



Horizon DaaS 8.0.1 Release Notes

VMware Horizon DaaS | 16 MAY 2019

Release notes last updated on 29 JUN 2022

See [Revision History](#) below for additions and updates to these release notes.

Links to release notes for other versions: [8.0.0](#) | [9.0.x](#) | [9.1.x](#)

What's in the Release Notes

The release notes cover the following topics:

- [Patch Information](#)
 - [Patch Dependencies](#)
 - [Affected Horizon DaaS Platform Versions](#)
 - [Patch Version](#)
- [NEW - Security Hotfixes - Released December 2021](#)
- [NEW - Issues Resolved in Latest Cumulative Update - Released July 2021](#)
- [NEW - DaaS Agent 8.0.3 - Released March 2020](#)
- [Note Regarding Agent Upgrade](#)
- [New Feature - Domain Security Settings on General Settings Page](#)
- [IPv6 Not Supported](#)
- [Known Limitations](#)
- [Issues Resolved in Horizon DaaS 8.0.1](#)
- [Known Issues](#)
- [Installing the Patch](#)
 - [Take a Snapshot of All Appliances Being Patched](#)
 - [Back Up Database on All Appliances Being Patched](#)
 - [Download 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](#)
 - [Perform Post-Patch Tasks](#)

Patch Information

Patch Dependencies

Horizon DaaS Platform 8.0.0 (Build #121, Patch version 11865_2015b11)

Affected Horizon DaaS Platform Versions

Horizon DaaS Platform 8.0.0 (Build #121, Patch version 11865_2015b11)

Patch Version

Horizon DaaS Platform 8.0.1 (Build #266, Patch Version 12003_62786b3)

NEW - Security Hotfixes - Released December 2021

Hotfixes to address a critical vulnerability in Apache Log4j identified by [CVE-2021-44228](#) and [CVE-2021-45046](#) are now available [My VMware](#) for download and manual install. Review [VMSA-2021-0028](#) for more details.

NEW - Issues Resolved in Latest Cumulative Update - Released July 2021

The latest cumulative update is available for download on the Horizon DaaS download page on [My VMware](#). This update includes fixes for the issues listed below.

Issue	Description
Resync task has failed	Resync task has failed (NGVC requestID was not created)
VDI stuck in power_state 'suspending'	VDI was stuck in power_state 'suspending' for several hours
User connection is assigned a desktop whose Resync has not completed successfully	User connection is assigned a desktop whose Resync has not completed successfully
Unable to reassign desktop compute resource or cluster	Unable to reassign a desktop compute resource or cluster for a Tenant after DaaS 8.0.1 Update 1 was installed
Clicking Save repeatedly for a duplicate Instant Clone image causes errors	When a system administrator clicks Save repeatedly for a duplicate Instant Clone image, error messages are shown on the Activity page in the Administration Console

Editing Active Directory	Description
deactivates the domain bind option	Editing Active Directory deactivates the domain bind option
Task Status gets stuck as SubmittedtoElement during image publishing	Task Status gets stuck as SubmittedtoElement during image publishing
Instant clone not getting re-provisioned	Error seen on vCenter while deploying SVM:The attempted operation cannot be performed in the current state ("Powered off")
Admin Console - Authentication Bypass	The Administration Console might allow unauthenticated attackers to access it without credentials. If an attacker supplies the admin login page a username of either ")" or "(" (without the quotes) then a valid session is returned by the server, allowing the attacker to access some authenticated information.
Unable to deploy the tenant appliance as eth0 is assigned the backbone network instead of eth1	Unable to deploy the tenant appliance so that the service provider is unable to deliver the tenant to their customer
Streaming application sessions do not expand to take up the full browser window	Note: View agent 7.5.4 (build # 16831150) is released as part of this fix
Security fixes	This update contains security fixes for issues found in Horizon DaaS 8.0.1 including the issue described in VMSA-2020-0021 .
New tenant deployment failure	New tenant deployment failed due to the .pgpass file copy failure during tenant deployment
Instant clones desktops go into unknown status	Instant clones desktops go into unknown status and java.net.UnknownHostException is observed in tenant logs
Unable to add command line parameters to the	Administrators are unable to add command line parameters to the remote application because clicking on "+" symbol does not open the parameter dialog

remote application Issue	Description
Users are unable to change passwords through the Horizon Client and App Blast portal	Users are unable to change passwords through the Horizon Client and App Blast portal
Unable to delete assigned users from assignment	Unable to remove users from an assignment for a deleted desktop
Tenant full service report fetches report from other tenants	Downloading "Full Service Report" from a specific tenant fetches the details of all other tenants as well
Unable to edit subnet details for additional desktop managers	Unable to edit subnet details for additional desktop managers because subnet mask test boxes are not editable
VDI in floating pool remains powered-off when user shuts it down	VDI in floating pool remains powered-off when user shuts it down from guest OS
dtService of Resource Manager stops responding unexpectedly	NGVC service fails to provision the clones and throws NullPointerException which causes dtService in Resource Manager to not respond
Assigning partitioned cluster to a desktop manager does not work	Assigning partitioned cluster to a desktop manager which was previously assigned to a dedicated cluster does not work
Fails to create SP02 appliance with multiple DNS servers	Fails to create SP02 appliance reservation with multiple DNS servers specified
Auxiliary domain bind account user cannot login when domain bind password is changed	Auxiliary domain bind account user cannot login when domain bind password is changed from domain

Issue	Description
User activity for certain hours is missing in the Usage Activity Report	User activity for certain hours is missing in the Usage Activity Report
Slony logs are not getting rotated	Slony logs present under the /var/log path grows indefinitely without rotations, which causes out of disc space issues
Support for Nvidia T4 / P60 / P40 / V100 cards	Horizon DaaS 8.0.1 does not support for Nvidia T4 / P60 / P40 / V100 cards
Enterprise admin portal is not accessible due to postgresql log rotation	Enterprise admin portal is not accessible due to postgresql log rotation issue.
Unable to create file share in Administration console	Tenant administrators are unable to create file shares in the Administration console
Desktop recycling fails due to connection pool exhaustion	Desktop recycling fails due to connection pool exhaustion in resource managers.
Downloading appliance support bundle fails	Downloading appliance support bundle fails and no proper error is displayed in the logs
Gray screen displayed when connecting to VDI	Gray screen displayed when connecting to VDI via HTML5 with Blast by using UAG 3.6 in specific browsers
AAU fails on dedicated desktop assignments when the desktops have mixed versions of agents	AAU fails on dedicated desktop assignments when the desktops have mixed versions of agents
Requested and actual capacity do not match in the	Requested and actual capacity do not match in the database for an

Issue	Description
Unable to scroll up from last row in Administration Console if there are a larger number of items	Unable to scroll up from last row in Administration Console if there are more than 21 assigned items
Instant clone VMs remained with "resync" status after logging off	Many instant clone VMs remained with "resync" status after logging off due to DB connection shortages in tenant appliances

NEW - DaaS Agent 8.0.3 - Released March 2020

DaaS Agent 8.0.3 has been released.

- DaaS Agent 8.0.3 addresses an issue in previous DaaS Agent 8.0.x versions that caused the agent to crash.
- The new agent includes qualification of the Horizon 7.5.4 Agent with Horizon DaaS 8.0.1, which resolves a security vulnerability identified in earlier versions of Horizon Agent. The issue affects customers who have enabled the ThinPrint feature in Horizon Agent. To learn more about this security vulnerability and mitigation recommendation, see [VMSA-2019-0023](#).
- DaaS Agent 8.0.3 and Horizon 7.5.4 agent will now be available for download on [My VMware](#).

Note Regarding Agent Upgrade

After performing an agent software upgrade, you might see an old version of the DaaS agent still installed on the VM. If you see this, it is not an issue and it is safe to ignore it.

New Feature - Domain Security Settings on General Settings Page

You use these settings to prevent communication of Active Directory domain names to unauthenticated users using the various Horizon clients. These settings govern whether the information about the Active Directory domains that are registered with your Horizon DaaS environment is sent to the Horizon end user clients and, if sent, how it is displayed in end-user clients' login screens.

Configuring your Horizon DaaS environment includes registering your environment with your Active Directory domains. When your end users use a Horizon client to access their entitled desktops and remote applications, those domains are associated with their entitled access. Prior to this release, the system and clients had default behavior with no options to adjust that default

behavior. Starting in this release, you can optionally use the new Domain Security Settings controls to change from the defaults.

Important: When changing these settings, it can take up to 5 minutes for the update to take effect.

This section has the following sub-sections:

- [Domain Security Settings](#)
- [This Release's Default Behavior Compared with Past Releases](#)
- [Single Active Directory Domain Scenarios and User Login Requirements](#)
- [Multiple Active Directory Domain Scenarios and User Login Requirements](#)

Domain Security Settings

Combinations of these settings determine whether domain information is sent to the client and whether a domain selection menu is available to the end user in the client.

Caution: These settings change the user experience in the clients. The behavior for end users using versions of Horizon Client prior to version 5.0 is different than for Horizon Client 5.0 and later. Certain combinations can set requirements on how your end users specify their domain information in the client login screen, especially when using older clients, command-line clients, and when your environment is configured with multiple Active Directory domains. How these settings affect the client user experience depends on the client. You might need to balance your desired end-user experience according to your organization's security policies. See sub-sections [Single Active Directory Domain Scenarios and User Login Requirements](#) and [Multiple Active Directory Domain Scenarios and User Login Requirements](#).

Domain Security Settings on the General Settings Page

Option	Description
	This option controls what domain information the system sends to connecting clients prior to user authentication.
Show Default Domain Only	<ul style="list-style-type: none">• Yes - The system sends only the literal string value *DefaultDomain*.• No - The system sends the list of registered Active Directory domain names to the client.
	This option controls the visibility in the client login screen of whatever domain-related information is sent to the client, based on the Show Default Domain Only setting.
Hide Domain Field	<ul style="list-style-type: none">• Yes - Nothing about domains is displayed in the client login screen, regardless of what Show Default Domain Only is set to. Neither the literal string value *DefaultDomain* nor the domain names are displayed in the client login screen.• No - The client login screen displays one of the following items, depending on the Show Default Domain Only

setting.

- The literal text *DefaultDomain*, when **Show Default Domain Only** is Yes. This combination is optimized for user experience in Horizon Clients older than version 5.0, while also providing improved security.
- The list of domain names in a drop-down menu, when **Show Default Domain Only** is No.

This Release's Default Behavior Compared with Past Releases

There is no change in the default behavior in this release.

Single Active Directory Domain Scenarios and User Login Requirements

The following table describes the behavior for various setting combinations when your environment has a single Active Directory domain, without two-factor authentication, and your end users use the Horizon Clients 5.0 and later versions. These clients are the newest ones starting in this release.

Behavior For Horizon Clients 5.0 and Later Versions and You Have One Active Directory Domain

Show Default Domain Only (enabled sends *DefaultDomain*)	Hide Domain Field	Horizon Client 5.0 Login Screen Details	How Users Log In
Yes	Yes	The client's login screen has the standard user name and password fields. No domain field is displayed. No domain name is sent.	<p>When there is a single domain, to log in, end users can enter either of the following values in the User name text box. The domain name is not required.</p> <ul style="list-style-type: none">• username• domain\username <p>Using the command-line client launch and specifying the domain in the command works.</p> <p>When there is a single domain, to log in, end users can enter either of the following values in the User</p>

Yes	No	<p>The client's login screen has the standard user name and password fields. The domain field displays *DefaultDomain*. No domain name is sent.</p>	<p>name text box. The domain name is not required.</p> <ul style="list-style-type: none"> • username • domain\username <p>Using the command-line client launch and specifying the domain in the command works.</p>
No	Yes	<p>The client's login screen has the standard user name and password fields. No domain field is displayed. The system sends the domain name to the client.</p> <p>Note: This combination is atypical. You would not normally use this combination because it hides the domain field even though the system is sending the domain name.</p> <p>The login screen looks the same as the one in the first row of this table, with no domain field displayed.</p>	<p>An end user must include the domain name in the User name text box. For example: domain\username</p>
No	No	<p>The client's login screen has the standard user name and password fields and a standard drop-down domain selector displays the one available domain name. The domain name is sent.</p>	<p>The end user can specify their user name in the User name text box and use the single domain that is in the list visible in the client.</p> <p>Using the command-line client launch and specifying the domain in the command works.</p>

The table below describes the behavior when your environment has a single Active Directory domain and your end users use previous versions of the Horizon clients (pre-5.0).

Important Using the command-line client launch of older (pre-5.0) clients and specifying the domain in the command fails for all of the combinations below. To work around this behavior,

either use *DefaultDomain* for the command's domain option or upgrade the client to the 5.0 version. However, when you have more than one Active Directory domain, passing *DefaultDomain* does not work.

Behavior For Older Horizon Clients (Before 5.0) and You Have One Active Directory Domain

Show Default Domain Only (enabled sends *DefaultDomain*)	Hide Domain Field	Pre-5.0 Horizon Client Login Screen Details	How Users Log In
Yes	Yes	The client's login screen has the standard user name and password fields. No domain field is displayed. No domain name is sent.	An end user must include the domain name in the User name text box. For example: domain\username
Yes	No	The client's login screen has the standard user name and password fields. The domain field displays *DefaultDomain*. No domain name is sent.	An end user must enter username in the User name text box. When the domain name is included, an error message displays that states the specified domain name does not exist in the domain list.
No	Yes	<p>The client's login screen has the standard user name and password fields. No domain field is displayed. The system sends the domain name to the client.</p> <p>Note: This combination is atypical. You would not normally use this combination because it hides the domain field even though the system is sending the domain name.</p>	An end user must include the domain name in the User name text box. For example: domain\username
		The client's login screen has the standard user name and password fields and a	The end user can specify their user name in the User

No	No	standard drop-down domain selector displays the one available domain name. The domain name is sent.	name text box and use the single domain that is in the list visible in the client.
----	----	---	---

Multiple Active Directory Domain Scenarios and User Login Requirements

This table describes the behavior for various setting combinations when your environment has multiple Active Directory domains, without two-factor authentication, and your end users use the Horizon Clients 5.0 and later versions.

Basically, the end user has to include the domain name when they type in their user name, like domain\username, except for the legacy combination where the domain names are sent and are visible in the client.

Behavior For Horizon Clients 5.0 and Later Versions and You Have Multiple Active Directory Domains

Show Default Domain Only (enabled sends *DefaultDomain*)	Hide Domain Field	Horizon Client 5.0 Login Screen Details	How Users Log In
Yes	Yes	The client's login screen has the standard user name and password fields. No domain field is displayed. No domain names are sent.	<p>An end user must include the domain name in the User name text box. For example: <i>domain\username</i></p> <p>Using the command-line client launch and specifying the domain in the command works.</p>
Yes	No	The client's login screen has the standard user name and password fields. The domain field displays *DefaultDomain*. No domain names are sent.	<p>An end user must include the domain name in the User name text box. For example: <i>domain\username</i></p> <p>Using the command-line client launch and specifying the domain in the command works.</p>
		The client's login screen has the standard user	

No	Yes	name and password fields. No domain field is displayed. The system sends the domain names to the client.	An end user must include the domain name in the User name text box. For example: domain\username
		Note: This combination is atypical. You would not normally use this combination because it hides the domain field even though the system is sending the domain names.	
No	No	The client's login screen has the standard user name and password fields and a standard drop-down domain selector displays the list of domain names. The domain names are sent.	The end user can specify their user name in the User name text box and select their domain from the list visible in the client.
			Using the command-line client launch and specifying the domain in the command works.

The table below describes the behavior when your environment has multiple Active Directory domains and your end users use previous versions of the Horizon clients (pre-5.0).

Important

- Setting **Hide Domain Field** to Yes allows end users to enter their domain in the User name text box in these pre-5.0 Horizon clients. When you have multiple domains and you want to support use of pre-5.0 Horizon clients by your end users, you must set **Hide Domain Field** to Yes so that your end users can include the domain name when they type in their user name.
- Using the command-line client launch of older (pre-5.0) clients and specifying the domain in the command fails for all of the combinations below. The only work around when you have multiple Active Directory domains and want to use command-line client launch is to upgrade the client to the 5.0 version.

Behavior For Older Horizon Clients (Before 5.0) and You Have Multiple Active Directory Domains

Show Default Domain Only	Hide	Pre-5.0 Horizon Client
--------------------------	------	------------------------

(enabled sends *DefaultDomain*)	Domain Field	Login Screen Details	How Users Log In
Yes	Yes	The client's login screen has the standard user name and password fields.	An end user must include the domain name in the User name text box. For example: <i>domain\username</i>
Yes	No	The client's login screen has the standard user name and npassword fields. The domain field displays *DefaultDomain*. No domain names are sent.	This combination is unsupported for environments with multiple Active Directory domains.
No	Yes	<p>The client's login screen has the standard user name and password fields. No domain field is displayed. The system sends the domain names to the client.</p> <p>Note: This combination is atypical. You would not normally use this combination because it hides the domain field even though the system is sending the domain names.</p>	An end user must include the domain name in the User name text box. For example: <i>domain\username</i>
No	No	The client's login screen has the standard user name and password fields and a standard drop-down domain selector displays the list of domain names. The domain names are sent.	The end user can specify their user name in the User name text box and select their domain from the list visible in the client.

IPv6 Not Supported

The IPv6 protocol is not supported in Horizon DaaS 8.0.1.

Known Limitations

- Command line parameters for the Update Agent Software function are not supported for the Daas Agent in the current version of Horizon DaaS. For View Agent command line options, see the relevant View Agent documentation for more details.
- For this release, it is required that before you re-initialize Slony for an organization, all the appliances in the organization must be reachable over SSH from Service Provider appliances.
- Activity on a tenant can take up to six hours to appear on the Customer Usage Report downloaded in the Service Center. This is the case because the tenant and service provider appliances sync at six hour intervals.

Resolved Issues

- Users were receiving an HTTP 500 Internal Server Error when connecting to the tenant web portal using `https://<FQDN>/portal/help/en/Default_CSH.htm`. This has been fixed so that the error no longer occurs. [2193878]
- The option to configure a custom style sheet in the Tenant Administration Console (**Settings > General Settings > User Portal Configuration**) has not been working. This option is now functioning as expected. [2236698 / 2278399 / 2197305]
- Some ESXi hosts were not appearing in the Service Center user interface. This has been remedied so that hosts appear as expected. [2241569]
- Users had been unable to configure separate datastores for desktop managers in the Service Center. This issue has been addressed in the patch so that datastores can be configured as expected. [2245246 / 2289527]
- If a user converted a desktop to an image and then deleted the assignment to which the desktop had belonged, any attempt to convert the image back to a desktop would fail. This has been fixed in the current patch so this problem no longer occurs. [2245274 / 2289532]
- Users have been unable to add or remove the domain group in a assignment. This has been remedied so that groups can be added and removed as expected. [2246350 / 2289519]
- The Administration Console has not been accessible for some tenants because of issues with required services not starting. This issue has been fixed so that the the Administration Console can be launched for those tenants. [2246366]
- Some users were experiencing unusually high CPU usage on HA pairs of appliances. This issue has been fixed in the current patch, so that this high CPU usage is no longer observed. [2259439]
- Attempts to access the Tenant Administration Console had been failing with a 504 Gateway Time-out. This has been remedied so that this error no longer occurs. [2259443]

- In environments without internet access, tenant deployment had been failing with an "Unable to execute 'apt-get update'" error. This has been fixed in the current patch so that users are able to deploy tenants as expected. [2275510 / 2289522]
- Clicking on the **Back to List** button on the Software Updates page in the Service Center had been failing with a 404 error. This issue has been fixed so the error no longer appears. [2279257]
- In the Service Center, refreshing either the **configuration > domains** or **configuration > roles & permissions** page causes a 500 error, This has been fixed in the current patch so the error no longer occurs. [2283081]
- On the **Desktop Capacity & Model Definition** page, the selected multiplier for the desktop model was not being applied to the vGPU value. The multiplier would apply to the vCPU and vRAM as expected, but the vGPU value would not be multiplied. This issue has been remedied so that the vGPU value is multiplied as expected. [2197446]
- Users were not able to deploy the secondary service provider appliance (SP2) because the IPv6 address was not being generated correctly from the MAC address. This has been fixed so that the IPv6 address now generates correctly and the deployment occurs as expected. [2213658]
- Powering on the primary service provider appliance (SP1) was causing a variety of issues, including interruptions in Service Center access, SP appliances appearing as being down, and problems with assignments in the Administration Console. This has been remedied so that the SP1 appliance is no longer causing problems. [2262150]
- Users had been unable to configure VMware Identity Manager with an FQDN URL containing **.local**. This has been fixed in the current patch. [2245277 / 2289514]

Known Issues

- **New created or cloned VM is not listed in Imported VMs due to duplicate key value violating the unique constraint "t_general_machine_mac_address_key".**

Workaround : None. This issue will be resolved in future releases.

[2887657]

- If you upgrade to Horizon DaaS 9.0.x using blue-green upgrade and then manually roll back to Horizon DaaS 8.0.x manually, then `authorized_keys` is empty on the secondary Resource Manager. This causes an issue where the log bundle of the secondary Resource Manager cannot be collected from Service Center.

Workaround: Copy `authorized_keys` from the primary Resource Manager to the secondary Resource Manager, and set the permission of the file to 644.

[2796840]

- Attempts to rename imported VMs have failed. The user performs the rename operation, but the VM name is not changed.

Workaround:

1. On the VM, unjoin the domain.
2. Change the VM name in the Administration Console.
3. On the VM, rejoin the domain.

[2067656]

- When using wbemcli client, users are unable to connect to SFCB service. In these cases, any query returns the following error:

```
wbemcli -nl ei 'https://cim-  
user:Password@<IP_ADDRESS>:5989/root/cimv2:Desktoner_ApplicationServerStatistics' -noverify
```

*

* wbemcli: Http Exception: SSL connect error

This occurs because the older version of the Ubuntu wbemcli client package does not support TLS and relies on SSLv3. The current version of Horizon DaaS does not support SSLv3.

Workaround:

1. Install new CentOS 7 server.
2. Install the available sbliim-wbemcli package, which is https://centos.pkgs.org/7/centos-x86_64/sbliim-wbemcli-1.6.2-11.el7.x86_64.rpm.html.
3. Run your desired queries.

[2207112]

- Users have been unable to add universal groups to assignments in multi-forest environments.

Workaround: In Service Center, set the fabric.ad.follow.referrals property to 'false'.
[2334173]

- Update Agent Software may fail intermittently for Windows Server 2016 images.

Workaround: None. This issue will be resolved in the next release. [2339703]

Installing the Patch

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.
- Download 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 Service Provider appliances.

- Install the patch file on all Service Provider appliances.
- Install the patch file on all Tenant appliances.
- Perform post-patch tasks on patched appliances.

WARNING: There is no automated process for rolling back (uninstalling) Horizon DaaS Platform 8.0.1. 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)

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

Note: Before executing prePatchScript-8.0.1.sh, confirm that all tenant appliances are reachable over SSH from the primary Service Provider appliance. If any of the tenant appliances are not reachable over SSH, the script will fail.

- To ignore the tenant organizations of such appliances, run the script (last command in step 2 below) with the '-i' option as follows:

`./prePatchScript-8.0.1.sh -i <ignore list>` where *<ignore list>* is a list of comma-separated tenant organization IDs without any spaces

For example:

```
./prePatchScript-8.0.1.sh -i 1001,1002
```

- Any attempt to install the VMware Horizon DaaS 8.0.1 patch on the tenant organizations in the ignore list will fail.
- The Service Provider Organization ID (1000) cannot be included in the ignore list.

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

1. Download the pre-post-patchFiles-8.0.1_version_2.tar file from VMware Horizon DaaS 8.0.1 download site onto any directory of the primary Service Provider appliance.

Note: It is recommended that you not extract the pre-post-patchFiles-8.0.1_version_2.tar file into the /tmp directory as the contents of the /tmp directory will be deleted during appliance reboot. Note the directory you use for these files, since you will need to access it for the post-patch script as well.

2. Execute following commands as root user on primary Service Provider appliance:

```
cd <path> where <path> is the directory into which pre-post-patchFiles-8.0.1_version_2.tar is saved
```

```
tar -xvf pre-post-patchFiles-8.0.1_version_2.tar
```

```
cd pre-post-patchFiles-8.0.1_version_2/pre-patch/
```

```
./prePatchScript-8.0.1.sh
```

Note: While the service is restarting, there may be errors reported by monitoring systems 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.

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. 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. 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 re-displays to show those organizations that have appliances that have not been patched.
3. Mark the checkbox for organization 1000 only.

Note: Do not install the patch for any tenant organizations until the installation for the service provider organization is completed. Attempting to install for tenant and service provider organizations at the same time can cause issues with the installation.

4. 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 re-displays to show those organizations that have appliances that have not been patched.
3. For each Tenant, mark the checkbox for the organizations you need to patch
4. Click **Install**.

Perform 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 performed only for existing appliances which have been patched to 8.0.1.
- After organization 1000 has been patched successfully to 8.0.1 (including post-patch tasks), it is not required to perform post-patch tasks for the following:
 - Newly restored appliances
 - Newly created organization

1. Execute the following commands:

`cd <path>` where "path" is the directory where `pre-post-patchFiles-8.0.1_version_2.tar` is saved.

`cd pre-post-patchFiles-8.0.1_version_2/post-patch/`

2. 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 in the example below.

`orgid.upgrade = 1000,1001,1002`

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

```
./appliance_service.sh
```

The Help screen displays with the following options:

1. Next
 2. Do not show "Help Screen" again and go to next screen
 3. Exit
5. Select option 1 or 2 to advance to the next screen (option 2 also deactivates repeating the "Help Screen"). The system displays the next screen with the following options:

```
=====
Appliance Service Utility (8.0.1)
=====
1. Upgrade database for configured organizations
2. Display Executed Operations History
3. Exit
=====
```

6. When prompted, enter Service Provider administrator credentials to proceed with the database upgrade.
7. Select option 1 to perform database upgrade for the organizations configured in the appliance_service.properties file.

Note: In order to avoid downtime for all the tenants, it is recommended that you execute option 1 for as few tenant organization IDs concurrently as possible.

During execution of option 1, appliance_servicesh will generate following logs for progress monitoring:

- Event logs (process execution status): /var/log/deskton/appliance_service_edr.log
- Command execution logs: /var/log/deskton/appliance_service_cmd.log
- Stack trace: /var/log/deskton/appliance_service_stack.log

The following are the success and failure status messages for option 1. These messages can be verified in the /var/log/deskton/appliance_service_edr.log file.

- Success message:
DATABASE UPGRADE HAS COMPLETED SUCCESSFULLY
- Failure message:
DATABASE UPGRADE HAS FAILED

8. Select option 2 to display the executed operations history with timestamp (operation history is stored in a file in the same directory where appliance_service.sh is present).

Note: In the future, execute following command to restore the database from backup in the appliance (if post-patch task execution was completed for the appliance):

env PGPASSWORD=DB_PASSWORD pg_restore -w -Uadmin -d fdb -v --clean DB_BACKUP_FILE_NAME

Note: If you receive an error during the post-patch workflow beginning with text similar to this, you can safely ignore it: Detected an error while getting a datasource connection to url `xx.xxx.xx.xx` as user slave. This is a temporary issue that is corrected when the system update is complete.

Revision History

Date	Description
16 MAY 2019	Initial release
26 JUN 2019	Replaced pre-post-patchFiles-8.0.1 with pre-post-patchFiles-8.0.1_version_2 Edited Post-Patch Tasks
26 AUG 2019	Added non-support for IPv6
26 SEP 2019	Added 8.0.2 agent
08 OCT 2019	Edited 8.0.2 agent item
24 MAR 2020	Added 8.0.3 agent, removed 8.0.2 agent
17 SEP 2020	Added Cumulative Update section
21 JAN 2021	Updated Cumulative Update section
05 MAY 2021	Added Note regarding agent upgrade
28 JUL 2021	Updated Cumulative Update section
12 JAN 2022	Added Known Issue 2796840
29 JUN 2022	Added Known Issue 2887657

