Horizon System Recommendations

Hardware/OS recommendations for self-hosting our server-based Horizon Software suite.

- Horizon Suite Host Server
- Remote Desktop Session Host Servers
- End User Workstations

Horizon Suite Host Server

This document contains general hardware recommendations for servers hosting the Horizon Suite files, data, and other dependencies. Also documented here are any concerns or caveats regarding the configuration or operation of the Horizon Suite software.

Hardware

The Horizon Software suite is relatively light-weight as it operates primarily over the SMB protocol. For the best performance and end-user experience, the server hosting Horizon Software data should be configured with fast, redundant storage and low-latency/high-throughput network hardware. Our general hardware recommendations are as follows:

Component	**Recommendation**
Processor	Any Intel or AMD x64 processor 2.0 GHz or faster 4 cores or more
Memory	At least 16GB
Storage	At least 500GB on an independent/dedicated disk or volume SSDs are recommended RAID-1, RAID-5, or RAID-10 recommended
Network	1Gbps NIC and infrastructure required 2.5Gbps or 10Gbps NIC and infrastructure recommended

Virtualization

Horizon recommends virtualization whenever possible. This makes deployment, configuration, migration, and recovery easy and quick as well as enabling more reliable VM-based and virtual disk-based backup methods. When virtualizing servers for a Horizon Software deployment, the following hardware recommendations are for the Horizon Software host server VM, not the hypervisor host! The hypervisor host hardware specs should be determined accordingly to *cumulatively* support the hardware recommendations of **all servers** being virtualized on that host.

Operating System

The Horizon Suite can be hosted on any currently-supported Windows Server operating system. The Horizon Software suite supports any currently-supported version of Microsoft Server as per the

Microsoft Fixed Lifecycle Policy. Currently-supported versions of Windows Server are:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016 (Extended Support)
- Windows Server 2012 R2 (Extended Support)

Data Storage/Management

The Horizon Suite can function using the DataFlex embedded database alone, however there are size limitations with this database type as well as some caveats when backing up this type of database. We recommend hosting your data in a Microsoft SQL database; This improves speed, reliability, and eliminates size limitations imposed by the embedded database. Microsoft SQL databases are also able to be backed up and restored far more efficiently.

The Horizon Software suite can be hosted on any currently-supported version of Microsoft SQL Server as per the Microsoft Lifecycle Policy for SQL Server. We recommend deploying the Standard Edition for most customers.

- SQL Server 2022
- SQL Server 2019
- SQL Server 2017 (Extended Support)
- SQL Server 2016 (Extended Support)

Software Considerations

Antivirus/Antimalware/Data Protection Software

Any file- or process-scanning security software should be closely monitored for possible issues with Horizon Software programs and/or data. Typically, no special considerations are required for any such software on the **host** server, however it is recommended to limit any scanning or monitoring of the primary Horizon Software file share to the server on which the share is hosted. Any workstations or Remote Desktop Session Host servers accessing the Horizon Software file share should have the share excluded from any security software scanning to prevent network traffic and disk issues.

Windows Defender

In our testing, we have seen Windows Defender cause significant latency issues with Horizon Suite programs. Even when a third-party security suite/software is being used, Windows Defender sometimes remains active and consumes significant resources to scan files and programs both locally and across remote file shares. If Windows Defender cannot be completely disabled, exclusions should be created for Horizon Suite programs and directories.

SMB

Horizon Suite programs depend on the Server Message Block (SMB) protocol to operate and access data from the Horizon host server. For best performance, SMBv2/3 should be enabled on your Horizon host server and any workstations or Remote Desktop Session Host servers accessing the Horizon Software file share. You can check the SMB protocols on your device using these instructions.

As per Microsoft's recommendation, the SMBv1 protocol should be disabled on at least all Windows devices as applicable in your environment. Since Windows 10 Fall Creators Update and Windows Server version 1709 (RS3), the SMBv1 protocol is no longer installed by default.

Horizon recommends using the latest version of SMB supported in your environment, though no older than SMBv2.

File-Based Backup Software

As mentioned above, there are generally no special concerns regarding backing up Horizon Software data when using Microsoft SQL Server. However, if your Horizon data is stored using the DataFlex embedded database, extra consideration is required - These database files utilize locks which are incompatible with most backup software which uses Microsoft's Volume Shadow Copy Service technology. This means Shadow Copies cannot be enabled on the disk which hosts the Horizon Software file share. Third-party file-based or snapshot-based backup software should be configured to back up files outside of normal business hours to prevent data corruption issues.

This issue in particular can be avoided when virtualizing the Horizon Software host server by using a backup software which supports virtualization platforms, such as Veeam.

In any case, we recommend utilizing an independent, dedicated disk or volume to host Horizon Software files and data.

Remote Desktop Session Host Servers

This document contains general hardware recommendations for Remote Desktop Session Host servers running the Horizon Suite. Also documented here are any concerns or caveats regarding the configuration or operation of the Horizon Suite software.

Hardware

For the best performance and end-user experience, any Remote Desktop Session Host server hosting Horizon Software user sessions should be configured with fast storage and low-latency/high-throughput network hardware. Our general hardware recommendations are as follows:

Component	**Recommendation**
Processor	Any Intel or AMD x64 processor 2.0 GHz or faster **1 core per concurrent user**
Memory	8GB base for OS/software **1GB additional per concurrent user**
Storage	At least 250GB **10GB additional per user**
Network	1Gbps NIC and infrastructure required 2.5Gbps or 10Gbps NIC and infrastructure recommended

Virtualization

Horizon recommends virtualization whenever possible. This makes deployment, configuration, migration, and recovery easy and quick as well as enabling more reliable VM-based and virtual disk-based backup methods. When virtualizing servers for a Horizon Software deployment, the following hardware recommendations are for the Horizon Software host server VM, not the hypervisor host! The hypervisor host hardware specs should be determined accordingly to *cumulatively* support the hardware recommendations of **all servers** being virtualized on that host.

Operating System

The Horizon Software suite can be installed and used in a Remote Desktop environment consisting of any server(s) running a currently-supported Windows Server operating system as per the Microsoft Fixed Lifecycle Policy. Currently-supported versions of Windows Server are:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016 (Extended Support)
- Windows Server 2012 R2 (Extended Support)

Software Considerations

Antivirus/Antimalware/Data Protection Software

Any workstations or Remote Desktop Session Host servers accessing the Horizon Software file share should have the share excluded from scanning to prevent network traffic and disk issues. Ideally, any server-based network share or mapped drive should be excluded as those would be scanned locally on their respective host server, this included the Horizon Software file share.

Windows Defender

In our testing, we have seen Windows Defender cause significant latency issues with Horizon Suite programs. Even when a third-party security suite/software is being used, Windows Defender sometimes remains active and consumes significant resources to scan files and programs both locally and across remote file shares. If Windows Defender cannot be completely disabled, exclusions should be created for Horizon Suite programs and directories on any workstation or client server accessing the Horizon Software file share.

SMB

Horizon Suite programs depend on the Server Message Block (SMB) protocol to operate and access data from the Horizon host server. For best performance, SMBv2/3 should be enabled on your Horizon host server and any workstations or Remote Desktop Session Host servers accessing the Horizon Software file share. You can check the SMB protocols on your device using these instructions.

As per Microsoft's recommendation, the SMBv1 protocol should be disabled on at least all Windows devices as applicable in your environment. Since Windows 10 Fall Creators Update and Windows Server version 1709 (RS3), the SMBv1 protocol is no longer installed by default.

Horizon recommends using the latest version of SMB supported in your environment, though no older than SMBv2.

File-Based Backup Software

Any file-based backup software installed on a Remote Desktop Session Host server should be configured to exclude backing up network shares or mapped drives, including the primary Horizon Software file share. This file share should be backed up using a supported method from the host server.

End User Workstations

This document contains general hardware recommendations for end-user workstations running the Horizon Suite. Also documented here are any concerns or caveats regarding the configuration or operation of the Horizon Suite software.

Hardware

For the best performance and end-user experience, any workstation running Horizon Suite programs should be configured with fast storage and low-latency/high-throughput network hardware. Our general hardware recommendations are as follows:

Component	Recommendation
Processor	Any modern Intel or AMD x64 processor 2.0 GHz or faster
Memory	8GB minimum 16GB recommended
Storage	At least 250GB SSD recommended
Network	1Gbps NIC required **WiFi is not recommended** **Remote VPN use is not recommended**

WiFi/VPN Use

Due to the nature of Horizon Suite programs and the minimal latency required for database operations, we do not recommend running any Horizon Suite programs over WiFi. Doing so can lead to data corruption issues, and generally causes significant delays during usage of the software.

As with the latency concerns above, Horizon Suite programs should **never** be used when the Horizon host server is being accessed over a VPN connection. Any workstation running Horizon Suite programs and the server hosting the Horizon data should be on the same physical LAN.

MPLS, SD-WAN, and P2P networks should be avoided as well, unless the connection backbone is fiber-based from end-to-end with <5ms latency and >1Gbps bandwidth.

If any Horizon Suite users require accessing the Horizon data remotely outside of the host server's physical LAN, a Remote Desktop Services deployment should be configured for them to use. Alternatively, Horizon offers **Horizon View Hosting**, a cloud-based, fully-managed, complete Horizon Suite environment which enables users to securely run the Horizon Suite software in any web browser on any device with an internet connection.

Operating System

The Horizon Suite can be installed and used on any currently-supported Windows operating system as per the Microsoft Modern Lifecycle Policy. Currently-supported versions of Windows are:

- Windows 11
- Windows 10

Software Considerations

Antivirus/Antimalware/Data Protection Software

Any workstations or Remote Desktop Session Host servers accessing the Horizon Software file share should have the share excluded from scanning to prevent network traffic and disk issues. Ideally, any server-based network share or mapped drive should be excluded as those would be scanned locally on their respective host server, this included the Horizon Software file share.

Windows Defender

In our testing, we have seen Windows Defender cause significant latency issues with Horizon Suite programs. Even when a third-party security suite/software is being used, Windows Defender sometimes remains active and consumes significant resources to scan files and programs both locally and across remote file shares. If Windows Defender cannot be completely disabled, exclusions should be created for Horizon Suite programs and directories on any workstation or client server accessing the Horizon Software file share.

SMB

Horizon Suite programs depend on the Server Message Block (SMB) protocol to operate and access data from the Horizon host server. For best performance, SMBv2/3 should be enabled on your Horizon host server and any workstations or Remote Desktop Session Host servers accessing the Horizon Software file share. You can check the SMB protocols on your device using these instructions.

As per Microsoft's recommendation, the SMBv1 protocol should be disabled on at least all Windows devices as applicable in your environment. Since Windows 10 Fall Creators Update and Windows Server version 1709 (RS3), the SMBv1 protocol is no longer installed by default.

Horizon recommends using the latest version of SMB supported in your environment, though no older than SMBv2.

File-Based Backup Software

Any file-based backup software installed on a workstation should be configured to exclude backing up network shares or mapped drives, including the primary Horizon Software file share. This file share should be backed up using a supported method from the host server.