VMware VCP6-DTM Study guide

Written by: Paul E. Grevink
Adventures in a Virtual World: http://paulgrevink.wordpress.com/
e: paul.grevink@gmail.com t: @paulgrevink

Contents

Introduction

These posts were written in preparation for my VCP6-DTM exam and are based on the official VMware Blueprint.

This guide should meet the following goals:

- Based on the official Blueprint, follow the objectives as close as possible.
- Refer to the official VMware documentation as much as possible. For that reason, every Objective starts with one or more references to the VMware documentation.
- In case official documentation is not available or not complete, provide an alternative.
- Write down the essence of every objective (the Summary part).
- If necessary, provide additional explanation, instructions, examples and references to other posts. All this without providing too much information.

I hope all this will help you in your preparation for your exam. I welcome your comments, feedback and questions.

e: paul.grevink@gmail.com
t: @paulgrevink

Resources

For my preparations, besides a home lab, I have used the following resources:

VMware Horizon 6 Documentation

- **Exam Blueprint**: latest version and other info can be found here : https://mylearn.vmware.com/mgrReg/plan.cfm?plan=64299&ui=www_cert
- **Official documentation**, landing page: https://www.vmware.com/support/pubs/view_pubs.html and select a release

Video Based Training

- **PluralSight**: VMware View 5 Essentials, part 1 and 2. This training covers subjects like; View Components, Installing View, Configuring and maintaining Desktops, User Profiles, Printing, ThinApp etc.
  Although based on View 5, this training provides a lot of useful information.

Books

- **VMware Horizon Suite: Building End User Services** by Paul O'Doherty and Stephan Asselin, link.

Section 1: Install Horizon (with View) Server Components

Objective 1.1: Describe and differentiate between component functions and features

Knowledge

Identify hardware and software requirements for installation

Official Documentation: Horizon View Installation Guide, chapter 1 "System Requirements for Server Components".

Summary:

System requirements (hardware- and software requirements for the following components can be found in the Horizon View Installation Guide:

- View Connection Server.
- View Composer.
- View Administrator (View Administrator is a Web-based application that is installed when you install View Connection Server)

Chapter 2 "System Requirements for Guest Operating Systems" discusses requirements for Systems running View Agent or Standalone View Persona Management

Identify functionality of connection server

Official Documentation: Horizon View Architecture Planning Guide, chapter 1, "Introduction to View".

Summary:

The following diagram from the "Horizon View Architecture Planning Guide" shows the relationships between the major components of a View architecture.

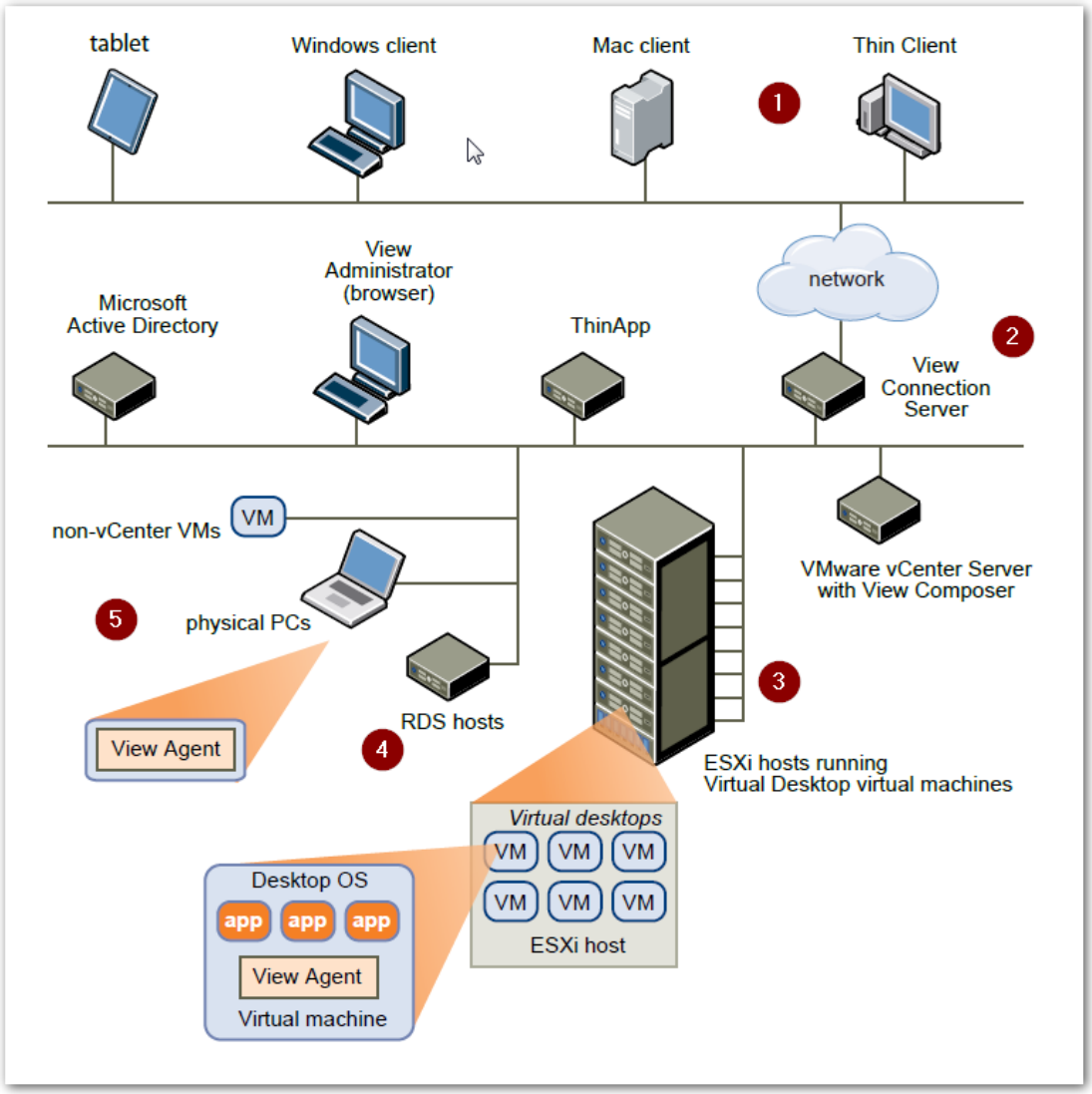

Figure 1 – Image provided by VMware

End users start Horizon Client (1) to log in to View Connection Server (2).
This server, which integrates with Windows Active Directory, provides access to remote desktops hosted on a VMware vSphere server (3), a physical PC (5), or a Microsoft RDS host (4). Horizon Client also provides access to remote applications on a Microsoft RDS host (4).

Main Components:

- Client Devices
- View Connection Server
- View Security Server
- View Composer Server
- RDS host
- View Agent

Client Devices
A horizon Client can be a (company) laptop, (home) PC, a Mac, a tablet (Android or Apple) or Smart phone.

View Connection Server,
acts as a **broker** for client connections. View Connection Server **authenticates** users through Windows Active Directory and directs the request to the appropriate virtual machine, physical PC, or Microsoft RDS host.

View Security Servers
are placed in a DMZ and communicate with a View Connection Server inside the firewall. Security servers ensure that the only remote desktop and application traffic that can enter the corporate data center is traffic on behalf of a strongly authenticated user.

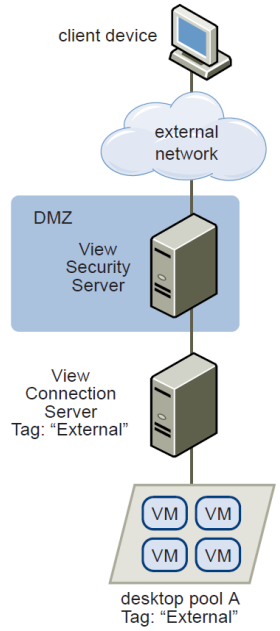

Figure 2 - Image provided by VMware

View Composer Server
With View Composer, you can create a pool of **linked clones** from a specified parent virtual machine. This strategy **reduces storage costs** by up to 90 percent. Each linked clone **acts like an independent desktop**, with a unique host name and IP address, yet the linked clone requires significantly less storage because it shares a base image with the parent. Because linked-clone desktop pools share a base image, you can quickly deploy updates and patches by updating only the parent virtual machine. End users' settings, data, and applications are not affected.

RDS host
Instead of providing end users with remote applications rather than remote desktops, they can use the Horizon client to access remote Windows-based applications. To provide a remote application, install the application on a Microsoft Remote Desktop Session (RDS) host. One or more RDS hosts make up a farm, and from that farm administrators create application pools in a similar manner to creating desktop pools.

View Agent
The View Agent service is installed on all virtual machines, physical systems, and Microsoft RDS hosts that are used as sources for remote desktops and applications. On virtual machines, this agent communicates with Horizon Client to provide features such as connection monitoring, virtual printing, View Persona Management, and access to locally connected USB devices.

Other References:

Identify functionality of View Composer
This subject is discussed in a previous section.

Identify functionality of a Replication Server
Official Documentation: Horizon View Installation Guide, chapter 4 "Installing View Connection Server", section "Install a Replicated Instance of View Connection Server".

Summary:
To provide high availability and load balancing, you can install one or more additional instances of View Connection Server that replicate an existing View Connection Server instance. After a replica installation, **the existing and newly installed instances of View Connection Server are identical**.

When you install a replicated instance, View copies the View LDAP configuration data from the existing View Connection Server instance.
After the installation, **identical View LDAP configuration data is maintained on all View Connection Server instances in the replicated group**. When a change is made on one instance, the updated information is copied to the other instances.

Identify functionality of a Security Server
This subject is discussed in a previous section.

Describe the Horizon View agent
Official Documentation: Horizon View Architecture Planning Guide, chapter 1, "Introduction to View".

Summary:

The View Agent service is installed on all virtual machines, physical systems, and Microsoft RDS hosts that are used as sources for remote desktops and applications. On virtual machines, this agent communicates with Horizon Client to provide features such as connection monitoring, virtual printing, View Persona Management, and access to locally connected USB devices.

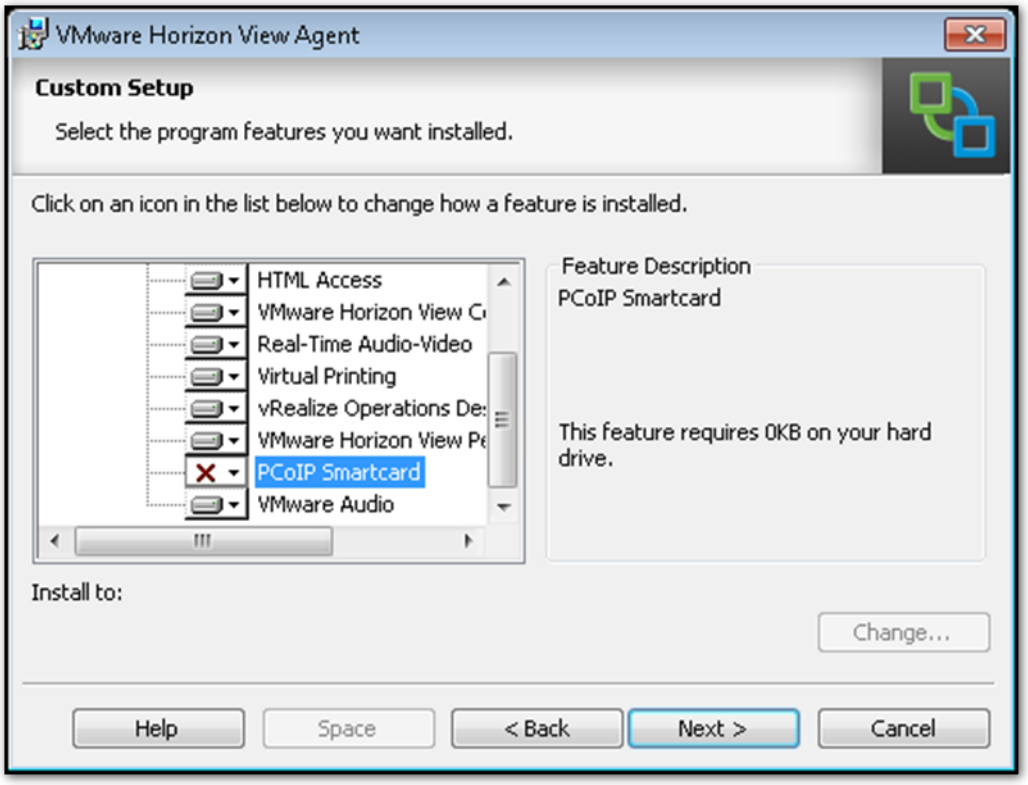

Figure 3 - View Agent installation

Differentiate Horizon View client access options

Official Documentation: Horizon View Architecture Planning Guide, chapter 1, "Introduction to View".

Summary:

The client software for accessing remote desktops and applications can run on a tablet, a phone, a Windows, Linux, or Mac PC or laptop, a thin client, and more.
After logging in, users select from a list of remote desktops and applications that they are authorized to use.
Authorization can require Active Directory credentials, a UPN, a smart card PIN, or an RSA SecurID or other two-factor authentication token.
Features differ according to which Horizon Client you use.

The final access option is the web access method, see also Figure 4.

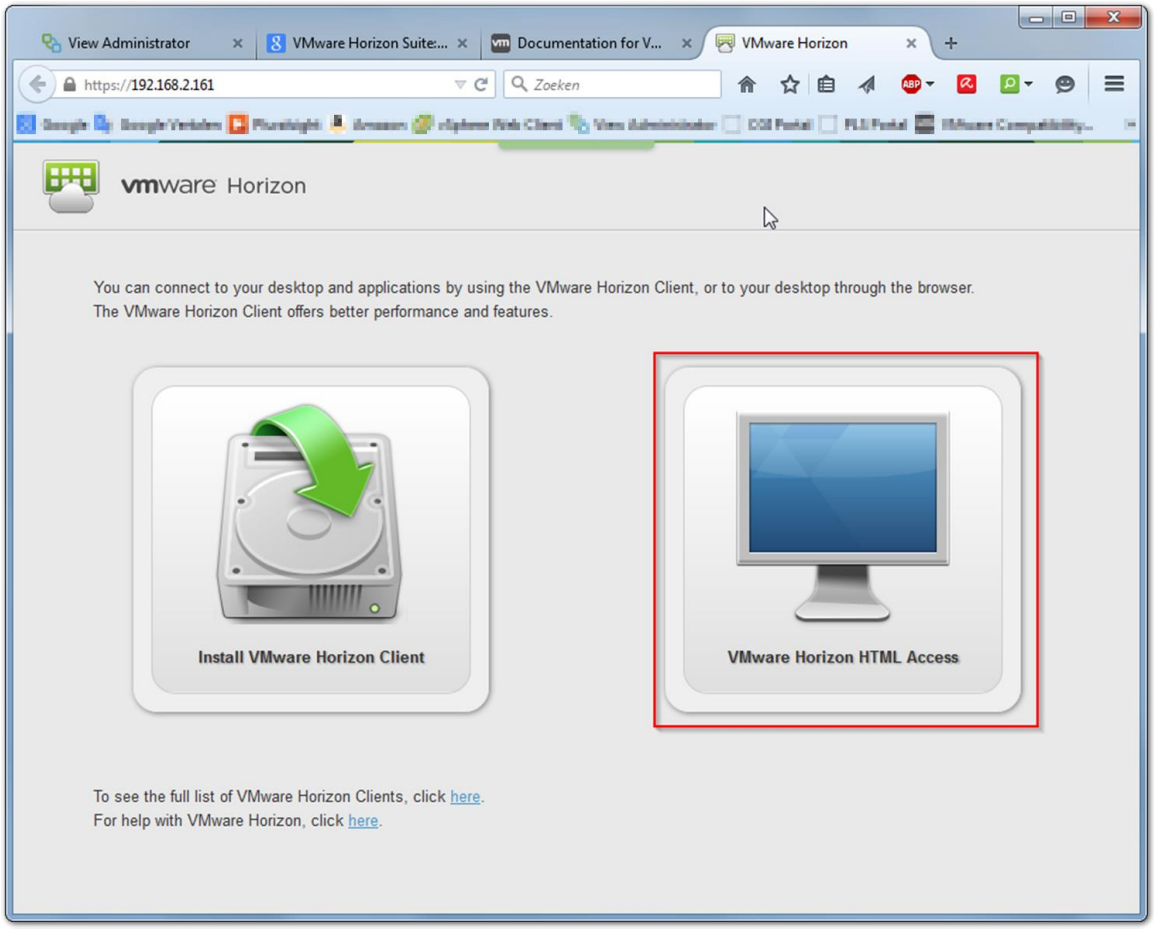

Figure 4 - HTML access

Tools

[Horizon View Administration Guide]

[Horizon View Installation Guide]

[VMware Horizon Reference Architecture]

Horizon View Administrator

Objective 1.2: Install Horizon (with View) Composer Server

Knowledge

Describe Horizon View Composer database and connectivity

Official Documentation: Horizon View Installation Guide, chapter 4 “Installing View Composer”, section “Prepare a View Composer Database”.

Summary:
You can run View Composer as a standalone server or on a vCenter Server.

View Composer requires an **SQL database** to store data. The View Composer database must reside on, or be available to, the View Composer server host.

The View Composer database stores information about connections and components that are used by View Composer:

- vCenter Server connections
- Active Directory connections
- Linked-clone desktops that are deployed by View Composer
- Replicas that are created by View Composer

Each instance of the View Composer service must have its **own** View Composer database. Multiple View Composer services **cannot share** a View Composer database.

If a database server instance already exists for vCenter Server, View Composer can use that existing instance if it is a version matches the requirements (see table). For example, View Composer can use the Microsoft SQL Server instance provided with vCenter Server. If a database server instance does not already exist, you must install one.

The following table lists the supported database servers and versions. For a complete list of database versions supported with vCenter Server, **always check** the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Database	vCenter Server 5.5	vCenter Server 5.1	vCenter Server 5.0	vCenter Server 4.1
Microsoft SQL Server 2012 Express (32- and 64-bit)	Yes	Yes	Yes	No
Microsoft SQL Server 2012 (SP1) Standard and Enterprise (32- and 64-bit)	Yes	Yes	Yes	No
Microsoft SQL Server 2008 Express (R2 SP2) (64-bit)	Yes	Yes	Yes	No
Microsoft SQL Server 2008 (SP3), Standard, Enterprise, and Datacenter (32- and 64-bit)	No	Yes	Yes	Yes
Microsoft SQL Server 2008 (R2 SP2), Standard and Enterprise (32- and 64-bit)	Yes	Yes	Yes	Yes
Oracle 10g Release 2, Standard, Standard ONE, and Enterprise [10.2.0.4] (32- and 64-bit)	No	Yes	Yes	Yes
Oracle 11g Release 2, Standard, Standard ONE, and Enterprise [11.2.0.3] (32- and 64-bit)	Yes	Yes	Yes	Yes

Figure 5 - Image provided by VMware

The preparation of the View Composer database:

- Create a database for the View Composer, either a SQL server or an Oracle database.
- (optional, but highly recommended in a production environment), set correct database permissions.
- Add an ODBC Data Source to the database server.

The whole procedure is outlined in great detail in the official documentation.

Other References:

Describe Horizon View Composer service and dependencies

Official Documentation: Horizon View Installation Guide, chapter 4 “Installing View Composer”, section “Install the View Composer Service”

Summary:

To use View Composer, you must install the **View Composer service**. View uses View Composer to create and deploy linked-clone desktops in vCenter Server.

You can install the View Composer service:

- on the Windows Server computer on which vCenter Server is installed or

- on a separate Windows Server computer. A standalone View Composer installation works with vCenter Server installed on a Windows Server computer and with the Linux-based vCenter Server Appliance.

The View Composer software cannot coexist on the same virtual or physical machine with any other View software component, including a replica server, security server, View Connection Server, View Agent, or Horizon Client.

You need to fulfill the requirements before installing the View Composer Service:

- **Supported OS**; always check the Compatibility guide, but in general: Windows Server 2008 R2 (SP1) and Windows Server 2012 R2, 64-bit version in Standard and Enterprise Edition.
- **Hardware Requirements**; no very special requirements, the server needs an fixed IP address.
- **Database Requirement**, see previous item.
- Verify you have a license to install View Composer.
- If you plan to configure an **SSL certificate signed by a CA** for View Composer during the installation, verify that your certificate is imported in the Windows local computer certificate store.
- Verify that no applications that run on the View Composer computer use **Windows SSL libraries that require SSL version 2 (SSLv2)** provided through the Microsoft Secure Channel (Schannel) security package. The View Composer installer disables SSLv2 on the Microsoft Schannel. **Applications such as Tomcat, which uses Java SSL, or Apache, which uses OpenSSL, are not affected by this constraint**.
- To run the View Composer installer, you must be a **user with administrator privileges** on the system.

Other References:

Navigate the Horizon View Composer installation wizard

Official Documentation: Horizon View Installation Guide, chapter 4 “Installing View Composer”, section “Install the View Composer Service”.

Summary:
A quick walkthrough on the installation wizard; Welcome & License Windows and other non-critical Windows have been skipped.

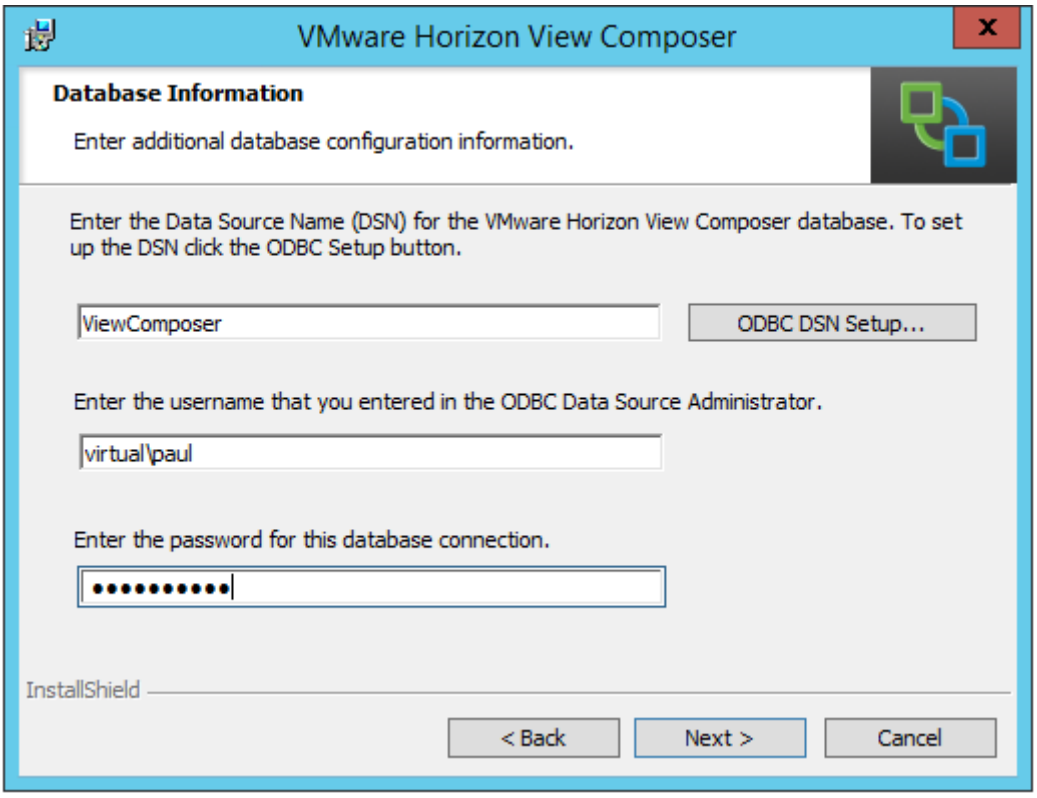

Figure 6 – Database Information

Figure 7 - port settings with default port

In the SSL Certificate Window, choose between the following options:

- **Create default SSL certificate**. After the installation, you can replace the default certificate with an SSL certificate signed by a CA.
- **Use an existing SSL certificate**. Use this option to install a signed certificate.

After finishing the installation, the link between the vCenter Server and the View Composer will be created using the View Administrator.

Other References:

Identify when to install Horizon View Composer in stand-alone mode

Official Documentation: Horizon View Installation Guide, chapter 4 "Installing View Composer", section "Install the View Composer Service".

Summary:
You will need to install the View Composer in stand-alone mode:

- While using the vCenter Server Appliance. The appliance is Linux-based. You cannot install the View Composer on a Linux based OS.
- In case the (Windows) based vCenter Server does not meet the View Composer Requirements (example?).

Other References:

Tools

Horizon View Installation Guide

Horizon View Security Guide

Horizon View Administration Guide

Horizon View Architecture Planning Guide

Horizon View Administrator

Objective 1.3: Install Horizon (with View) Connection Server

Knowledge

Identify required firewall rules

Official Documentation: Horizon View Installation Guide, chapter 4 "Installing View Connection Server", section "Firewall Rules for View Connection Server".

Summary:

When you install View Connection Server, the installation program can optionally configure the required Windows Firewall rules for you. These rules open the ports that are used by default. If you change the default ports after installation, you must manually configure Windows Firewall to allow Horizon Client devices to connect to View through the updated ports.

The following table lists the default ports that can be opened automatically during installation. Ports are **incoming** unless otherwise noted.

Protocol	Ports	View Connection Server Instance Type
JMS	TCP 4001	Standard and replica
JMSIR	TCP 4100	Standard and replica
AJP13	TCP 8009	Standard and replica
HTTP	TCP 80	Standard, replica and Security Server
PCoIP	TCP 4172 in; UDP 4172 both directions	Standard, replica and Security Server
HTTPS	TCP 8443	Standard, replica, and security server. After the initial connection to View is made, the Web browser on a client device connects to the **Blast Secure Gateway** on TCP port 8443. The Blast Secure Gateway must be enabled on a security server or View Connection Server instance to allow this second connection to take place.
HTTPS	TCP 8472	Standard and replica For the Cloud Pod Architecture feature: used for interpod communication.
HTTP	TCP 22389	Standard and replica For the Cloud Pod Architecture feature: used for global LDAP replication.
HTTPS	TCP 22636	Standard and replica For the Cloud Pod Architecture feature: used for secure global LDAP replication.

Figure 8

If your network topology includes a back-end firewall between security servers and View Connection Server instances, you must configure certain protocols and ports on the firewall to support IPsec.

See section "Configuring a Back-End Firewall to Support IPsec" for more information.

Other References:

- See also Horizon View Architecture Planning Guide, chapter 5 “Planning for Security Features”.

Install Horizon View Connection servers

Official Documentation: Horizon View Installation Guide, chapter 4 “Installing View Connection Server”, section “Firewall Rules for View Connection Server”.

Summary:
Depending on the performance, availability, and security needs of your View deployment, you can install a single instance of View Connection Server, replicated instances of View Connection Server, and security servers. You must install at least one instance of View Connection Server.

When you install View Connection Server, you select a type of installation.

Standard installation
Generates a View Connection Server instance with a new View LDAP configuration.

Replica installation
Generates a View Connection Server instance with a View LDAP configuration that is copied from an existing instance.

Security server installation
Generates a View Connection Server instance that adds an additional layer of security between the Internet and your internal network.

You need to fulfill the requirements before installing the View Connection Server:

- **Supported OS**; always check the Compatibility guide, but in general: Windows Server 2008 R2 (SP1) and Windows Server 2012 R2, 64-bit version in Standard and Enterprise Edition.
- **Hardware Requirements**; no very special requirements, the server needs an fixed IP address.
- Have a valid license key
- You must join the View Connection Server host to an Active Directory domain. View Connection Server supports Active Directory Domain Services (AD DS) domain functional levels between Windows Server 2003 and 2012 R2.
- View Connection server must not be a domain controller, have the Windows Terminal Server role or a vCenter Server.
- To run the View Connection Server installer, you must use a domain user account with Administrator privileges on the system.

A quick walkthrough on the installation of the first View Connection Server; Welcome & License Windows and other non-critical Windows have been skipped.

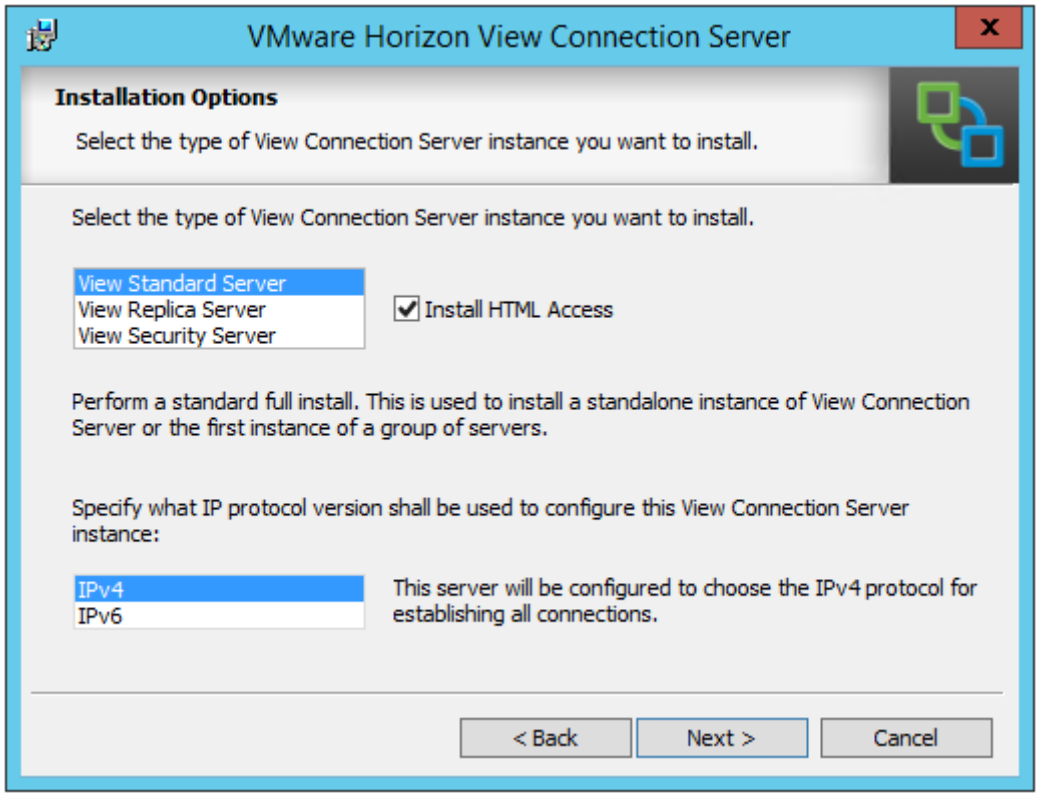

Figure 9 –

- Select the **View Standard Server** installation option.
- Make sure that **Install HTML Access** is selected if you intend to allow users to connect to their desktops by using HTML Access.
- Specify the correct **IP protocol.**

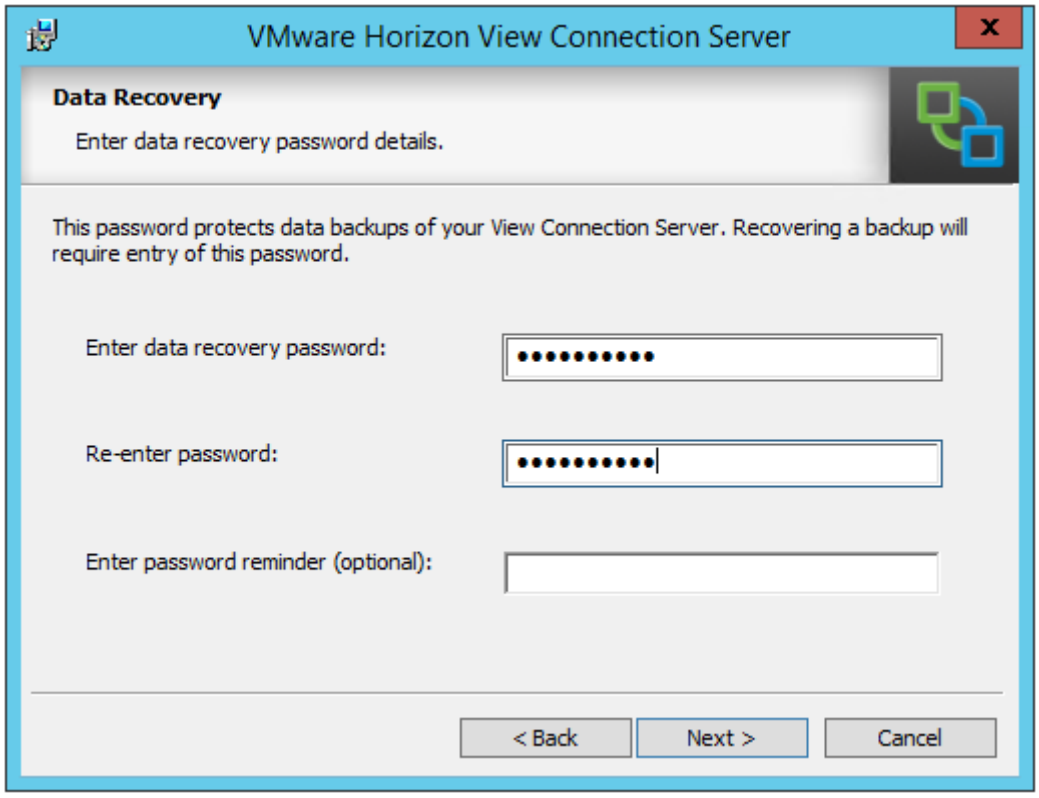

Figure 10 –

When you back up View Connection Server, the View LDAP configuration is exported as encrypted LDIF data. To restore the encrypted backup View configuration, you must provide the data recovery password. The password must contain between 1 and 128 characters.

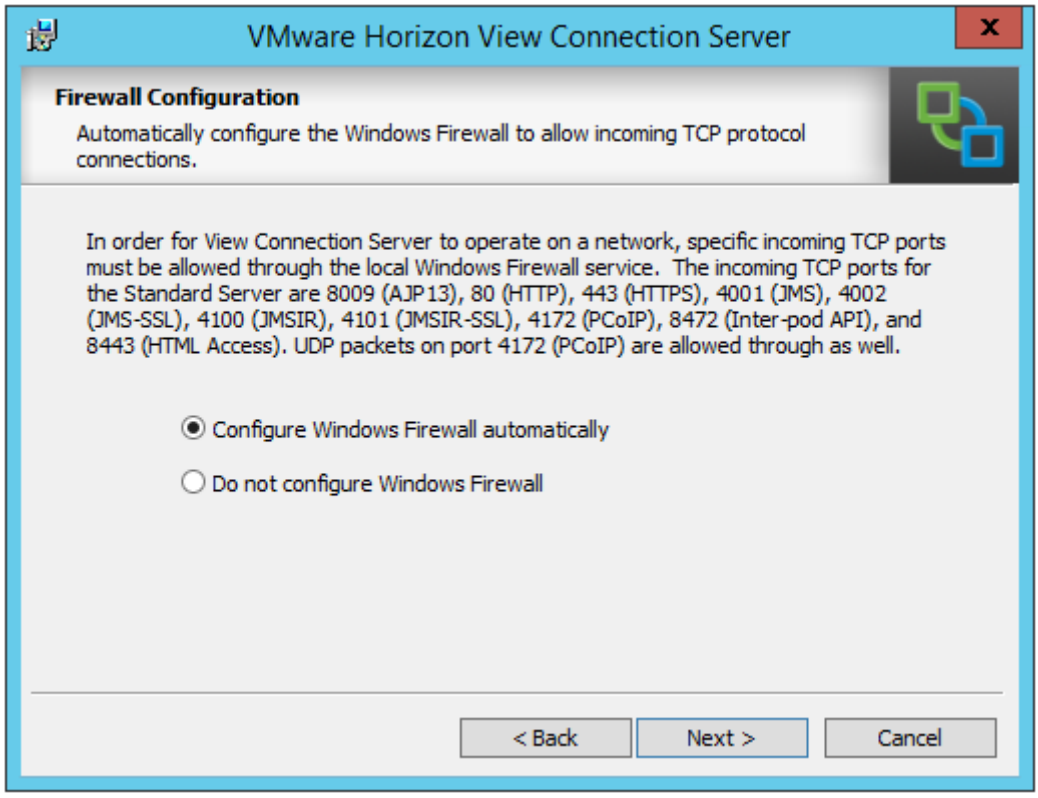

Figure 11

By default option Configure Windows Firewall Automatically is selected. Use the other option only if your organization uses its own predefined rules for configuring Windows Firewall.

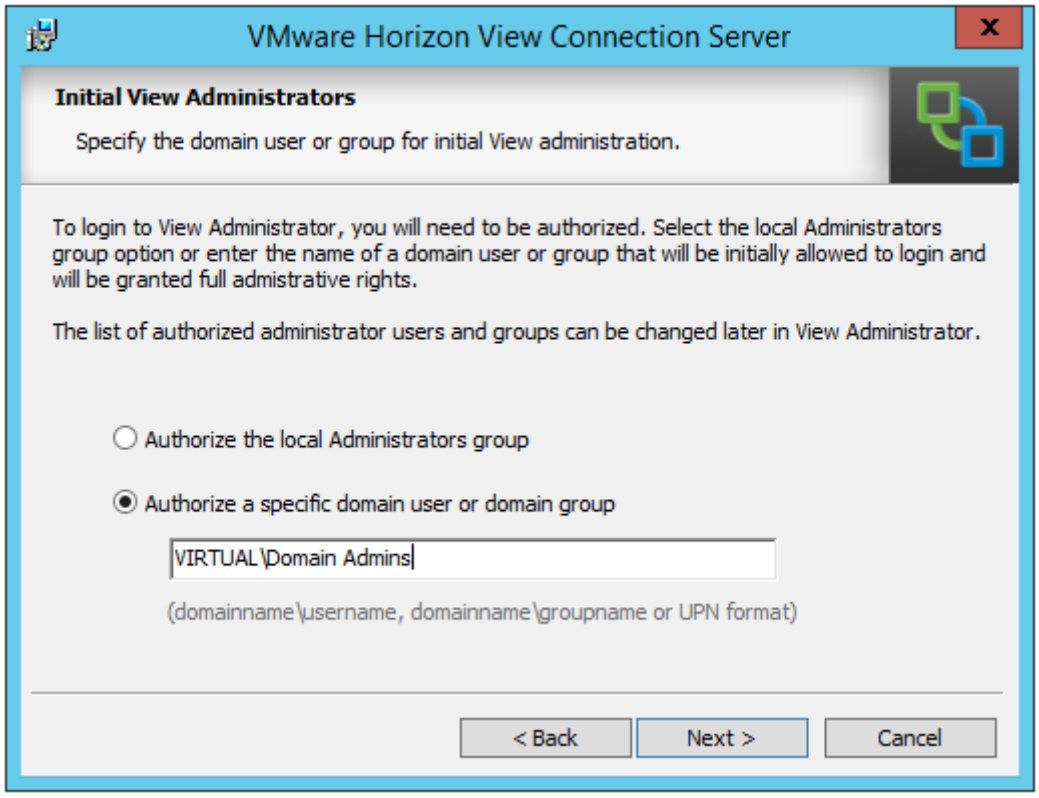

Figure 12

Authorize a View Administrators account. Only members of this account can log in to View Administrator, exercise full administration rights, and install replicated View Connection Server instances and other View servers.

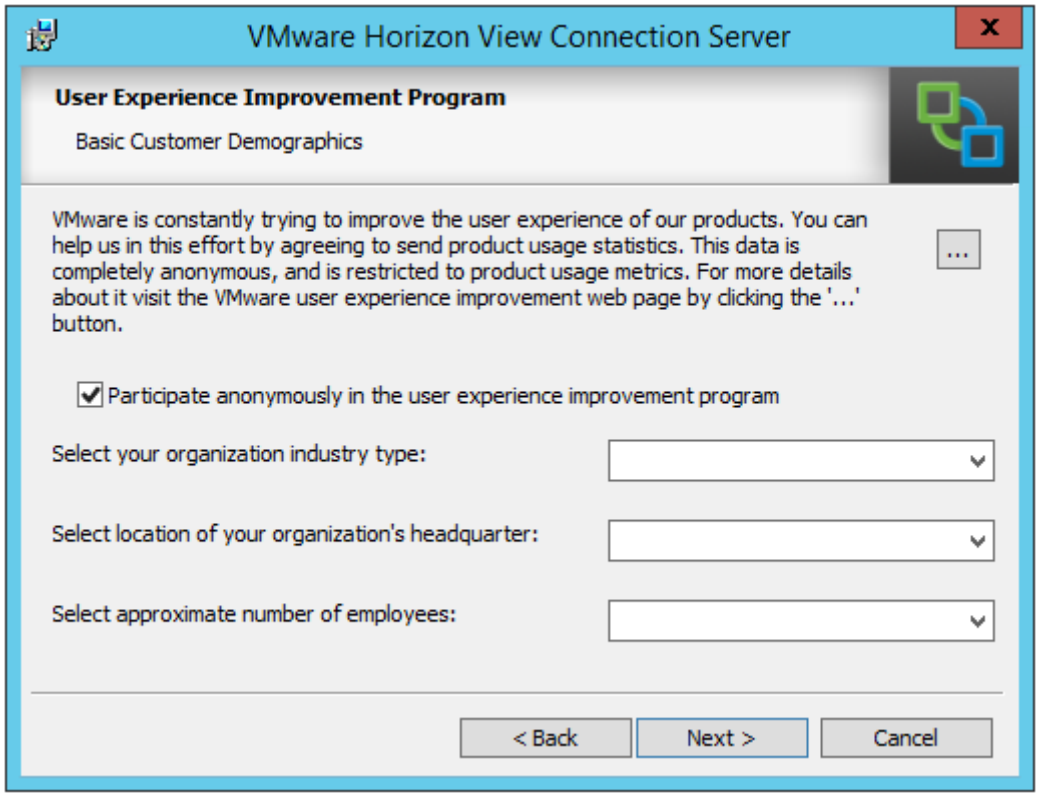

Figure 13

Choose whether to participate in the customer experience improvement program.

You can use the **silent installation feature** of the Microsoft Windows Installer (MSI) to perform a standard installation of View Connection Server on several Windows computers.

You need to fulfill the requirements; the actual command line may look something like this one:

```
VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn
VDM_SERVER_INSTANCE_TYPE=1 VDM_INITIAL_ADMIN_SID=S-1-5-32-544
VDM_SERVER_RECOVERY_PWD=mini
VDM_SERVER_RECOVERY_PWD_REMINDER=""First car"""
```

Other References:

- Pete Long at http://www.petenetlive.com wrote a series of blogposts how to deploy View 5. From setting up Active Directory, deploying servers and setting up desktop pools. Pete has also created some videos. The first post can be found here.

Differentiate between standard and replica servers

Official Documentation: Horizon View Installation Guide, chapter 4 "Installing View Connection Server", section "Install a Replicated Instance of View Connection Server".

Summary:

To provide high availability and load balancing, you can install one or more additional instances of

View Connection Server that replicate an existing View Connection Server instance. After a replica installation, **the existing and newly installed instances of View Connection Server are identical**.

When you install a replicated instance, View copies the View LDAP configuration data from the existing View Connection Server instance.
After the installation, **identical View LDAP configuration data is maintained on all View Connection Server instances in the replicated group**. When a change is made on one instance, the updated information is copied to the other instances.

Most of the prerequisites are identical to the first View Connection server, plus some extra:

- It is possible to install a View Replica Server in different domain than the View Connection Server. In that case, the domain user must also have View Administrator privileges on the Windows Server computer where the first instance is installed.

The installation procedure is almost identical to the installation of the View Connection Server:

- In the **Installation Options** window, select **View Replica Server**.
- In the **Source Server** windows, enter the host name or IP address of the existing View Connection Server instance you are replicating.

Other References:

Tools

Horizon View Installation Guide

Horizon View Security Guide

Horizon View Administration Guide

Horizon View Administrator

Objective 1.4: Install Horizon (with View) Security Server

Knowledge

Identify required firewall rules

Official Documentation: Horizon View Installation Guide, chapter 4 "Installing View Connection Server", section "Install a Security Server".

Summary:

A security server is an instance of View Connection Server that adds an additional layer of security between the Internet and your internal network. You can install one or more security servers to be connected to a View Connection Server instance.

Security servers are typically deployed in a DMZ and are not joined to a Windows domain. Security Servers have a one-to-one relationship with a Connection Server.

To allow traffic to pass through the external firewall to a security server, NAT rules must be applied.

Protocol	Port	Source	Destination
HTTPS	443	View Client	Security Server
HTTP[1]	80	View Client	Security Server
PCoIP (TCP, UDP)	4172	View Client	Security Server
PCoIP (TCP, UDP)	4172	Security Server	View Desktops
RDP	3389	Security Server	View Desktops
MMR	9427	Security Server	View Desktops
AJP13	8009	Security Server	Connection Server
JMS	4001	Security Server	Connection Server
IPsec, ESP	500	Security Server	Connection Server
NAT traversing	4500	Security Server	Connection Server
IPsec, ESP	500	Connection Server	Security Server
NAT traversing	4500	Connection Server	Security Server

Other References:

- See also Horizon View Architecture Planning Guide, chapter 5 "Planning for Security Features".

Configure Horizon View security server pairing

Official Documentation: Horizon View Installation Guide, chapter 4 "Installing View Connection Server", section "Configure a Security Server Pairing Password".

[1] Not recommended

Summary:
Before you can install a security server, you must configure a security server pairing password. When you install a security server with the View Connection Server installation program, the program prompts you for this password during the installation process.

The security server pairing password is a **one-time password** that permits a security server to be paired with a View Connection Server instance. The password becomes invalid after you provide it to the View Connection Server installation program.

You need the View Administrator to configure the password.

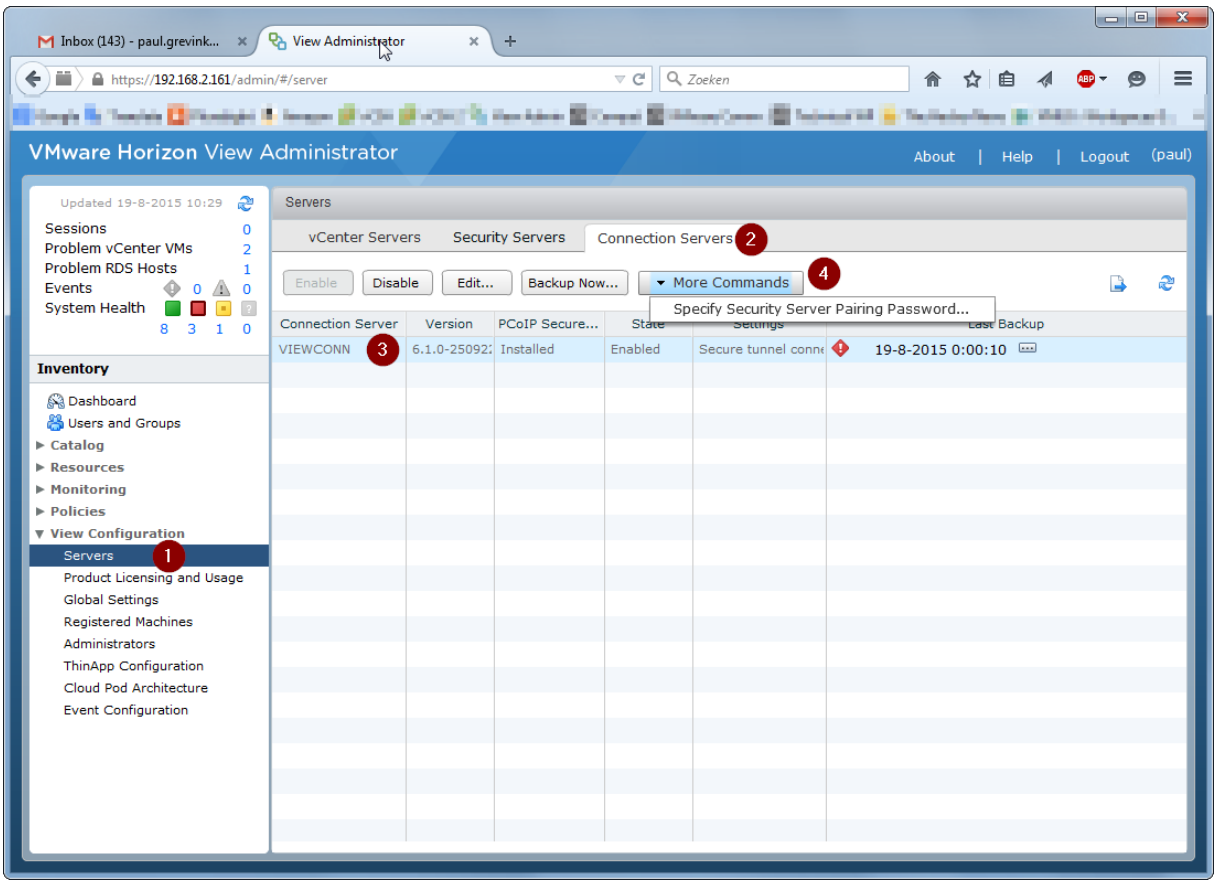

Figure 14

Specify the password and a timeout value.

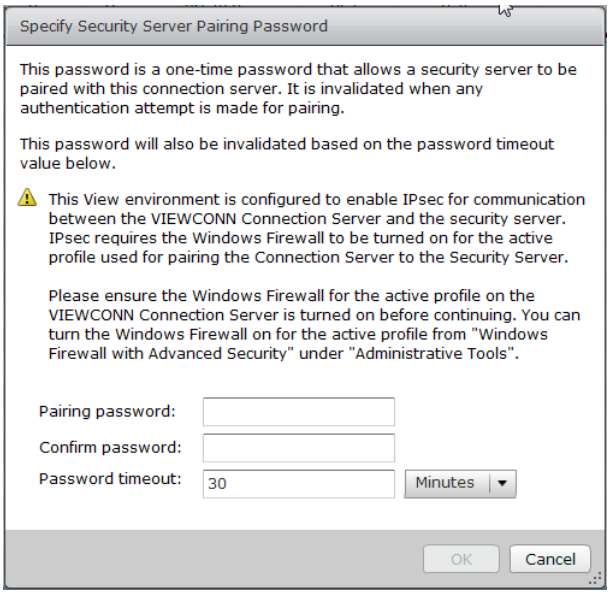

Figure 15

Other References:

Navigate the View Connection server installation wizard

Official Documentation: Horizon View Installation Guide, chapter 4 "Installing View Connection Server", section "Install a Security Server".

Summary:

Most of the prerequisites are identical to the first View Connection server, plus some extra:

- Determine the type of topology to use. For example, determine which load balancing solution to use. Decide if the View Connection Server instances that are paired with security servers will be dedicated to users of the external network.
- Verify that the View Connection Server instance to be paired with the security server is installed and configured and is running a View Connection Server version that is compatible with the security server version.
- Configure a security server pairing password.
- Familiarize yourself with the format of external URLs.
- A quick walkthrough on the installation of the first View Connection Server; Welcome & License Windows and other non-critical Windows have been skipped.

A quick walkthrough on the installation of the first View Connection Server; Welcome & License Windows and other non-critical Windows have been skipped.

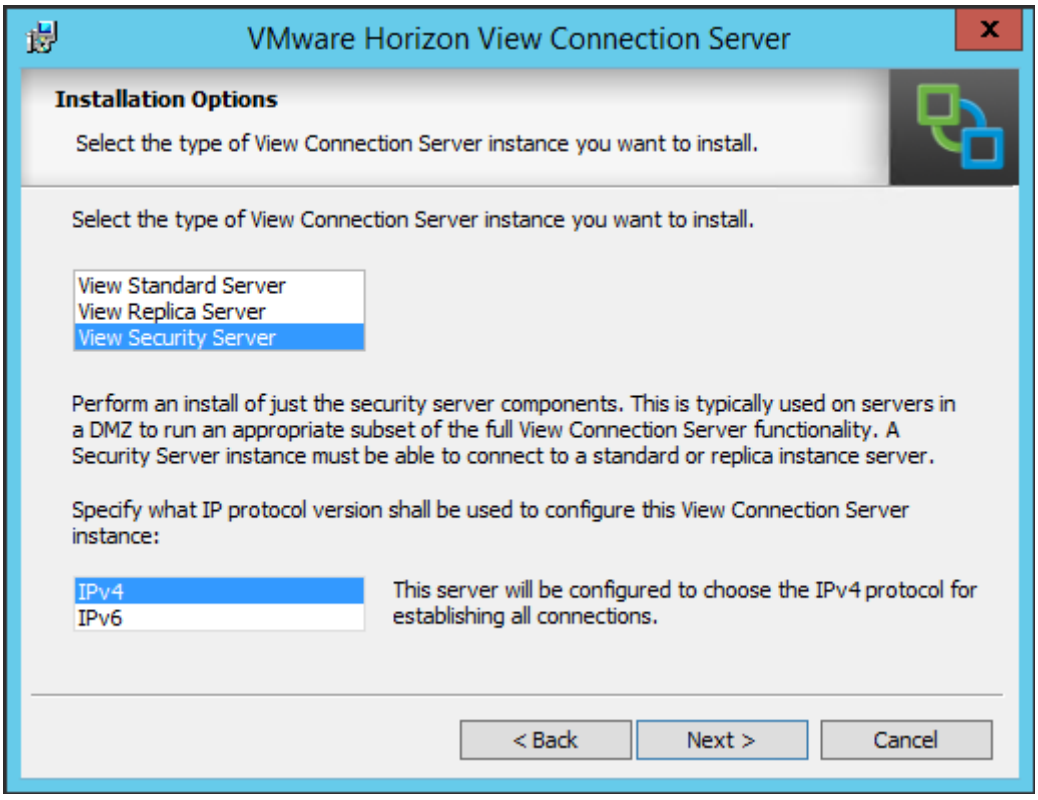

Figure 16 – Select View Security Server

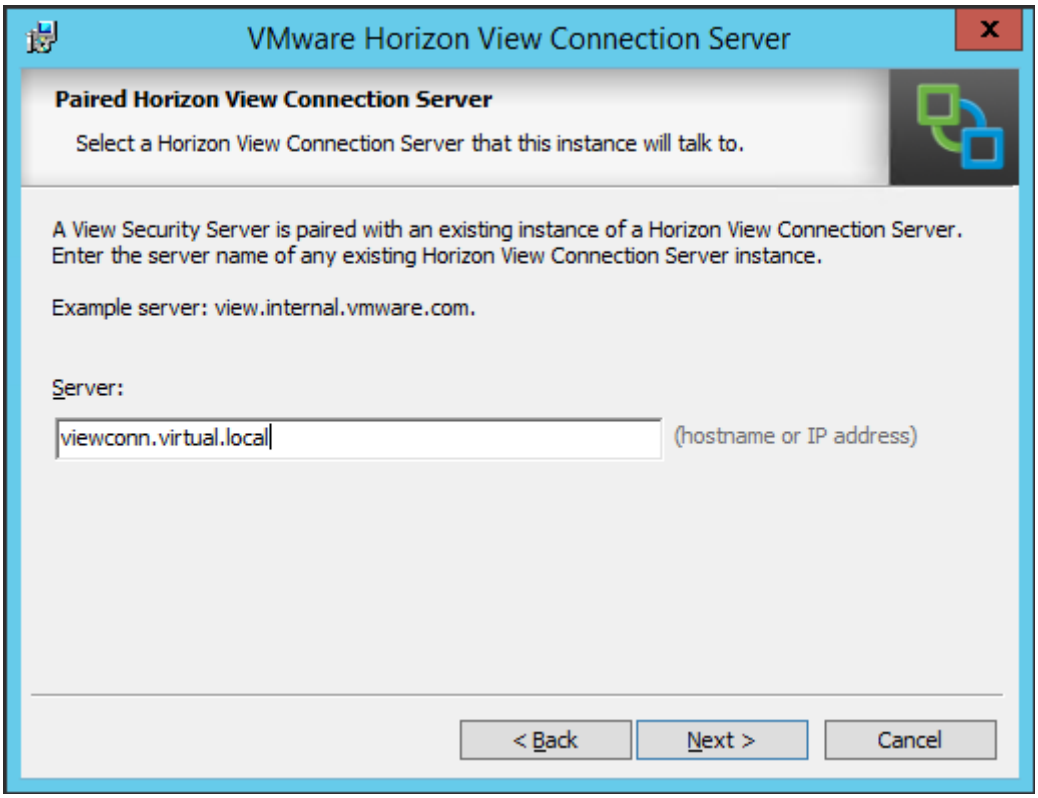

Figure 17

Type the FQDN or the IP address of the View Connection server instance to pair with the new Security server.

Figure 18

Provide the security server pairing password.

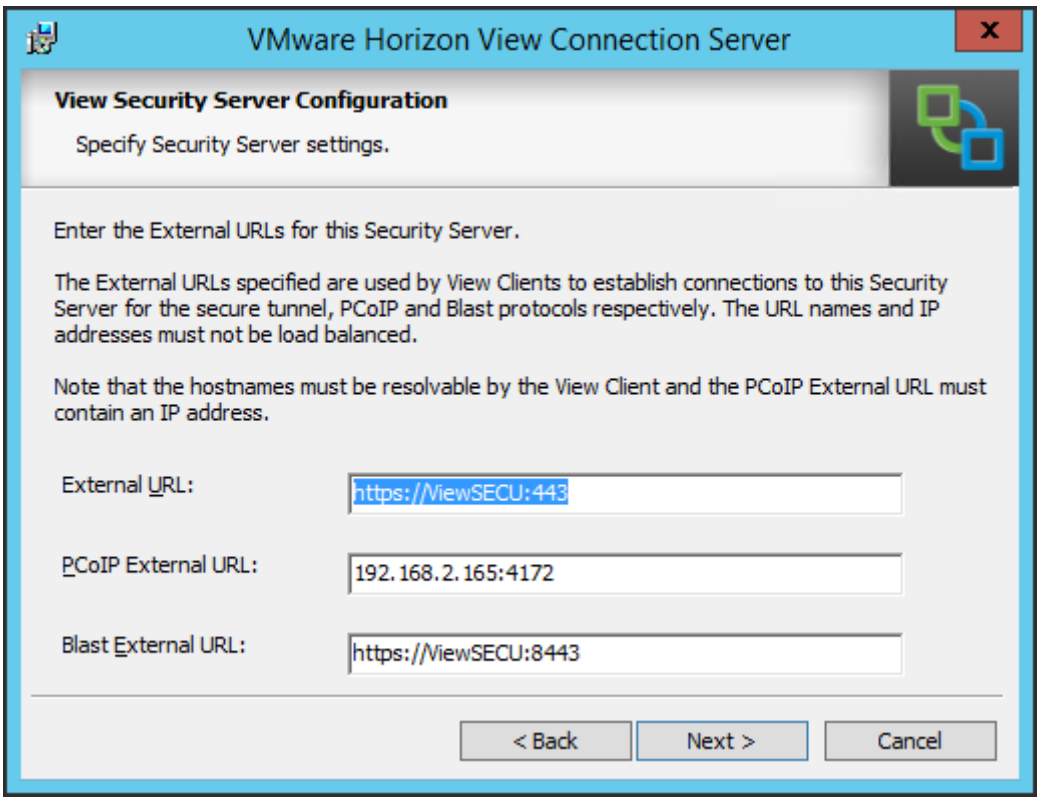

Figure 19

The values in Figure 22 are the defaults provided during the installation (I did not create a DMZ etc).

The **External URL** is the external URL of the security server for client endpoints that use the RDP or PCoIP display protocols. The URL must contain the protocol, client-resolvable security server name, and port number. Tunnel clients that run outside of your network use this URL to connect to the security server. It should look something like this: **https://view.mycompany.com:443**

The **PCoIP External URL** is the external URL of the security server for client endpoints that use the PCoIP display protocol. Specify the PCoIP external URL as an IP address with the port number 4172. Do not include a protocol name.

The **Blast External URL** is the external URL of the security server for users who use **HTML Access** to connect to remote desktops. The URL must contain the HTTPS protocol, client-resolvable host name, and port number. For example: https://view.mycompany.com:8443

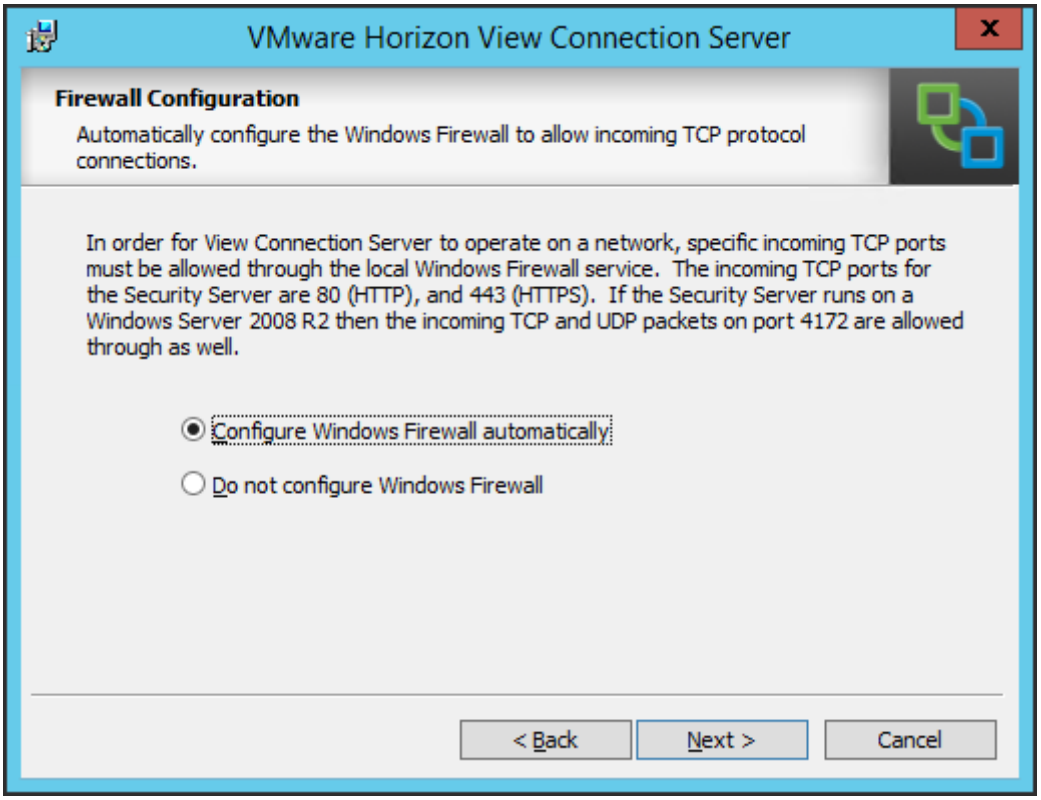

Figure 20

Choose how to configure the firewall.

After finishing the installation, the Security Server should appear in the Security Servers pane in View Administrator.

Other References:

Tools

Horizon View Installation Guide

Horizon View Security Guide

Horizon View Administration Guide

Horizon View Administrator

Objective 1.5: Prepare Environment for Horizon (with View)

Knowledge

Describe characteristics of required Active Directory domain accounts, groups, and permissions

Official Documentation: Horizon View Installation Guide, chapter 3 “Preparing Active Directory” and chapter7 “Configuring View for the First time”.

Summary:

Create Group for Users

You should create groups for different types of users in Active Directory. For example, you can create a group called View Users for your end users and another group called View Administrators for users that will administer remote desktops and applications.

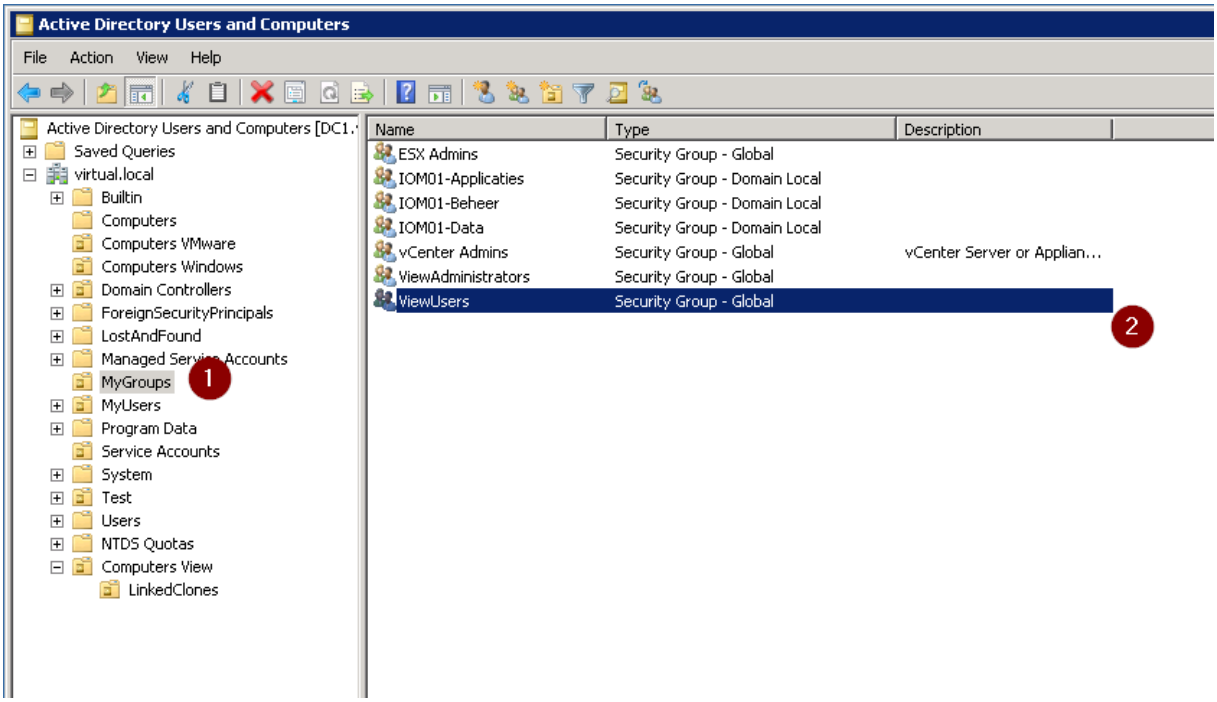

Figure 21

Configure User accounts for vCenter Server and View Composer

When you configure View for the first time, you provide the following user accounts in View Administrator. For each account, the required permissions are listed.

- The **vCenter Server user** allows View and View Composer to perform operations in vCenter Server.
    - The user account must be in the same domain as your View Connection Server host or in a trusted domain.
    - You must give the user account privileges to perform certain operations in vCenter Server. You can create a vCenter Server role with the appropriate privileges and assign the role to the vCenter Server user. The list of privileges you add to the

vCenter Server role varies, depending on whether you use View with or without View Composer.
    - Only if you install View Composer on the same server as the vCenter Server; you must add the vCenter Server user to the local Administrators group on the vCenter Server machine.
- The **standalone View Composer Server user** allows View to authenticate to the View Composer service on a standalone machine.
  If you install View Composer on the same machine as vCenter Server, the vCenter Server user performs both of the preceding functions, and **you do not use a standalone View Composer Server user**.
    - The user account must be in the same domain as your View Connection Server host or in a trusted domain.
    - You must add the user account to the local Administrators group on the standalone View Composer machine.
- The **View Composer user for AD** operations allows View Composer to perform certain operations in Active Directory.
    - The user account must be in the same domain as your View Connection Server host or in a trusted domain.
    - Add the **Create Computer Objects**, **Delete Computer Objects**, and **Write All Properties** permissions to the account in the Active Directory container in which the linked-clone computer accounts are placed.

After you create and configure these user accounts, you specify the user names in View Administrator.

- You specify a **vCenter Server user** when you **add vCenter Server** to View.
- You specify a **standalone View Composer Server user** when you **configure View Composer settings** and select Standalone View Composer Server.
- You specify a **View Composer user for AD** operations when you **configure View Composer domains**.
- You specify the **View Composer user for AD** operations when you **create linked-clone pools**.

Detailed information about the permission for these accounts can be found in Chapter 3.

Other References:

Identify and describe the Group Policy Object (GPO) template files

Official Documentation: Horizon View Installation Guide, chapter 3 “Preparing Active Directory”, section “Using View Group Policy Administrative Template Files”.

Summary:
View includes several component-specific group policy administrative (ADM and ADMX) template files.

All ADM and ADMX files that provide group policy settings for View are available in a bundled .zip file named **VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip**, where x.x.x is the version and yyyyyyy is the build number. You can download the file from the VMware Horizon (with View) download site at http://www.vmware.com/go/downloadview .

You can optimize and secure remote desktops by adding the policy settings in these files to a new or existing GPO in Active Directory and then linking that GPO to the OU that contains your desktops.

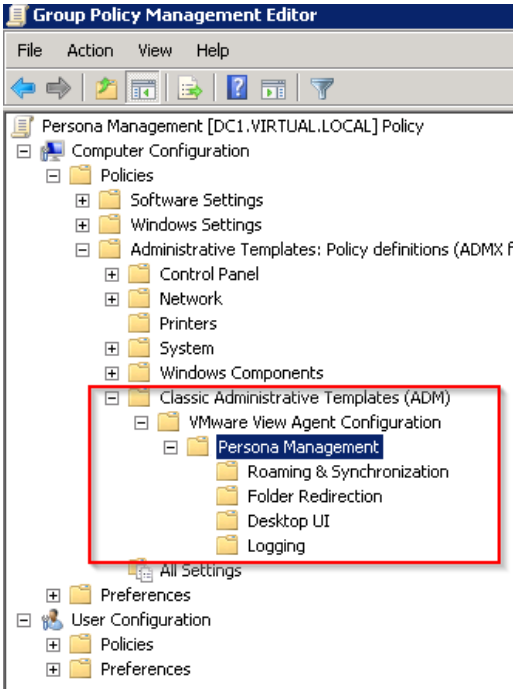

Figure 22

These group policy settings are part of **View Persona Management** (VMware's answer to Roaming profiles). The Horizon View Administration Guide and the Setting Up Desktop and Application Pools in Horizon View , chapter 16 "Configuring Policies for Desktop and Application Pools", provide more information about the group policy settings.

Other References:

Describe Organizational Units (OUs) for machine accounts and kiosk mode client accounts

Official Documentation: Horizon View Installation Guide, chapter 3 "Preparing Active Directory", section "Creating OUs and Groups for Kiosk Mode Client Accounts".

Summary:

A client in kiosk mode is a thin client or a locked-down PC that runs the client software to connect to a View 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.

Creating dedicated OUs and groups for kiosk mode client accounts partitions client systems against unwarranted intrusion and **simplifies client configuration and administration**.

The Horizon View Administration Guide provides more information.

Other References:

Verify trust relationships

Official Documentation: Horizon View Installation Guide, chapter 3 "Preparing Active Directory", "Configuring Domains and Trust Relationships".

Summary:
You must join **each View Connection Server host** to an Active Directory domain. The host must not be a domain controller. You place remote desktops in the **same domain** as the View Connection Server host or in a domain that has a **two-way trust relationship** with the View Connection Server host's domain. Specifically this must be an **external non-transitive two-way trust**.

For a quick refresh on Trust Transitivity, see here.

To determine which domains it can access, a View Connection Server instance traverses trust relationships beginning with its own domain.

You can use the **vdmadmin** command to configure domain filtering to limit the domains that a View Connection Server instance searches and that it displays to users.

Other References:

Describe DHCP requirements for Horizon View desktops

Official Documentation: Setting Up Desktop and Application Pools in Horizon View

Summary:
DHCP requirements are related to the subject of **pool deployments**. Automated desktop pools are based on virtual machine templates. A template includes an installed guest operating system and a set of applications. Part of this process is the Guest Customization, which provides configuration information for general properties such as licensing, domain attachment, and DHCP settings.

When using DHCP, the configuration of the DHCP server, especially the number of available IP addresses must match the maximum number of machines in the desktop pool(s). Other parameters must also be correct (DNS and Default gateway settings).

Other References:

Tools

Horizon View Installation Guide

Horizon View Security Guide

Horizon View Administration Guide

Setting Up Desktop and Application Pools in Horizon

Horizon View Administrator

Objective 1.6: Install, Configure and Manage vRealize Operations Manager For Horizon

Knowledge

Identify Software Requirements for vRealize Operations Manager for Horizon View

Official Documentation: VMware vRealize Operations for Horizon Installation, chapter 1 and 2.

Summary:

vRealize Operations for Horizon collects performance data from monitored software and hardware objects in your View environment and provides predictive analysis and real-time information about problems in your View infrastructure.

vRealize Operations for Horizon builds on vRealize Operations Manager and consists of these components:

- Horizon Desktop Agent
- Horizon Broker Agent
- View Adapter

The following diagram shows the correlation between the components:

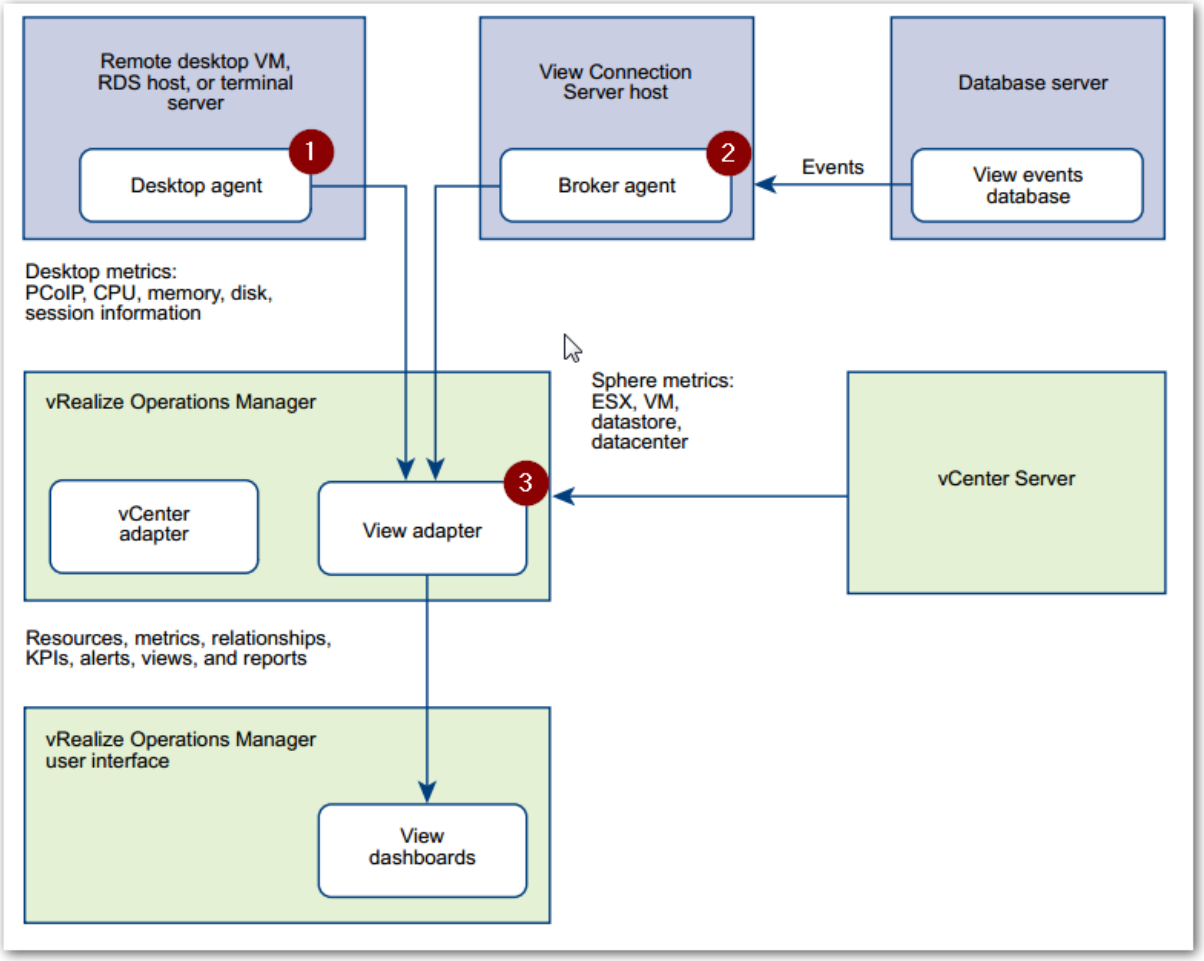

Figure 23 - Image provided by VMware

The **vRealize Operations for Horizon desktop agent** runs on **each remote desktop virtual machine, RDS host, or terminal server** in your View environment. It collect metrics and performance data and send that data to the View adapter.

In Horizon View 5.2 and later and Horizon 6.0.x with View environments, the desktop agent is installed as part of the View Agent installation. See Figure 3.

If you have a View 5.0 or 5.1 environments, you must manually install the desktop agent on your desktops.

The **vRealize Operations for Horizon broker agent** is a Windows service that runs on a **View Connection Server host**, collects View inventory information, and sends that information to the View adapter.

If your View environment includes an events database, you must configure the broker agent to collect events from the database and send them to the View adapter. You can optionally configure the broker agent to monitor only specific desktop pools in your View environment.

You install the broker agent on **one View Connection Server host in each View pod** in your environment. You must install only one broker agent in each View pod.

The broker agent has the following software requirements:

- View Connection Server 5.0 or later
- Microsoft .NET Framework version 3.5
- View Connection Server 5.3: PowerShell 3.0
- View Connection Server 5.2 or earlier: PowerShell 2.0

NOTE View Connection Server 6.0 uses the View API instead of PowerShell.

The **View adapter** runs on a **cluster node** or **remote collector node** in vRealize Operations Manager. You can create a single View adapter instance to monitor multiple View pods. During broker agent configuration, you pair the broker agent with a View adapter instance.

If you are monitoring multiple View pods, you can pair the broker agent installed in each pod with the same View adapter instance as long as the total number of desktops that the View adapter instance handles does not exceed 10,000. If you need to create multiple View adapter instances, you must create each adapter instance on a unique cluster node or remote collector.

IMPORTANT Creating more than one View adapter instance per cluster node or remote collector is not supported.

The View adapter has the following software requirements.

- vRealize Operations Manager 6.0
- Licenses that enable vRealize Operations for Horizon 6.0 and vRealize Operations Manager 6.0

General Product compatibility; vRealize Operations for Horizon is compatible with the following View and VMware vRealize Operations Manager versions.

- VMware View 5.0 or 5.1.x
- VMware Horizon View 5.2.x or 5.3.x
- VMware Horizon 6.0.x with View
- VMware vRealize Operations Manager 6.0

Other References:

Create an instance of the vRealize Operations Manager for Horizon View Adapter

Official Documentation: VMware vRealize Operations for Horizon Installation, chapter 3.

Summary:

Before you can start, prerequisites must be met:

- View must be installed and running.
- vRealize Operations Manager is deployed and running.
- vCenter adapter instance is configured for each vCenter Server instance in your View infrastructure.

The complete procedure:

1. Install vRealize Operations for Horizon solution from a PAK file in vRealize Operations Manager.
2. Add a vRealize Operations for Horizon License Key.
3. Associate View Objects with Your vRealize Operations for Horizon License Key.
4. Create an Instance of the View Adapter.
5. Install the vRealize Operations for Horizon Broker Agent on one View Connection Server host in each View pod in your View environment.
6. Configure the vRealize Operations for Horizon Broker Agent using the wizard.
7. Verify your vRealize Operations for Horizon Installation.

Install vRealize Operations for Horizon solution from a PAK file

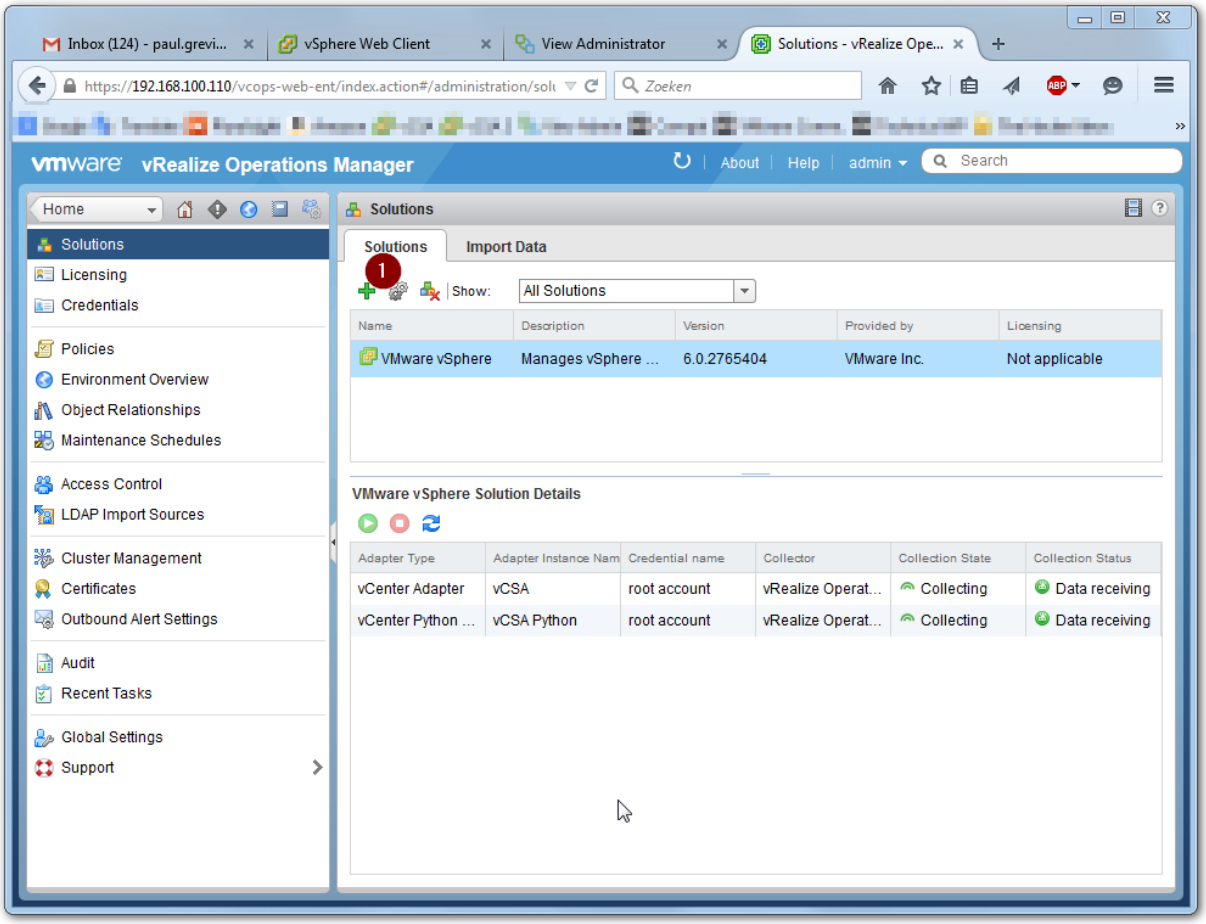

Figure 24 - Add solution

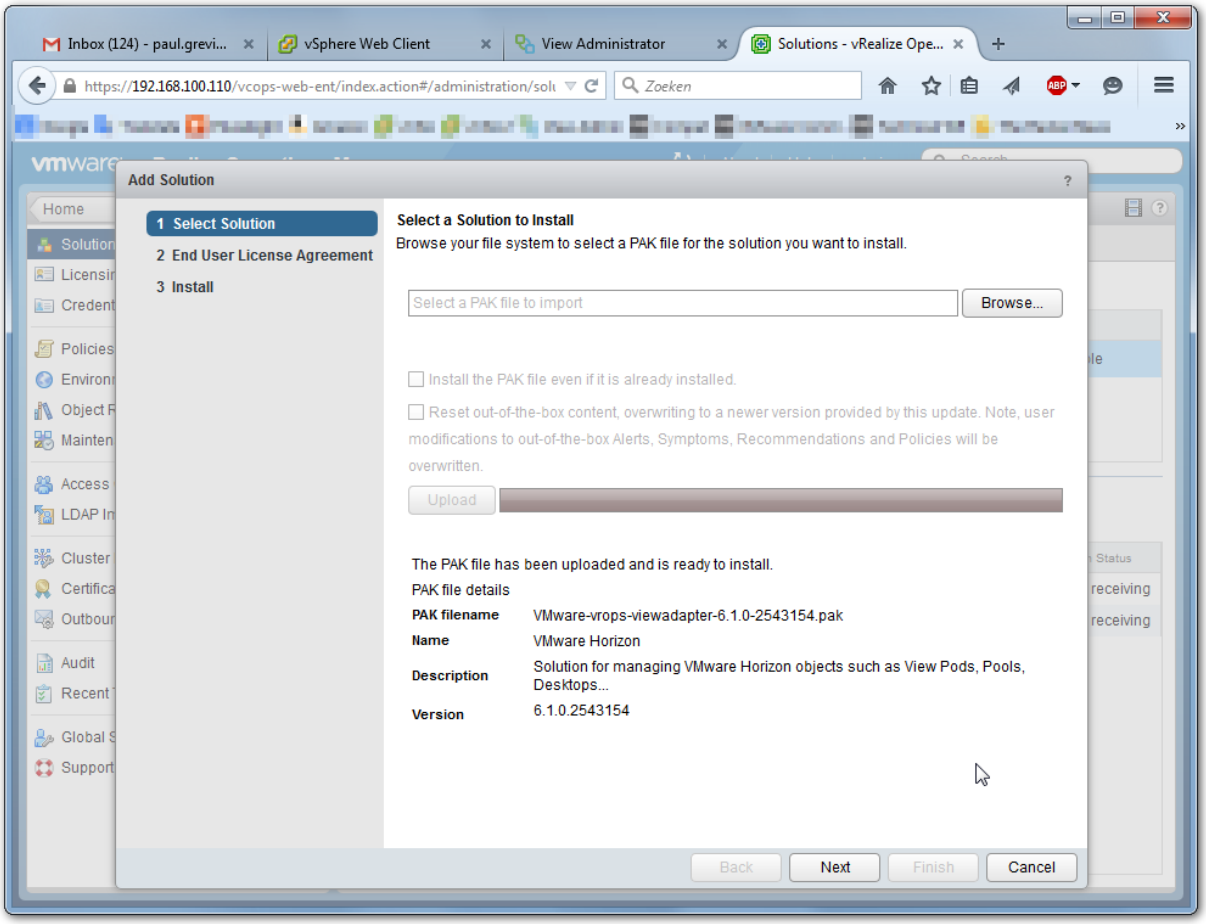

Figure 25 - Browse for .PAK file and Upload

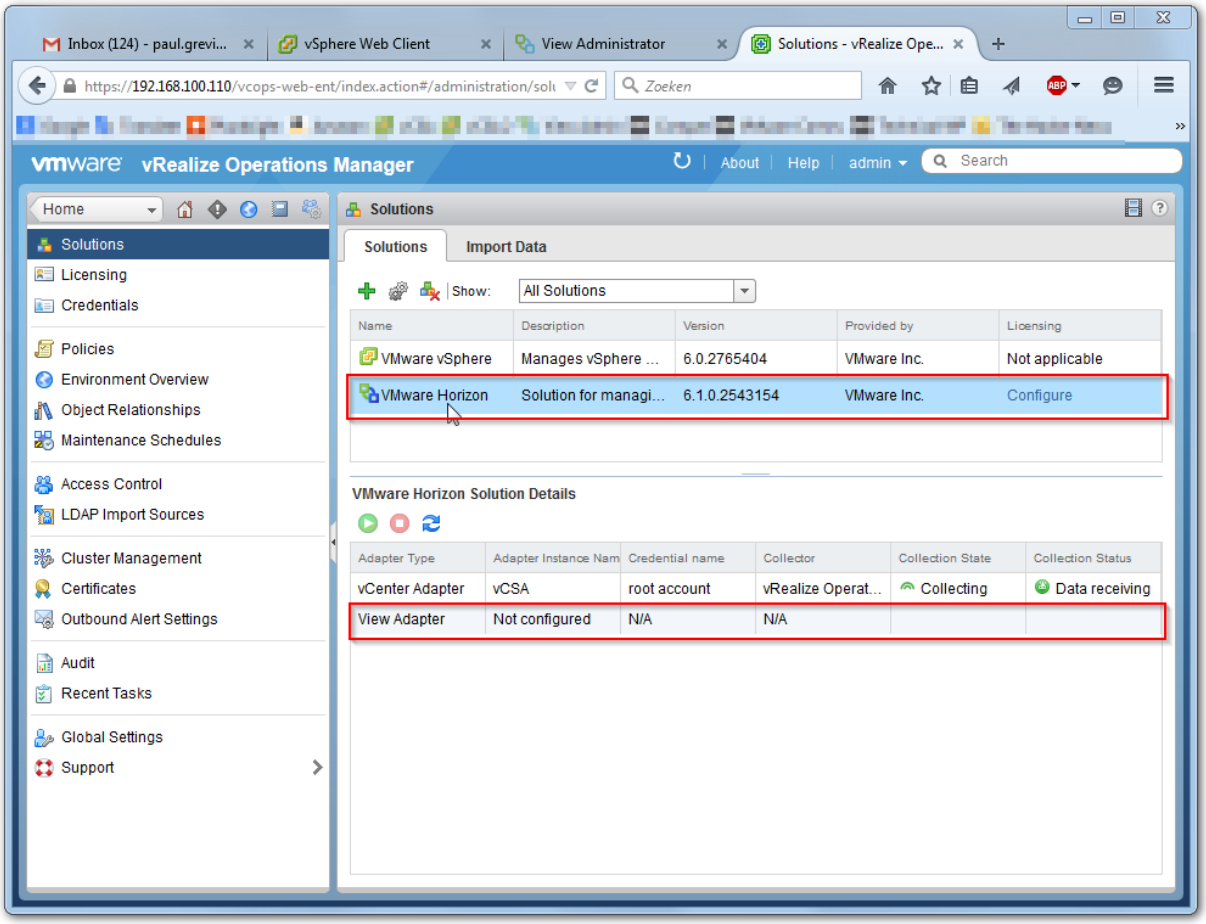

Figure 26 - Installation is finished

Adding the License key

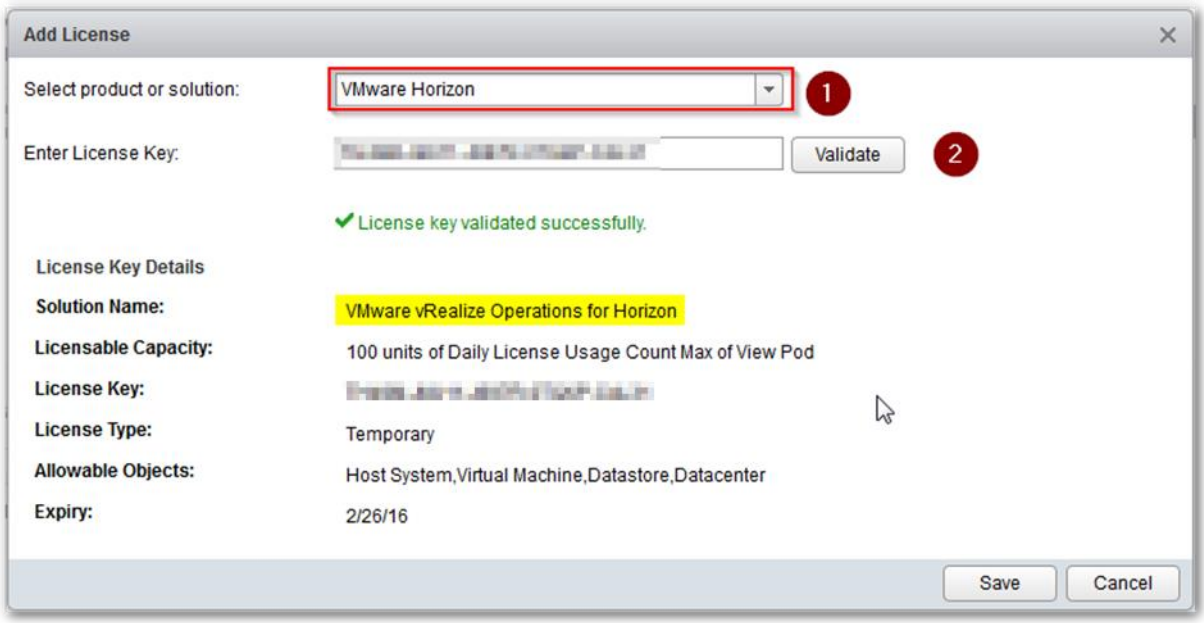

Figure 27 – Add and validate the key

After adding the license key, the next step is to associate View Objects with the license key

A **license group** is a way to gather certain objects, called license group members, under a particular license key. By default, the vRealize Operations Manager and vRealize Operations for Horizon license groups both include all host, virtual machine, and datastore objects. Because these objects are members of both license groups, they are covered by both your vRealize Operations Manager license and your vRealize Operations for Horizon license.

Each license group includes membership criteria that you can use to filter the objects that are members of the license group. By editing the membership criteria for the vRealize Operations Manager and vRealize Operations for Horizon license groups, you can **specify that certain objects are covered only under your vRealize Operations for Horizon license key**.

The steps are described in great detail in the official documentation. It comes down to edit the membership criteria for both license groups.

The license group for vRealize Operations for **Horizon** is called **VMware Horizon Solution Licensing**. The license group for vRealize Operations **Manager** is called **Product Licensing**.

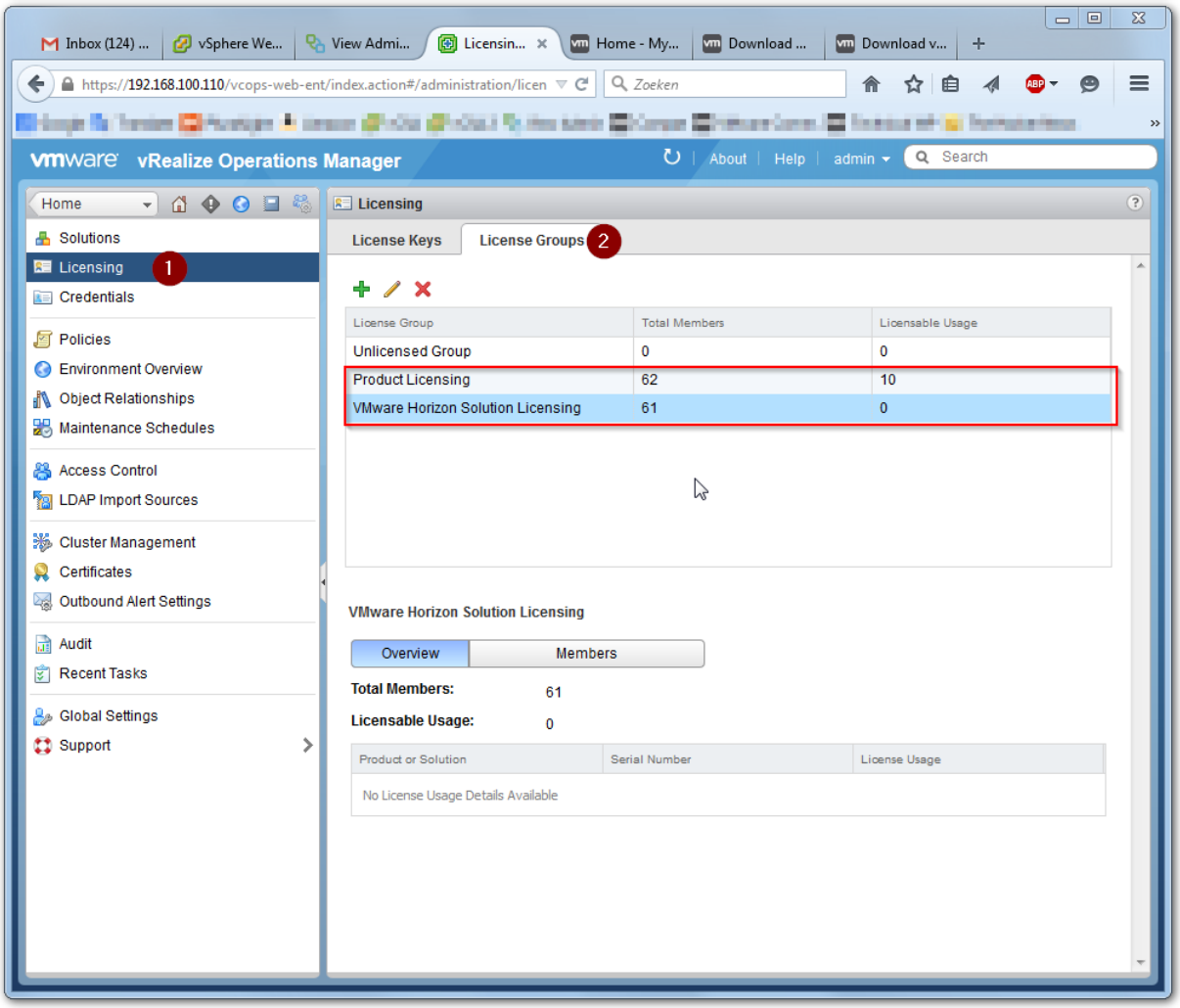

Figure 28

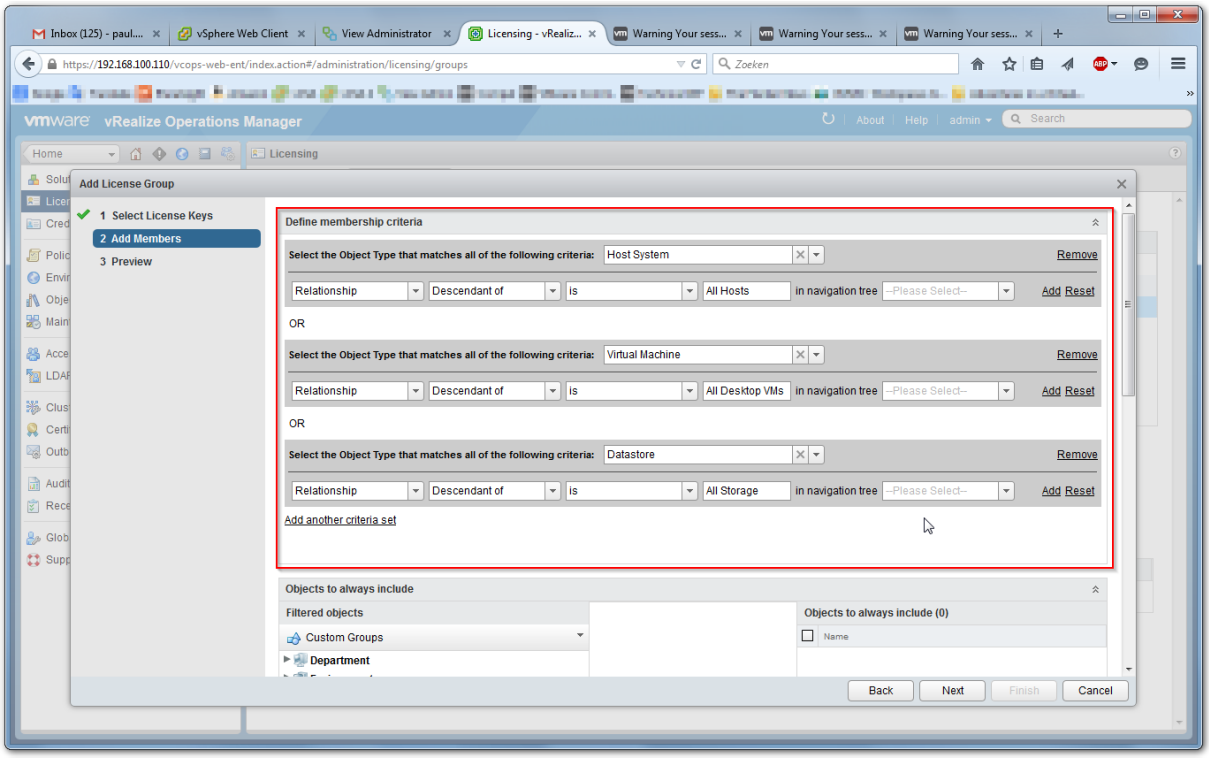

Figure 29 - Editing Membership citeria

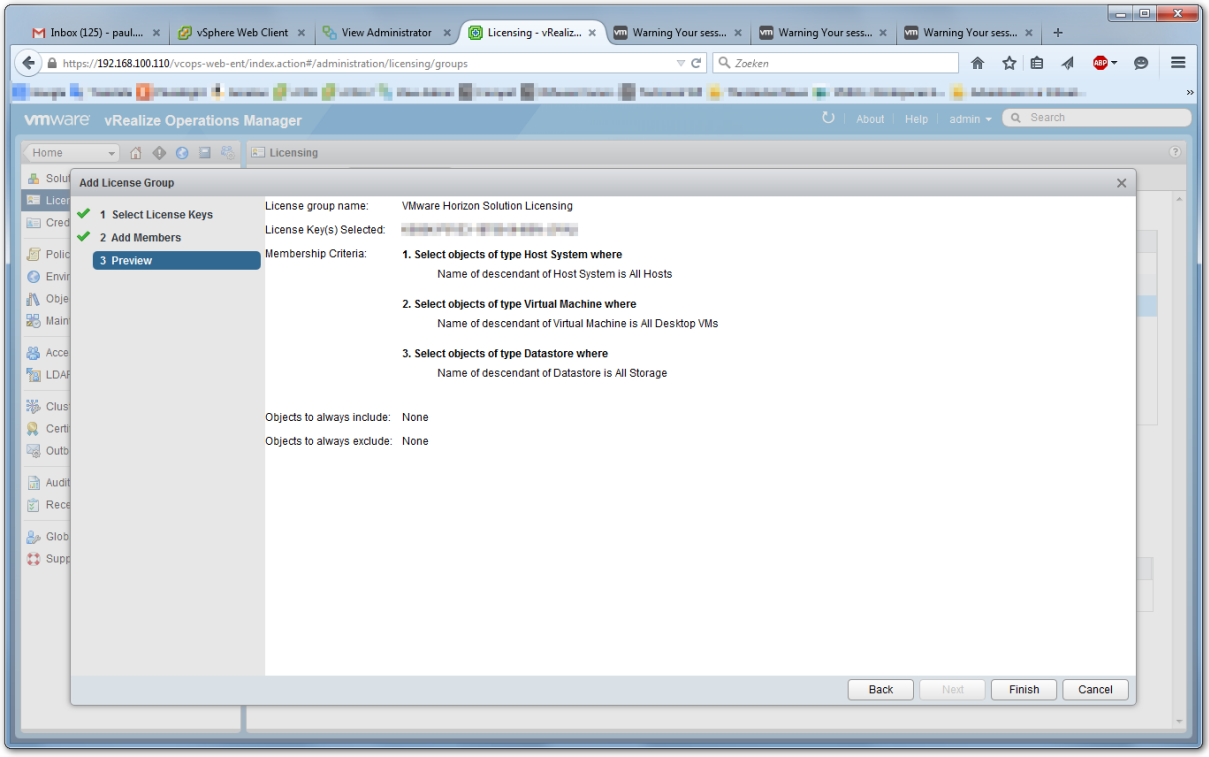

Figure 30

The next step is the configuration of the View Adapter.

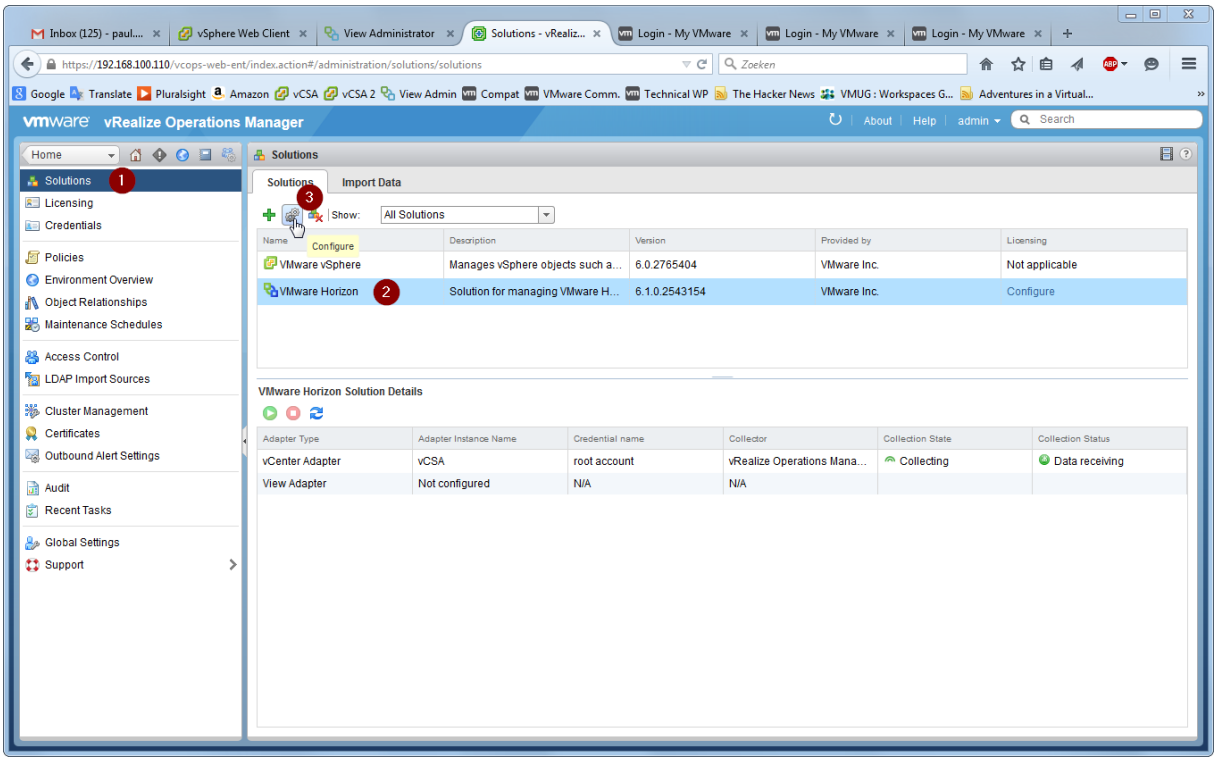

Figure 31 -

Select the VMware Horizon Solution and click the Configure button

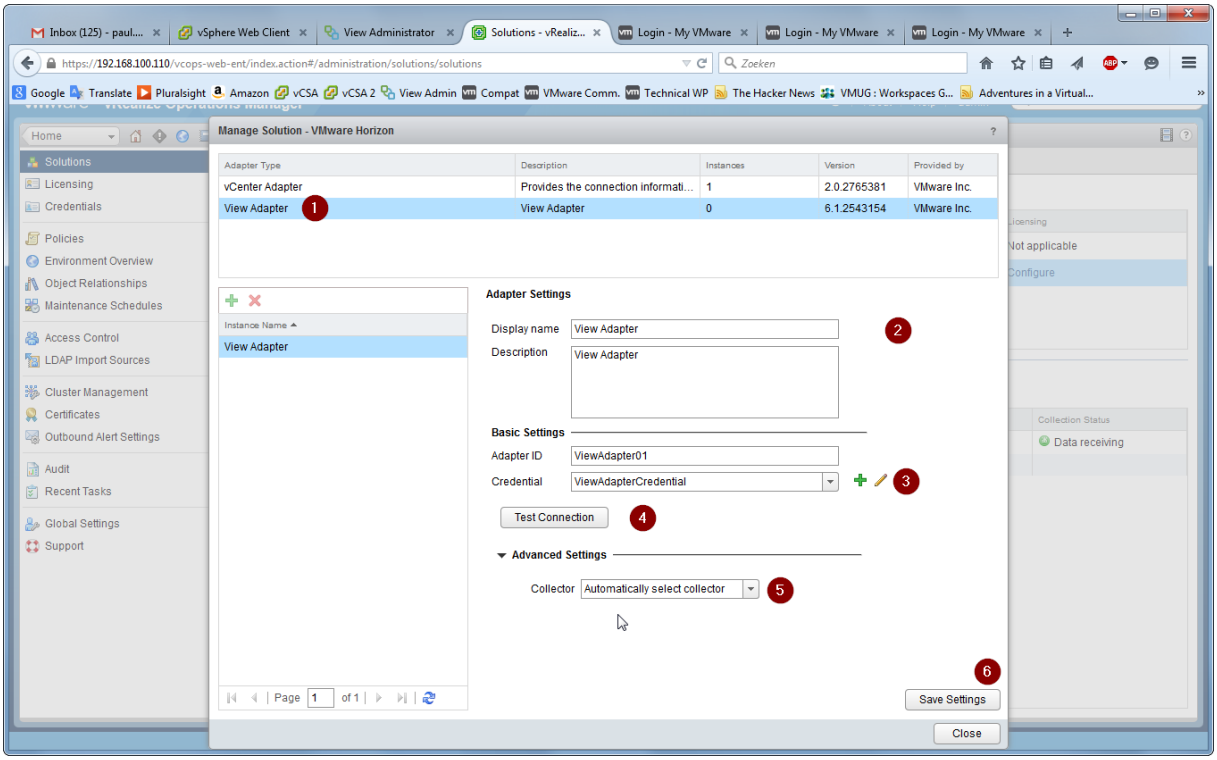

Figure 32

- Select the View Adapter
- Provide a name and description

- Create a new credential
- Test Connection
- Select Collector
- Save Settings

After the installation and configuration of the Broker Agent, you can verify your work.

In to the vRealize Operations Manager user interface, select **Dashboard List > View**, and click the **View Adapter Self Health** tab. From here, select a View adapter in the Select **View Adapter** widget to view the status of the adapter. Use the **View Broker Agent Status** widget to view metrics for the selected broker agent.

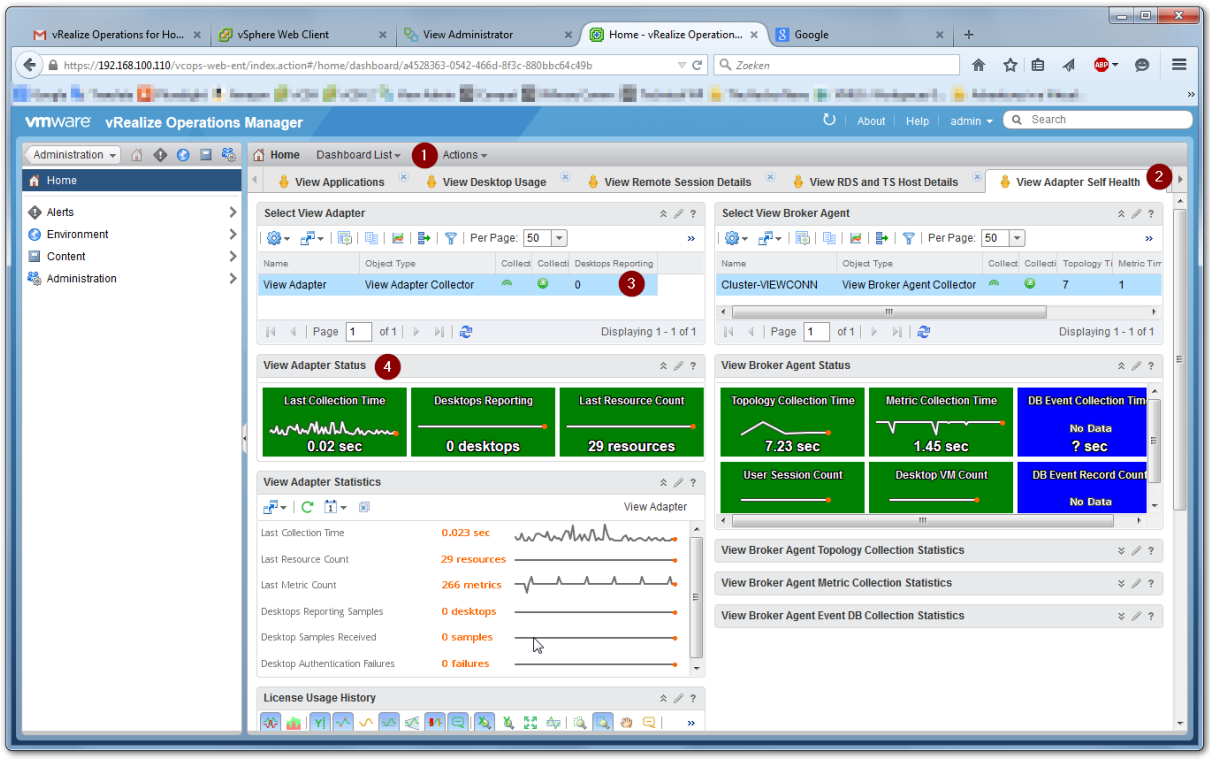

Figure 33 – check status of View Adapter and View Broker Agent

Other References:

- http://www.virtuallyvirtuoso.com/vrealize-operations-for-horizon-view-6-quick-setup-guide/

Install and Configure a Horizon Broker Agent

Official Documentation: VMware vRealize Operations for Horizon Installation, chapter 3.

Summary:

Procedure:

- Make sure Microsoft .NET Framework version 3.5 is installed.
- The installation is pretty basic

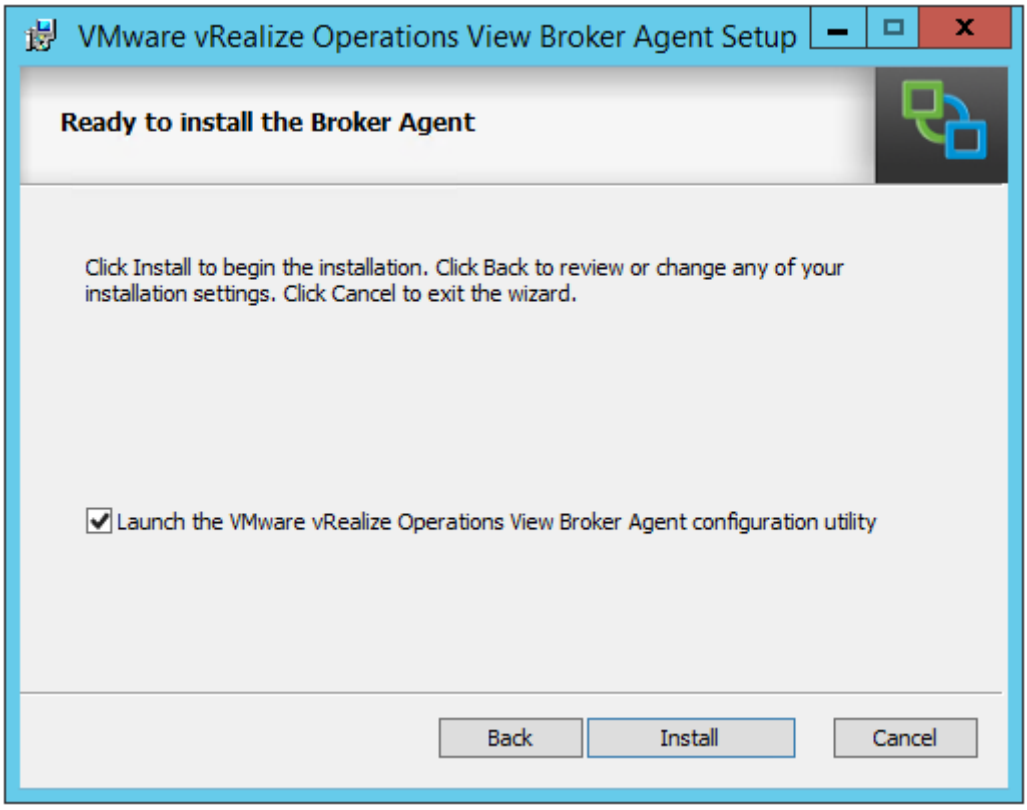

Figure 34 -

After the installation, the configuration wizard automatically loads. The complete procedure is described in great detail in the official guide. A few screenshots.

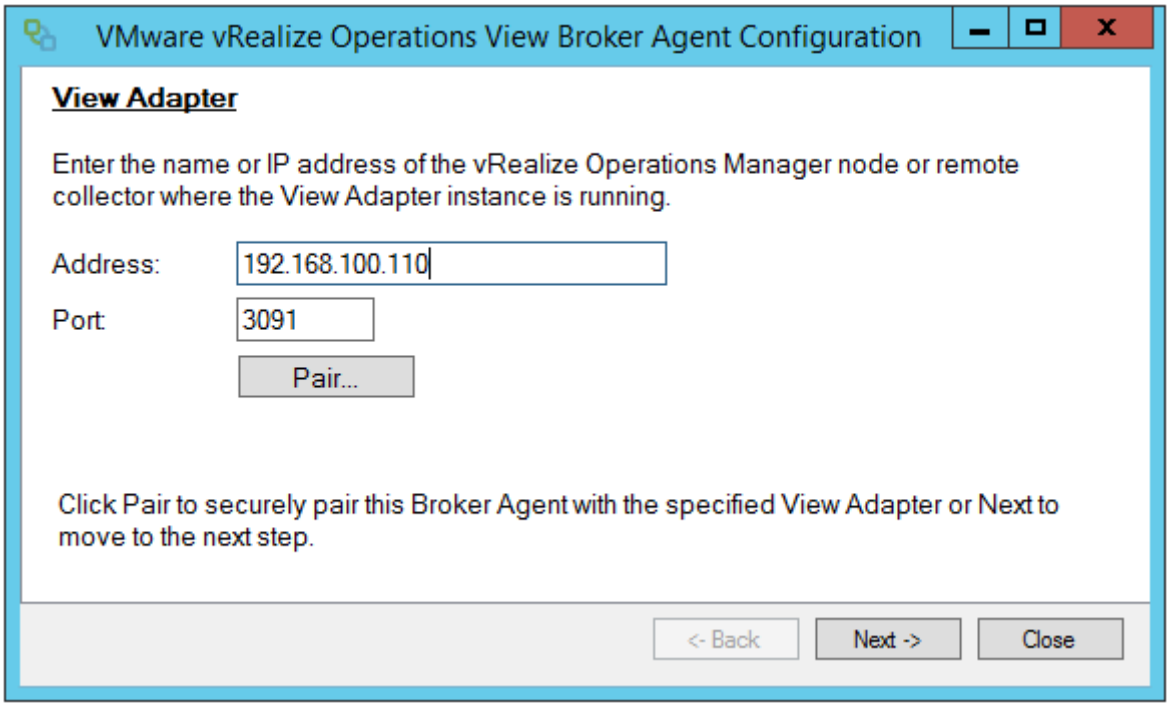

Figure 35 – provide address of the vRealize Operations Manager node

Pair the Broker Agent, specify the key defined during the configuration of the View Adapter.

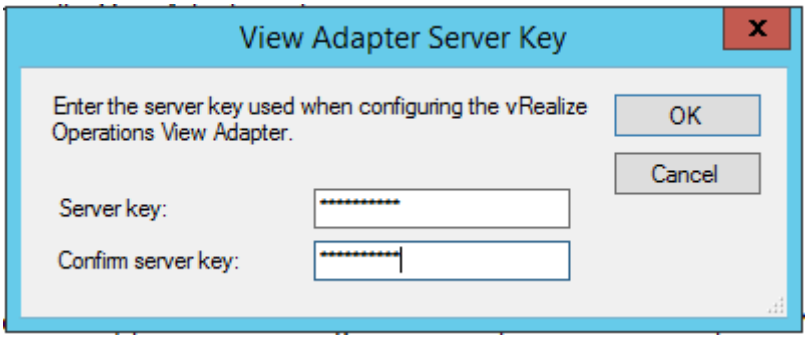

Figure 36

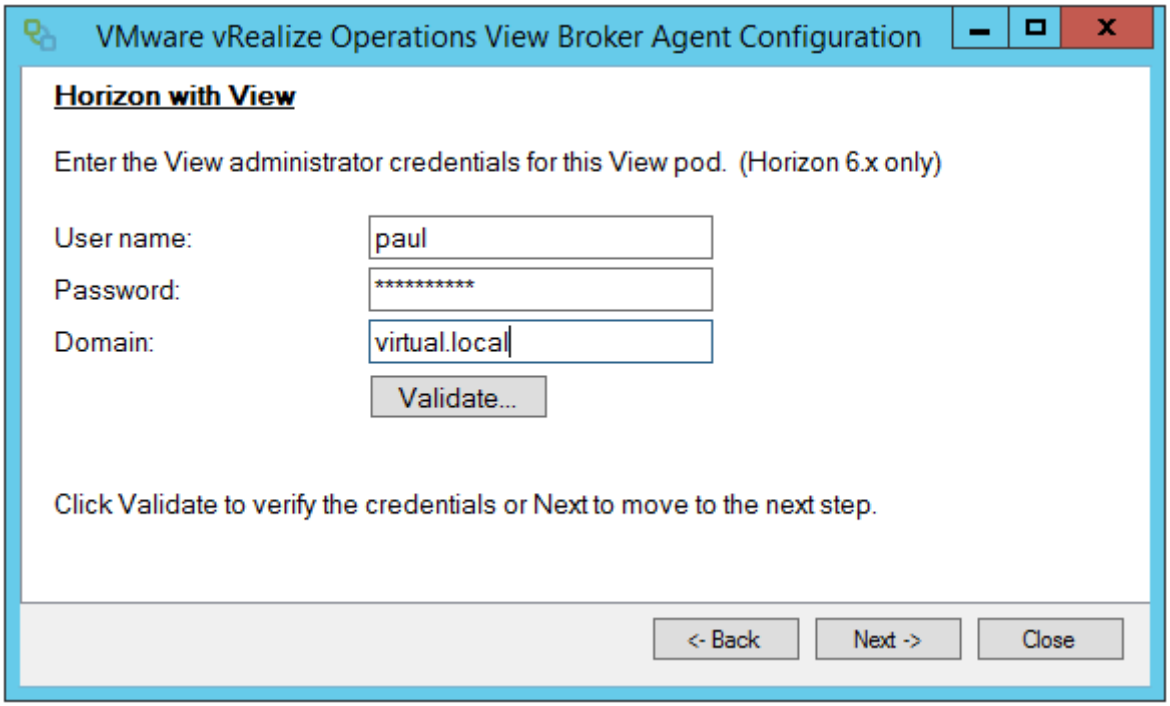

Figure 37 - Provide credentials and Validate

You can choose to monitor specific Desktop pools or all pools.

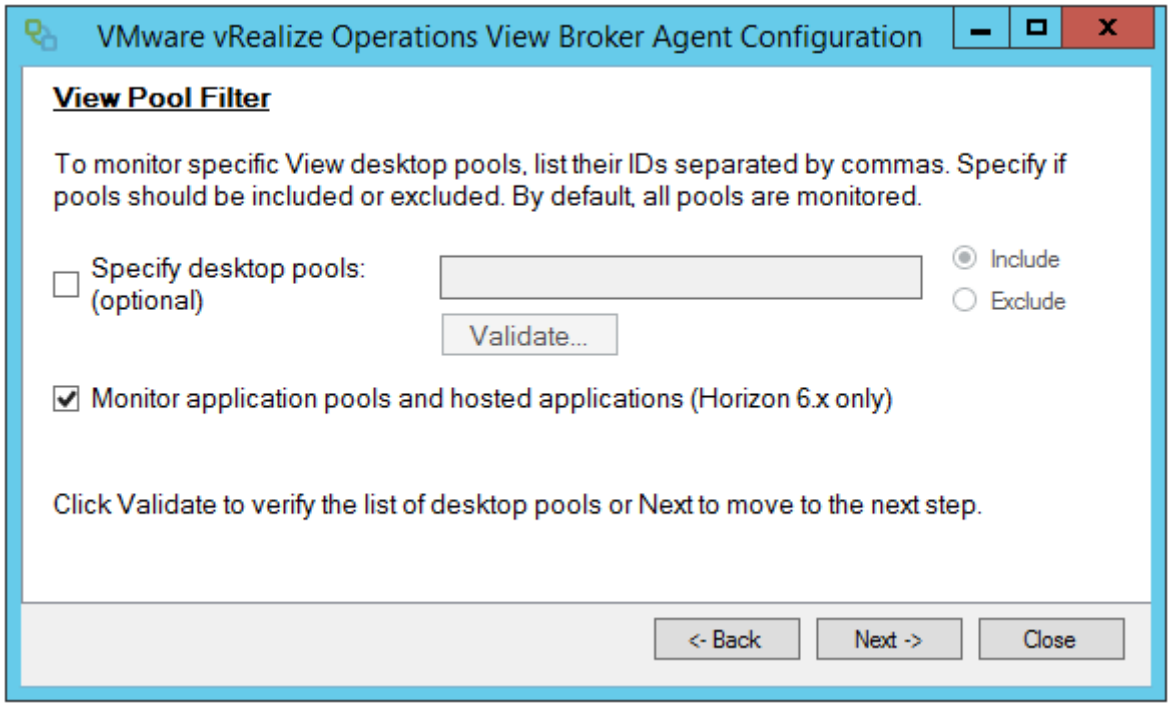

Figure 38

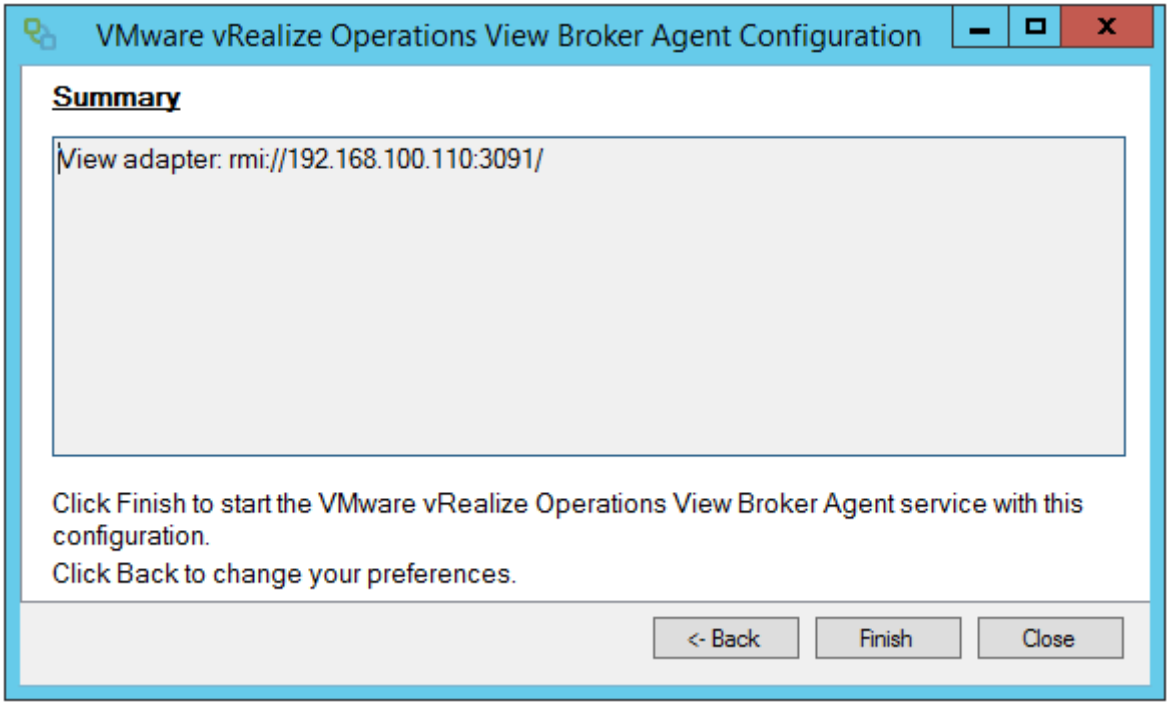

Figure 39

After finishing the wizard, the Configuration pane shows up.
Note, in my example, I have not configured the Event database.

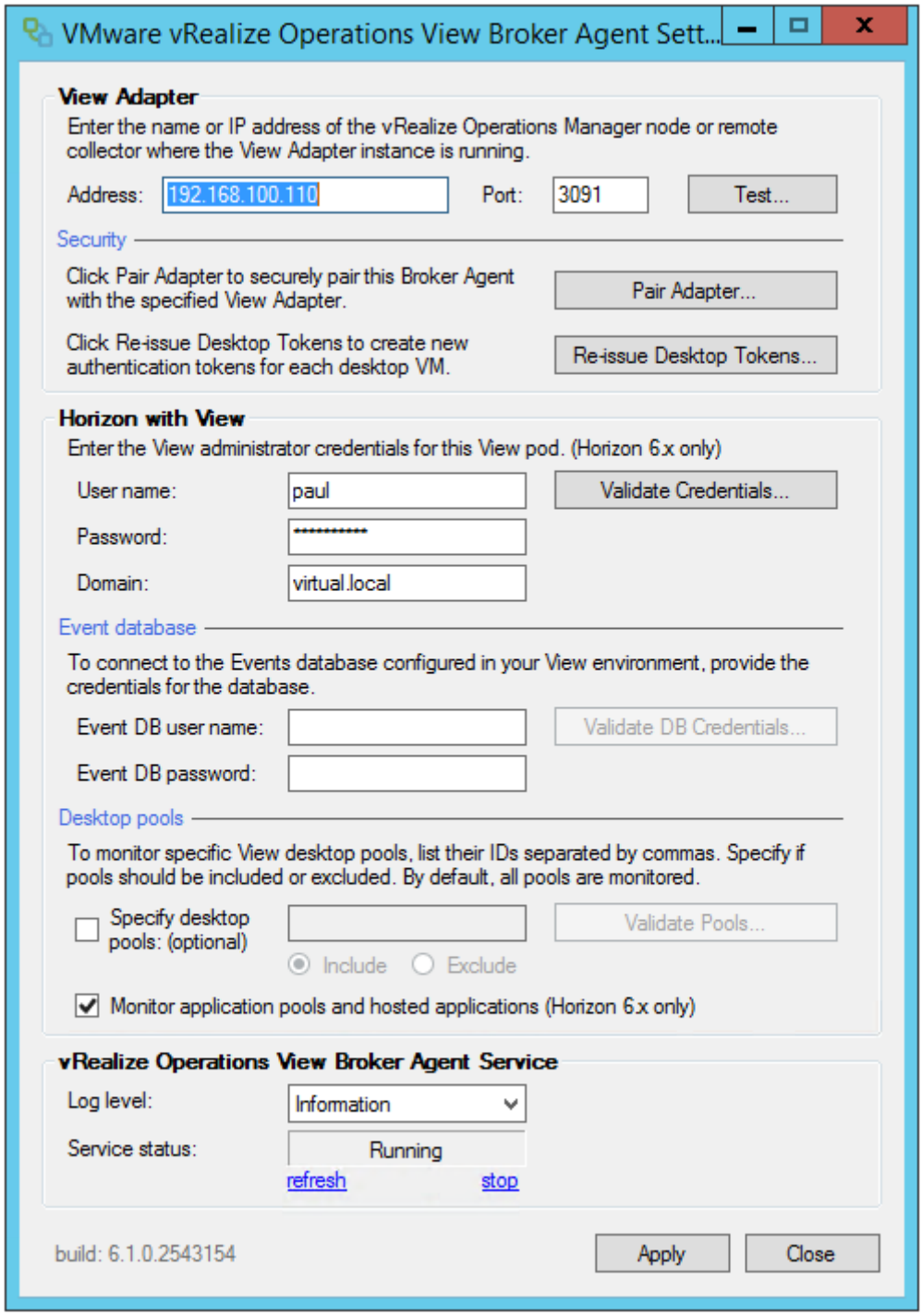

Figure 40

Apply the settings and Close the Window.

Other References:

Reference View Dashboards and Reports

Official Documentation: VMware vRealize Operations for Horizon Administrator Guide and Maximizing the Use of VMware vRealize Operations for Horizon

Summary:

Especially the Maximizing the Use of VMware vRealize Operations for Horizon provides a lot of useful information in getting up to speed with vRealize Operations for Horizon. This guide provides an introduction to this product and exercises how to use Dashboards, Alerts and Reports.

Other References:

Tools

VMware vRealize Operations for Horizon Administrator Guide

VMware vRealize Operations for Horizon Installation

VMware vRealize Operations for Horizon Security

Maximizing the Use of VMware vRealize Operations for Horizon

Horizon View Administrator