM HAS COMPLETED SUCCESSFULLY	RSA KEY GENERATION FOR PLATFORM HAS FAILED

In the event of any failure during the execution of this utility, capture the above logs and timestamp them before taking any further remedial action.

- The table below shows the average time required for each post-patch operation in a multi-datacenter environment where each datacenter contains one tenant and one of the tenants is an extended tenant.

Sr. No.	Operation Type	Time Required (in minutes)	Number Of Appliances Covered
1	Generate RSA key from template key for complete platform	31	14
2	Generate SSH host key for complete platform	15	14
3	Generate SHA2 certificates for configured organizations	8	14

4	Upgrade database for configured organizations	30	14
5	Update glibc package for configured organizations	4	14

- In order to avoid downtime for all the tenants, it is recommended that you execute operations 3 through 5 for as few tenant organization IDs concurrently as possible.

Copyright © 2021 VMware, Inc. All rights reserved.