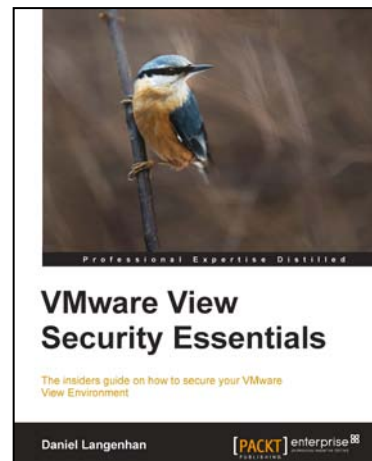


VMware View Security Essentials

Daniel Langenhan



Chapter No. 5 " Backup and Recovery "

In this package, you will find:

A Biography of the author of the book

A preview chapter from the book, Chapter NO.5 " Backup and Recovery "

A synopsis of the book's content

Information on where to buy this book

About the Author

Daniel Langenhan is a client-focused virtualization expert with more than 18years of international industry experience.

His skills span the breadth of virtualization, ranging from Architecture, Design, and implementation for large multitier enterprise client systems to delivering captivating education and training sessions in security technologies, and practices to diverse audiences.

He also possesses an extensive knowledge and experience in Process management, Enterprise level storage, and Linux and Solaris operating systems.

Utilizing his extensive knowledge, experience, and skills, he has a proven track record of successful integration of virtualization into different business areas, while minimizing cost and maximizing reliability and effectiveness of the solution for his clients.

He has gained some experience working with major Australian and International vendors and clients. Daniel's consulting company is well established with strong industry ties in many verticals; for example, Finance, Telecommunications, and Print. His consulting business also provided services to VMware International.

I would like to thank my wife Renata for her tireless support, without her this book would have not been possible.

For More Information:

www.packtpub.com/vmware-view-security-essentials/book

VMware View Security Essentials

Most people associate security with network security and focus on firewalls and network monitoring. But security is more than that. It starts with establishing a stable environment, protecting this environment not only from intrusion but also from malicious intent. Last but not the least it is about tracking the issue and recovering from it. All this is security and needs to be addressed.

What This Book Covers

Chapter 1, Introduction to View, gives a short overview of what a typical View environment contains as well as definitions of all the technical terms we will be using.

Chapter 2, Securing Your Base, explains that a VMware virtual machine image is hardware independent, replacing the physical corporate desktops with thin clients makes changes to the corporate desktop image a lot easier as well as centralizing the management of it. This centralization also creates the need to rethink provisioning and redundancy compared to the traditional IT methods. As everyone who uses a vDesktop is now dependent on the centralized virtual environment, it is of the utmost importance that this infrastructure is safe and available. We will discuss how to harden the View servers and integrate them into the existing VMware vSphere settings, such as HA, DRS, and event monitoring. We will also take a bit of time to understand how View logfiles work and how to read them.

Chapter 3, Securing the Connection, explains that corporate working environments are not limited to one site and it becomes more and more important for personnel to work from other places than the office. In being able to operate in the new mobile world it is even more important to secure your environment against intrusion. This chapter focuses on network security like firewalls, DMZ deployments, and user authentication.

Chapter 4, Securing the Client, addresses the issue of securing the client which most corporations find critical. Most corporate data theft comes from within the organization not from external threats and data theft. This means not only the control of who is able to log into what is of importance, but also addressing the usage of USB devices that can be used to extract corporate data.

Chapter 5, Backup and Recovery, deals with fundamental things that most people don't associate with security, but which still is of the utmost importance. Backup and restore of the VMware View environment itself is explained in this chapter.

For More Information:

www.packtpub.com/vmware-view-security-essentials/book

5

Backup and Recovery

In this chapter, we will explore how to backup and recover a View environment.

We will also learn how to back up Views, which is a rather important security feature when things go wrong.

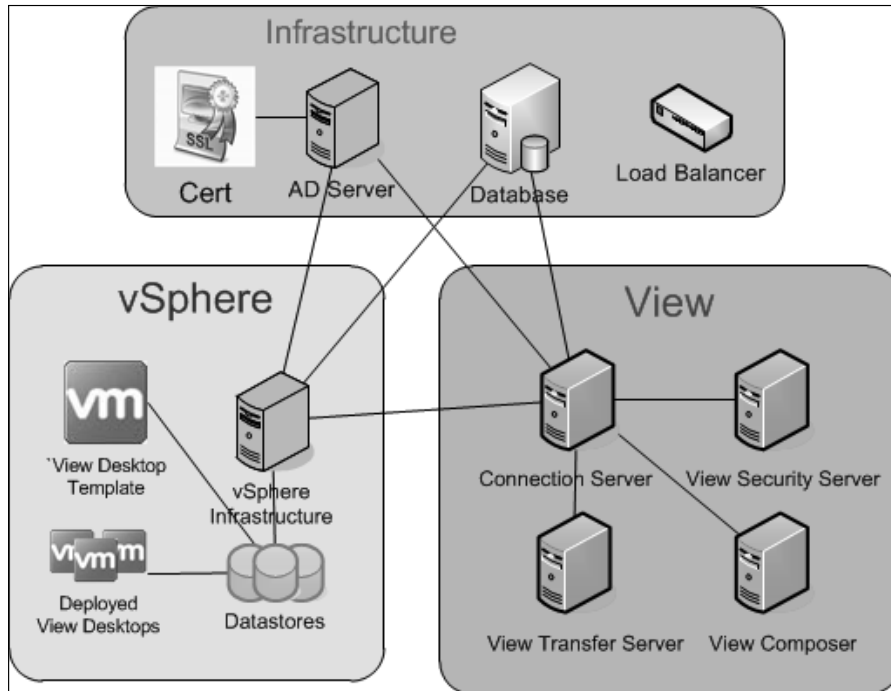
Backup and recovery

When we talk about backup, most people automatically think about the backup of the View desktops or the data within them. Only a very small set of View desktops need backup regularly, these are mostly persistent desktops for Admin or for special development purposes. In my opinion, the general View desktop doesn't need backup. All data that users touch should be on file servers and the View desktop just a tool that can be redeployed on demand.

For More Information:

www.packtpub.com/vmware-view-security-essentials/book

In regards of backup, each View environment splits up in three containers: VMware View Servers, vSphere, and infrastructure. Each of these components has its own backup requirements. But all these requirements need to be aligned as shown in the following diagram:



The vSphere environment

Let us start this section by diving into the backup at the root, the vSphere environment. The vSphere environment is the base on which VMware View runs. Not only do the View desktops run here but also the various View Servers. Backing up the vSphere environment is a book in itself; however I will shortly discuss the main components that require backup.

When we look at a vSphere 5.1 environment, we are looking at the following three main components: SSO, Inventory, and vCenter service. SSO and vCenter each require a database. Backing up the VM on which SSO and vCenter service are running is only good if you want a very fast recovery, however the most important piece to backup is the database where SSO and vCenter store their configuration.

You might want to backup the vSphere management VMs if you have added special configurations into the operation system, such as firewall rules or certificates. Most enterprises use tools from the storage or backup vendor to backup the complete datastores where all the VM's are stored. This makes the recovery of the base vSphere environment much easier and faster. But as said before the central pieces is the backup of the SSO and vCenter database. If you lose the database you will lose all configuration information of vSphere, which includes the configuration you set up for View (for example, users, folders, and many more). The important thing to understand here is that even if you rebuild the vCenter with the same folder or resource pool names, View will not be able to reconnect and use vCenter. The reason for this is that each object in vSphere has a **Managed object Reference (MoRef)** and View (as well as all other VMware products) uses the MoRef to talk to vCenter. The MoRef for each vSphere object is stored in the vCenter database.

As View and vSphere rely on each other, a backup of your View environment without a backup of the vSphere environment doesn't make any sense.

VMware View Servers

The View environment consists of the View Connection Servers, the View Security Servers, the View Composer (and its database) as well as some other components. The good news is that backup is a bit easier using the View Manager. The View Manager is able to extract all needed information from all the View servers and back them up centrally. However, the View Composer database should always be backed up regardless.

View Manager stores all information in its database. This database is an **Active Directory Application Mode (ADAM)** database, which is basically a LDAP based shared database. (see also <http://technet.microsoft.com/en-us/library/cc755705%28v=ws.10%29.aspx>) This database is located on the View Connection Servers. All entries in this database are replicated between all the View Connection Servers, which is another reason to create more than one View Connection Server.

Backing up all the View Connection Servers themselves is not really recommended. As all View Connection Servers share the same database, it is better to backup the configuration or one View Connection server and reinstall the others as replicas.

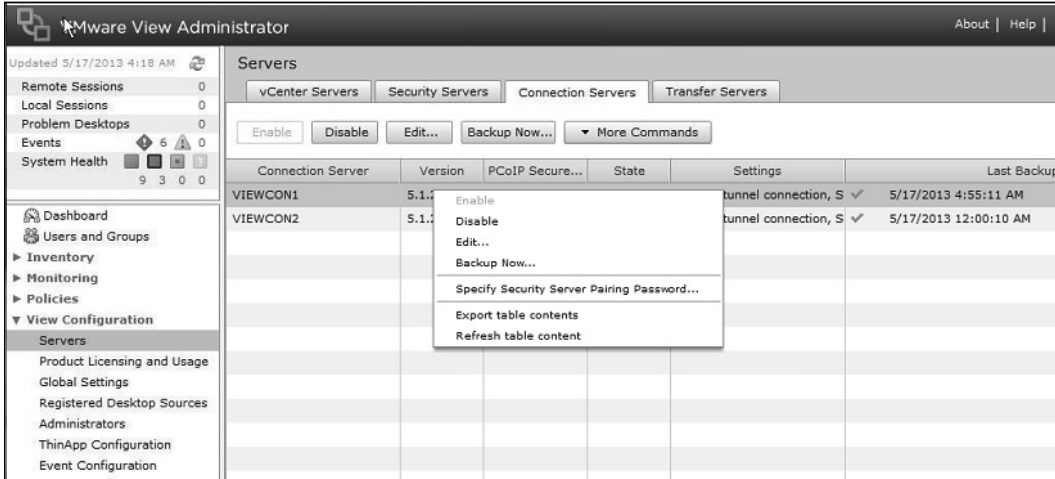
We will now run through a setup of the automated backup of the View ADAM database and the View Composer database. After this, we will look at the manual backup method.

For More Information:

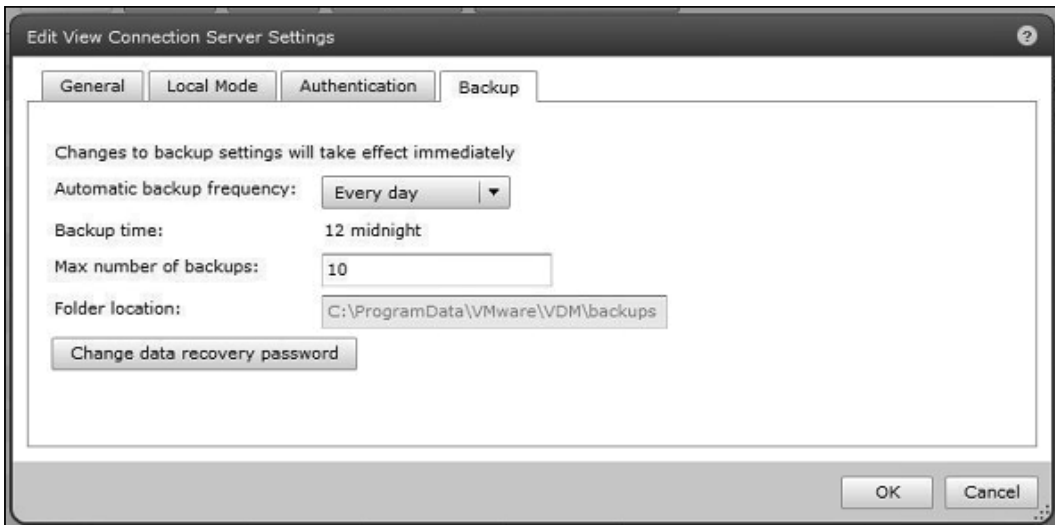
www.packtpub.com/vmware-view-security-essentials/book

To configure the automated backup of the View database follow these steps:

1. Log into the **View Administrator** console.
2. Expand **View Configuration** and click on **Servers**.
3. Right-click on one of the View Connection Servers and select **Edit**, as shown in the following screenshot:



4. Click on the **Backup** tab, as shown in the following screenshot:



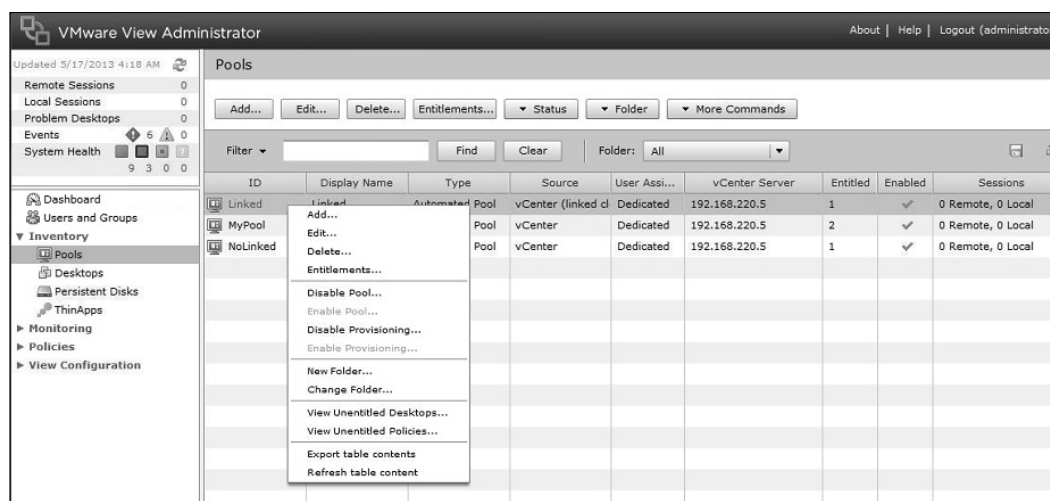
For More Information:

www.packtpub.com/vmware-view-security-essentials/book

5. Now, you can specify the following **Backup** settings. You have to set these only once as all View Connection Servers replicate their information:
 - **Automatic backup frequency:** How often should the backup run? You can configure these settings from **Every Hour** to **Never**.
 - **Max number of backups:** Defines number of backup files that will be stored in the location. Old files will be deleted.
 - **Folder location:** Defines where the backup files are stored, you may want to consider a network path here.
 - **Change data recovery password:** You can set and change the recovery password. The password protects the backup files.
6. Click on **OK** to close the dialog.

To manually backup the View database follow these steps:

1. Log into the **View Administrator** console
2. Select **Pools** and select a View desktop pool.
3. Right-click on the pool, and for the new VMs, select **Disable provisioning**. Repeat this action for all pool to make sure no new data is written to the ADAM Database, refer to the following screenshot:



4. Repeat this for all View desktop pools. This will make sure that during the time of the back up no additional information will be written to the View database.

For More Information:

www.packtpub.com/vmware-view-security-essentials/book

5. From here, there are two methods that can be used, either the manual method that allows for scripting the backup or the View Administrator console initiated version.

Let us see how to manually back up via DOS console.

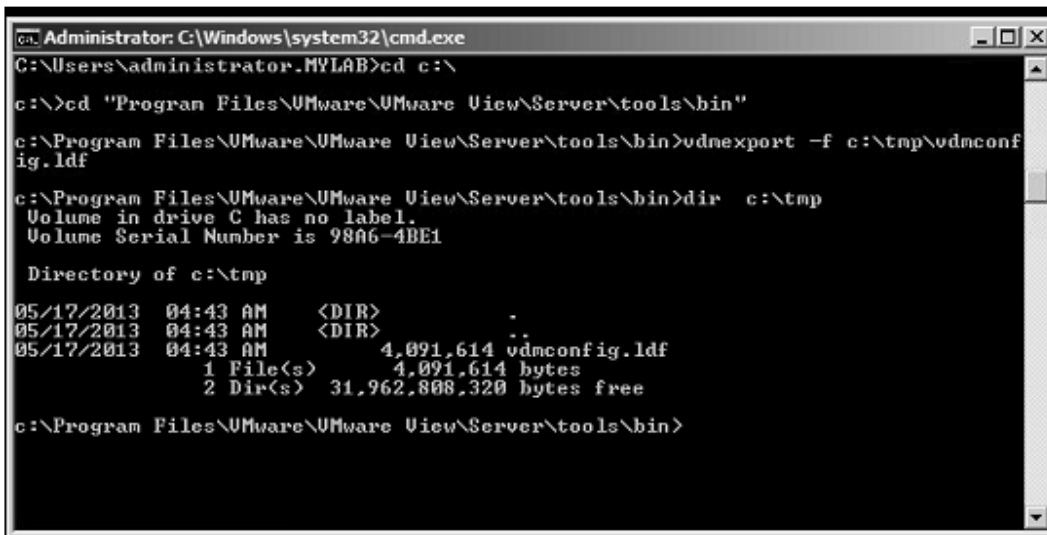
1. The export of the ADAM database is done via the export tool that is installed on the View Connections Server:

```
C:\Program Files\VMware\VMware View\Server\tools\bin\ vdmexport.exe
```

2. Run the `vdmexport.exe` command with the `-f` key to specify a location:

```
vdmexport -f c:\tmp\vdmconfig.ldf
```

The following screenshot shows how to do this:



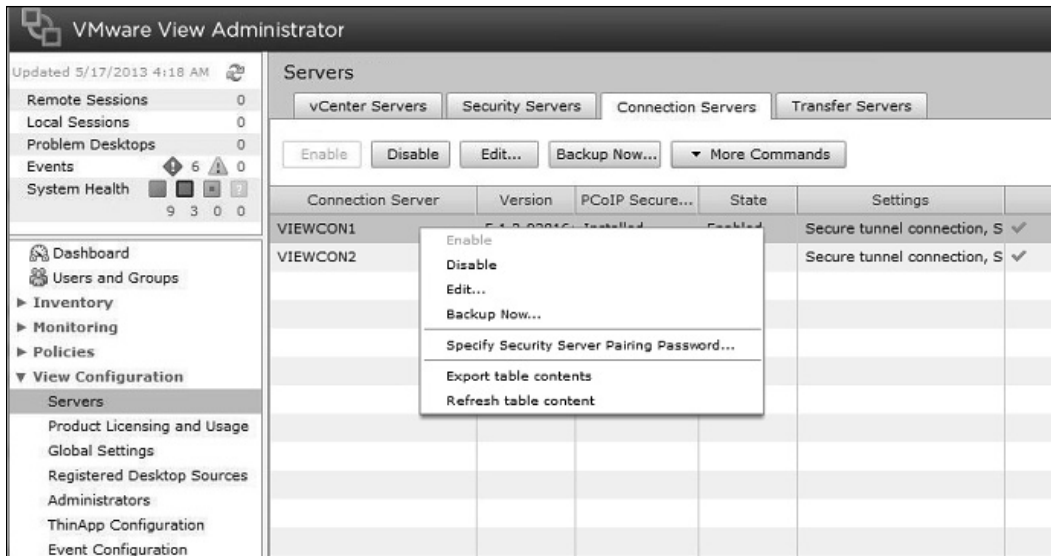
```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\administrator.MYLAB>cd c:\
c:\>cd "Program Files\VMware\VMware View\Server\tools\bin"
c:\Program Files\VMware\VMware View\Server\tools\bin>vdmexport -f c:\tmp\vdmconfig.ldf
c:\Program Files\VMware\VMware View\Server\tools\bin>dir c:\tmp
Volume in drive C has no label.
Volume Serial Number is 9806-4BE1

Directory of c:\tmp
05/17/2013  04:43 AM    <DIR>          .
05/17/2013  04:43 AM    <DIR>          ..
05/17/2013  04:43 AM                4,091,614 vdmconfig.ldf
               1 File(s)          4,091,614 bytes
               2 Dir(s)    31,962,808,320 bytes free

c:\Program Files\VMware\VMware View\Server\tools\bin>
```

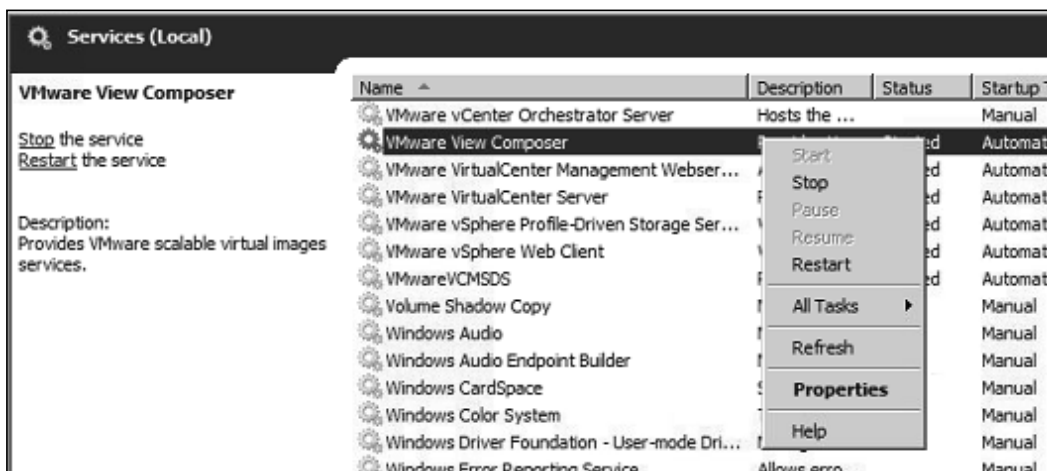
Let us see how to manually back up via the View Administrator console

1. In the **View Administrator** console, click on **Inventory** and select **Servers**.
2. Select any one of the View Connection Server.
3. Right-click and choose **Backup Now** as shown in the following screenshot:



To manually backup the View Composer database follow these steps:

1. Log in to the View Administrator console.
2. Select **Pools** and select a View desktop pool.
3. Right-click on the **Pool** and for new VMs, select **Disable provisioning**.
4. Log in to the VM where the View Composer is installed.
5. Stop the View Composer service. This will stop all further provisioning request for creating linked clones, which would change data in the View Composer database as shown in the following screenshot:



For More Information:

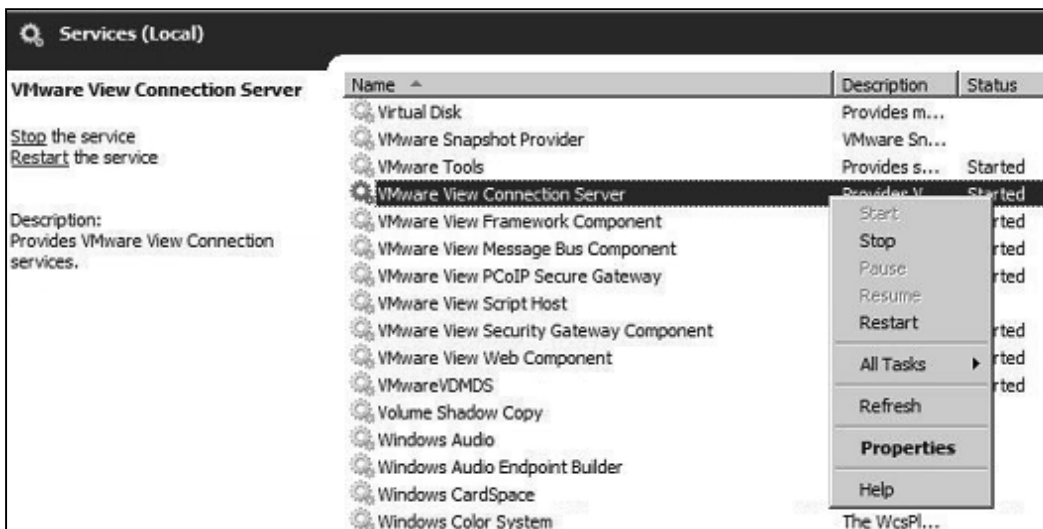
www.packtpub.com/vmware-view-security-essentials/book

6. After the Composer service is stopped the Composer database can be backed up using best practice for the given database.
7. Start the View Composer service again.

After backup the next important thing is restore. We will now walk through a restore of the View ADAM database configuration and then the View Composer Database.

To restore a View ADAM Database follow these steps:

1. If you have multiple View Connection Servers, the best way is to stop them and delete them. You will later have to reinstall them as replica servers.
2. Log in to the **View Connection Server**.
3. Stop the View Connection Server service as shown in the following screenshot:



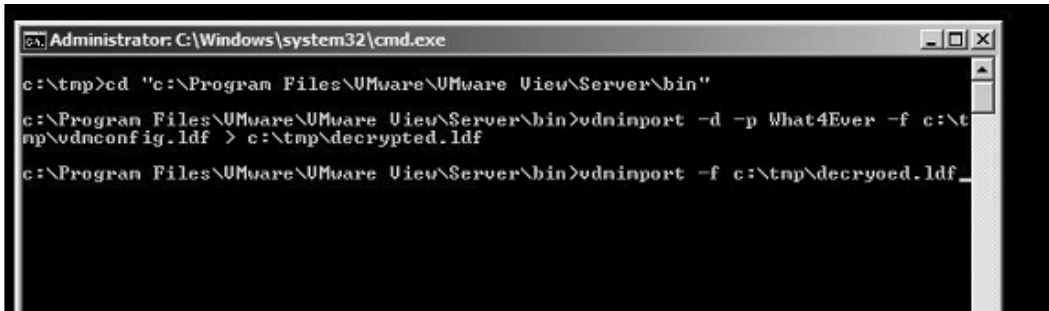
4. Locate the export/backup of the ADAM database (you are looking for an .ldf file).
5. The import is a two-step process. First, we will have to decrypt the file.
 1. To decrypt the file, use the vdmimport tool locate on any View Connection Server in C:\Program Files\VMware\VMware View\Server\tools\bin.
 2. Then use the following command:

```
vdmimport -d -p [Recovery password] -f [.ldf file] > [decrypted file]
```

- The second step is to import the decrypted file, again using the `vdmimport` tool. Run the following command:

```
vdmimport -f [decrypted file]
```

The following screenshot shows how to do this:



```
Administrator: C:\Windows\system32\cmd.exe
c:\tmp>cd "c:\Program Files\VMware\VMware View\Server\bin"
c:\Program Files\VMware\VMware View\Server\bin>vdmimport -d -p What4Ever -f c:\tmp\vdnconfig.ldb > c:\tmp\decrypted.ldb
c:\Program Files\VMware\VMware View\Server\bin>vdmimport -f c:\tmp\decryped.ldb
```

- The View ADAM database is now updated.
- Start the View Connection service.
- Reinstall all other View Connection Server as replica servers.

To restore a View Composer database follow these steps:

- Log into the VM where the View Composer is installed.
- Stop the **View Composer** service.
- Restore the View Composer database using best practice of the database vendor.
- Start the **View Composer** service.

Basic infrastructure

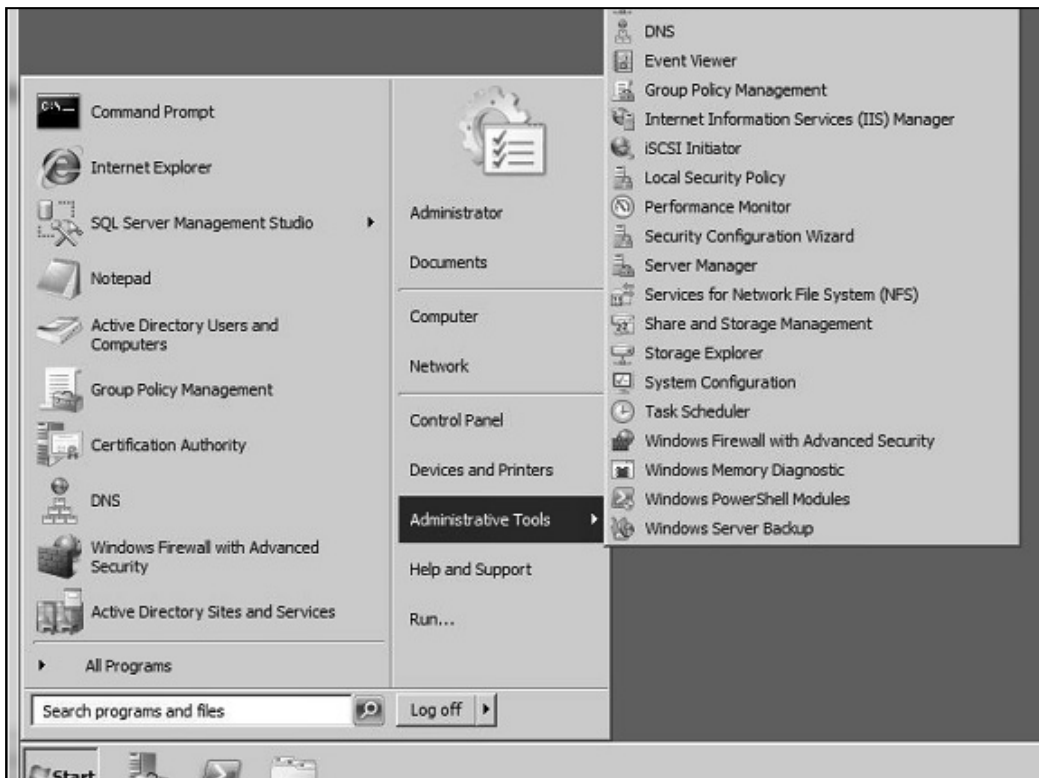
Next to the VMware vSphere environment, the common Infrastructure environment is rather important in the backup process.

The clearest target for backup is the database server that contains the vSphere, View Composer database, and the View Connection server event database. How to back up these databases is up to the best practice of the database vendor. However these databases should be backed up regularly. Restoring these databases requires that the system that uses them is shut down.

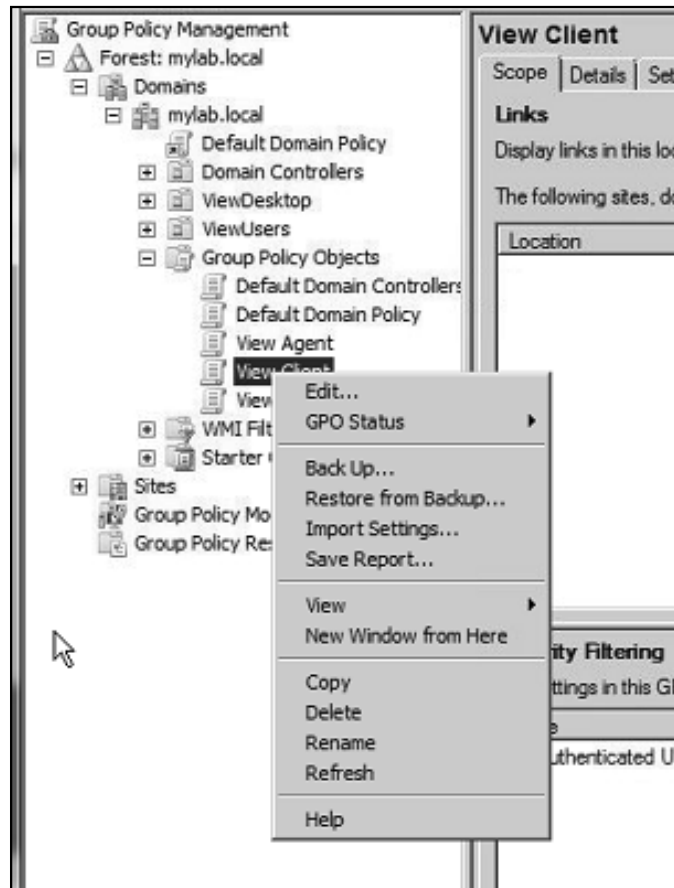
The other important thing about backup is the **Active Directory (AD)** part. We will leave the best methods of backing up and restoring AD to best practice of Microsoft. You might already know why AD is such an important thing. In the preparation to install View, you created certain **Organization Units (OUs)** and users with special rights (review *VMware Installation Guide*). In addition to that we used AD in the last chapter to configure security rules for client connections, USB access, and so on. If your AD is also a CA for your SSL Certs, then it even becomes more important to backup your AD. Restoring your AD is again left to best-practice of Microsoft. When AD is restored, we just can resume operations.

With respect to AD, it is a good idea when creating new GPO rules to create a separate backup for these rules. This is how you create a backup of an GPO:

1. Login to your AD server.
2. Open the **Group Policy Management** by navigating to **Start | Administrative Tools | Group Policy Management**, as shown in the following screenshot:

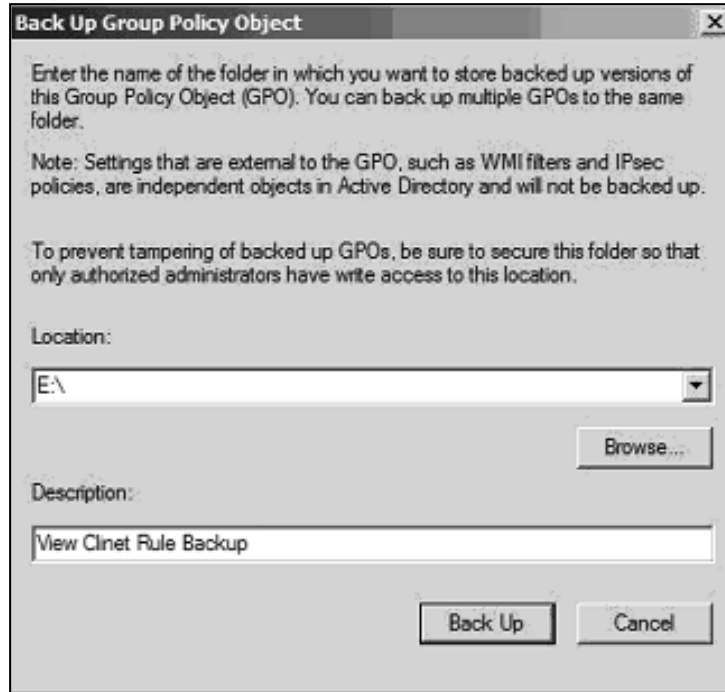


- Expand your domain and find the **Group Policy Object (GPO)**.
- Find the GPO you configured and right-click on it as shown in the following screenshot:



- Select **Back Up ...** from the right-click menu.

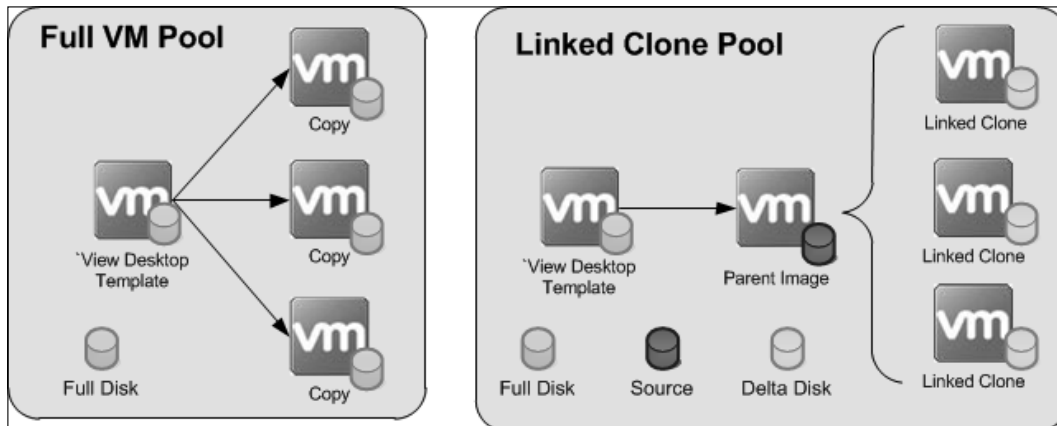
6. Select a location to store the backup, as shown in the following screenshot:



7. Click on **Back Up** to save the GPO.
8. The last but not the least important thing here is the load balancer that is setup for balancing the load of the View Connection or View Security Servers. Depending on the setup, the load balancer might have SSL Certificate installed or special configurations, backing these settings up once is enough.

Desktop pools and linked cloning

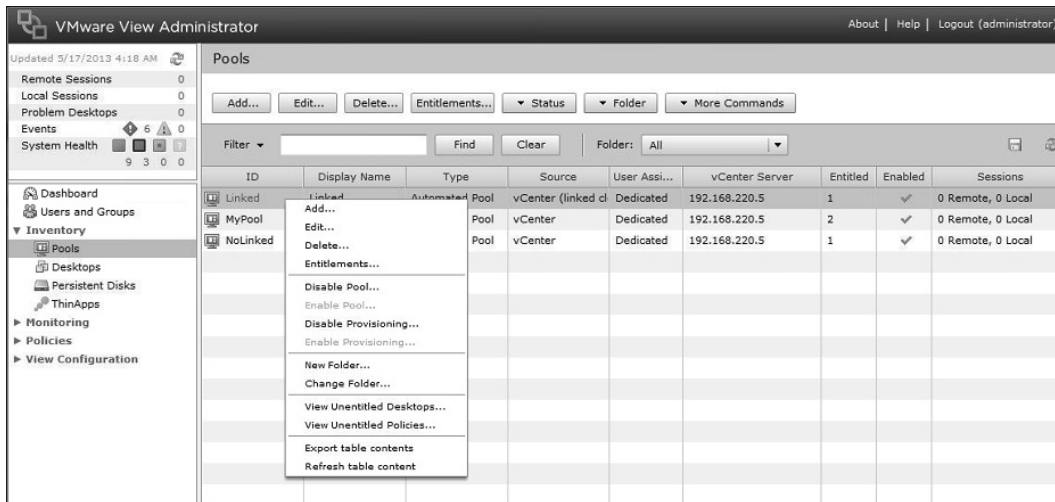
Backup becomes much more complicated when we take a look at already provisioned View desktop. There are basically two types of desktop pools: full provisioned VM and linked clone pools. The following screenshot shows the exact structure:



When a View desktop is provisioned as a full VM Pool, the View template VM is cloned and the View client connects to the View Agent installed on the VM. If the View desktop template is missing, the View VMs will still be working fine, however no new View desktops can be provisioned. When a linked View desktop pool is provisioned and the View desktop template is missing, new desktops can be provisioned because the linked clone parent still exists and additional linked clones can be provisioned. However it's better to go back and rectify this situation as soon as possible. That is done by recomposing a linked clone pool.

Follow these instructions to recompose a linked clone environment:

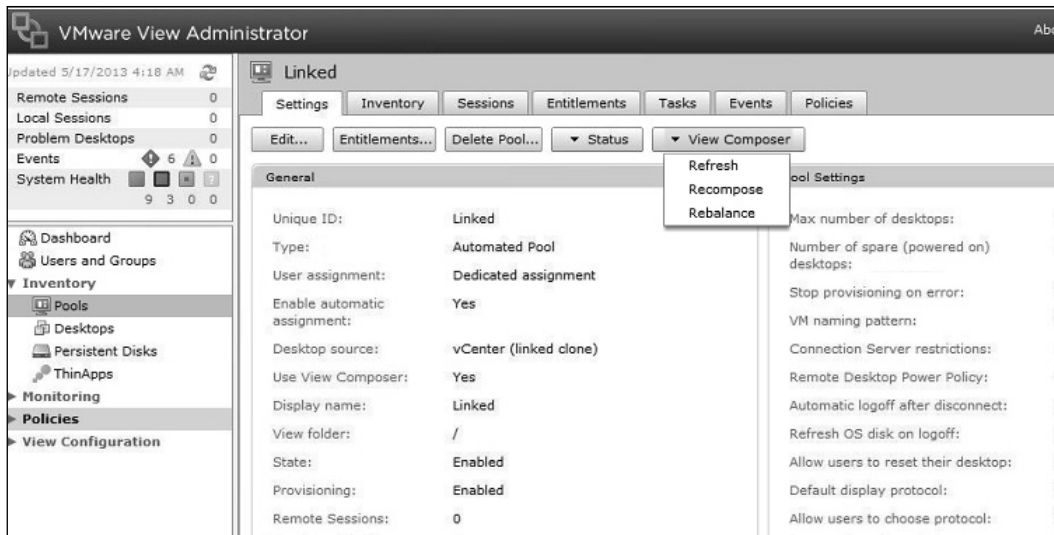
1. Log into the **View Administrator** console.
2. Expand **Inventory** and select **Pools**.
3. By disabling the pool provisioning, you make sure that while the reconfigure is running no new desktops are provisioned, as shown in the following screenshot:



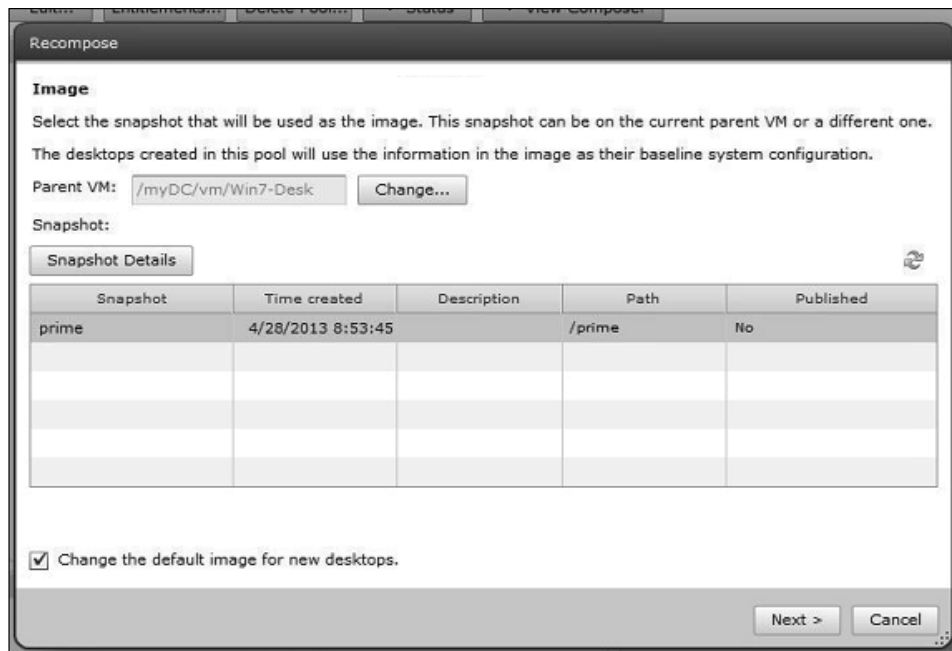
4. Double-click on the desktop pool you want to recompose.
5. Click on **View Composer** and select **Recompose** all desktops in the Pool, as shown in the following screenshot:

For More Information:

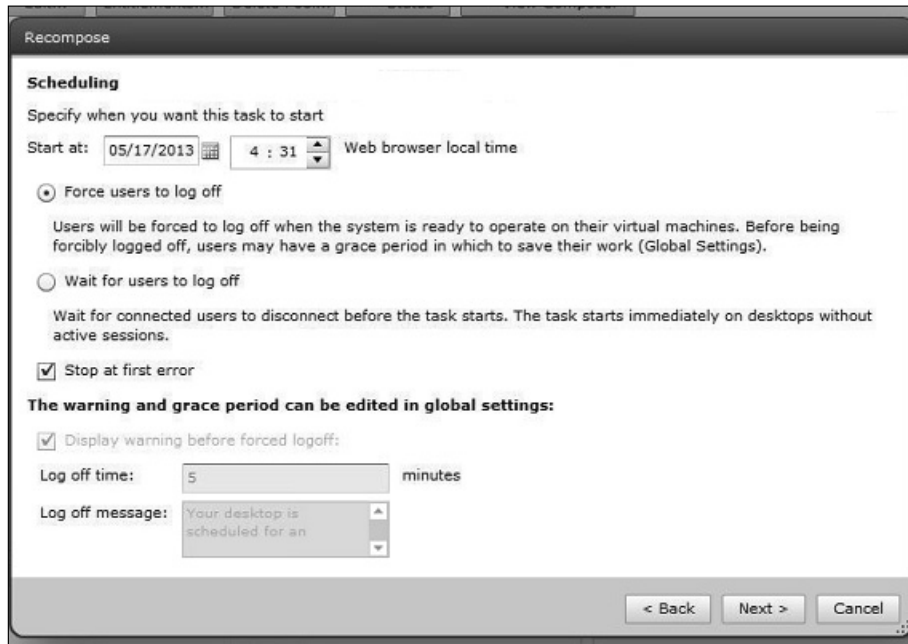
www.packtpub.com/vmware-view-security-essentials/book



- Choose the new image (the recovered one and an appropriate snapshot) and make sure to tick the **Change the default image for new desktops** option, as shown in the following screenshot:



7. While users are logged in, desktops cannot be recomposed. To rectify this you can either force the users to log off, wait until they log off, or schedule a time when the recompose should run (for example, at night). You should also consider sending a message to all users in this pool telling them what is going on. Refer to the following screenshot to see how it is done:



8. Finish the wizard implementation. The desktop will now recompose.

If linked clones or the parent image has gone missing there is nothing that can be done, but to redeploy the pool from the View desktop template. Linked clones cannot be restored, except if a *full* datastore backup is restored which contains the parent and all the cloned VM's. This works only if the VMs are still registered in vSphere, so when the datastore returns the VM's still have the correct MoRef for View Composer and View Connection Server to be able to use them.

When a full VM is deleted it can be recovered, as long as the VM is still registered in vSphere. If this is not the case the MoRef has changed. The VM will still run but VMware View Connection Server will not be able to connect the VM to a View Client.

The important lesson from this section is to make sure that important data is not stored on the View desktops. Using remote profiles and shares to store the user data will improve the security and backup of this data.

Documenting – the ultimate backup

One of the best backup methods is to document all settings and changes in a document. Actually there should be several documents, such as design, configuration, and build documents.

A design document would record all design decisions made and explain why they were made. This is an important document that will help to redesign, expand, and update a View installation. A design document is not changed often, as it shows basic layout of the solution and should only be updated if the layout changes.

A configuration document records all configuration settings for each of the components installed. Typically there would be one configuration documents for the View Connection Servers, one for the AD domains, and one for the DMZ. Each of these documents show all settings and should be updated when these settings are changed.

A build document contains detailed instructions on how to install certain software. These documents change only between versions of the software. The idea of these documents is to record all special installations steps that have to be done in a given environment.

The basic principle of documentation is that it is the last line of defense and a source of information. Information is important. I cannot count the amount of projects that were impacted because certain software installation had no documentation that explained what they interacted with, how they were configured and installed. Not having this information leads to delays or worse to the cancelation of projects.

Backup timing

Backup is all about timing. Creating a backup consumes space and also documentation. Should you need to restore, you will need to know which backup to restore from. This requires the knowledge of what backup was taken when and from what. Let's shed some light on some of these.

Let's start with something easy like the View desktop template. As discussed earlier, the View desktop template is the source of all View desktop pools. The View desktop template is an inactive VM that sits on the vSphere environment. Backup is only required if the template changes. So a once off backup is enough. However, it is also a good idea to document the settings of the View desktop pools.

For More Information:

www.packtpub.com/vmware-view-security-essentials/book

The same goes for the AD GPO's and the certificates; a backup/export of them is a good idea when they change.

Things that need a more regularly backup are View databases as well as the settings of the View and the vSphere environment.

The other aspect of timing is to understand how fast you need to restore. All these things should normally be covered in the design document. However let's review some ideas on this topic. Typical questions you should ask yourself are:

- How long can your business function without desktops?
- Which desktops need to be recovered first, for example, administrative desktops?
- If there are different View environments (for example, DMZ) are they all critical to be recovered at the same time?
- What pre-requisites must be recovered before a given View environment or pool can be recovered (for example, data sources)?
- When is a good time for backup? What time are no provisioning or destroy actions running on the View environment?
- Is the backup I'm running restorable? And how long do certain restore scenarios take?

The last question is the most important question. It is imperative to test the restore of your environment. This will provide you with a lot of benefits such as: the actual recovery timing, training on how to do it, the accuracy of the restore documentation, and last but not the least does your current backup regiment fulfill your requirements.

Patching the View environment

One of the many things you should do on a regular basis is patching, which should include the patching of the View servers and the View desktops.

This is not only done for View updates but more importantly for Windows updates to the server and to the desktop templates. To patch a View server with View updates, I highly recommend following the instructions that come with the View update (the release notes).

View server

To patch the View servers it is best if you have multiple View servers of any flavor, so you can patch the whole environment without interruption to the clients. It is however important to think back to the basics. When patching a View Connection Server that is the target of a View Security Server it makes sense to follow these steps:

1. Log onto the View Connection Server.
2. Stop the View Connection service.
3. Patch the View Connection Server with Windows updates.
4. Log onto the View Security Server associated with this View Connection Server.
5. Stop the View Security service.
6. Patch the View Security Server with Windows updates.
7. Start the View Connection service.
8. Start the View Security service.

View desktops

The patching of View desktop is a bit different. Patching a linked clone View desktop pool it is rather easy, you can use the recompose function, as we did earlier when we talked about restoring a desktop pool while, if you are patching a full clone pool, you will have to roll out new clones

The first basic steps are the same for linked and non-linked desktop pools:

1. Log in to the **View Administrator** console.
2. Select **Pools** and select a View desktop pool.
3. Right-click on the pool and for new VMs, select **Disable provisioning**. This step will insure that no new cloning activities are started and that we can modify the source.
4. Log in to vSphere.
5. Find your View desktop template.
6. If you are using multiple snapshots in the same VM, you need to select the one you want to alter.
7. Power-on the View desktop template.
8. Connect to the View desktop template and update the image as required.
9. Shut down the View desktop template.

At this stage we need to split off into linked and non-linked desktop pools.

For linked clone pools, follow these instructions:

1. Log into the **View Administrator** console.
2. Select **Pools** and select a View desktop pool.
3. Double-click on the pool you want to recompose.
4. Choose recompose all desktops in the pool.
5. Click on **View Composer** and select **Recompose**.
6. Finish the wizard implementation. The desktop will now recompose.

For non-linked clone, follow these instructions:

1. Log into the **View Administrator** console.
2. Select **Pools** and select a View desktop pool.
3. Right-click and select refresh.

Desktops with local mode must be checked in when recomposed. Alternatively you can roll back the local View desktop to force the new image onto the client.

Summary

This concludes our overview of backup and restore of a View environment. We looked at the vSphere backups and talked about the View environment backups and how interconnected they are. We discussed what to backup when and the important points of what really needs backup. Last but not the least, we also took a good look at restore operations, both automated and manually.

The patching of an View environment was also discussed. We talked about how to apply patching and what systems will be impacted, making it easier to assess the impact of patching on a productive environment.

Where to buy this book

You can buy VMware View Security Essentials from the Packt Publishing website:
<http://www.packtpub.com/vmware-view-security-essentials/book>

Free shipping to the US, UK, Europe and selected Asian countries. For more information, please read our [shipping policy](#).

Alternatively, you can buy the book from Amazon, BN.com, Computer Manuals and most internet book retailers.



www.PacktPub.com

For More Information:

www.packtpub.com/vmware-view-security-essentials/book