# Release Notes for VMware Horizon 7 version 7.0

Released 22 March 2016

**Last Updated**: 13 March 2021

These release notes include the following topics:



## What's New in This Release

VMware Horizon 7 version 7.0 provides the following new features and enhancements:

### Instant Clones

- A new type of desktop virtual machines that can be provisioned significantly faster than the traditional View Composer linked clones.
- A fully functional desktop can be provisioned in two seconds or less.
- Recreating a desktop pool with a new OS image can be accomplished in a fraction of the time it takes a View Composer desktop pool because the parent image can be prepared well ahead of the scheduled time of pool recreation.
- Clones are automatically rebalanced across available datastores.
- View storage accelerator is automatically enabled.

### Cloud Pod Architecture Improvements

- The Cloud Pod Architecture feature now supports a pod federation of up to 25 pods across up to five sites for a scale of 50,000 sessions.
- In the event that resources at a user's home site are exhausted or otherwise not available, the user is now automatically directed to available desktops at other sites.
- Home site administration is now fully supported in View Administrator.
- The Cloud Pod Architecture feature now allows home site assignments for nested AD security groups.
- VMware Identity Manager is now fully integrated with the Cloud Pod Architecture feature.

### Smart Policies

- Control of the clipboard cut-and-paste, client drive redirection, USB redirection, and virtual printing desktop features through defined policies.
- PCoIP session control through PCoIP profiles.
- Conditional policies based on user location, desktop tagging, pool name, and Horizon Client registry values.

## VMware Blast Extreme

- VMware Blast Extreme is now fully supported on the Horizon platform.
  - Administrators can select the VMware Blast display protocol as the default or available protocol for pools, farms, and entitlements.
  - End users can select the VMware Blast display protocol when connecting to remote desktops and applications.
- VMware Blast Extreme features include:
  - TCP and UDP transport support
  - H.264 support for the best performance across more devices
  - Reduced device power consumption for longer battery life
  - NVIDIA GRID acceleration for more graphical workloads per server, better performance, and a superior remote user experience

## True SSO

- For VMware Identity Manager integration, True SSO streamlines the end-to-end login experience. After users log in to VMware Identity Manager using a smart card or an RSA SecurID or RADIUS token, users are not required to also enter Active Directory credentials in order to use a remote desktop or application.
- Uses a short-lived Horizon virtual certificate to enable a password-free Windows login.
- Supports using either a native Horizon Client or HTML Access.
- System health status for True SSO appears in the View Administrator dashboard.
- Can be used in a single domain, in a single forest with multiple domains, and in a multiple-forest, multiple-domain setup.

## Access Point 2.5 Integration

- Smart card authentication is now fully supported.
- RSA SecurID and RADIUS authentication have been added.
- Smart policies can be used with Access Point.
- VMware Blast protocol can now be directed to port 443. Previously, port 8443 was required.

Note: Access Point 2.6 version serves as a reverse proxy for VMware Identity Manager only.

## URL Content Redirection for Windows Horizon Clients

- For specific URLs, you can configure whether, when end users click a link to that URL in an Internet Explorer browser or an application, or if they type the URL into an Internet Explorer browser, that link gets opened always on a Windows-based client system or always in a remote desktop or application.
- URL links can be links to Web pages, telephone numbers, email addresses, and more.
- Configured through group policy.

## Flash Redirection for Windows Horizon Clients (Tech Preview)

- Flash content in an Internet Explorer browser is sent to the Windows-based client and played in a Flash container window, thereby offloading demand on the ESXi host.
- Configured through an agent-side group policy that specifies a white list of Web sites to use Flash Redirection.

## Windows Server 2016 Support (Tech Preview)

- Windows Server 2016 can be used as an RDS host for providing remote desktops and hosted applications.

For this release, Windows Universal apps are not supported as hosted remote applications. For example, Universal apps do not appear in the list of apps provided by a Windows Server 2016 RDS farm. Universal apps, such as the Microsoft Edge browser or the Calculator included with Windows 10 or a Windows Server 2016 RDS host, are built on the Universal Windows Platform (UWP). Universal apps require Windows Explorer to be run. In addition, manually launching Universal apps through the Command Prompt will show an error message.

### Horizon 7 for Linux Desktops

- Support for SLED 11 SP3/SP4. However, Single Sign-on is not supported.
- Support for HTML Access 4.0.0 on Chrome.
- Support for CentOS 7.1 Linux distribution.
- Support to check the dependency packages unique to a Linux distribution before installing Horizon Agent.
- Support to use the **Subnet** option of `/etc/vmware/viewagent-custom.conf` to specify the subnet used for Linux desktop connections with multiple subnets connected.

### Additional Features

- Support for IPv6 with VMware Blast Extreme on security servers.
- View Administrator security protection layer. See VMware Knowledge Base (KB) article 2144303 for more information.
- Protection against inadvertent pool deletion.
- RDS per-device licensing improvements.
- Support for Intel vDGA.
- Support for AMD Multiuser GPU Using vDGA.
- More resilient upgrades.
- Display scaling for Windows Horizon Clients.
  DPI scaling is supported if it is set at the system level and the scaling level is greater than 100.

For information about the issues that are resolved in this release, see Resolved Issues.

## Before You Begin

- Important note about installing VMware Tools
  If you plan to install a version of VMware Tools downloaded from VMware Product Downloads, rather than the default version provided with vSphere, make sure that the VMware Tools version is supported. To determine which VMware Tools versions are supported, go to the VMware Product Interoperability Matrix, select the solution **VMware Horizon View** and the version, then select **VMware Tools (downloadable only)**.
- The Horizon 7 release includes new configuration requirements that differ from some earlier releases. See the README document. This short overview can help you to avoid potential pitfalls when you install or upgrade to this release. The *View Upgrades* document provides upgrade instructions.
- If you intend to upgrade a pre-6.2 installation of View, and the Connection Server, security server, or View Composer server uses the self-signed certificate that was installed by default, you must remove the existing self-signed certificate before you perform the upgrade. Connections might not work if the existing self-signed certificates remain in place. During an upgrade, the installer does not replace any existing certificate. Removing the old self-signed certificate ensures that a new certificate is installed. The self-signed certificate in this release has a longer RSA key (2048 bits instead of 1024) and a stronger signature (SHA-256 with RSA instead of SHA-1 with RSA) than in pre-6.2 releases. Note that self-signed certificates are insecure and should be replaced by CA-signed certificates as soon as possible, and that SHA-1 certificates are no longer considered secure and should be replaced by SHA-2 certificates.
  Do not remove CA-signed certificates that were installed for production use, as recommended by VMware. CA-signed certificates will continue to work after you upgrade to this release.
- To take advantage of Horizon 7 features such as Virtual SAN 6.1, GRID vGPU, and Virtual Volumes,

install vSphere 6.0 and subsequent patch releases.

- If your deployment uses RDS Per Device Client Access Licenses (CALs), follow the configuration guidelines in VMware Knowledge Base (KB) article 2076660, Managing RDS Per Device CALs in View, before your end users begin connecting to RDS desktops and applications.
- When you upgrade to this release, upgrade all View Connection Server instances in a pod before you begin upgrading View Agent, as described in the *View Upgrades* document.
- The download page in this release includes a Horizon View HTML Access Direct-Connection file that provides web server static content for supporting HTML Access with View Agent Direct-Connection (VADC). For information about setting up HTML Access for VADC, see Setting Up HTML Access in the *View Agent Direct-Connection Plug-in Administration* document.
- Selecting the Scanner Redirection setup option with Horizon Agent installation can significantly affect the host consolidation ratio. To ensure the optimal host consolidation, make sure that the Scanner Redirection setup option is only selected for those users who need it. (By default, the Scanner Redirection option is not selected when you install Horizon Agent.) For the particular users who need the Scanner Redirection feature, configure a separate desktop pool and select the setup option only in that pool.
- Horizon 7 uses only TLSv1.1 and TLSv1.2. In FIPS mode, it uses only TLSv1.2. You might not be able to connect to vSphere unless you apply vSphere patches. For information about re-enabling TLSv1.0, see Enable TLSv1 on vCenter Connections from Connection Server and Enable TLSv1 on vCenter and ESXi Connections from View Composer in the *View Upgrade* document.
- FIPS mode is not supported on releases earlier than 6.2. If you enable FIPS mode in Windows and upgrade View Composer or View Agent from a release earlier than 6.2 to 7.0, the FIPS mode option may be shown as available. However, you must not select the FIPS mode option because upgrading from non-FIPS mode to FIPS mode is not supported. You must do a fresh install instead to install Horizon 7 in FIPS mode.
- Linux desktops use port 22443 for the VMware Blast display protocol.

# Internationalization

The View Administrator user interface, View Administrator online help, and Horizon 7 product documentation are available in Japanese, French, German, simplified Chinese, traditional Chinese, and Korean. For the documentation, see the Documentation Center for VMware Horizon 7.

# Compatibility Notes

- For the supported guest operating systems for Horizon Agent on single-user machines and RDS hosts, see Supported Operating Systems for Horizon Agent in the *View Installation* document.
- If you use Horizon 7 servers with a version of View Agent older than 6.2, you will need to enable TLSv1.0 for PCoIP connections. View Agent versions that are older than 6.2 support the security protocol TLSv1.0 only for PCoIP. Horizon 7 servers, including connection servers and security servers, have TLSv1.0 disabled by default. You can enable TLSv1.0 for PCoIP connections on these servers by following the instructions in VMware Knowledge Base (KB) article 2130798, Configure security protocols for PCoIP for Horizon 6 version 6.2 and later, and Horizon Client 3.5 and later.
- For the supported Linux guest operating systems for Horizon Agent, see System Requirements for Horizon 7 for Linux in the *Setting Up Horizon 7 for Linux Desktops* document.
- For the supported operating systems for View Connection Server, security server, and View Composer, see System Requirements for Server Components in the *View Installation* document.
- Horizon 7 functionality is enhanced by an updated set of Horizon Clients provided with this release. For example, Horizon Client 4.0 or later is required for VMware Blast Extreme connections. See the VMware Horizon Clients Documentation page for information about supported Horizon Clients.
- The instant clones feature requires vSphere 6.0 Update 1 or later.
- Windows 7 and Windows 10 are supported for instant clones, but not Windows 8 or Windows 8.1.
- See the VMware Product Interoperability Matrix for information about the compatibility of Horizon 7 with current and previous versions of vSphere.
- For the supported Active Directory Domain Services (AD DS) domain functional levels, see

Preparing Active Directory in the *View Installation* document.

- For more system requirements, such as the supported browsers for View Administrator and View Portal, see the *View Installation* document.
- RC4, SSLv3, and TLSv1.0 are disabled by default in View components, in accordance with RFC 7465, "Prohibiting RC4 Cipher Suites," RFC 7568, "Deprecating Secure Sockets Layer Version 3.0," PCI-DSS 3.1, "Payment Card Industry (PCI) Data Security Standard", and SP800-52r1, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations." If you need to re-enable RC4, SSLv3, or TLSv1.0 on a View Connection Server, security server, View Composer, or Horizon Agent machine, see Older Protocols and Ciphers Disabled in View in the *View Security* document.
- If a PCoIP Secure Gateway (PSG) has been deployed for PCoIP connections, zero client firmware must be version 4.0 or later.
- When using Client Drive Redirection (CDR), deploy Horizon Client 3.5 or later and View Agent 6.2 or later to ensure that CDR data is sent over an encrypted virtual channel from an external client device to the PCoIP security server and from the security server to the remote desktop. If you deploy earlier versions of Horizon Client or View Agent, external connections to the PCoIP security server are encrypted, but within the corporate network, the data is sent from the security server to the remote desktop without encryption. You can disable CDR by configuring a Microsoft Remote Desktop Services group policy setting in Active Directory. For details, see Managing Access to Client Drive Redirection in the *Setting Up Desktop and Application Pools in View* document.
- The USB Redirection setup option in the Horizon Agent installer is deselected by default. You must select this option to install the USB redirection feature. For guidance on using USB redirection securely, see Deploying USB Devices in a Secure View Environment in the *View Security* document.
- The Global Policy, Multimedia redirection (MMR), defaults to **Deny**. To use MMR, you must open View Administrator, edit Global Policies, and explicitly set this value to **Allow**. To control access to MMR, you can enable or disable the Multimedia redirection (MMR) policy globally or for an individual pool or user.
  Multimedia Redirection (MMR) data is sent across the network without application-based encryption and might contain sensitive data, depending on the content being redirected. To ensure that this data cannot be monitored on the network, use MMR only on a secure network.
- Before you set the level of Transparent Page Sharing (TPS) in View Administrator, VMware recommends that the security implications be understood. For guidance, see the VMware Knowledge Base (KB) article 2080735, Security considerations and disallowing inter-Virtual Machine Transparent Page Sharing.
- To use View Storage Accelerator in a vSphere 5.5 or later environment, a desktop virtual machine must be 512GB or smaller. View Storage Accelerator is disabled on virtual machines that are larger than 512GB. Virtual machine size is defined by the total VMDK capacity. For example, one VMDK file might be 512GB or a set of VMDK files might total 512GB. This requirement also applies to virtual machines that were created in an earlier vSphere release and upgraded to vSphere 5.5.
- Horizon 7 does not support vSphere Flash Read Cache (formerly known as vFlash).
- In Horizon (with View) version 6.0 and later releases, the View PowerCLI cmdlets Get-TerminalServer, Add-TerminalServerPool, and Update-TerminalServerPool have been deprecated.
- Kiosk mode clients are not supported in a Cloud Pod Architecture implementation.
- Screen DMA is disabled by default in virtual machines that are created in vSphere 6.0 and later. View requires screen DMA to be enabled. If screen DMA is disabled, users see a black screen when they connect to the remote desktop. When Horizon 7 provisions a desktop pool, it automatically enables screen DMA for all vCenter Server-managed virtual machines in the pool. However, if Horizon Agent is installed in a virtual machine in unmanaged mode (VDM_VC_MANAGED_AGENT=0), screen DMA is not enabled. For information about manually enabling screen DMA, see VMware Knowledge Base (KB) article 2144475, Manually enabling screen DMA in a virtual machine.

# Support for Red Hat Enterprise Linux Workstation

Horizon Agent for Linux supports installation on systems running Red Hat Enterprise Linux Workstation. Red Hat Enterprise Linux Server is not supported.

In the Setting Up Horizon 7 for Linux Desktops document, all occurrences of "Red Hat Enterprise Linux" and "RHEL" refer to Red Hat Enterprise Linux Workstation only.

For the list of supported versions of Red Hat Enterprise Linux Workstation, see System Requirements For Horizon 7 for Linux.

# Prior Releases of View

Features that were introduced in prior releases of View are described in the release notes for each release, along with existing known issues.

# Resolved Issues

The resolved issues are grouped as follows:

- RDS Desktops and Applications
- Access Point
- Horizon 7 for Linux Desktops
- Windows Media MMR
- 3D Graphics Acceleration
- Client Drive Redirection
- Windows 10 and Windows 8.x Support
- View Persona Management

## RDS Desktops and Applications

- A single client device connecting to RDS desktops and applications over PCoIP could use up more than one RDS Per Device Client Access License (CAL). This issue is resolved by the RDS per-device licensing improvements feature.

## Access Point

- If Access Point was configured to use smart card authentication and you also set an idle session timeout for View Connection Server, then after the idle session timeout period elapses, you could no longer log in again. For example, if the idle session timeout was set to 3 minutes and you left the session idle for more than 3 minutes, when the session timeout dialog box appeared and you clicked "Continue," you were prompted to enter Active Directory credentials rather than a smart card PIN. Even if you entered AD credentials, the status displayed "`Authenticating ...`" and froze.
- In Access Point 2.0, smart card authentication is a Tech Preview feature, meaning that you can use smart card authentication in a test environment but not in a production environment, and technical support is not available for this Tech Preview feature. Smart card authentication is fully supported in Access Point 2.5.
- Smart card authentication did not work if you used View Administrator to configure a pre-login message. If a pre-login message was configured in View Administrator, when you logged in using smart card authentication and you were prompted to confirm the pre-login message, after you confirmed the message, the pre-login message reappeared.
- When you used the Access Point REST administration API, you could not use the "`/v1/config/settings`" resource to update authentication settings.
- When deploying the Access Point appliance, either by using the command-line VMware OVF Tool or by using the deployment wizard, you had to enter only one DNS address. If you entered multiple addresses, DNS resolution did not work.
- If you set the View Edge Setting "`blastEnabled`" to `False`, you are not able to access remote desktops and applications through HTML Access. Generally, because Access Point is deployed in a DMZ, the "`blastEnabled`" option is set to `True`, and this issue does not occur. If you want to set "`blastEnabled`" to `False` and also use HTML Access, you must also set the "`proxyPattern`"

option to "`/|/portal(.*)`".

### Horizon 7 for Linux Desktops

- If you disconnect from a Linux desktop before the guest operating system has completed the log-in process, View Agent for Linux waits at least five minutes before logging off, even if the desktop pool setting, **Automatically logoff after disconnect**, is set to **Immediately** or to a waiting time that is less than five minutes.

### Windows Media MMR

- Windows Media MMR did not perform ideally on certain graphics cards, such as certain AMD models, which have slow video memory read back performance.

### 3D Graphics Acceleration

- On AMD vDGA, the Autofit feature might stop working if the client window was resized to a resolution smaller than 640x480. This issue is resolved by upgrading to Horizon Client 4.0.1 or later.

### Client Drive Redirection

- When using client drive redirection (CDR) or file association (opening local files with a remote application) with the secure tunnel enabled, you might have encountered performance issues when transferring CDR data between Horizon clients and remote desktop machines.
- If you disabled client drive redirection with the Microsoft Remote Desktop Services group policy setting, **Do not allow drive redirection**, users could still select the **Options** > **Share Folders** option in Horizon Client and use the UI to select shared drives. The drives were not shared and did not appear in the remote desktop. This issue did not occur if you did not install the Client Drive Redirection option when you installed View Agent.

### Windows 10 and Windows 8.x Support

- If you upgraded from a Windows 8.1 desktop to Windows 10, logged in to the desktop, and pressed a key on the login screen, Windows displayed a black screen and the desktop was unusable.
- Windows 10 unmanaged machines were displayed as Windows 8 on the Registered Machines page in View Administrator.

### View Persona Management

- With Persona Management, if a folder was renamed or moved, and a program tried to access the folder or a file inside that folder at its original location, the folder, including its contents, was recreated at its original location. This issue often occurred with applications such as Microsoft Outlook and other email clients that frequently create and delete folders and files.

## Known Issues

The known issues are grouped as follows:

- 3D Graphics Acceleration
- Smart Card
- Scanner Redirection
- Serial Port Redirection
- View Persona Management
- vSphere Platform Support
- View Composer
- Windows 10 and Windows 8.x Support
- Windows Server for Desktop Use
- VMware Identity Manager (formerly VMware Workspace Portal) Integration
- Virtual SAN and Virtual Volumes
- Cloud Pod Architecture
- Miscellaneous

## Installation, Upgrade, and Uninstall Operations

- When you upgrade View Agent 6.1.1 to View Agent 6.2.x on an RDS host running on Windows Server 2012 or 2012 R2, the upgrade fails with an "Internal Error 25030" message.
  **Workaround:** Uninstall View Agent 6.1.1, restart the RDS host, and install View Agent 6.2.x.
- The USB HUB device driver might not be installed properly when you install View Agent on a desktop in a manual desktop pool. This issue can occur if, during the View Agent installation, you restart the system before the USB HUB device driver is fully installed.
  **Workaround**: When you install View Agent and you are prompted to restart the system, check the system tray to see if the USB HUB device driver software is still being installed. Wait until the device driver software is completely installed (typically about 30 seconds) before you restart the system.
  If you use a command-line script to install View Agent silently, make sure to wait or sleep the script for long enough to allow the driver installation to complete before you restart the system.
  If you encounter this issue after View Agent is installed, or you could not delay the system restart during a silent installation, update the USB HUB device driver by taking these steps:
  1. In the Device Manager, under **Other Devices**, right-click **VMware View Virtual USB Hub**.
  2. Click **Update Driver Software** > **Browse my computer for driver software**.
  3. Go to `C:\Program Files\VMware\VMware View\Agent\bin\drivers` and click **Next** to let Windows install the driver.
- To upgrade a desktop from Windows 8 to Windows 8.1, you must uninstall View Agent, upgrade the operating system from Windows 8 to Windows 8.1, and then reinstall View Agent. Alternatively, you can perform a fresh installation of Windows 8.1 and then install View Agent.
- If you upgrade to vSphere 5.5 or a later release, verify that the domain administrator account that you use as the vCenter Server user was explicitly assigned permissions to log in to vCenter Server by a vCenter Server local user.
- USB redirection fails in linked-clone images after you upgrade the master image from View Agent 5.1.*x* or earlier to the current View Agent version. This issue does not occur if you upgrade from View Agent 5.2 or later to the current version.
  **Workaround**: See VMware Knowledge Base (KB) article 2062215, USB redirection fails in linked-clone images after you upgrade to View Agent 5.3.
- When you run the View Agent installer on a Windows 8 virtual machine, the Windows desktop appears black when the video driver is being installed. The Windows desktop might appear black for several minutes before the installation completes successfully.
  **Workaround**: Apply the Windows 8.0 May 2013 roll-up before you install View Agent. See Microsoft KB article 2836988.
- When you run any View installer on a Windows 8.1 or Windows Server 2012/2012 R2 virtual machine (deployed as an RDS host or VDI desktop), the installer can take an unusual amount of time to finish. This problem occurs if the virtual machine's domain controller, or another domain controller in its hierarchy, is unresponsive or unreachable.
  **Workaround**: Verify that the domain controllers have the latest patches, enough free disk space, and can communicate with each other.
- When you uninstall View Agent from an RDS host, an error dialog can be displayed, which prevents the uninstall operation from being completed. The dialog states that the uninstall operation failed to

stop an RDS video driver. This issue can occur when disconnected desktop sessions are still running on the RDS host.
**Workaround:** Reboot the RDS host to complete the uninstallation of View Agent. As a best practice, ensure that all RDS sessions are logged off before you uninstall View Agent.

- During a View 6.2.x View Connection Server Hot Patch deployment, you will see a generic icon instead of the correct VMware icon for VMware Horizon 6 HTML Access in the Programs and Features applet in the Control Panel. This is a cosmetic issue and does not affect the functionality of the HTML Access feature.
  **Workaround:** Uninstall earlier version of Connection Server and then install the Hot Patch.
- During the upgrade of View Agent 6.2 to View Agent 6.2.x on an RDS host running Windows Server 2008, you may see a message asking you to close the "VMware Horizon View Agent and Server Manager" application and click Retry to continue. You can safely ignore this message and click Retry. The upgrade will proceed and be successful.
  **Workaround:** Not required.

## Instant Clones

- During provisioning of an instant-clone desktop pool, if there is not enough space available on the datastores, the error message that is displayed in View Administrator is "Cloning of VM <VM name> has failed - VC_FAULT_FATAL: Failed to extend swap file from 0 KB to 2097152 KB." This message does not clearly indicate the root cause of the problem.
  **Workaround:** Not required.
- In View Administrator, if you go to **Catalog** > **Desktop Pools**, double-click an instant-clone desktop pool, go to the **Inventory** tab and click **Machines (InstantClone Details)**, the window displays details of the instant clones. However, the OS Disk datastore column displays no information.
  **Workaround:** None

## Smart Policies

- If you use Horizon Client 3.5.x or earlier for Linux, Mac OS X, or Windows with USB auto-connection enabled, and you connect to a remote desktop for which USB redirection has been disabled with Smart Policies, USB devices attached to the client system disappear from the client system.
  **Workaround:** Upgrade to Horizon Client 4.0, or implement one of the workarounds described in VMware Knowledge Base (KB) article 2144334, USB devices on your local system disappear when you connect to a remote desktop with Horizon Client 3.5.x or earlier.

## Access Point

- Radius Authentication fails when Access Point does not resolve the host name within the appliance.
  **Workaround:** Add the <host name> of Access Point to the `/etc/hosts` file. For example, `127.0.0.1 localhost <r-replica2>`.
- Desktop connectivity issues might occur when you deploy Access Point on the same network (VLAN) as the clients and desktops. If you connect to a desktop through Access Point using the Blast protocol, you might face desktop connectivity issues. To access the desktop, you might need to connect again using the Horizon Client.
  **Workaround:** Since this issue only occurs when Access Point is deployed on the same VLAN on which the client machines and desktops are deployed, prevent the issue by deploying Access Point on a different VLAN.

## RDS Desktops and Applications

- For this release, Windows Universal apps are not supported as hosted remote applications. For example, Universal apps do not appear in the list of apps provided by a Windows Server 2016 RDS farm. Universal apps, such as the Edge browser or the Calculator included with Windows 10 or a Windows Server 2016 RDS host, are built on the Universal Windows Platform (UWP). Universal apps require Windows Explorer to be run. In addition, manually launching Universal apps through the Command Prompt will show an error message.

- If you deploy an automated farm from a Windows Server 2012 parent virtual machine that has the RDS role enabled, Sysprep customization will fail on the deployed linked-clone virtual machines. This 3rd-party issue does not occur on other Windows Server versions that have the RDS role enabled.
  **Workaround**: On the Windows Server 2012 parent virtual machine, apply the Microsoft hotfix available at https://support.microsoft.com/en-us/kb/3020396.
- When multiple connections are made consecutively to a single RDS host, a few users (for example, one or two of 120 users) might not be able to start or restart RDS desktop sessions.
  **Workaround**: Increase the number of vCPUs and the RAM size on the RDS host.
- The first connection to an RDS desktop or application fails if it has been more than 120 days since the RDS role was configured on the RDS host, and no previous connection was made. This issue also occurs with RDP.
  **Workaround**: Wait a few seconds and connect to the RDS desktop or application again.
- Persistent settings for location-based printers are not supported if the settings are saved in the printer driver's private space and not in the DEVMODE extended part of the printer driver, as recommended by Microsoft.
  **Workaround**: Use printers that have the user preference settings saved in the DEVMODE part of the printer driver.
- View Agent cannot install the virtual printing feature on RDS hosts that are physical machines. Virtual printing is supported on RDS desktops when View Agent is installed on RDS hosts that are virtual machines.
  **Workaround**: Configure RDS hosts on virtual machines and install View Agent.
- In a desktop session running on a Windows Server 2008 R2 SP1 RDS host, you cannot play back an H.264 video file, or play back AAC audio with a video file, in Windows Media Player. This is a known third-party issue.
  **Workaround**: Go to the Microsoft KB article 2483177 and download the `Desktop Experience Decoder Update for Windows Server 2008 R2` package.
- When you play a YouTube video in a Chrome browser in a desktop session running on a Windows Server 2012 R2 RDS host, the video display can be corrupted. For example, black boxes might pop up in the browser window. This issue does not occur on any other browser or on Windows Server 2008 R2 SP1 RDS hosts.
  **Workaround**: In your Chrome browser, select **Chrome** > **Settings** > **Show advanced settings** > **System**, and deselect **Use hardware acceleration when available**.
- If you play a video in a desktop running on a Windows 2008 R2 SP1 physical RDS host, and you move the video display from the main monitor to another monitor, the video stops playing or the visual frames stop updating (although the audio might continue to play). This issue does not occur on a virtual machine RDS host or in a single monitor configuration, and it only occurs on Windows Server 2008 R2 SP1.
  **Workaround**: Play videos on the main monitor only, or configure your RDS desktop pool on a virtual machine RDS host.
- If you launch a remote application that becomes unresponsive and then launch another application, the second application's icon is not added to the taskbar on the client device.
  **Workaround**: Wait for the first application to become responsive. (For example, an application might be unresponsive while large files are being loaded.) If the first application continues to be unresponsive, terminate the application process on the RDS virtual machine.
- The application Lync 2013 that does not have the February, 2013 update and is hosted on an RDS host running Windows Server 2012 R2 will crash shortly after launch with the error message "Microsoft Lync has stopped working." This is a known issue with Lync 2013.
  **Workaround**: Apply the February, 2013 update of Lync. The update is available at Microsoft KB article 2812461.
- For RDS host farms that are created with VMware Blast display protocol support, enabling the UDP network protocol for VMware Blast sessions reduces Blast Secure Gateway scale and sessions might fall back to the TCP network protocol.
  **Workaround**: Do not enable the UDP network protocol for VMware Blast sessions on RDS hosts.

## Configuration and View Administrator

- For True SSO, the connectivity status between the connection server and the enrollment server is displayed only on the System Health Status dashboard for the connection server that you are using to access View Administrator. For example, if you are using `https://server1.example.com/admin` for View Administrator, the connectivity status to the enrollment server is collected only for the `server1.example.com` connection server. You might see one or both of the following messages:
    - `The primary enrollment server cannot be contacted to manage sessions on this connection server.`
    - `The secondary enrollment server cannot be contacted to manage sessions on this connection server.`

  It is mandatory to configure one enrollment server as primary. Configuring a secondary enrollment server is optional. If you have only one enrollment server you will see only the first message (on error). If you have both a primary and a secondary enrollment server and both have connectivity issues, you will see both messages.
- When you setup True SSO in an environment with CAs and SubCAs with different templates setup on each of them, you are allowed to configure True SSO with a combination of template from a CA or SubCA with another CA or SubCA. As a result, the dashboard might display the status of True SSO as green. However, it fails when you try to use True SSO.
- When using View Administrator from a Firefox browser, if you enter Korean characters in a text field using the Korean Input Method Editor (IME), the Korean characters are not displayed correctly. This issue occurs only with Firefox. This is a 3rd-party issue.
  **Workaround**: Use a different browser. If you still want to use Firefox, input Korean characters one by one.
- If you change the VMware View Blast Secure Gateway (`absg.log`) log level on a View Connection Server instance from `Info` to `Debug`, the log level remains `Info`. (You change the log level by opening the **Set View Connection Server Log Levels** on a View Connection Server instance, changing the `absg` log level, and restarting the VMware View Blast Secure Gateway service.) Changing the log level from `Debug` to `Info` works properly.
  **Workaround**: None.
- The View PCoIP ADM (`pcoip.adm`) group policy setting, **Configure SSL connections to satisfy Security Tools**, is not supported in this release of View. If you attempt to implement certain options in this group policy setting, unexpected results might occur in your View deployment.
  **Workaround**: Do not use this setting in this release of View.
- Setting the size of the retry port range to 0 when configuring the **Configure the TCP port to which PCoIP Server binds and listens** or **Configure the UDP port to which PCoIP Server binds and listens** group policy causes a connection failure when users log in to the desktop with the PCoIP display protocol. Horizon Client returns the error message `The Display protocol for this desktop is currently not available. Please contact your system administrator`. The help text for the group policies incorrectly states that the port range is 0 through 10.
  **Note**: On RDS hosts, the default base TCP and UDP port is 4173. When PCoIP is used with RDS hosts, a separate PCoIP port is used for each user connection. The default port range that is set by the Remote Desktop Service is large enough to accommodate the expected maximum of concurrent user connections.
  **Workaround**:
  **PCoIP on single-user machines**: Set the retry port range to a value between 1 and 10. (The correct port range is 1 through 10.)
  **PCoIP on RDS hosts**: As a best practice, do not use these policy settings to change the default port range on RDS hosts, or change the TCP or UDP port value from the default of 4173. Most important, do not set the TCP or UDP port value to 4172. Resetting this value to 4172 will adversely affect PCoIP performance in RDS sessions.
- On rare occasions, the system health status of Event Database may be displayed as red on the View Administrator dashboard, with the error message "Cannot drop the view 'VE_user_events', because it does not exist or you do not have permission." This condition does not indicate a real error and will resolve itself after a short period of time.
  **Workaround**: None.

## Horizon Client and Remote Desktop Experience

- If a Linux client 2.3.4 connects to a Horizon 6.0.1 View Agent, and the status of the remote desktop is "available" (not "disconnected"), clipboard redirection between the desktop and client device does not work. This issue occurs even when the View PCoIP General Session Variable group policy setting, `Configure clipboard redirection`, is set to `Enabled in both directions`.
  **Workaround:** Disconnect and reconnect to the desktop, or upgrade the Linux client to version 3.1.
- Horizon clients cannot connect to View Connection Server if the server name or fully qualified domain name (FQDN) for View Connection Server contains non-ASCII characters.
  **Workaround:** None.
- On desktops that connect using PCoIP and are configured with multiple monitors, if a user plays a slide show in Microsoft PowerPoint 2010 or 2007, specifies a resolution, and plays the slides on the second monitor, part of each slide appears on each monitor.
  **Workaround:** On the host client system, resize the screen resolution on the second monitor to the desired resolution. Return to the View desktop and start the slide show on the second monitor.
- On desktops that connect using PCoIP, if users play slides in Microsoft PowerPoint 2010 or 2007 and specify a resolution, the slides are played at that chosen resolution and are not scaled to the current resolution.
  **Workaround:** Choose "Use current resolution" as the playback resolution.
- The virtual printing feature is supported only when you install it from View Agent. It is not supported if you install it with VMware Tools.
- When you play videos in Windows Media Player on a desktop, PCoIP disconnections might occur under certain circumstances.
  **Workaround:** On the desktop, open the Windows registry and navigate to the `HKLM\Software\Wow6432Node\Policies\Teradici\PCoIP\pcoip_admin_defaults` registry key for 64-bit Windows or the `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults` registry key for 32-bit Windows. Add the `pcoip.enable_tera2800 DWORD` registry value and set the value to 1.
- For Windows 2008 R2 SP1 desktop pools hosted on an RDS host, the language sync setting (from client to guest) is turned on by default and cannot be turned off. Therefore, disabling the group policy "Turn on PCoIP user default input language synchronization" for View Agent has no effect. The remote desktop language always synchronizes with the language used on the client system.
  **Workaround:** None.

## Horizon 7 for Linux Desktops

- If you configure two monitors with different resolutions, and the resolution of the primary screen is lower than that of the secondary screen, you might not be able to move the mouse or drag application windows to certain areas of the screen.
  **Workaround:** Make sure that the primary monitor's resolution is at least as large as the secondary monitor's.
- Configuring four monitors at 2560x1600 resolution on RHEL 6.6 or CentOS 6.6 virtual machines in vSphere 6.0 is not supported.
  **Workaround:** Use 2048x1536 resolution or deploy this configuration in vSphere 5.5.
- If you configure two or more monitors at 2560x1600 resolution on RHEL 6.6 virtual machines in a vDGA environment, desktop performance is poor. For example, application windows do not move smoothly. This issue occurs when RHEL Desktop Effects are enabled.
  **Workaround:** Disable Desktop Effects by going to **System** > **Preference** > **Desktop Effects** and selecting **Standard**.
- Unicode keyboard input does not work correctly with HTML Access in Horizon 7 for Linux Desktops.

## Windows Media MMR

- Windows Media MMR does not work on Windows 10 desktops.
  **Workaround:** None
- If you switch browser tabs while playing a redirected video in Internet Explorer, part of the video window continues to be displayed behind or next to the browser window. This issue only occurs on Windows 7 desktops.
  **Workaround:** Use Windows 8.1 desktops. Alternatively, do not switch to another tab while a

redirected video is playing.

## 3D Graphics Acceleration

- For Intel vDGA, only the Haswell and Broadwell series of Intel integrated GPUs are supported. Broadwell integrated GPUs are supported only on vSphere 6 Update 1b and later. Haswell integrated GPUs are supported on vSphere 5.5 and later. Also note that the GPU needs to be enabled in the BIOS before it can be recognized by ESXi. For more information, see the documentation for your specific ESXi host. Intel recommends leaving the graphics memory settings in the BIOS set to their default values. If you choose to change the settings, keep the aperture setting at its default (256M).
- For Intel vDGA, multiple-monitor support is limited to no more than 3 monitors. The Intel driver supports only up to 3 monitors with a resolution of up to 3840 X 2160. If you try to connect with 4 monitors, the connection shows 3 black screens with just one screen working.
- When 4K monitors are configured on machines where 3D Rendering and vSGA are enabled, moving, resizing, or toggling the Windows Media Player window to full screen mode can be very slow. This issue does not occur with 2D, software 3D Rendering, or monitors with 2560x1440 resolution.
  **Workaround:** None
- If NVIDIA drivers are installed on a virtual machine that you use as a parent or template to deploy a desktop pool, and the machines are deployed on non-NVIDIA GRID hardware on the ESXi hosts, users might not be able to start desktop sessions correctly. This issue might occur if the virtual machine was used previously in an NVIDIA GRID vGPU deployment.
  **Workaround:** Remove the NVIDIA drivers from the virtual machine before you take a snapshot or make a template and deploy the desktop pool.
- If vDGA is enabled on a Windows 7 virtual machine that is configured to use NVIDIA driver version 347.25, the desktop session can be disconnected. This issue does not occur on Windows 8.1 or on other NVIDIA driver versions.
  **Workaround:** Do not use NVIDIA driver version 347.25.
- On Windows 8/8.1 desktops, 3D screen savers operate even when the 3D Renderer setting is disabled, and the screen savers do not render correctly. This issue does not occur on Windows 7 desktops.
  **Workaround:** Make sure your end users do not use 3D screen savers, or enable the 3D Renderer setting for the desktop pool.
- With NVIDIA M60 GPU and driver version 361.89 or 361.94, users might see a blurred screen when they first connect to the Windows desktop, or when they right click on the desktop and then select **NVIDIA Control Panel** > **System Information**.
  **Workaround:** Changing the resolution of the display or changing to full-screen mode fixes the problem and you can revert back to the original resolution or screen mode. The problem disappears after the first time it occurs. Also, the problem does not occur with NVIDIA driver 361.51.

## Smart Card

- Using a smart card to log in to an RDS desktop takes longer than with a VDI, single-user desktop. This issue is less acute on Windows clients than other clients.
  **Workaround:** None.
- On Windows 7 client machines, Horizon Client exits when the smart card removal policy is triggered.
- Users running View Client 5.4.2 (the executable is wswc.exe) fail to login using smart card authentication.
  **Workaround:** Install and run Horizon Client 3.0 or later.

## Scanner Redirection

- Microsoft Windows Fax and Scan does not work with Scanner Redirection on Windows 10 desktops.
  **Workaround:** Use another scan application on Windows 10 desktops or change to another desktop platform.
- Selecting the Scanner Redirection setup option with View Agent installation can significantly affect

the host consolidation ratio. By default, the Scanner Redirection option is not selected when you install View Agent.
**Workaround:** Make sure that the Scanner Redirection setup option is not selected for most users. For the particular users who need the Scanner Redirection feature, configure a separate desktop pool and select the setup option only in that pool.

- Sometimes the scanner settings do not take effect on WIA scanners. For example, if you select grayscale mode and select a partial area of the original image, the scanner might use color and scan the whole image.
  **Workaround:** Use a TWAIN scanner.
- In some environments, if you switch to a different WIA scanner, the images might continue to be scanned from the original scanner.
  **Workaround:** Log off the View desktop session. Launch a new desktop session and perform the scan using the selected scanner.
- When you uninstall View Agent with the Scanner Redirection feature installed, the uninstall process requires you to close any running applications.
  **Workaround:** None. You must close the listed applications before you continue to uninstall View Agent.

## Serial Port Redirection

- The **Bandwidth limit** group policy setting does not take effect. The value you enter in the setting is ignored, and the existing bandwidth is used for serial port redirection. The bandwidth consumption depends on the number of concurrently used serial port devices and the baud rate used by each device.
  **Workaround:** None.

## View Persona Management

- View Persona Management might not correctly replicate a user persona to the central repository if the desktop virtual machine is extremely low on disk space.
- With View Persona Management, you can use group policy settings to redirect user profile folders to a network share. When a folder is redirected, all data is stored directly on the network share during the user session. Windows folder redirection has a check box called **Grant user exclusive rights to *folder-name***, which gives the specified user exclusive rights to the redirected folder. As a security measure, this check box is selected by default. When this check box is selected, administrators do not have access to the redirected folder. If an administrator attempts to force change the access rights for a user's redirected folder, View Persona Management no longer works for that user.
  **Workaround:** See VMware Knowledge Base (KB) article 2058932, Granting domain administrators access to redirected folders for View Persona Management.
- View Persona Management is not supported on session-based desktop pools that run on RDS hosts.
  **Workaround:** Install View Persona Management in automated or manual desktop pools that run on single-user machines.

## vSphere Platform Support

- View Storage Accelerator might take tens of minutes to generate or regenerate the digest files for large virtual disks (for example, a 100GB virtual disk). As a result, the desktop might be inaccessible for longer than expected.
  **Workaround:** Use the blackout period to control when digest regeneration operations are allowed. Also, use the digest regeneration interval to reduce the frequency of these operations. Alternatively, disable View Storage Accelerator in desktop pools that contain very large virtual machines.
- If a linked-clone pool consists of vSphere 5.5 virtual machines, a View Composer rebalance operation can fail with a `FileAlreadyExists` error. This problem occurs only when the desktop pool uses different datastores for the OS disk and the user data disk and the datastore selection for

the user data disk changes before the View Composer rebalance operation takes place.
**Workaround**: Detach the persistent disk from the linked clone desktop that has the `FileAlreadyExists` error. Later, you can attach the archived disk to a new virtual machine and recreate the linked-clone desktop or attach it to an existing linked-clone desktop as a secondary disk. You can prevent this problem from occurring by either keeping the OS disk and user data disk on the same datastore or by not changing the datastore selections before a View Composer rebalance operation.
- After you upgrade to vSphere 5.5, a heap size error can occur if you use space-efficient virtual disks and you have more than 200 linked-clone virtual machines per ESXi host. For example: `Error: Heap seSparse could not be grown by 12288 bytes for allocation of 12288 bytes`
**Workaround**: Reduce the number of linked-clone virtual machines that use space-efficient virtual disks to less than 200 per ESXi host.

## View Composer

- When View Administrator provisions a linked-clone pool with thousands of desktops, a few machines (one or two per thousand) might fail with a "Customization timed out" error. If automatic recovery is enabled (the recommended setting for production environments), machines in error are automatically recreated and provisioned. No workaround is required.
**Workaround**: If automatic recovery is disabled, manually delete the machines in error in View Administrator. View Administrator will provision new machines as part of normal pool management.
- When deleting a large desktop pool, a number of folders containing an `.hlog` file and an empty subfolder named `.sdd.sf` might remain undeleted.
**Workaround**: Manually delete the folders that are left behind after a deletion operation. For instructions, see the Solution in VMware Knowledge Base (KB) article 2108928, Rebalance operation leaves VM folders in previous datastores.
- If you upgrade a virtual machine with an IDE controller from Windows XP to Windows 7, take a snapshot of the virtual machine, and create a linked-clone pool, the linked clones cannot be customized, and pool creation fails.
**Workaround**: Add a SCSI controller and a disk to the virtual machine. Next, launch VMware Tools and install a VMware SCSI controller driver on the virtual machine. Next, take a snapshot and create the linked-clone pool.
- When you provision linked-clone desktops that are customized by Sysprep, some desktops might fail to customize.
**Workaround**: Refresh the desktops. If a small number of desktops still fail to customize, refresh them again.
- Do not change the log on account for the VMware View Composer Guest Agent Server service in a parent virtual machine. By default, this is the Local System account. If you change this account, the linked clones created from the parent do not start.
- Desktop pool provisioning fails with the error message `Polling progress failure: Unable to connect to View Composer server <https://machine-name:18443>: java.net.ConnectException: Connection refused: connect.`
**Workaround**: Restart the VMware vCenter Server service and then reprovision the desktop pool.

## Windows 10 and Windows 8.x Support

- Windows 10 is not supported as a guest operating system for ThinApp in this release of Horizon 6.
**Workaround**: None
- On some occasions, when you reconnect to a Windows 8.x desktop session, you might not see the desktop display immediately. A black screen might be displayed for up to 20 seconds.
**Workaround**: None
- When a space reclamation operation is run for Windows 8.x linked clone virtual machines, the size of the system disposable disk and user persistent disk might increase to its maximum capacity. This space increase only happens the first time space reclamation is done. For the OS disk, space reclamation works as expected and reclaims the unused space. This issue does not affect View Composer desktops that do not use system disposable disks or user persistent disks.
**Workaround**: When you configure View Composer desktops on Windows 8 or 8.1 virtual machines

and enable space reclamation, do not configure system disposable disks or user persistent disks.

- Adobe Flash optimization settings that use high quality and aggressive throttling are not fully enabled when end users use Internet Explorer 10 or Internet Explorer 11 on Windows 8 or Windows 8.1 desktops.
  **Workaround**: None.
- On a Windows 8 desktop, if you enable the View Persona Management setting, `Remove local persona at logoff`, and a user creates a PDF file, logs off of the desktop, and logs back in again, the user cannot open the offline PDF file. The Windows 8 Reader cannot download the offline PDF content.
  **Workaround**: Manually download the file by right-clicking the file and selecting **Properties** or selecting **Open with... Adobe Reader**.
- When using Internet Explorer 10 or 11 on a Windows 8 or later computer, if you set the browser locale to Traditional Chinese, and you log in to View Administrator, the navigation panel might be displayed in Simplified Chinese.
  **Workaround**: Use an alternate browser to log in to View Administrator.
- If a user of a Windows 8 View desktop logs in using Kerberos authentication, and the desktop is locked, the user account for unlocking the desktop that Windows 8 shows the user by default is the related Windows Active Directory account, not the original account from the Kerberos domain. The user does not see the account he or she logged in with.
  This is a Windows 8 issue, not directly a View issue. This issue could, but does not usually, occur in Windows 7.
  **Workaround**: The user must unlock the desktop by selecting "Other user." Windows then shows the correct Kerberos domain and the user can log in using the Kerberos identity.
- When provisioning 64- or 32-bit Windows 8 desktops in a vSphere 5.1 environment, the Sysprep customization can fail. The desktops end up in an ERROR state with a `Customization timed out` error message. This issue occurs when anti-virus software is installed in the parent virtual machine or template. The issue applies to full clone and linked clone desktops. It does not apply to linked clone desktops customized with QuickPrep.
  **Workaround**: Uninstall the anti-virus software on the parent virtual machine or template and recreate the pool.
- When recomposing Windows 8.1 desktops, the Sysprep customization can fail with a `Customization operation timed out` error message. This problem is caused by a Windows 8.1 scheduled maintenance task that recovers disk space by removing unused features.
  **Workaround**: Use the following command to disable the maintenance task immediately after completing Setup: `Schtasks.exe /change /disable /tn "\Microsoft\Windows\AppxDeployment Client\Pre-staged app cleanup"`
- After a recompose, refresh, or rebalance operation with a persistent disk, Windows 10 desktops might fail to start, or become untiled from the Start menu. Windows applications can include applications such as Windows Store, native applications, Edge Browser, and Cortana Search. This issue affects multiple version of Windows 10 intermittently, depending on applications used. This problem affects the following desktop types:
  - Linked-clone dedicated desktops with a persistent disk where the persistent disk is used to store app settings.
  - Linked-clone floating desktops with Persona Management enabled that use a persistent disk as a local disk and the Persona Management setting **Roam Local Settings Folders** enabled.
  - This issue is not seen with floating or dedicated linked-clone desktop pools where the user profile is redirected to network share with or without Persona Management enabled. If Persona Management is enabled, the user profile is set to roam with VMware Persona GPO settings.
  - This issue is not seen when persistent disk and/or Persona Management are used to persist only My Documents and Exchange 365 .pst/ost files.

## Windows Server for Desktop Use

- You cannot connect to a Windows Server 2008 R2 SP1 desktop, or you encounter a black screen the first time that you use Horizon Client, even though the desktop that you are connecting to is in the Available state.

**Workaround**: Shut down and power on the Windows Server 2008 R2 SP1 virtual machine. When the desktop is in the Available state, try to connect again. Note: Resetting or restarting the virtual machine does not solve this problem. You must shut down the virtual machine first and then power it back on.

## VMware Identity Manager (formerly VMware Workspace Portal) Integration

- If you change the default HTTPS port, 443, on a View Connection Server instance or security server, and Horizon users try to start their desktops from the Horizon User Portal, the desktops fail to launch. This issue occurs when users attempt to access their desktops via Horizon Workspace with either Horizon Client or HTML Access.
  **Workaround**: Keep the default HTTPS port 443.
- When you add a SAML Authenticator in View Administrator, an "Invalid certificate detected" window might be displayed, even when the Metadata URL points to a trusted certificate in the Trusted Root Certificate Authorities folder in the Windows certificate store. This issue can occur when an existing SAML Authenticator with a self-signed certificate was using the same Metadata URL when the trusted certificate was added to the Windows certificate store.
  **Workaround:**
  1. Remove any trusted certificates for the Metadata URL from the Trusted Root Certificate Authorities folder in the Windows certificate store.
  2. Remove the SAML Authenticator with the self-signed certificate.
  3. Add the trusted certificate for the Metadata URL to the Trusted Root Certificate Authorities folder in the Windows certificate store.
  4. Add the SAML Authenticator again.

## Virtual SAN and Virtual Volumes

- In a hybrid vSAN environment, about three percent of the virtual machines might not use View Storage Accelerator. These machines will take few seconds longer to start up.
  **Workaround:** Delete and recreate the virtual machines that failed to use View Storage Accelerator.
- In this release, View Storage Accelerator is not supported on Virtual Volume datastores.
  **Workaround:** None
- Provisioning View Composer linked clones fails on some Virtual Volumes storage arrays. The following message is displayed: "Error creating disk Error creating VVol Object. This may be due to insufficient available space on the datastore or the datastore's inability to support the selected provisioning type." View Composer creates a small internal disk in thick-provisioned format, although all other linked clone disks use thin provisioning. This issue occurs if the 3rd-party Virtual Volumes storage array does not support thick-provisioned disks by default.
  **Workaround**: Enable thick provisioning on the storage array to allow Virtual Volumes to create thick-provisioned disks.
- When you attach or recreate a View Composer persistent disk stored on a Virtual SAN datastore, the virtual disk's storage policy in vCenter Server is shown as "Out of date." The original storage profile is not preserved.
  **Workaround:** In vSphere Web Client, reapply the storage policy to the virtual disks.
- Virtual SAN datastores are only accessible from hosts that belong to the Virtual SAN cluster, and not from hosts that belong to a different cluster. Therefore, rebalance of pools from one Virtual SAN datastore to another Virtual SAN datastore in a different cluster is not supported.
- In an environment where a large VDI desktop pool (for example, 2,000 desktops) is created on Virtual Volumes datastores that reside on a NetApp storage system running ONTAP 8.2.x or earlier, a recompose operation may fail for a small number of desktops with the error message "The VVol target encountered a vendor specific error."
  **Workaround:** Upgrade the NetApp storage system to ONTAP 8.3 or later.

## Cloud Pod Architecture

- Cloud Pod Architecture configuration changes made by another View administrator while you

are logged in to View Administrator are not visible in your current View Administrator session.
**Workaround:** Log out of View Administrator and log in again to see the changes.

## Miscellaneous

- The ViewDbChk utility can display an "Archiving persistent disks..." message while removing machines from an automated linked-clone pool with floating assignment or an automated farm.
  **Workaround:** None.
- For virtual machines that have hardware version 8, the maximum allowed video RAM is 128MB. For virtual machines that have hardware version 9 and later, the maximum allowed video RAM is 512MB. If you configure a value from View Administrator that exceeds the video RAM limit for a virtual machine's hardware version, errors appear in the vSphere Client Recent Tasks pane and the configuration operation keeps repeating. This problem occurs only if you configure the video memory value through View Administrator (Pool Settings page) and not through vSphere Client.
  **Workaround**: Either upgrade the hardware version of the virtual machines in vSphere Client, or use View Administrator to set the proper value for video memory based on the current virtual machine hardware version.
- When you try to add a SAML authenticator in View Administrator, the **Add** button is disabled on the Manage SAML Authenticators page.
  **Workaround**: Log in to View Administrator as a user who has the Administrators or Local Administrators role.