Installing VMWare Horizon View 8

In this post, I will cover VMWare Horizon View 8 2006 installation and configuration. Within the lab, I will be using Windows Sever 2019 virtual machines, Windows 10 Enterprise virtual machines and vCenter Server Appliance 7. I will not go into the basic setup of virtual machines and vCenter. You can visit my blog for vCenter installation at www.infotechram.com

As per VMWare Horizon View 8 2006 will be released to General Public in Nov 2020

The **Horizon 8** 2006 **release** is expected **to** be generally **available** in **VMware's** Fiscal Q3 FY21, ending on October 30, 2020. **To** trial **Horizon**, sign up for a 90-day free trial.

Here are few useful screenshots on the above.

∨ Purpose

This KB documents the supported operations systems for installing the Horizon Connection Server as well as the Microsoft AD domain funcitonal levels Horizon supports. The following content is applicable for Horizon starting with the release of Horizon 8 2006. Support for Horizon 7 can be found in the Horizon 7 Installation Guide of the corresponding release.

∨ Resolution

Supported Operating Systems for Horizon Connection Server

You must install Horizon Connection Server on a supported Windows Server operating system.

The following operating systems support all Horizon Connection Server installation types, including standard, replica installations

Operating System	Editions Supported in Horizon 8 2006
Windows Server 2012 R2	Standard (64-bit) Datacenter (64-bit)
Windows Server 2016	Standard (64-bit) Datacenter (64-bit)
Windows Server 2019	Standard (64-bit) Datacenter (64-bit)

Supported Microsoft AD Domain Functional Levels for Horizon

Horizon uses your existing Microsoft Active Directory infrastructure for user authentication and management. You must perform certain tasks to prepare Active Directory for use with Horizon.

Horizon supports the following Active Directory Domain Services (AD DS) domain functional levels:

Microsoft AD Domain Functional Levels	Supported in Horizon 8 2006
Windows Server 2012R2	Supported
Windows Server 2016	Supported
Windows Server 2019	Supported

Note: Starting with the Horizon 8 release the product versioning has changed to a 'YYMM' format (i.e. year and month of the release). This format aligns with the industry versioning standard. Version 2006 is the first release in the YYMM format.

Version	Release Date	Build Number
Horizon 8 2006	8/11/2020	8.0.0.16592062
Horizon Connection Server 7.12	3/17/2020	15770369
Horizon Composer 7.12	3/17/2020	15747753
Horizon Agent 7.12	3/17/2020	15805436
Horizon Connection Server 7.11	12/12/2019	15231595
Horizon Composer 7.11	12/12/2019	15119999
Horizon Agent 7.11	12/12/2019	15238678
Horizon Connection Server 7.10.2 (ESB Release)	5/21/2020	16253308
Horizon Composer 7.10.2 (ESB Release)	5/21/2020	15807429
Horizon Agent 7.10.2 (ESB Release)	5/21/2020	16176137
Horizon Agent 7.10.1 (ESB Release)	12/20/2019	15247623
Horizon Connection Server 7.10	9/17/2019	14584133
Horizon Composer 7.10	9/17/2019	14535354
Horizon Agent 7.10	9/17/2019	14590940
Horizon Connection Server 7.9	7/2/2019	13956742
Horizon Composer 7.9	7/2/2019	13810618

Below screen shot are from VMWare and other sites.

The last time VMware released a new major version of Horizon was back in 2016. In the four years since Horizon 7 was released, there have been significant additions to the core product, including HTML5-based management and support consoles, significant enhancements to the Blast protocol and the Instant Clone provisioning model, the introduction of an Extended Service Branch for long-term support, and new client redirection features to support access to local drives, Skype for Business, and multimedia redirection.

Today, VMware has released the next major release of VMware Horizon. Horizon 8, also known as Horizon 2006, brings several changes to the platform. Some of these changes are large changes that bring new functionality to the platform, and other changes are deprecating or removing obsolete features.

Some of the features that are being removed, and their replacements are:

Deprecated/Removed Feature	Replacement
Linked Clones and Composer*	Instant Clones (available in all desktop SKUs)
Persistent Disks* and Persona Management	DEM Standard/Enterprise and AV User Writable Volumes
Windows 7, Windows 8.1 and Server 2008 Support	Windows 10 and Server 2012R2 and Newer
JMP Server	Multicloud Assignments (Part of Horizon Subscription)
Horizon Administrator (FLEX/Flash Based)	Horizon Console (HTML5)
ThinPrint	VMware Integrated Printing
Security Server	Unified Access Gateway
vRealize Operations for Horizon	Cloud Monitoring Service and ControlUp Entitlement (Part of Horizon Subscription)

*Note: Linked Clones, Composer, and Persistent Disks are deprecated. All other features listed have been removed from Horizon 2006.

Some of these changes have been in the works for a while. Instant Clones have been around since Horizon 7 was released in 2016, and they have seen significant improvements with every release. As part of Horizon 2006, Instant Clones will no longer be restricted to Horizon Enterprise and Horizon Apps Advanced. Unified Access Gateway has been the designated Security Server replacement for a while now.

One of the most visible changes that comes with Horizon 8 is a change in branding and versioning. Horizon is now moving to a naming scheme that involves the month and the year in the version that is in line with how many other brand their products. This will make it easier to keep track of when a version is released. The first release of Horizon 8 will be 2006.

Some of the other changes that are included with Horizon 2006 are:

- Expanded REST API that includes new primitives for managing entitlements and inventory items such as desktop pools and RDSH farms.
- A new Instant Clone provisioning model that frees up resources on hosts by removing the instant clone parent VM that is deployed on each host.
- Built-in digital watermarking tool to help protect intellectual property in virtual desktops

The Basics

The smallest Horizon environment only requires three components to deliver a remote desktop session to end users: a desktop, a View Connection Server, and Active Directory. Technically speaking, you do not need vCenter or ESXi as the Horizon agent can be installed on physical desktops.

Many environments, though, are built on vSphere, and the virtual infrastructure for this type of environment doesn't need to be anything special. For small proof of concepts or upgrade testing, one server with direct attached storage and enough RAM could support a few users.

All Horizon environments, from the simple one above to a complex multi-site Cloud Pod environment, are built on this foundation. The core of this foundation is the View Connection Server.

Connection Servers are at the core of a Horizon environment. They handle desktop provisioning, user authentication and broker user sessions to desktops. They manage connections to multi-user desktops and published applications.

There are three roles that can be installed using the Connection Server installer, and all three roles have the same requirements. These roles are:

- Standard Connection Server – The first Connection Server installed in the environment.
- Replica Connection Server – Additional Connection Servers that replicate from the standard connection server
- Enrollment Server – The Enrollment Server was introduced in Horizon 7. role is used to facilitate the new True SSO feature in conjunction with Workspace ONE Access and a local certificate authority.

The requirements for a Connection Server are:

- 1 CPU, 4 vCPUs recommended
- Minimum 4GB RAM, 10GB recommended if 50 or more users are connecting
- Windows Server 2012 R2 or newer
- Joined to an Active Directory domain
- Static IP Address

Note: The requirements for the Enrollment Server are the same as the requirements for Connection Server.

Aside from the latest version of the Connection Server, the requirements are:

ESXi – ESXi is required for hosting the virtual machine The versions of ESXi that are supported by Horizon 2006 can be found in the VMware compatibility matrix.

vCenter Server – The versions of vCenter that are supported by Horizon 2006 can be found in the VMware compatibility matrix.

Active Directory – An Active Directory environment is required to handle user authentication to virtual desktops, and the domain must be set to at least the Server 2012 R2 functional level. Group Policy is used for configuring parts of the environment, including desktop settings, user data redirection, UEM, and the remoting protocol.

Advanced Features

Horizon has a lot of features, and many of those features require additional components to take advantage of them. These components add options like secure remote access, profile management, and instant clone desktops.

Secure Remote Access – The options for delivering secure remote access with Horizon have been simplified in Horizon 2006. Traditionally, remote access had been provided by the Horizon Security Server, but this feature has been removed. The Unified Access Gateway replaces the Security Server for all remote access functionality.

Networking Requirements – Horizon requires a number of ports to be opened to allow communication between the user's endpoint and the remote desktop as well as communication between the management components. The best source for showing all of the ports required by the various components is the VMware Horizon Network Ports diagram. The Network Ports diagram can be found on TechZone.

Instant Clone Desktops – Instant Clones are a rapid desktop provisioning model. With instant clones, desktops are created when the user signs in and are provisioned and ready to use within seconds. When the user signs out, the desktop is destroyed. Instant clones allow for elastic capacity and rolling image upgrades. They support both floating and dedicated desktops.

One new feature of Horizon 2006 is a change to the Instant Clone provisioning model. In Horizon 7, Instant Clones relied on a tree of VMs, including a powered-on parent VM on each host in the cluster that all of the desktops are forked from. An additional deplopyment model is being added in Horizon 2006 that enables the benefits of Instant Clones without having to have that parent VM consuming resources on each host.

Other Components: The Horizon Suite includes a number of tools to provide administrators with a full-fledged ecosystem for managing their virtual end-user computing environments. These tools are App Volumes, Dynamic Environment Manager, and an on-premises version of Workspace ONE Access.

Horizon subscription licensing, including Horizon Universal Licensing, include the Horizon Service and it's associated cloud features including Cloud Monitoring Service, Image Management Service, and Universal Broker, and an entitlement to ControlUp for user experience monitoring. The Horizon subscription licensing SKUs are required for running Horizon on cloud-based SDDCs like VMware Cloud on AWS, Azure VMware Service, and Google Cloud VMware Engine. These licenses also allow customers to utilize Horizon Cloud on Azure and Horizon Cloud on IBM Cloud.

Virtual Desktop Design

Virtual desktop environments are all about the end user and what they need. So before you go shopping for storage arrays and servers, you need to start looking at your desktops.

Typically, when people think about desktop design, the first thing they think about is what provisioning engine they want to use. This is not the place to start. However, since this is one of the things that people want to know more about, I'll start by discussing the provisioning methods in Horizon.

There are four methods for provisioning desktops in Horizon 2006:

- Full Clone Desktops – Each desktop is a full virtual machine deployed from a template and managed as an independent virtual machine.
- Instant Clone Desktops – Instant Clone desktops are new to Horizon 7, and they are built off of the VMfork technology introduced with vSphere 6.0. Instant Clones are essentially a rapid clone of a running virtual machine with extremely fast customization.
- Remote Desktop Session Host Pools – Horizon 6 expanded RDSH support to include PCoIP support and application remoting. When RDSH desktops and/or application remoting are used, multiple users are logged into servers that host user sessions. This feature requires Windows Server 2008 R2 or Server 2012 R2 with the RDSH features enabled.
- Manually Provisioned Desktops – Manually provisioned desktops are desktop or published app resources that are provisioned outside of Horizon. These can be virtual machines that are managed by vCenter, or unmanaged physical or virtual machines.

I didn't mention Linked Clones here. While Linked Clones are still available in Horizon 8, they have been officially deprecated, and Composer is slated to be removed in a future release. Instant Clones are the replacement for Linked Clones, and they are available in all Horizon 8 SKUs. If you currently use Linked Clones, you will want to transition to Instant Clones, and if you are starting a new project, you should not consider Linked Clones if you are using Horizon 8.

Desktops are more than just how they are provisioned. There are also options for how the desktops get assigned to users.

There are two desktop assignment types for desktop pools:

- Dedicated Assignment – users are assigned to a particular desktop during their first login, and they will be logged into this desktop on all subsequent logins.
- Floating Assignment – users are temporarily assigned to a desktop on each login. On logout, the desktop will be available for other users to log into. A user may not get the same desktop on each login.

As I mentioned above, there is a lot more to desktop design than the provisioning and assignment method. It also involves the VM specifications, applications, peripherals, and other attributes of the desktop environment. In fact, these attributes may determine what provisioning methods are available to you.

Understanding Use Cases

When you design a virtual desktop environment, you have to design around the use cases. Use cases are the users, applications, peripherals, and how they are used to complete a task, and they are used to define many of the requirements in the environment. The requirements of the applications in the type of desktops that are used and how they are assigned to users.

Unless you have some overriding constraints or requirements imposed upon your virtual desktop project, the desktop design choices that you make will influence and/or drive your subsequent purchases. For instance, if you're building virtual desktops to support CAD users, blade servers aren't an option because high-end graphics cards will be needed, and if you want/need full clone desktops, you won't invest in a storage array that doesn't offer deduplication.

Other factors that may impact the use cases or the desktop design decisions include existing management tools, security policies, and other policies.

The Importance of Desktop Assessments

So how do you define your use cases? What information do you need, and how do you collect it?

The knowledge of who the users are collectively, the applications and peripherals they use, and how often they use them may exist in the organization, but there is a good chance that this information is tribal knowledge, outdated, and may be missing key details.

This is where desktop assessments come in. A desktop assessment is a process that gathers information about the environment to assist in defining use cases and sizing requirements for an environment.

The assessment starts by deploying an application in the environment. This typically consists of a server or virtual appliance that processes data and an agent that is deployed on endpoints. The tool runs for at least 30 days to gather information from a full business cycle.

When the assessment is complete, you will have detailed information about the application and resource usage, which will help determine the virtual desktop sizing and, later in the project, the physical infrastructure requirements.

Putting Together a High Level Design

Once you have determined your use cases, completed a desktop assessment and understand the impacts that these have on the desktop design, you'll be able to put together a design document with the following items:

- Use Case definition, which includes the applications, peripherals, and other aspects of the user environment.

The use case definitions will then determine other aspects of the environment, including:

- Desktop definition based on the assessment data
- Number of parent images that need to be managed
- Number and type of desktop pools
- Number of desktops per pool
- Number of Connection Servers and Unified Access Gateways that are required

If you're following the methodology that VMware uses in their design exams, your desktop design document should provide you with your conceptual and logical designs.

The conceptual and logical designs, built on details from the use cases, will influence the infrastructure design. This phase would cover the physical hardware to run the virtual desktop environment, the network layer, storage fabric, and other infrastructure services such as antivirus.

The desktop design document will have a heavy influence on the decisions that are made when selecting components to implement Horizon 7. The components that are selected need to support and enable the type of desktop environment that you want to run.

Before moving onto the next section, I want to reiterate the importance of doing a desktop assessment. The assessment will provide you with the information you need to properly design the environment, and it will avoid costly mistakes.

Traditionally, virtual desktops run Windows, and the servers that provide the virtual desktop infrastructure services also run on Windows. Because of the heavy reliance on Windows, Active Directory plays a huge role in Horizon environments. Even Linux desktops can be configured for Active Directory and utilize the Horizon user's AD credentials for Single Sign-On.

When you're planning a new Horizon deployment, or re-architecting an existing deployment, the design of your Active Directory environment is a critical element that needs to be considered. How you organize your virtual desktops, templates, and security groups impacts Group Policy, helpdesk delegation rights, and Horizon Instant Clones and RDSH.

Some Active Directory objects need to be configured before any Horizon components are installed. Some of these objects require special configuration either in Active Directory or inside vCenter. The Active Directory objects that need to be set up are:

- An organizational unit structure for Horizon Desktops and desktop templates
- Basic Group Policy Objects for the different organizational units
- An organization unit for Microsoft RDS servers if published apps or RDSH-desktops are deployed
- In large environments with multiple sites and/or trusted domains, ensure that sites and services are set up properly to enable Horizon to properly locate domain controllers

Optionally, you may want to set up an organizational unit for any security groups that might be used for entitling access to the Horizon desktop pools. This can be useful for organizing those groups and/or delegating access to Help Desk or other staff who don't need Account Operator or Domain Administrator rights.

Horizon and Active Directory

Before I talk about creating Organizational Unit structures and Group Policy, I want to start with Active Directory architecture and how Horizon utilizes Active Directory. I recently wrote about that here, so I won't go too deep into that topic. But I will recap a few things to keep in mind.

Horizon utilizes the DCLocator function that is built into the Windows Server NetLogon process. This process utilizes DNS to identify server locator records that correspond to the Active Directory site the server is located in.

Sites and Services need to be set up properly in multisite environments. This means that you need to create sites in AD Sites and Services, ensure that your subnets are mapped to the proper sites, and create site links for your replication topology so that Horizon can locate the closest domain controllers.

There are additional considerations around site naming when working in a multi-forest environment where domains are connected by a trust.

To learn more about Horizon and Active Directory, please see my deep dive post on the topic here.
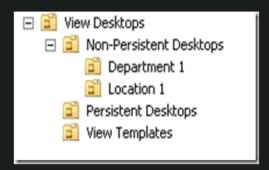
Creating an Organizational Unit Structure for Horizon Desktops

One of the first things that we need to plan and prepare before deploying desktops is an Active Directory organizational unit structure for Horizon desktops. This OU structure will hold all of the desktops created and used by Horizon.

A separate OU structure within your Active Directory environment is important because you will want to apply different group policies to your Horizon desktops than you would your regular desktops. There are also specific permissions that you will need to delegate to the Horizon Instant Clone Administrator service account.

Before I go into a method of organizing Active Directory, I want to make one thing clear. There is no one way to organize Active Directory for Horizon. These are guidelines that I like to follow because this organization makes sense to me. These guidelines should be modified to fit your environment and your business and technical requirements. There are a few things I highly recommend, though:

- A dedicated Organizational Unit tree for Virtual Deskops
- A dedicated Organizational Unit tree for RDSH Servers
- Creating new Group Policy Objects for virtual desktops and RDSH Servers instead of applying your standard desktop/server GPOs to these objects

My preferred organizational method looks like this:

View Desktops is a top-level OU (ie – one that sites in the root of the domain). I like to set up this OU for two reasons. One is that is completely segregates my VDI desktops from my non-VDI desktops and servers. The other is that it gives me one place to apply group policy that should apply to all VDI desktops.

I create three child OUs under the View Desktops OU to separate persistent desktops, non-persistent desktops, and desktop templates. This allows me to apply different group policies to the different types of desktops. For instance, you may want to disable Windows Updates and use Dynamic Environment Manager on non-persistent desktops but allow Windows Updates on the desktop templates or Persistent Desktops.

You don't need to create all three OUs. If your environment consists entirely of Persistent desktops, you don't need an OU for non-persistent desktops. The opposite is true as well. You may also choose to create more OUs depending on your organization. For instance, you may create OUs based business groups, regions or geography, or other ways.

Finally, I tend to create use-case specific OUs for pools that require additional Group Policy options above and beyond the top-level. These grandchild OUs are completely optional. If there is no need to set any custom policy for a specific use case, then they don't need to be created. However, if a grandchild OU is needed, then an entire pool will need to be created as desktop pools are assigned to OUs. Adding additional pools can add management overhead to a VDI environment.

I've found that there is less of a need for these use-case specific OUs as I've learned more about modern UEM tools like Dynamic Environment Manager. These tools can be a scalpel that allow administrators to dynamically apply context-aware policies and settings to specific users or groups without having to create additional pools or OUs for Group Policy configurations.

Creating an Organizational Unit for RDS Servers

RDSH servers need to be handled differently than virtual desktops. They're managed differently than your virtual desktops..

If application remoting or multi-user desktops are going to be deployed, an organizational unit for RDS servers should be created. This can be a child OU of a server organizational unit, but it may not be the best place.

If full clone or manually provisioned RDSH servers are being used, you may want to consider creating a maintenance OU. RDSH servers are often heavily locked down to block Windows Updates, software installers, and access to administrative tools and the command prompt through Group Policy. A maintenance OU would be an OU where these policies are not enforced, allowing admins access to these tools after a reboot to perform maintenance tasks.

One key thing to keep in mind is that server GPOs can be restrictive in some organizations, and they may conflict with applications or process that run in the RDSH server. If RDSH is new to your environment, it's important that the security and server teams understand that even though these are virtual machines running a server OS, they are being used like desktops to run applications. Less restrictive server policies may be required.

Horizon Group Policy Objects

Horizon contains a number of custom group policy objects that can be used for configuring the Horizon agent features and optimizing the PCoIP and Blast protocols. The templates are available in the Horizon Extras bundle on My VMware.
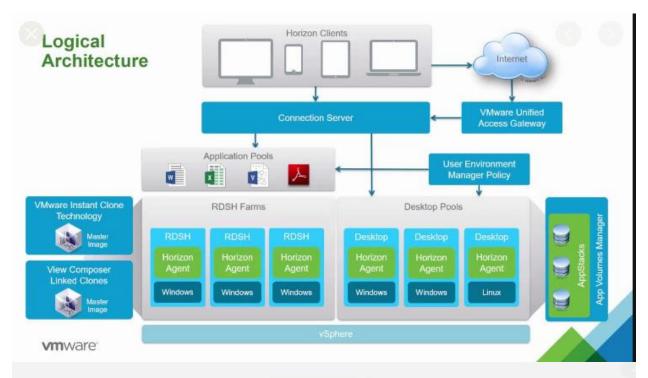
The templates are distributed in ADMX format, and they can be placed in the Group Policy Central Store.

Horizon Service Accounts

Horizon requires a service account for accessing vCenter to provision new virtual machines. If Instant Clones are used, a second service account will be needed to create computer accounts in Active Directory for managing computer accounts for the clones.

My lab infrastructure will be as follows:

1 Windows Server 2019 for Connection Server Standard – 6GB Memory	CONN1
1 Windows Server 2019 for Connection Server Replica – 6GB Memory	CONN2
1 Windows Server 2019 for Composer Server – 8GB Memory	COMP1
1 Windows 10 Enterprise version 2004 for VDI Clone Linked – Master – 3GB Memory	TEN01
1 Windows 10 Enterprise version 2004 for VDI Clone Instant – Master – 3GB Memory	TEN02
1 ESXi Host running vSphere 7	ESX7
1 vCenter Server Appliance 7	VC
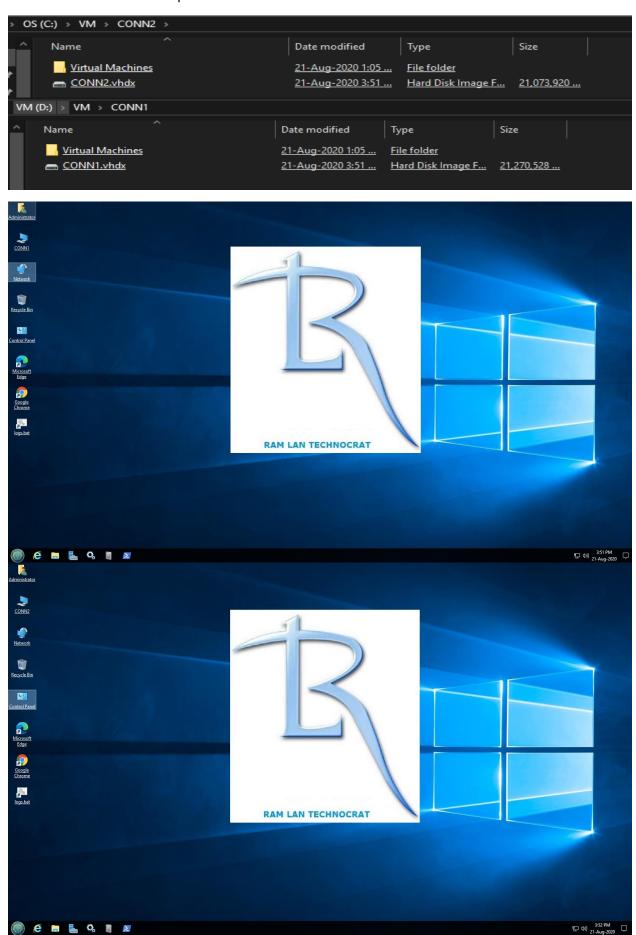
For above Virutal machines, I was able to sysprep and create templates out of it. Used the template to save time. Installed all the updates and restarted the servers and clients.

> OS (C:) > VM > CONN2 >

Name	Date modified	Type	Size
Virtual Machines	21-Aug-2020 1:05 ...	File folder	
CONN2.vhdx	21-Aug-2020 3:51 ...	Hard Disk Image F...	21,073,920 ...

VM (D:) > VM > CONN1

Name	Date modified	Type	Size
Virtual Machines	21-Aug-2020 1:05 ...	File folder	
CONN1.vhdx	21-Aug-2020 3:51 ...	Hard Disk Image F...	21,270,528 ...

Server Requirements – Connection and Composer:

Horizon Connection Server Hardware Requirements

Hardware Component	Required	Recommended
Processor	Pentium IV 2.0GHz processor or higher	4 CPUs
Network Adapter	100Mpbs NIC	1Gbps NICs
Memory	4GB RAM or higher	At least 10GB RAM for deployments of 50 or more remote desktops

The following operating systems support all Horizon Connection Server installation types, including standard, replica installations

Operating System	Editions Supported in Horizon 8 2006
Windows Server 2012 R2	Standard (64-bit) Datacenter (64-bit)
Windows Server 2016	Standard (64-bit) Datacenter (64-bit)
Windows Server 2019	Standard (64-bit) Datacenter (64-bit)

SQL Server 2019 is required for Composer to store database information

Client Requirements - Console:

Horizon Console is a web-based application that is installed when you install Connection Server. You can access and use Horizon Console with the following web browsers:

- Internet Explorer 11
- Firefox (latest versions)
- Chrome (latest versions)
- Safari (latest versions)
- Microsoft Edge (Windows 10)

Active Directory Requirements:

Configuring Domains and Trust Relationships
You must join each Connection Server host to an Active Directory domain. The host must not be a domain controller. [Read more]

Creating an OU for Remote Desktops
You should create an organizational unit (OU) specifically for your remote desktops. An OU is a subdivision in Active Directory that contains users, groups, computers, or other OUs. [Read more]

Creating OUs and Groups for Kiosk Mode Client Accounts
A client in kiosk mode is a thin client or a locked-down PC that runs the client software to connect to a Connection Server instance and launch a remote desktop session. If you configure clients in kiosk mode, you should create dedicated OUs and groups in Active Directory for kiosk mode client accounts. [Read more]

Creating Groups for Users
You should create groups for different types of users in Active Directory. For example, you can create a group called VMware HorizonUsers for your end users and another group called VMware Horizon Administrators for users that will administer remote desktops and applications. [Read more]

Creating a User Account for vCenter Server
You must create a user account in Active Directory to use with vCenter Server. You specify this user account when you add a vCenter Server instance in Horizon Console. [Read more]

Create a User Account for Instant-Clone Operations
Before you deploy instant clones, you must create a user account that has the permission to perform certain operations in Active Directory. [Read more]

Configure the Restricted Groups Policy
To be able to connect to a remote desktop, users must belong to the local Remote Desktop Users group of the remote desktop. You can use the Restricted Groups policy in Active Directory to add users or groups to the local Remote Desktop Users group of every remote desktop that is joined to your domain. [Read more]

Using VMware Horizon Group Policy Administrative Template Files
VMware Horizon includes several component-specific group policy administrative (ADMX) template files. [Read more]

Prepare Active Directory for Smart Card Authentication
You might need to perform certain tasks in Active Directory when you implement smart card authentication. [Read more]

Disable Weak Ciphers in SSL/TLS
To achieve greater security, you can configure the domain policy group policy object (GPO) to ensure that Windows-based machines running Horizon Agent do not use weak ciphers when they communicate by using the TLS protocol. [Read more]
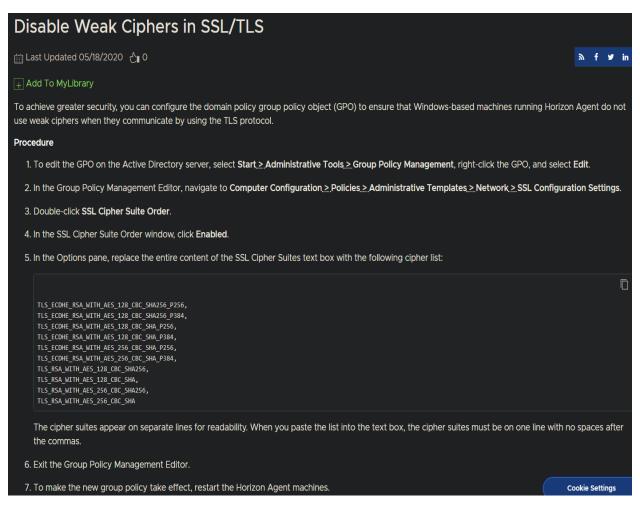
Lab OU Layout
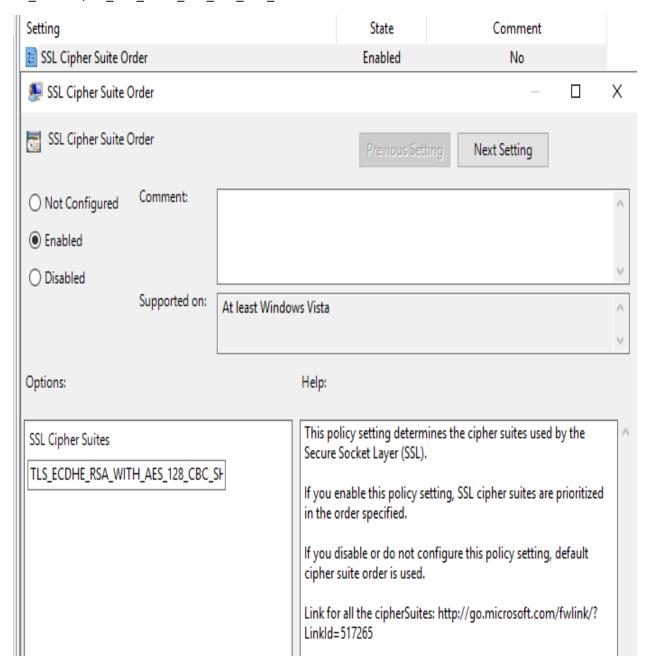
Check this link for more info - https://docs.vmware.com/en/VMware-Horizon/2006/horizon-installation/GUID-37D39B4F-5870-4188-8B11-B6C41AE9133C.html

Disable Weak Ciphers in SSL/TLS

Disable Weak Ciphers in SSL/TLS

Last Updated 05/18/2020 👍 0

➕ Add To MyLibrary

To achieve greater security, you can configure the domain policy group policy object (GPO) to ensure that Windows-based machines running Horizon Agent do not use weak ciphers when they communicate by using the TLS protocol.

Procedure

1. To edit the GPO on the Active Directory server, select **Start > Administrative Tools > Group Policy Management**, right-click the GPO, and select **Edit**.

2. In the Group Policy Management Editor, navigate to **Computer Configuration > Policies > Administrative Templates > Network > SSL Configuration Settings**.

3. Double-click **SSL Cipher Suite Order**.

4. In the SSL Cipher Suite Order window, click **Enabled**.

5. In the Options pane, replace the entire content of the SSL Cipher Suites text box with the following cipher list:

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA
```

The cipher suites appear on separate lines for readability. When you paste the list into the text box, the cipher suites must be on one line with no spaces after the commas.

6. Exit the Group Policy Management Editor.

7. To make the new group policy take effect, restart the Horizon Agent machines.

Cookie Settings

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA

Setting	State	Comment
SSL Cipher Suite Order	Enabled	No

SSL Cipher Suite Order — □ X

SSL Cipher Suite Order

Previous Setting   Next Setting

○ Not Configured   Comment:

◉ Enabled

○ Disabled

Supported on: At least Windows Vista

Options: Help:

SSL Cipher Suites

TLS_ECDHE_RSA_WITH_AES_128_CBC_SH

This policy setting determines the cipher suites used by the Secure Socket Layer (SSL).

If you enable this policy setting, SSL cipher suites are prioritized in the order specified.

If you disable or do not configure this policy setting, default cipher suite order is used.

Link for all the cipherSuites: http://go.microsoft.com/fwlink/?LinkId=517265

SSL Certificate:

You can select one of the options from below:

1. Purchase cheap SSL certificate
2. Create self signed SSL through internal Certificate Authority
3. Use Let's Encrypt to get FREE SSL certificate – **Will provide install steps later….**

I will list the steps for each of them, so you can use that suits your requirement.

Cheap SSL Certificate – 3rd Party – Create Certificate request and submit to get valid SSL Certificate from Cheapsslshop.com. The cost for one year SSL certificate is US$5 (C$7.50).

1. On your Windows desktop click **Start**, and in the search box type **mmc**
2. Click the **mmc.exe** icon
3. Go to **File** > **Add/Remove Snap-in**, and then click on **Certificates** > **Add** > **OK**
4. Now, select **Computer account** and click **Next**
5. Make sure the Local Computer is selected then hit **Finish** and **OK**
6. Next, under **Local Computer** expand the **Certificates** tree
7. Right-click Personal, then click the following sequences: **Select All Tasks** > **Advanced Operations** > **Create Custom Request**
8. In the **Certificate Enrollment** window click **Next**
9. Select the option **Proceed without enrolment policy** and hit **Next**
10. In the **Custom Request** window, from the drop-down list select **(No Template) Legacy Key**
11. Select the **PKCS#10** (Certification Request Standard) and click **Next**
12. In the **Certificate Information** window, click on the arrow next to **Details** and select **Prope**
13. In the **General** tab, in the **Friendly name** field, enter **vdm**

Certificate Properties ✕

General | **Subject** | Extensions | Private Key

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate
The user or computer that is receiving the certificate

Subject name:

Type:
| Email ⌄ |

Value:
| |

[Add >]
[< Remove]

| CN=ramlan.ca ▲ |
| **C=CA** |
| L=TORONTO |
| O=RAMLAN INC. |
| OU=I T |
| S=ONTARIO ▼ |
| Street= 275 SHUTER ST |

Alternative name:

Type:
| DNS ⌄ |

Value:
| |

[Add >]
[< Remove]

| DNS |
| **conn1.ramlan.ca** |

[OK] [Cancel] [Apply]

Certificate Properties ✕

General | Subject | Extensions | **Private Key**

| Cryptographic Service Provider ⌄ |

| **Key options** ⌃ |

Set the key length and export options for the private key.

Key size: | 2048 ⌄ |

☑ Make private key exportable

☐ Allow private key to be archived

☐ Strong private key protection

| Key type ⌄ |

| Key permissions ⌄ |

[OK] [Cancel] [Apply]

Certificate Information

Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

☑ Custom request   ⓘ **STATUS:** Available   Details ⌃

The following options describe the uses and validity period that apply to this type of certificate:
- Key usage:
- Application policies:
- Validity period (days):

[Properties]

[Next] [Cancel]

Save As

CONN1 > Documents

Organize ▼   New folder

Name	Date modified	Type	Size
No items match your search.			

Quick access
- Desktop
- Downloads
- Documents
- Pictures

CONN1

Network

File name: certreq

Save as type: Request Files (*.req)

∧ Hide Folders   [Save] [Cancel]

🖳 Certificate Enrollment

Where do you want to save the offline request?

If you want to save a copy of your certificate request or want to process the request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish.

File Name:

C:\Users\ADMINISTRATOR.RAMLAN\Documents\certreq   [Browse...]

File format:
- ◉ Base 64
- ○ Binary

[Finish] [Cancel]

📄 certreq - Notepad

File   Edit   Format   View   Help

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEDTCCAvUCAQAwgZ8xHDAaBgkqhkiG9w0BCQEWDVJBTUBSQU1MQU4uQ0ExFjAU
BgNVBAkMDTI3NSBTSFVURVIgU1QxEDAOBgNVBAgMB09OVEFSSU8xDDAKBgNVBAsM
A0kgVDEUMBIGA1UECgwLUkFNTEFOIE1OQy4xEDAOBgNVBAcMB1RPUk9OVE8xCzAJ
BgNVBAYTAkNBMRIwEAYDVQQDDA1yYW1sYW4uY2EwggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQDXOGcBfAi/InS1aXSlPzwA9arb5TsVCU1jMXBG5sJwPUBn
ocOXV4bl6lJ8rl/HCU0KUvTmtK6B/isEaS2/+1TcrGkj4ikgCQHcdV3A4afeAytl
tquuxMPX+urB7NJyMJsxo2N6vyY4JcUtna6zaVzt5SEl8v5y5q86b+5X5UOWyW+z
inLoi4s66uokjTzUUw8D29DW+azQYWIfbHEeoEbaAdCFJuZNVVztzmkTUDpogdY/
0v7njurtviyu2QGwEc+GlcSgxP2m2FtKm6Z5vCRyh8PcjaXTnJ/03Xq4vncZuxlJ
LWV/4A/UFZVNM5z1gUTTbAqvwJVhYwM75M4TbeQlAgMBAAGgggEmMBwGCisGAQQB
gjcNAgMxDhYMMTAuMC4xNzc2My4yMEIGCSsGAQQBgjcVFDE1MDMCAQUMD0NPTTk4x
LlJBTUxBTi5DQQwUUkFNTEFOXEFkbWluaXN0cmF0b3I1NQy5FWEUwWgYJKoZI
hvcNAQkOMU0wSzAaBgNVHREEEzARgg9jb25uMS5yYW1sYW4uY2EwHQYDVR0OBBYE
FHy/fYkBe0BOkT1Zn5t6vsF+XpPBMA4GA1UdDwEB/wQEAwIHgDBmBgorBgEEAYI3
DQICMVgwVgIBAh5OAE0AaQBjAHIAbwBzAG8AZgB0ACAAUwB0AHIAbwBuAGcAIABD
AHIAeQBwAHQAbwBnAHIAYQBwAGgAaQBjACAAUAByAG8AdgBpAGQAQZQByAwEAMA0G
CSqGSIb3DQEBBQUAA4IBAQBGn5JtWOc6tSC+Xf32pijNy2081mcenwjsFQEGverJ
wVziHl0y2g8Sr54gp5ijEjtHQKk9K9JMVu+HO6BbFufHiuEDLwJISTR/z+ywtoE9
Jn2EqckWtLm5JXG7wQuW+ZfZSIH22uqxccZFA00fE34naFRu/bCUkw8yjJyV/Ht7
DCgo+iC4eBnnbK02IgjhW1P13wjL7BS3haGa3DVb1cSC4QyhmtGtOiZRb8zBLanR
QFM9whk5AClYbcT/5Yc/sNRupUx3grxx6JcjQ14iIsvgxFS3Mm/9gTU21eoV7qr3
0MTAcxE1xUE+PSkFBkfqAX71gn0nbJAsUmt1vSFGXPCf
-----END NEW CERTIFICATE REQUEST-----

Internal Certificate Authority:

1. Logon to your Microsoft root CA. In this case I'm using Windows Server 2019. Launch the Certification Authority console.

Properties of New Template ✕

Subject Name	Server	Issuance Requirements

Superseded Templates		Extensions		Security

Compatibility	General	Request Handling	Cryptography	Key Attestation

Template display name:

VMWARESSL ⬅

Template name:

VMWARESSL

Validity period: Renewal period:

5 years ▾   6 weeks ▾

☐ Publish certificate in Active Directory

   ☐ Do not automatically reenroll if a duplicate certificate exists in Active
      Directory

OK	Cancel	Apply	Help

Properties of New Template ✕

Subject Name	Server	Issuance Requirements

Compatibility	General	Request Handling	Cryptography	Key Attestation

Superseded Templates		Extensions		Security

To modify an extension, select it, and then click Edit.

Extensions included in this template:

- 🔲 Application Policies ⬅
- 🔲 Basic Constraints
- 🔲 Certificate Template Information
- 🔲 Issuance Policies
- ⚠ Key Usage

➡   Edit...

Description of Application Policies:

Server Authentication

OK	Cancel	Apply	Help

Edit Application Policies Extension ✕

An application policy defines how a certificate can be used.

Application policies:

Server Authentication

[Add...] [Edit...] [Remove]

☐ Make this extension critical

[OK] [Cancel]

Add Application Policy ✕

An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

Application policies:

Any Purpose
Attestation Identity Key Certificate
Certificate Request Agent
Client Authentication
Code Signing
CTL Usage
Digital Rights
Directory Service Email Replication
Disallowed List
Document Encryption
Document Signing
Domain Name System (DNS) Server Trust
Dynamic Code Generator

[New...]

[OK] [Cancel]

Edit Application Policies Extension ✕

An application policy defines how a certificate can be used.

Application policies:

Client Authentication
Server Authentication

[Add...] [Edit...] [Remove]

☐ Make this extension critical

[OK] [Cancel]

Edit Key Usage Extension   ✕

Specify the required signature and security options for a key usage extension.

Signature
- ☑ Digital signature
- ☐ Signature is proof of origin (nonrepudiation)
- ☐ Certificate signing
- ☐ CRL signing

Encryption
- ◯ Allow key exchange without key encryption (key agreement)
- ◉ Allow key exchange only with key encryption (key encipherment)
  - ☑ Allow encryption of user data

☑ Make this extension critical

➤ [OK]   [Cancel]

Properties of New Template   ✕

Subject Name	Server	Issuance Requirements

Compatibility	General	Request Handling	Cryptography	Key Attestation

Superseded Templates	Extensions	Security

To modify an extension, select it, and then click Edit.

Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

[Edit...]

Description of Key Usage:

Signature requirements:
Digital signature

Allow key exchange only with key encryption
Allow encryption of user data
Critical extension.

➤ [OK]   [Cancel]   [Apply]   [Help]

Now we will issue the certificate

Now we have the certificate listed which can be used later. Make sure to check certificate security settings for Read, Write, Enroll and Auto Enroll.

Login to Connection Server – Click Run – MMC – Click Add Snap In – Select Certificates – Local Computer – OK
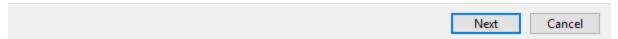
Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:
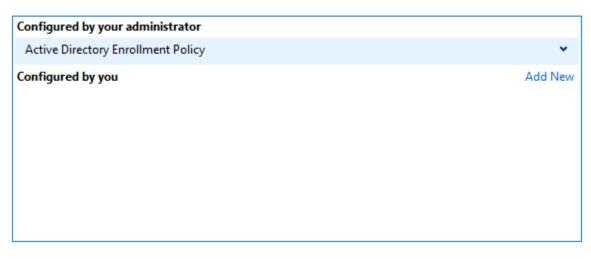
Your computer is connected to the network
You have credentials that can be used to verify your right to obtain the certificate

Next   Cancel

Select Certificate Enrollment Policy
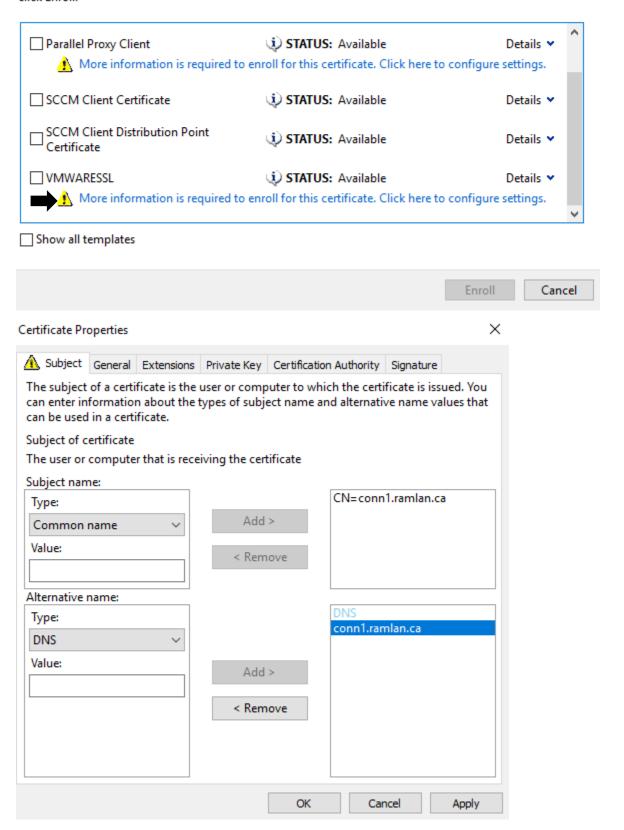
Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator

Active Directory Enrollment Policy   ⌄

Configured by you   Add New

Next   Cancel

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

☐ Parallel Proxy Client   ⓘ **STATUS:** Available   Details ⌄
    ⚠ More information is required to enroll for this certificate. Click here to configure settings.

☐ SCCM Client Certificate   ⓘ **STATUS:** Available   Details ⌄

☐ SCCM Client Distribution Point Certificate   ⓘ **STATUS:** Available   Details ⌄

☐ VMWARESSL   ⓘ **STATUS:** Available   Details ⌄
➡ ⚠ More information is required to enroll for this certificate. Click here to configure settings.

☐ Show all templates

[Enroll]   [Cancel]

Certificate Properties ✕

⚠ Subject | General | Extensions | Private Key | Certification Authority | Signature

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate
The user or computer that is receiving the certificate

Subject name:

Type:
[Common name ⌄]

Value:
[   ]

[Add >]

[< Remove]

CN=conn1.ramlan.ca

Alternative name:

Type:
[DNS ⌄]

Value:
[   ]

[Add >]

[< Remove]

DNS
conn1.ramlan.ca

[OK]   [Cancel]   [Apply]

Certificate Properties

⚠ Subject | General | Extensions | Private Key | Certification Authority | Signature

A friendly name and description will make it easier to identify and use a certificate.

Friendly name:

vdm

Description:

OK | Cancel | Apply

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

☐ Computer   ⓘ **STATUS:** Available   Details ⌄

☐ Parallel Proxy Client   ⓘ **STATUS:** Available   Details ⌄
    ⚠ More information is required to enroll for this certificate. Click here to configure settings.

☐ SCCM Client Certificate   ⓘ **STATUS:** Available   Details ⌄

☐ SCCM Client Distribution Point Certificate   ⓘ **STATUS:** Available   Details ⌄

☑ VMWARESSL   ⓘ **STATUS:** Available   Details ⌄

☐ Show all templates

Enroll | Cancel

Certificate Installation Results

The following certificates have been enrolled and installed on this computer.

Active Directory Enrollment Policy		
☑ VMWARESSL	✔ STATUS: Succeeded	Details ⌄

[green progress bar]

Finish

We will export the certificate so we can import to Trusted Root Store as well.

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

File   Action   View   Favorites   Window   Help

Console Root	Issued To	Issued By	Expiration Date	
Certificates (Local Computer)	3ed7dd77-4c23-416a-b005-f01d...	MS-Organization-Access	21-Aug-2030	
Personal	3ed7dd77-4c23-416a-b005-f01d...	MS-Organization-P2P-Access [20...	26-Aug-2020	
Certificates	CONN1.RAMLAN.CA	RAMLAN-DC-CA	21-Aug-2022	
Trusted Root Certification Authorities	conn1.ramlan.	RAMLAN-DC-CA	25-Aug-2022	
Enterprise Trust				
Intermediate Certification Authorities				
Trusted Publishers				
Untrusted Certificates				
Third-Party Root Certification Author				
Trusted People				
Client Authentication Issuers				
Preview Build Roots				
Test Roots				
AAD Token Issuer				

Right-click context menu:
- Open
- All Tasks →
  - Open
  - Request Certificate with New Key...
  - Renew Certificate with New Key...
  - Manage Private Keys...
  - Advanced Operations →
  - Export...
- Cut
- Copy
- Delete
- Properties
- Help

Certificate Export Wizard

Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Next   Cancel

Certificate Export Wizard

Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

◉ Yes, export the private key

◯ No, do not export the private key

[Next] [Cancel]

Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

◯ DER encoded binary X.509 (.CER)

◯ Base-64 encoded X.509 (.CER)

◯ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

☐ Include all certificates in the certification path if possible

◉ Personal Information Exchange - PKCS #12 (.PFX)

☑ Include all certificates in the certification path if possible

☐ Delete the private key if the export is successful

☐ Export all extended properties

☑ Enable certificate privacy

◯ Microsoft Serialized Certificate Store (.SST)

[Next] [Cancel]

Certificate Export Wizard

Security

To maintain security, you must protect the private key to a security principal or by using a password.

☐ Group or user names (recommended)

[Add]

[Remove]

☑ Password:

●●●●●●●●●

Confirm password:

●●●●●●●●●|

Encryption: TripleDES-SHA1 ▼

[Next] [Cancel]

← **Certificate Export Wizard**

File to Export

Specify the name of the file you want to export

File name:

C:\Users\ADMINISTRATOR.RAMLAN\Documents\vmware.pfx   [Browse...]

[Next] [Cancel]

Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\ADMINISTRATOR.RAMLAN\D
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Personal Information Exchange (*.pfx)

Finish   Cancel

Certificate Export Wizard   ✕

The export was successful.

OK

Once you have the file, you will need to import the certificate into Trusted Root Certification Authorities.

We will install Connection Server now (CONN1.RAMLAN.CA).

Name	Date modified	Type	Size
01 VMware-Horizon-Connection-Server-x86_64-8.0.0-16592062.exe	18-Aug-2020 1:29 ...	Application	310,518 KB

CONN1 > Downloads

Search Download

VMware Horizon Connection Server

vmware

VMware Horizon®

Welcome to the Installation Wizard for VMware Horizon Connection Server

The installation wizard will install VMware Horizon Connection Server on your computer. To continue, click Next.

Copyright (c) 1998-2020 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

Product version: 2006

< Back   Next >   Cancel

VMware Horizon Connection Server

License Agreement

Please read the following license agreement carefully.

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS

● I accept the terms in the license agreement
○ I do not accept the terms in the license agreement

< Back   Next >   Cancel

VMware Horizon Connection Server

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install VMware Horizon Connection Server to:

C:\Program Files\VMware\VMware View\Server\

[Change...]

[< Back] [Next >] [Cancel]

VMware Horizon Connection Server

Installation Options

Select the type of Horizon Connection Server instance you want to install.

Select the type of Horizon Connection Server instance you want to install.

Horizon Standard Server
Horizon Replica Server
Horizon Enrollment Server

☑ Install HTML Access

Perform a standard full install. This is used to install a standalone instance of Horizon Connection Server or the first instance of a group of servers.

Specify what IP protocol version shall be used to configure this Horizon Connection Server instance:

IPv4
IPv6

This server will be configured to choose the IPv4 protocol for establishing all connections.

[< Back] [Next >] [Cancel]

At this point, I was getting this error.

TCP port 80 is already in use. This port needs to be available for this product to be installed. Please remove any software that may be using this port and then try again.

[OK]

It is an easy fix – Stop Branch Cache service and continue with the install.

BranchCache   This service ...   Automatic   Network S...

VMware Horizon Connection Server

Data Recovery

Enter data recovery password details.

This password protects data backups of your Horizon Connection Server. Recovering a backup will require entry of this password.

Enter data recovery password:

`••••••••`

Re-enter password:

`••••••••`

Enter password reminder (optional):

`first month`

< Back	Next >	Cancel

VMware Horizon Connection Server

Firewall Configuration

Automatically configure the Windows Firewall to allow incoming TCP protocol connections.

In order for Horizon Connection Server to operate on a network, specific incoming TCP ports must be allowed through the local Windows Firewall service. The incoming TCP ports for the Standard Server are 8009 (AJP13), 80 (HTTP), 443 (HTTPS), 4001 (JMS), 4002 (JMS-SSL), 4100 (JMSIR), 4101 (JMSIR-SSL), 4172 (PCoIP), 8472 (Inter-pod API), and 8443 (HTML Access). UDP packets on port 4172 (PCoIP) are allowed through as well.

◉ Configure Windows Firewall automatically

○ Do not configure Windows Firewall

< Back	Next >	Cancel

VMware Horizon Connection Server

Initial Horizon Administrators

Specify the domain user or group for initial Horizon administration.

To login to Horizon Administrator, you will need to be authorized. Select the local Administrators group option or enter the name of a domain user or group that will be initially allowed to login and will be granted full admistrative rights.

The list of authorized administrator users and groups can be changed later in Horizon Administrator.

○ Authorize the local Administrators group

◉ Authorize a specific domain user or domain group

`RAMLAN\HorizonAdmins`

(domainname\username, domainname\groupname or UPN format)

< Back	Next >	Cancel

VMware Horizon Connection Server

User Experience Improvement Program

Basic Customer Demographics

VMware's Customer Experience Improvement Program ("CEIP") provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products.

Learn More

☑ Join the VMware Customer Experience Improvement Program

Select your organization industry type:

Business Services ⌄

Select location of your organization's headquarter:

America, North ⌄

Select approximate number of employees:

1-100 ⌄

< Back   Next >   Cancel

VMware Horizon Connection Server

Ready to Install the Program

The wizard is ready to begin installation.

VMware Horizon Connection Server will be installed in:

C:\Program Files\VMware\VMware View\Server\

Please select where you will deploy the Horizon connection server. Select General if none of the other types apply. Note that you cannot change the deployment location of the connection server after the installation is completed.

General ⌄

| General |
| AWS |
| Dell EMC |
| Azure |
| Google Cloud |
| Oracle Cloud |

ncel to exit the wizard.

< Back   Install   Cancel

VMware Horizon Connection Server

vmware

Installer Completed

The installer has successfully installed VMware Horizon Connection Server. Click Finish to exit the wizard.

Next Steps:

☑ Show the documentation

WARNING: Due to limited memory available on this system, the Horizon components have been configured to use reduced resources. Please refer to the Horizon View administration guides to determine how to correctly size this system.

VMware Horizon®

Product version: 2006

< Back   Finish   Cancel

Now we have to do the same on replica server (CONN2.RAMLAN.CA)

CONN2 > Downloads

Name	Date modified	Type	Size
01 VMware-Horizon-Connection-Server-x86_64-8.0.0-16592062.exe	18-Aug-2020 1:29 ...	Application	310,518 KB

VMware Horizon Connection Server

Welcome to the Installation Wizard for VMware Horizon Connection Server

The installation wizard will install VMware Horizon Connection Server on your computer. To continue, click Next.

Copyright (c) 1998-2020 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

VMware Horizon®

Product version: 2006

< Back   Next >   Cancel

VMware Horizon Connection Server

License Agreement

Please read the following license agreement carefully.

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS

⦿ I accept the terms in the license agreement
◯ I do not accept the terms in the license agreement

< Back   Next >   Cancel

VMware Horizon Connection Server

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install VMware Horizon Connection Server to:

C:\Program Files\VMware\VMware View\Server\

[Change...]

[< Back] [Next >] [Cancel]

VMware Horizon Connection Server

Installation Options

Select the type of Horizon Connection Server instance you want to install.

Select the type of Horizon Connection Server instance you want to install.

```
Horizon Standard Server
Horizon Replica Server
Horizon Enrollment Server
```

☑ Install HTML Access

Perform a replica instance install joining an existing server instance. This is used to install a second or subsequent server in a group of servers that all automatically share the same directory configuration.

Specify what IP protocol version shall be used to configure this Horizon Connection Server instance:

```
IPv4
IPv6
```

This server will be configured to choose the IPv4 protocol for establishing all connections.

[< Back] [Next >] [Cancel]

VMware Horizon Connection Server

Source Server

Select an existing Horizon Connection Server instance from which to replicate.

A group of Horizon Connection Server instances that share the same configuration data is called a Horizon Connection Server group. Setup will replicate configuration data from an existing server instance.

Enter the server name of an existing Horizon Connection Server instance to make this server part of that group.

Example server: view.internal.vmware.com.

Server: `CONN1.RAMLAN.CA` (hostname or IP address)

[< Back] [Next >] [Cancel]

VMware Horizon Connection Server   ✕

⚠ The currently logged on user does not have sufficient privileges on the Connection Server CONN1.RAMLAN.CA to be able to configure replication.

The currently logged on user account needs to have full Administrator rights in Horizon. If you are using a local administrator account on this server then the same named account with the same password needs to exist on the remote server. This account also needs to be a member of the local administrators group on the remote server, and the local Administrators group needs to have Administrator rights in Horizon.
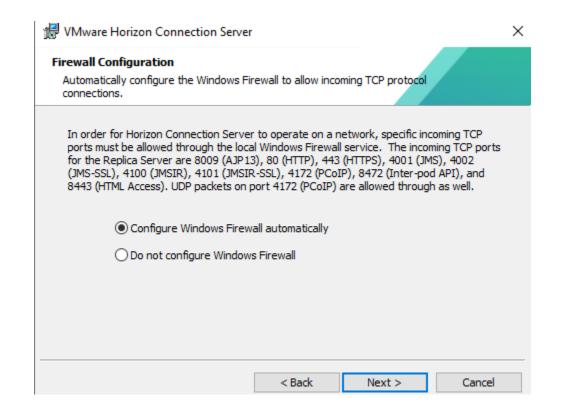
Alternatively, perform this installation using a domain account and ensure the user account or group has Administrator rights in Horizon.
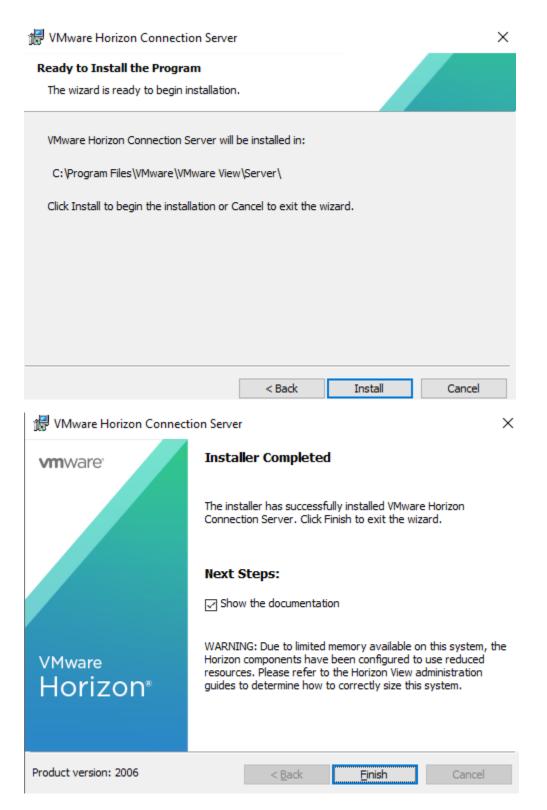
If Horizon rights have been granted by an update to your domain group membership since you logged in, you will need to log in again before attempting this installation again.

<div align="right">

OK

</div>

If you get above error – check local administrators' group. I did the following

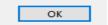| CONN1.RAMLAN.CA	CONN2.RAMLAN.CA
Administrators Properties	**Administrators Properties**
General	General
Administrators	Administrators
Description: Administrators to the compute	Description: Administrators to the compute
Members:	Members:
Administrator	Administrator
RAMLAN\Administrator	RAMLAN\Administrator
RAMLAN\CONN2	RAMLAN\CONN1
RAMLAN\Domain Admins	RAMLAN\Domain Admins
RAMLAN\HorizonAdmins	RAMLAN\HorizonAdmins

🎫 VMware Horizon Connection Server   ✕

Firewall Configuration
Automatically configure the Windows Firewall to allow incoming TCP protocol connections.

In order for Horizon Connection Server to operate on a network, specific incoming TCP ports must be allowed through the local Windows Firewall service. The incoming TCP ports for the Replica Server are 8009 (AJP13), 80 (HTTP), 443 (HTTPS), 4001 (JMS), 4002 (JMS-SSL), 4100 (JMSIR), 4101 (JMSIR-SSL), 4172 (PCoIP), 8472 (Inter-pod API), and 8443 (HTML Access). UDP packets on port 4172 (PCoIP) are allowed through as well.

◉ Configure Windows Firewall automatically

○ Do not configure Windows Firewall

< Back	Next >	Cancel

With this we have completed Connection Server install. The next install will be Composer on Windows Server 2019 virtual machine.

VMware Horizon® - Internet Explorer

https://localhost/admin/#/login

VMware Horizon®

VMware Horizon®

Version 2006

User Name

Password

RAMLAN

☐ Remember user name

Sign in

vmware

© 2020 VMware, Inc

✕
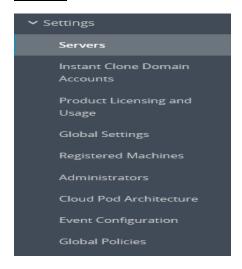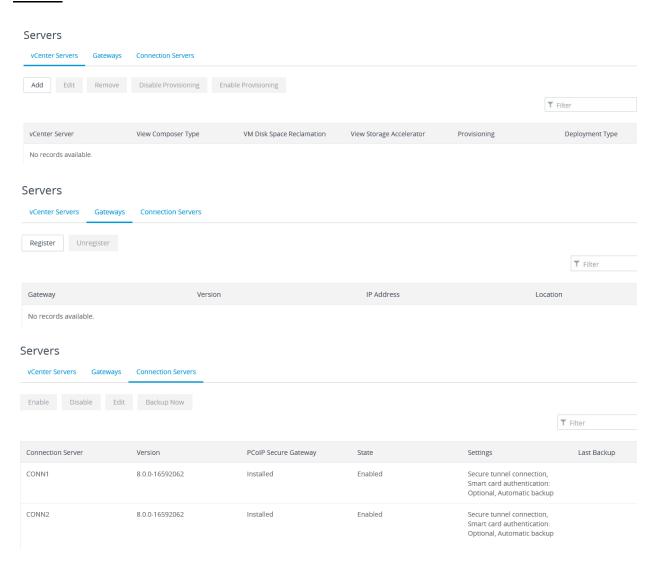
For the best experience, use a modern browser such as Google Chrome, Microsoft Edge, Firefox, or Safari.

Chrome   Edge   Firefox   Safari

Settings:

∨ Settings

Servers

Instant Clone Domain Accounts

Product Licensing and Usage

Global Settings

Registered Machines

Administrators

Cloud Pod Architecture

Event Configuration

Global Policies

Servers:

Servers

vCenter Servers | Gateways | Connection Servers

| Add | Edit | Remove | Disable Provisioning | Enable Provisioning |

▼ Filter

vCenter Server	View Composer Type	VM Disk Space Reclamation	View Storage Accelerator	Provisioning	Deployment Type
No records available.					

Servers

vCenter Servers | **Gateways** | Connection Servers

| Register | Unregister |

▼ Filter

Gateway	Version	IP Address	Location
No records available.			

Servers

vCenter Servers | Gateways | **Connection Servers**

| Enable | Disable | Edit | Backup Now |

▼ Filter

Connection Server	Version	PCoIP Secure Gateway	State	Settings	Last Backup
CONN1	8.0.0-16592062	Installed	Enabled	Secure tunnel connection, Smart card authentication: Optional, Automatic backup	
CONN2	8.0.0-16592062	Installed	Enabled	Secure tunnel connection, Smart card authentication: Optional, Automatic backup	

Product Licensing and Usage:

Licensing and Usage

Licensing   Usage   Customer Experience Program

Edit License

Licensing and Usage

Licensing   **Usage**   Customer Experience Program

[Reset Highest Count]   [Reset Named Users Count]

Session Mode	Current	Highest
Total Concurrent Connections	0	0
Total Named Users	1	N/A
Detailed Connection Breakdown		
Total Remote	0	0
Active - full virtual machines	0	0
Active - linked clone	0	0
Active - other machine sources	0	0
Active - applications	0	0
Active - collaboration sessions	0	0
Active - total collaborators	0	0

Licensing and Usage

Licensing   Usage   **Customer Experience Program**

[Edit Settings]

Customer Experience Improvement Program	Enabled
Geographic Location	America, North
Business Vertical	Business Services
Number of Employees	1-100

Global Settings:

Global Settings

General Settings   Security Settings   Client Restriction Settings

[Edit]

View Administrator Session Timeout **10 minutes**	Forcibly Disconnect Users **600 minutes**
Single Sign-On (SSO) **Enabled**	Auto Update **Disabled**

Client-Dependent Settings
Clients that Support Applications

Disconnect Applications and Discard SSO Credentials for Idle Users
Never

Other Clients

Discard SSO Credentials
15 minutes

Pre-Login Message **No**	Display Warning Before Forced Logoff **Yes**
Enable Windows Server Desktops **No**	Clean Up Credential When Tab Closed for HTML Access **No**
Hide Server Information in Client User Interface **No**	Hide Domain List in Client User Interface **Yes**
Send Domain List **No**	Enable 2 Factor Reauthentication **No**
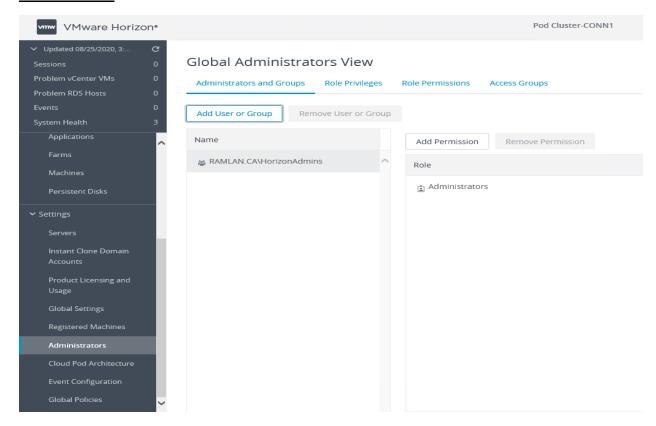
Global Settings

General Settings   **Security Settings**   Client Restriction Settings

Edit   Change Data Recovery Password

Reauthenticate Secure Tunnel Connections After Network Interruption
No

Message Security Mode
Enhanced

Enhanced Security Status
Enhanced

Global Settings

General Settings   Security Settings   **Client Restriction Settings**

Edit
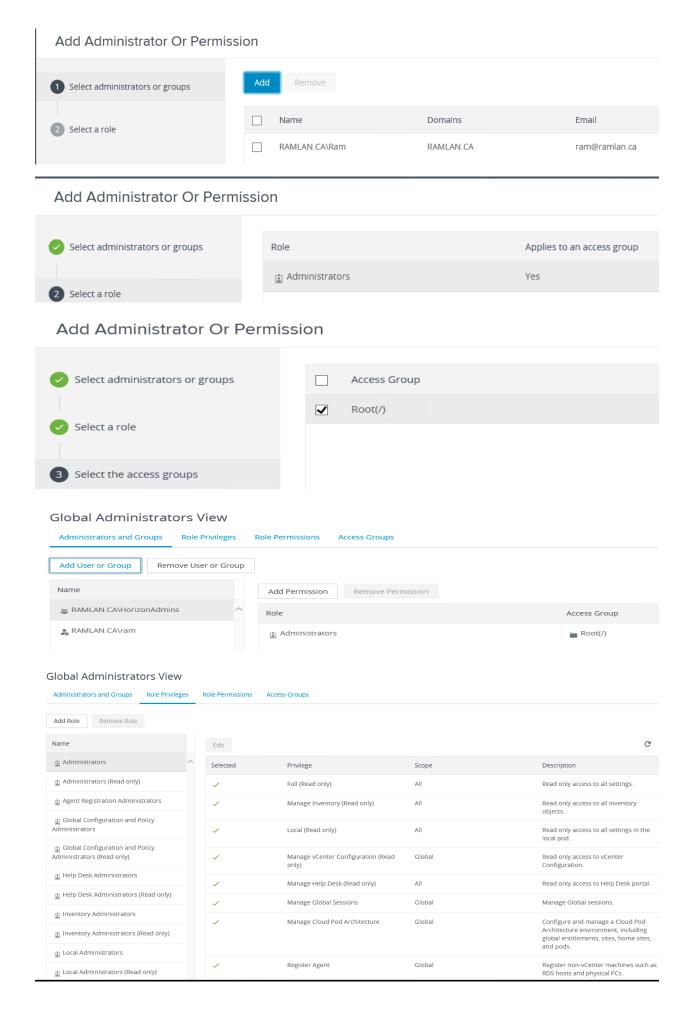
No Horizon Client restrictions have been configured. Click Edit to configure.

Administrators:

VMware Horizon®	Pod Cluster-CONN1

∨ Updated 08/25/2020, 3:... ⟳

Sessions	0
Problem vCenter VMs	0
Problem RDS Hosts	0
Events	0
System Health	3

Applications
Farms
Machines
Persistent Disks

∨ Settings

Servers
Instant Clone Domain Accounts
Product Licensing and Usage
Global Settings
Registered Machines
Administrators
Cloud Pod Architecture
Event Configuration
Global Policies

Global Administrators View

Administrators and Groups   Role Privileges   Role Permissions   Access Groups

Add User or Group   Remove User or Group

Name
👥 RAMLAN.CA\HorizonAdmins

Add Permission   Remove Permission

Role
👤 Administrators

Add Administrator Or Permission

| 1 | Select administrators or groups |
| 2 | Select a role |

Add   Remove

	Name	Domains	Email
☐	RAMLAN.CA\Ram	RAMLAN.CA	ram@ramlan.ca

Add Administrator Or Permission

| ✓ | Select administrators or groups |
| 2 | Select a role |

Role	Applies to an access group
🔲 Administrators	Yes

Add Administrator Or Permission

✓	Select administrators or groups
✓	Select a role
3	Select the access groups

	Access Group
☐	Access Group
☑	Root(/)

Global Administrators View

Administrators and Groups   Role Privileges   Role Permissions   Access Groups

Add User or Group   Remove User or Group

Name
👥 RAMLAN.CA\HorizonAdmins
👤 RAMLAN.CA\ram

Add Permission   Remove Permission

Role	Access Group
🔲 Administrators	📁 Root(/)

Global Administrators View

Administrators and Groups   **Role Privileges**   Role Permissions   Access Groups

Add Role   Remove Role

Name
🔲 Administrators
🔲 Administrators (Read only)
🔲 Agent Registration Administrators
📁 Global Configuration and Policy Administrators
📁 Global Configuration and Policy Administrators (Read only)
🔲 Help Desk Administrators
🔲 Help Desk Administrators (Read only)
🔲 Inventory Administrators
🔲 Inventory Administrators (Read only)
🔲 Local Administrators
🔲 Local Administrators (Read only)

Edit   ↻

Selected	Privilege	Scope	Description
✓	Full (Read only)	All	Read only access to all settings.
✓	Manage Inventory (Read only)	All	Read only access to all inventory objects.
✓	Local (Read only)	All	Read only access to all settings in the local pod.
✓	Manage vCenter Configuration (Read only)	Global	Read only access to vCenter Configuration.
✓	Manage Help Desk (Read only)	All	Read only access to Help Desk portal.
✓	Manage Global Sessions	Global	Manage Global sessions.
✓	Manage Cloud Pod Architecture	Global	Configure and manage a Cloud Pod Architecture environment, including global entitlements, sites, home sites, and pods.
✓	Register Agent	Global	Register non-vCenter machines such as RDS hosts and physical PCs.

Global Administrators View

Administrators and Groups   **Role Privileges**   **Role Permissions**   **Access Groups**

Add Role   Remove Role

Name
🔲 Administrators
🔲 Administrators (Read only)
🔲 Agent Registration Administrators
🔲 Global Configuration and Policy Administrators
🔲 Global Configuration and Policy Administrators (Read only)
🔲 Help Desk Administrators
🔲 Help Desk Administrators (Read only)
🔲 Inventory Administrators
🔲 Inventory Administrators (Read only)
🔲 Local Administrators
🔲 Local Administrators (Read only)

Add Permission   Remove Permission

Administrator	Access Group
👤 RAMLAN.CA\ram	📁 Root(/)
👥 RAMLAN.CA\HorizonAdmins	📁 Root(/)

Global Administrators View

Administrators and Groups   **Role Privileges**   **Role Permissions**   **Access Groups**

Add Access Group   Remove Access Group

📁 Root(/)

Add Permission   Remove Permission

Administrator	Role	Inherited
👤 RAMLAN.CA\ram	🔲 Administrators	
👥 RAMLAN.CA\HorizonAdmins	🔲 Administrators	

Instant Clone Engine Domain Accounts:

Instant Clone Engine Domain Accounts

Add   Edit   Remove

Domain	User
RAMLAN.CA	Noor

Registered Machines:

Registered Machines

RDS Hosts   **Others**

Edit   Remove   More ⌄

Filter

☑	DNS Name	Type	RDS Farm	Max Number of Con...	Sessions	Agent Version	Enabled	Status
	No records available.							

Registered Machines

RDS Hosts   **Others**

Remove

Filter

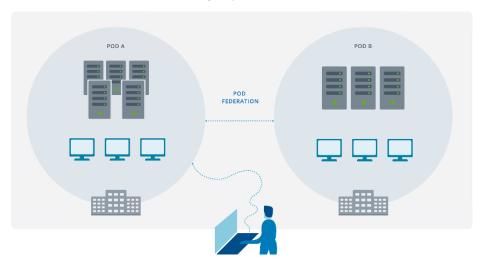| DNS Name	Type	Desktop Pool	Status
No records available.			

Cloud Prod Architecture:

Cloud Pod Architecture

With Cloud Pod Architecture, you can link together multiple pods to create a single desktop and brokering environment called a pod federation. A pod federation can span multiple sites and data centers.

Initialize the Cloud Pod Architecture feature

Join the pod federation

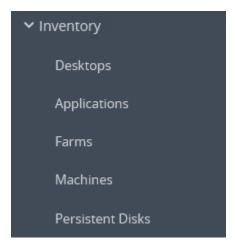## Event Configuration:

Event Configuration

Event Database

Edit

No database has been defined, events will not be recorded. Click 'Edit' to specify a database server.

Event Settings

Event settings cannot be configured until a database server has been specified.

Syslog

Configure syslog event logging using one or more methods below. Use of this feature on an unsecured network is not recommended.

Send to Syslog Servers

Add

No records available.

Events to File System

Log to File

○ Always

● Log to File on Error ⓘ
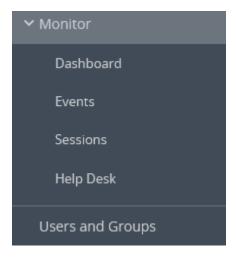
○ Never

Copy to Location

Add

Global Policies:

Global Policies

Edit Policies

Name	Global Policy
Multimedia Redirection (MMR)	Deny
USB Access	Allow
PCoIP Hardware Acceleration	Allow - Medium priority
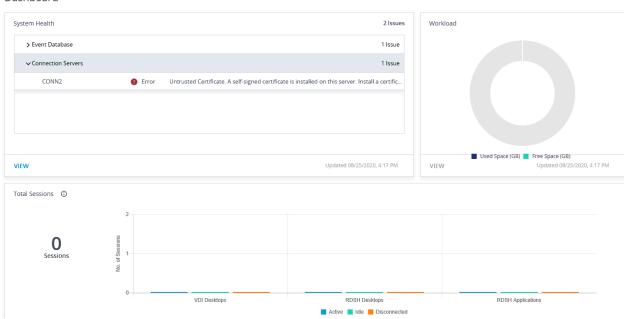
Inventory:

Monitor:

Dashboard

System Health			2 Issues
› Event Database			1 Issue
⌄ Connection Servers			1 Issue
CONN2	🛑 Error	Untrusted Certificate. A self-signed certificate is installed on this server. Install a certific...	

VIEW   Updated 08/25/2020, 4:17 PM

Workload

■ Used Space (GB) ■ Free Space (GB)

VIEW   Updated 08/25/2020, 4:17 PM

Total Sessions ⓘ

0
Sessions

No. of Sessions

2

1

0
        VDI Desktops   RDSH Desktops   RDSH Applications

■ Active ■ Idle ■ Disconnected

Events

Time Period ⌄

User	Severity	Time	Module	Message

Sessions

Sessions [All ⌄]

| Disconnect Session | Logoff Session | Restart Desktop | Reset Virtual Machine | Send Message |

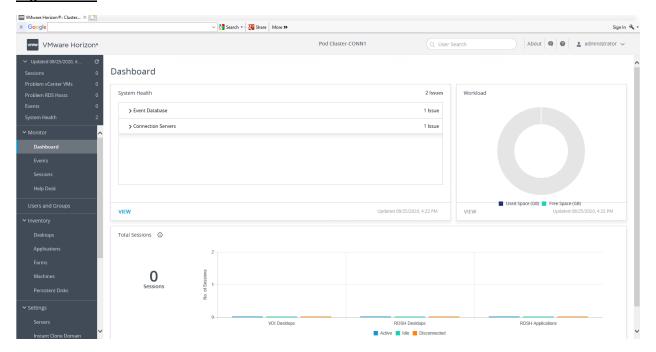| ☐	User	Type	Pool or Farm	DNS Name	Client ID

Pod Cluster-CONN1   🔍 User Search

Help Desk Tool

Enter a username in the search bar at the top of the page to view user session status and perform troubleshooting and maintenance in real time.

Login Screen:

Thanks

Ram Lan
25th Aug 2020