VMware View Administration Guide - Notes

Chapter 1 - Configuring View Connection Server

1. Using View Administrator

(EQ) View Administrator is the Web interface through which you configure View Connection Server and manage your View desktops

-Each security server is associated with one View Connection Server instance.

-Each View Transfer Server instance can communicate with any View Connection Server instance in a group of replicated instances

2. Configuring vCenter Server and View Composer

To use virtual machines as desktop sources, you must configure View Manager to communicate with **vCenter Server**

To create and manage linked-clone desktops, you must configure **View Composer** settings in View Manager

If you plan to have View Connection Server connect to the vCenter Server instance using a secure channel (SSL), **install a server SSL certificate on the vCenter Server host**

*. Set the **maximum number of concurrent provisioning operations** - This setting determines the largest number of concurrent requests that View Manager can make to provision full virtual machines in this vCenter Server instance. **Default value is 8**. This setting does not control linked-clone provisioning

*. Set the **maximum number of concurrent power operations** - This setting determines the largest number of power operations (startup, shutdown, suspend, and so on) **Default value is five**. This setting controls power operations for full virtual machines and linked clones

Create a User Account for View Composer (Use when adding View Composer)

Create a user in AD for View Composer. Permissions like **Create Computer Objects, Delete Computer Objects and Write all properties**

Default permissions are **Read all properties, Read permissions and List contents**

Configure View Composer Settings for vCenter Server

Add View Composer in View Manager with the user account created for View Composer. While specifying user account when adding use the following format: **domain.com\username** and in password enter the **password** of the account

3. Backing up View Connection Server

You should schedule regular backups of your **View Manager** and **View Composer** configuration data

4. Configuring Settings for Client Sessions

Global Settings for Client Sessions and Connections

- Session timeout
- Require SSL for client connections and View Administrator
- Re-authenticate secure tunnel connections after network interruption
- Message security mode
- Disable Single Sign-on for Local Mode operations
- Enable automatic status updates
- Display a pre-login message
- Display warning before forced logoff

Message Security Mode for View Components (JMS Messages)

You can set the level of security for communications between View components

Modes – Disabled\Enabled\Mixed

Configure the Secure Tunnel Connection and PCoIP Secure Gateway

- Use secure tunnel connection to desktop (Default – Enabled)
- Use PCoIP Secure Gateway for PCoIP connections to desktop (Default – Disabled)

Set a Single Sign-on Timeout Limit for View Users

You configure the SSO timeout limit by setting a value in View LDAP (ADSI)

The default value is **15** mins. A value of **-1** means that no SSO timeout limit is set. A value of **0** disables SSO

5. Disable or Enable View Connection Server

6. Edit the External URLs

*Tunnel clients that run outside of your network must use a **client-resolvable URL** to connect to a View Connection Server or security server host

7. View LDAP Directory (Schemas, DITs, ACLs)

*Security server instances do not contain a View LDAP directory

8. Configuring View Connection Server Settings

Use **View Administrator** to modify configuration settings for View Connection Server instances

Chapter 2 - Configuring Role-Based Delegated Administration

1. Understanding Roles and Privileges

An administrator role is a collection of privileges. Privileges grant the ability to perform specific actions, such as entitling a user to a desktop pool. Privileges also control what an administrator can see in View Administrator

*Administrator privileges are either **global (system wide) or object-specific (inventory objects)**

2. Using Folders to Delegate Administration

By default, desktop pools are created in the root folder, which appears as Root (/)

A desktop inherits the folder from its pool. An attached persistent disk inherits the folder from its desktop. You can have a maximum of **100** folders, including the root folder.

A role must contain at least one object-specific privilege to apply to a folder. Roles that contain only global privileges cannot be applied to folders

3. Understanding Permissions

4. Manage Administrators

Administrator's role is the most powerful role in View Administrator

5. Manage and Review Permissions

- Create a permission that includes a specific administrator user or group
- Create a permission that includes a specific role
- Create a permission that includes a specific folder

6. Manage and Review Folders (Max **100** folders including root folder)

Can **Add** a Folder, **Move** a Desktop Pool to a Different Folder, **Remove** a Folder, **Review the Desktop Pools** in a Folder, **Review the Desktops** in a Folder

7. Manage Custom Roles

Can **Add** a Custom Role, **Modify** the Privileges in a Custom Role and **Remove** a Custom Role

8. Predefined Roles and Privileges (Read this for exam again from the PDF)

View Administrator includes predefined roles. You can also create your own administrator roles by combining selected privileges

***Predefined Roles** – Administrators, Administrators (Read-only), Agent Registration Administrators, Global Configuration and Policy Administrators, Global Configuration and Policy Administrators (Read-only), Inventory Administrators, Inventory Administrators (Read only)

***Global Privileges** – Console Interaction (Use View Administrator), Direct Interaction (PowerShell and vdmexport), Manage Global Configuration and Policies (View and modify global policies and configuration), Manage Roles and Permissions (Create, modify, and delete administrator roles and permissions), Register Agent (Install View Agent on unmanaged desktop Sources)

***Internal Privileges** – Some of the predefined administrator roles contain internal privileges. You cannot select internal privileges when you create custom roles

9. Required Privileges for Common Tasks

- Privileges for Managing Pools
- Privileges for Managing Desktops
- Privileges for Managing Persistent Disks
- Privileges for Managing Users and Administrators
- Privileges for General Administration Tasks and Commands

10. Best Practices for Administrator Users and Groups

*Create separate administrators that can modify **global policies** and **View configuration** settings

Chapter 3 - Preparing Unmanaged Desktop Sources

Unmanaged desktop sources can include physical computer, terminal servers, and virtual machines running on VMware Server and other virtualization platforms

1. Prepare an Unmanaged Desktop Source for View Desktop Deployment

Verify that you have **administrative rights** on the unmanaged desktop source.

To make sure that View desktop users are added to the local Remote Desktop Users group of the unmanaged desktop source, create a **restricted Remote Desktop Users group** in Active Directory

2. Install View Agent on an Unmanaged Desktop Source

If you selected the USB redirection option, restart the unmanaged desktop source to enable USB support (W2K3 & W2K8 **do not support** USB redirection)

*.To use PCoIP with unmanaged desktops, install PCoIP Server component

PCoIP Smartcard lets users authenticate with smart cards when they use the PCoIP display protocol

Chapter 4 - Creating and Preparing Virtual Machines

1. Creating Virtual Machines for View Desktop Deployment

***Network** - For Windows 7 and Windows Vista operating systems, you must select the **VMXNET 3** network adapter.
Using the default E1000 adapter can cause customization timeout error on virtual machines. To use the VMXNET 3 adapter, you must install a Microsoft hotfix patch
***SCSI** - For Windows 7 and Windows XP guest operating systems, you should specify the **LSI Logic** adapter

PCoIP display protocol set the power option **Turn off the display** to **Never**
*(Optional) Disable Hot Plug PCI devices - This step prevents users from accidentally disconnecting the virtual network device (vNIC) from the VM

2. Install View Agent on a Virtual Machine

If you did not enable Remote Desktop support during guest operating system preparation, the View Agent installation program prompts you to enable it
If you selected the **View Composer Agent** option, the VMware View Composer Guest Agent Server service is started on the virtual machine

View Persona Management - Synchronizes the user profile on the local desktop with a remote profile repository, so that users have access to their profiles whenever they log in to a desktop

3. Install View Agent Silently

Silent Installation Feature	Custom setup option in an Interactive Installation
Core (Required when ADDLOCAL is Used)	None (Core is installed by default)
SVIAgent	View Composer Agent
ThinPrint	Virtual Printing
ThinPrintPCoIP	Virtual Printing with PCoIP
PCoIP	PCoIP Protocol
USB	USB Redirection
VPA	View Persona Management

4. Configure a Virtual Machine with Multiple NICs for View Agent

Regedit.exe - HKLM\Software\VMware, Inc.\VMware VDM\Node Manager\subnet = n.n.n.n/m (REG_SZ)

5. Optimize Windows Guest Operating System Performance (applies to all Windows operating systems). Listed below are few settings:

- Verify that hardware acceleration is enabled
- Disable the Indexing Service component
- Remove or minimize System Restore points
- Disable any unnecessary services
- Set visual effects to **Adjust for best performance**

6. Optimize Windows 7 Guest Operating System Performance (additional)

- Uninstall Tablet PC Components, unless this feature is needed
- Use the File System Utility (fsutil) command to disable the setting that keeps track of the last time a file was accessed
- Start the Registry Editor (regedit.exe) and change the **TimeOutValue**
- Change the virtual machine video card RAM setting to 128 MB

7. Optimizing Windows 7 for Linked-Clone Desktops

Service or Task	Impact on Linked-Clone OS Disks	Impact on IOPS	Turn Off This Service or Task?
Windows Hibernation	High	High	Yes
Windows Scheduled Disk Defrag	High	High	Yes
Windows Update Service	Med-High	Med-High	Yes
Windows Diagnostic Policy Service	Med-High	Small-Med	Yes
Prefetch/Superfetch	Medium	Medium	Yes
Windows Registry Backup	Medium	Medium	Yes
*System Restore	Small-Med	No major impact	Yes
Windows Defender	Med-High	Med-High	Yes
Microsoft Feeds Synchronization	Medium	Medium	Yes

8. Preparing Virtual Machines for View Composer

You cannot use View Composer to deploy desktops that run Windows Vista Ultimate Edition or Windows XP Professional SP1
*You cannot deploy linked clones from a parent virtual machine that contains more than one volume. The View Composer service does not support multiple disk partitions. Multiple **virtual disks** are supported
*Disable the **hibernation** option to reduce the size of linked-clone OS disks that are created from the parent virtual machine

Activating Windows 7 and Windows Vista on Linked-Clone Desktops (Use KMS)
View Composer does not support Multiple Activation Key (MAK) licensing

Disable Windows Hibernation in the Parent Virtual Machine
*. Disabling the hibernation option reduces the size of linked-clones
Hiberfil.sys is created when the hybrid sleep setting is turned on

Configure a Parent Virtual Machine to Use Local Storage
To store VM's swap files on the local datastore. This optional strategy lets you take advantage of local storage

Disposable Disk
To configure the disposable-file disk, you must know the maximum paging-file size in the parent virtual machine. You must configure this disk to be larger than the paging file in the guest OS

Increase the Timeout Limit of QuickPrep Customization Scripts
View Composer terminates a QuickPrep post-synchronization or power-off script that takes longer than 20 seconds
Change the **ExecScriptTimeout** Windows registry value on the parent virtual machine. The default value is 20000 milliseconds (20 seconds)

9. Creating Virtual Machine Templates (Only for Full Virtual Machines)

You must create a virtual machine template before you can create an automated pool that contains full virtual machines. Virtual machine template is a master copy

10. Creating Customization Specifications

When you use a Sysprep customization specification to join a Windows 7 desktop to a domain, you must use the **fully qualified domain name (FQDN)** of the AD domain. You **cannot** use the NetBIOS name of the AD domain

Chapter 5 - Creating Desktop Pools

1. Automated Pools That Contain Full Virtual Machines

Delete desktop after logoff - If you select floating user assignment, choose whether to delete desktops after users log off
Number of spare (powered on) desktops - If you specify names manually or use a naming pattern, specify a number of desktops that View Manager keeps available and powered on for new users
Minimum number of desktops - If you provision desktops on demand, View Manager creates desktops as users connect to the pool for the first time

Create an Automated Pool That Contains Full Virtual Machines (Only SYSPREP)
Virtual machine template - creates a new virtual machine in vCenter Server for each desktop
After creating the Automated Pool that contains Full VM, entitle users to access the pool
***Automated Pool, Dedicated Assignment – Below settings is not available**
Allow multiple sessions per user
Delete desktop after logoff

2. Linked-Clone Desktop Pools (Uses SYSPRERP or QuickPrep)

Delete or refresh desktop on logoff - If you select floating user assignment, choose whether to refresh desktops, delete desktops, or do nothing after users log off
***Redirect Windows profile to persistent disks –** For **dedicated user assignments**, use persistent disks
Disposable File Redirection - Redirect the guest OS's paging and temp files to a separate, nonpersistent disk. Disposable file redirection is supported in **vSphere mode only**
Publish **base image** to the Transfer Server repository for local mode operations
Storage Overcommit - As the level increases, more linked clones fit on the datastore and less space is **reserved** to let individual clones grow (only for linked-clones)
View Composer also creates a replica virtual machine that serves as the master image for provisioning the linked clones. The **replica** is created as a thin disk

If you do not store the replica on a separate datastore, View Composer creates a replica on each datastore on which linked clones are created
If you store the replica on a separate datastore, one replica is created for the entire pool, even when linked clones are created on multiple datastores

Linked-Clone Pool, Dedicated Assignment - Below settings is not available
Allow multiple sessions per user
Delete or refresh desktop on logoff
Linked-Clone Pool, Floating Assignment - Below settings is not available
Refresh OS disk after logoff

If you use **Sysprep**, a unique SID is generated for each clone
If you use **QuickPrep**, no new SID is generated. The parent virtual machine's SID is replicated on all provisioned linked-clone desktops in the pool

Sizing Formulas for Linked-Clone Pools
OS Disks - Number of VMs * (2 * memory of VM) + (2 * replica disk)
Persistent disk - Number of VMs * 20% of persistent disk
Sizing Formulas for Creating Linked Clones When You Edit a Pool or Store Replicas on a Separate Datastore
OS Disks - Number of VMs * (2 * memory of VM)
Persistent disk - Number of VMs * 20% of persistent disk
Storage Overcommit Levels

Option	**Description**
None	Storage is not overcommitted.
Conservative	4 times the size of the datastore. This is the **default level**.
Moderate	7 times the size of the datastore.
Aggressive	15 times the size of the datastore.

It would make sense to set an **aggressive** overcommit level for a floating-assignment desktop pool in which the desktops are set to delete or refresh after logoff
To enhance the availability of the linked-clone desktops, you can configure a high-availability solution for the datastore on which you store the replicas

Linked-Clone Desktop Data Disks
1. OS Disk,
2. QuickPrep Configuration-Data Disk (20 MB, cannot be configured),
3. View Composer Persistent Disk (For user-profile data (Optional)). This can be stored on the same datastore where OS Disk resides or on a diff datastore
4. Disposable-Data Disk (guest OS's paging and temp files (Optional))

3. Manual Desktop Pools
Managed - Desktop sources managed by vCenter Server
Unmanaged - View desktops delivered by machines that are not managed by vCenter Server

4. Microsoft Terminal Services Pools
Terminal Services pools support the **RDP display protocol** only
*Configure **Adobe Flash Throttling with IE in Terminal Services Sessions - IE->Internet Options->Enable third-party browser extensions->OK**
Restart **IE**

5. Provisioning Desktop Pools
Floating-assignment desktops let you reduce software licensing costs

Using a Naming Pattern for Automated Desktop Pools
*Desktop names have a 15-character limit

Number of Desktops in the Pool	**Maximum Prefix Length**
1-99	13 characters
100-999	12 characters
1,000 or more	11 characters

Using a Token in a Desktop Name
Ex: **amber-{n:fixed=3} or amber-{n}**

NOTE: You can start desktops in maintenance mode if you manually specify desktop names for the pool, not if you name desktops by providing a naming pattern

Prevent Access to View Desktops through RDP - Use Add\Edit Pool Wizard
Disable RDP in View Administrator when creating or editing the Pool using the wizard

6. Setting Power Policies for Desktop Pools
Power Policy Examples for Automated Pools with Floating Assignments
- Number of spare, powered-on desktops (is important to make desktops available for users immediately without long delays)

A View desktop can become temporarily inaccessible if the power policy configured for the virtual machine desktop is not compatible with a power option configured for the guest operating system

Chapter 6 - Entitling Users and Groups
Domain local groups are filtered out of search results for mixed-mode domains. You cannot entitle users in domain local groups if your domain is configured in mixed mode
Restricting View Desktop Access
*. When users log in through a tagged View Connection Server instance, they can access only those desktop pools that have at least one matching tag or no tags

You can also use restricted entitlements to control desktop access based on the user-authentication method that you configure for a particular View Connection Server instance. For example, you can make certain desktop pools available only to users who have authenticated with a smart card

View Connection Server	**Desktop Pool**	**Access Permitted?**
No tags	No tags	Yes
No tags	One or more tags	No
One or more tags	No tags	Yes
One or more tags	One or more tags	Only when tags match

You must configure restricted entitlements on the View Connection Server instance the security server is paired with
You cannot configure restricted entitlements on a security server
*. Even if a user is entitled to a particular desktop, the user will not be able to access that desktop if the desktop pool's tag does not match the tag assigned to the View Connection Server instance that the user connected to

You can assign a tag when you add or edit a desktop pool

Chapter 7 – Setting Up User Authentication
Smart card authentication is not supported by View Client for Mac or View Administrator
Display protocol switching is not supported with smart card authentication. To change display protocols after authenticating with a smart card, a user must log off and log in again
Step 1: Obtain the Root Certificate from the CA
The best certificate to select is usually the intermediate authority above the user certificate
Step 2: Export a Root Certificate from a User Certificate
If you have a CA-signed user certificate or a smart card that contains one, you can export the root certificate if it is trusted by your system
Step 3: Add the Root Certificate to a Server Truststore File
You must add the root certificate for all trusted users to a server truststore file so that View Connection Server instances and security servers can authenticate smart card users and connect them to their View desktops
Step 4: Modify View Connection Server Configuration Properties
To enable smart card authentication, you must modify View Connection Server configuration properties on your View Connection Server or security server host
- Create or edit **locked.properties**

Configuring Smart Card Authentication in View Administrator
If you configured smart card authentication for a View Connection Server instance, configure smart card authentication settings in **View Administrator**
*. You do not need to configure smart card authentication settings for a security server
When smart card authentication is required, authentication fails for users who select the **Log in as current user** check box when they connect to the View Connection Server instance

Prerequisites:
- Locked.properties needs to be modified
- Require SSL for client connections and View Administrator in View Administrator
Modify:
Authentication -> Smart card authentication -> Options (Not allowed, Optional, Required)

You must restart the View Connection Server service for changes to smart card settings to take effect. Changing from Optional to Required doesn't require a restart

1. Add UPNs for Smart Card Users – Because smart card logins rely on user principal names (UPNs), users that use smart cards to authenticate in View must have a valid UPN

2. Add the Root Certificate to the Enterprise NTAuth Store – use the certutil command to publish the certificate to the Enterprise NTAuth store

3. Add the Root Certificate to Trusted Root Certification Authorities – If you use a certification authority (CA) to issue smart card login or domain controller certificates, you must add the root certificate to the Trusted Root Certification Authorities group policy in Active Directory

4. Add an Intermediate Certificate to Intermediate Certification Authorities – If you use an intermediate certification authority (CA) to issue smart card login or domain controller certificates, you must add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory

Verify Your Smart Card Authentication Configuration

- Locked.properties, View Administrator -> Smart card authentication (optional\required), UPN's

For PCoIP display protocol -> View Agent PCoIP Smartcard sub-feature is installed

- In logs - messages stating that smart card authentication is enabled

Using RSA SecurID Authentication

Because RSA SecurID authentication works with RSA Authentication Manager, an RSA Authentication Manager server is required and must be directly accessible from the View Connection Server host

After successful validation against RSA Authentication Manager, users are prompted to enter their Active Directory credentials

Enable RSA SecurID Authentication in View Administrator

- Install and configure the RSA SecurID software
- Export the sdconf.rec file for the View Connection Server

Troubleshooting RSA SecurID Access Denial

The RSA Agent host node secret needs to be reset "Clear node secret"

Using the Log in as Current User Feature

You can use View Client group policy settings to control the availability of the **Log in as current user** check box and to specify its default value

Limitations and requirements:

-Log in as current user will not work for **Smart card authentication**

-Local mode will not work for **Log in as current user**

Time synchronization is required

-The client machine must be able to communicate with the corporate Active Directory server and not use cached credentials for authentication

Chapter 8 - Configuring Policies

You use Active Directory group policy settings to control the behavior of View components and certain features

1. Setting Policies in View Administrator

You use View Administrator to set policies for client sessions

- Policies that affect specific users and desktop pools are called user-level policies and desktop-level policies
- Policies that affect all sessions and users are called global policies

- You can configure global policies to control the behavior of all client sessions - users
- You can configure desktop-level policies to affect specific desktop pools. Desktop-level policy settings take precedence over their equivalent global policy settings
- You can configure user-level policies to affect specific users. User-level policy settings always take precedence over their equivalent global and desktop-level policy settings

View Policies

MMR, USB Access, Remote mode (Default value is "allow" for first three),
PCoIP Hardware Acceleration (Default value is "allow at medium" priority)

Local mode policies

Local mode (Allow),
User-initiated rollback (Allow),
Max timeout without server contact (7 days),
Target replication frequency (No replication),
User deferred replication (Deny),
Disks replicated (Persistent disks),
User-initiated check-in (Allow),
User-initiated replication (Allow)

2. Using Active Directory Group Policies

You can use Microsoft Windows Group Policy to optimize and secure View desktops, control the behavior of View components, and to configure location-based printing

When you enable loopback processing, a consistent set of policies applies to all users that log in to a particular computer, regardless of their location in Active Directory

3. Using the View Group Policy Administrative Template Files

View ADM template files contain both **Computer Configuration and User Configuration** group policies

View applies policies at View desktop startup and when users log in

VMware View Agent Configuration - **vdm_agent.adm -** Policy settings related to the authentication and environmental components of View Agent

VMware View Client Configuration - **vdm_client.adm (Connection, Security, Display, General) -** Contains policy settings related to View Client configuration

VMware View Server Configuration - **vdm_server.adm** - Contains policy settings related to View Connection Server

VMware View Common Configuration - **vdm_common.adm -** Contains policy settings that are common to all View components

VMware View PCoIP Session Variables - **pcoip.adm** - Contains policy settings related to the PCoIP display protocol

VMware View Persona Management Configuration - **ViewPM.adm** - Contains policy settings related to View Persona Management

VDM_AGENT.ADM (Computer Configuration and a User Configuration) - AllowDirectRDP - When connecting to a virtual desktop from View Client for Mac OS X, do not disable the AllowDirectRDP setting. This setting is enabled by default. AllowSingleSignon, ConnectionTicketTimeout, etc

VDM_CLIENT.ADM (Computer Configuration and a User Configuration) - Disable 3rd-party Terminal Services plugins - Determines whether View Client checks third-party Terminal Services plugins that are installed as normal RDP plugins

Server URL - Specifies the URL that View Client uses during login, for example, http://view1.example.com

Log in as current user settings can be done using this template

(Security) - Certificate verification mode, Enable Single Sign-On for smart card authentication, etc

(RDP) - Audio redirection, Display related settings, etc

(General settings)

VDM_SERVER.ADM (Computer Configuration) - (related to all View Connection Server) - Recursive Enumeration of Trusted Domains - This information is passed to View Connection Server so that all trusted domains are available to the client on login

VDM_COMMON.ADM - (Computer configuration) - Logs, Performance alarms

PCoIP.ADM - View PCoIP Session Variables ADM template file contains two subcategories. **Overridable Administrator Defaults & Not Overridable Administrator Settings**

***Configure clipboard redirection -** Enabled client to server only, Disabled in both directions, Enabled in both directions, Enabled server to client only

***Configure PCoIP image quality levels -** Minimum Image Quality, Maximum Initial Image Quality, and Maximum Frame Rate

***Configure PCoIP session encryption algorithms -** Salsa20-256round12 and AES-128-GCM algorithms

***Configure the Client PCoIP UDP port** - default, the base port is 50002 and the port range is 64

Configure the TCP port to which the PCoIP host binds and listens - By default, the base TCP port is 4172 for View 4.5 and later and 50002 for View 4.0.*x* and earlier

Configure the UDP port to which the PCoIP host binds and listens - By default, the base TCP port is 4172 for View 4.5 and later and 50002 for View 4.0.*x* and earlier

The PCoIP protocol is efficient enough to provide the **build-to-lossless feature** in all conditions, which allows this feature to stay on by default

4. Setting up Location-Based Printing

The location-based printing feature is available for both Windows and non-Windows client systems

Using this feature does require that the correct printer drivers be installed in the View desktop

AutoConnect Map Additional Printers for VMware View (Name changed in View 5)

You can define translation rules based on the client system's IP address, name, and MAC address, and on the user's name and group

4.1 Register the Location-Based Printing Group Policy DLL File

Before you can configure the group policy setting for location-based printing, register the DLL file **"TPVMGPoACmap.dll" -** regsvr32 "C:\TPVMGPoACmap.dll"
*View provides 32-bit and 64-bit versions of TPVMGPoACmap.dll in the directory

4.2 Configure the Location-Based Printing Group Policy

IP Range -Translation rule that specifies a range of IP addresses for client systems
Client Name - Translation rule that specifies a computer name
Mac Address - Translation rule that specifies a MAC address
User/Group - Translation rule that specifies a user or group name

5. Using Terminal Services Group Policies

General Terminal Services group policy - control log in and log off behavior, remote sessions, and desktop appearance
Terminal Services group policy - control disconnected and idle client sessions
(EQ) You can combine these settings with View **desktop power policies**

6. Active Directory Group Policy Example

One way to implement Active Directory group policies in View is to create an OU for your View desktops and link one or more GPOs to that OU
You can use these GPOs to apply group policy settings to your View desktops and to enable loopback processing
***Enable Loopback Processing for View Desktops**
To make User Configuration settings that usually apply to a computer apply to all of the users that log in to that computer, **enable loopback processing**

Chapter 9 - Configuring User Profiles with View Persona Management

With View Persona Management, you can configure user profiles that are dynamically synchronized with a remote profile repository
This feature gives users access to a personalized desktop experience whenever they log in to a desktop
View Persona Management expands the functionality and improves the **performance** of Windows roaming profiles
You configure group policy settings to enable View Persona Management and control various aspects of your View Persona Management deployment
*To enable and use View Persona Management, you must have a **View Premier license**

1. Providing User Personas in View

With the View Persona Management feature, a user's remote profile is dynamically downloaded when the user logs in to a View desktop
*View Persona Management is **an alternative** to Windows roaming profiles
A user profile comprises a variety of user-generated information:
- User-specific data and desktop settings
- Application data and settings
- Windows registry entries configured by user applications (including Sandbox data can be stored in the user profile)
- View Persona Management minimizes the time it takes to log in to and log off of desktops
- During login, View downloads only the files that Windows requires, such as user registry files. Other files are copied to the local desktop when the user or an application opens them from the local profile folder
- View copies recent changes in the local profile to the remote repository, typically once every few minutes. The default is every 10 minutes. You can specify how often to upload the local profile
- During logoff, only files that were updated since the last replication are copied to the remote repository

2. Persona Management and Windows Roaming Profiles

When Persona Management is enabled, you **cannot manage** View users' personas by using the Windows roaming profiles functions
You can specify files and folders within users' personas that are managed by Windows roaming profiles functionality instead of View Persona Management

3. Configuring a View Persona Management Deployment

Steps:
- You set up a remote repository that stores user profiles (New network share or an existing AD user profile path which is used for Windows roaming profiles)
- Install View Agent with the **View Persona Management** setup option on virtual machine desktops
- Add and configure View Persona Management group policy (ViewPM.adm) settings, and deploy desktop pools (To whole deployment or for one pool alone)
- Enable View Persona Management by enabling the **Manage user persona** group policy setting
- If you configured a network share for the remote profile repository, enable the **Persona repository location** group policy setting and specify the network share path
- (Optional) Configure other group policy settings in Active Directory or the Local Computer Policy configuration
- Create desktop pools from the virtual machines on which you installed View Agent with the **View Persona Management** setup option

NOTE: You can configure View Persona Management without having to configure Windows roaming profiles
(EQ) You can create the shared folder on a server, a network-attached storage (NAS) device, or a network server
If users are entitled to more than one pool, the pools that share users must be *configured with the same profile repository
NOTE A user cannot access the same profile if the user switches between desktops that have v1 user profiles and v2 user profiles. Windows XP uses v1 profiles. Windows Vista and Windows 7 use v2 profiles

Verify that a native RTO Virtual Profiles 2.0 is not installed on the virtual machine (uninstall this before installing View Persona Management)
On Windows XP virtual machines, download and install the Microsoft User Profile Hive Cleanup Service **(UPHClean)** in the guest operating system
UPHClean service is included with Windows 7 and Windows Vista operating systems. You do not have to install the service on these operating systems

Configure View Persona Management Policies
*To use View Persona Management, you must enable the **Manage user persona** group policy setting, which activates the View Persona Management software
To set up a user profile repository without using an Active Directory user profile path, you must configure the **Persona repository location** group policy setting

*Use **Administrative Templates** under **Computer Configuration**
*You cannot use View Persona Management with desktops that run in local mode
You can configure View Persona Management with pools that contain full virtual machines or linked-clones. The pools can use dedicated or floating assignments

4. Best Practices for Configuring a View Persona Management Deployment

Determining Whether to Remove Local User Profiles at Logoff
By **default** is disabled, View Persona Management does not delete user profiles from the local desktops when users log off
Handling Deployments That Include View Persona Management and Windows Roaming Profiles
If users intend to share data between existing Windows roaming profiles and View Persona Management profiles, you can configure Windows folder redirection

It is highly recommended that you use standard practices to back up network shares on which View Persona Management stores the profile repository (do not use software such as MozyPro or Windows Volume backup service with View Persona)
Use separate Persistent disks can enhance the performance of View Persona Management (when you use refresh and recompose)

As a best practice, download the actual ThinApp sandbox data in the background. Enable the **Folders to background download** group policy setting and add the ThinApp sandbox folders (does not download sandbox on when user logs in)

With View Composer persistent disks, you can preserve user data and settings while you manage linked-clone OS disks with refresh, recompose, and rebalance operations. You can configure persistent disks only with dedicated-assignment, linked-clone desktops
If you configure persistent disks, do not enable the **Remove local persona at log off** policy. Enabling this policy deletes the user data from the persistent disks when users log off

5. View Persona Management Group Policy Settings

The group policy settings are contained in these folders:
- Roaming & Synchronization (turns View Persona Management on and off)
- Folder Redirection (you can redirect user profile folders to a network share)
- Desktop UI (controls View Persona settings that users see on their desktops)
- Logging (determines name, location, and behavior of the View Persona log files)

Chapter 10 - Managing Linked-Clone Desktops

1. Reduce Linked-Clone Size with Desktop Refresh

A desktop refresh operation restores the operating system disk of each linked clone to its original state and size, reducing storage costs

You can schedule only one refresh operation at a time for a given set of linked clones. You can schedule multiple refresh operations if they affect different linked clones

*A refresh operation does not affect View Composer **persistent disks**

*View Composer can refresh a linked clone in as little **as half the time** it takes to delete and recreate the clone

2. Update Linked-Clone Desktops

Before you recompose a linked-clone desktop pool, you must update the parent virtual machine that you used as a base image for the linked clones

In a desktop recomposition, you can provide operating system patches, install or update applications, or modify the desktop hardware settings in all the linked clones in a desktop pool

Selecting the **Stop at first error** option does not affect customization. If a customization error occurs on a linked clone, other clones continue to be provisioned and customized

Verify that provisioning for the pool is enabled. When pool provisioning is disabled, View Manager stops the desktops from being customized after they are recomposed

NOTE: If you used a Sysprep customization specification to customize the linked clones when you created the desktop pool, new SIDs might be generated for the recomposed virtual machines

You can recompose linked-clone desktops that can run in local mode. However, the desktops must be checked in or rolled back to the datacenter before the recompose operation can take place

NOTE Desktops that were in local mode during the recompose operation continue to use the old base image. These desktops are not recomposed when users check them in

Recomposition also refreshes the linked clones, reducing the size of their OS disks

*Desktop recompositions do not affect View Composer persistent disks

You cannot recompose Windows 7 linked clones that use one OS disk controller to a new or updated parent virtual machine that uses a different OS disk controller

3. Rebalance Linked-Clone Desktops

A **desktop rebalance** operation evenly redistributes linked-clone desktops among available datastores

Verify that provisioning for the pool is enabled. When pool provisioning is disabled, View Manager stops the desktops from being customized after they are rebalanced

4. Manage View Composer Persistent Disks

You can detach a View Composer persistent disk from a linked-clone desktop and attach it to another linked clone. This feature lets you manage user information separately from linked-clone desktops

A View Composer persistent disk contains user settings and other user-generated data. You create persistent disks when you create a linked-clone desktop pool

View Manager can manage persistent disks from linked-clone pools that were created in View Manager 4.5 or later

You can attach a detached persistent disk as a secondary disk on the selected linked-clone desktop

Verify that the selected desktop uses the same operating system as the linked clone in which the persistent disk was created

You can assign a detached View Composer persistent disk to a new pool or user if the original pool or user was deleted from View Manager

---

Chapter 11 - Managing Desktops and Desktop Pools

1. Managing Desktop Pools

You can edit, disable, and delete desktop pools in View Administrator

You can edit only certain settings of a Pool. And certain settings are available only for Automated Pools

When you provision an automated desktop pool by using a naming pattern, you can increase or decrease the size of the pool by changing the maximum number of desktops

NOTE: When you decrease the size of a pool, the actual number of desktops might be larger than **Max number of desktops** if more users are currently logged in or assigned to desktops than the maximum number

Delete a Desktop Pool from View Manager

Users in currently active sessions can continue to use full virtual-machine desktops if you keep the virtual machines in vCenter Server. After the users log off, they cannot access the deleted desktops. With linked-clone desktops, vCenter Server always deletes the virtual machines from disk

2. Reducing Adobe Flash Bandwidth

You can reduce the amount of bandwidth used by Adobe Flash content that runs in View desktop sessions

Adobe Flash Quality (low, medium and high). Throttling (conservative, moderate and aggressive)

You can set Adobe Flash quality and throttling modes to reduce the amount of bandwidth that is used by Adobe Flash content in View desktops

To make use of Adobe Flash bandwidth-reduction settings, Adobe Flash must not be running in full screen mode

To ensure that Adobe Flash throttling works with IE in **Terminal Services** sessions, users must enable third-party browser extensions

3. Managing Virtual-Machine Desktops

You can search for, manage, and delete virtual-machine desktops and manage desktop sessions

Options - Disconnect session, Logoff session, Reset, Send message

You place existing desktops in maintenance mode one at a time. You can remove multiple desktops from maintenance mode in one operation

When you create a pool, you can start all the desktops in the pool in maintenance mode if you specify desktop **names manually**

***. Desktop Status of Virtual Machines**

*Provisioning	Provisioning	The virtual machine is being provisioned
*Provisioning error	Provisioning	An error occurred during provisioning
*Waiting for Agent	Agent state	View CS is waiting to establish communication with View Agent on a virtual machine in a manual pool. *This state is the same as the Customizing state for a VM in an automated pool
*Startup	Agent state	View Agent has started on the virtual machine, but other required services such as the display protocol are still starting
*Agent unreachable	Agent state	View Connection Server cannot establish communication with View Agent on a virtual machine
*Configuration error	Agent state	The display protocol such as RDP or PCoIP is not enabled
*Provisioned	Availability	The virtual machine is powered off
Error	Miscellaneous	An unknown error occurred in the VM

4. Export View Information to External Files

You can view and manage the information in a spreadsheet or another tool

When you export a View Administrator table, it is saved as a comma-separated **cvs** file. This feature exports the entire table, not individual pages

The default filename is **global_table_data_export.csv**

Chapter 12 - Managing Physical Computers and Terminal Servers

Virtual machines that are not managed by vCenter Server, physical computers, blade PCs, and Microsoft Terminal Services sources

NOTE: When you reconfigure a setting that affects an unmanaged desktop source, it can take up to 10 minutes for the new setting to take effect

1. Add an Unmanaged Desktop Source to a Pool

You can increase the size of a manual desktop pool that uses unmanaged desktop sources by adding desktop sources to the pool

2. Remove an Unmanaged Desktop Source from a Pool

You can reduce the size of a manual desktop pool that uses unmanaged desktop sources by removing desktop sources from the pool

3. Delete a Pool That Contains Unmanaged Desktops

When you delete a desktop pool that contains unmanaged desktop sources, the pool is removed from View Manager

View Manager does not delete the registration information for the unmanaged desktop sources that belong to the pool

4. Unregister an Unmanaged Desktop Source

All desktop sources that vCenter Server manages are registered when you install View Agent. You can unregister only unmanaged desktop sources

When you unregister a desktop source, it becomes unavailable in View Manager. To make a source available again, reinstall View Agent in the desktop source

When removing or deleting the unmanaged desktop sources from a pool active sessions can:

Leave active - Active sessions remain until the user logs off. View Connection Server does not keep track of these sessions

Terminate - Active sessions end immediately

5. Desktop Status of Physical Computers and Terminal Servers

Waiting for Agent	View Connection Server is waiting to receive the first request from View Agent on a physical-computer or terminal-server desktop
Agent not reachable	View Connection Server cannot establish communication with View Agent on the desktop. The desktop-source computer might be **powered off**
Configuration error	The display protocol such as RDP is not enabled, a terminal server is not enabled, or another protocol is not enabled

Chapter 13 - Managing ThinApp Applications in View Administrator

Must have license to use the ThinApp management feature in View Administrator

1. View Requirements for ThinApp Applications (ThinApp 4.6 or later required)

Configure the file and sharing permissions on the shared folder to give Read access to the built-in Active Directory group **Domain Computers**

If you plan to distribute ThinApp applications to domain controllers, you must also give Read access to the built-in Active Directory group **Domain Controllers**

For **streaming** ThinApp application, **Read & Execute** for users is required

Make sure that a disjoint namespace does not prevent domain member computers from accessing the network share that hosts the MSI packages

2. Capturing and Storing Application Packages (Streaming - MSIStreaming=1)

ThinApp provides application virtualization by decoupling an application from the underlying operating system and its libraries and framework

NOTE: If you have multiple application repositories, you can use third-party solutions to manage load balancing and availability. View does not one inbuilt

***Package Your Applications, Create a Windows Network Share, Register an Application Repository, Add ThinApp Applications to View Administrator, Create a ThinApp Template (Optional),**

The network share path must be in the form \\*ServerComputerName**ShareName* where *ServerComputerName* is the DNS name of the server computer. Do not specify an IP address

3. Assigning ThinApp Applications to Desktops and Pools

*When you assign a ThinApp application to a **desktop**, View Administrator begins installing the application on the desktop a few minutes later.

*When you assign a ThinApp application to a **pool**, View Administrator begins installing the application the first time a user logs in to a desktop in the pool

IMPORTANT: You can assign ThinApp applications to desktops and pools that have virtual machine sources only. You cannot assign ThinApp applications to Terminal Servers, Blade PCs, or traditional PCs

View Administrator returns an application assignment error if a ThinApp template contains an application that is already assigned to the desktop or pool

4. Maintaining ThinApp Applications in View Administrator

NOTE: To upgrade a ThinApp application, you must unassign and remove the older version of the application and add and assign the newer version

IMPORTANT: If an end user is using the ThinApp application at the time when View Administrator attempts to uninstall the application, the uninstallation fails and the application status changes to Uninstall Error. When this error occurs, you must first manually uninstall the ThinApp application files from the View desktop and then click **Force Clear Assignment** in View Administrator

NOTE: You cannot remove a ThinApp application if it is already assigned to a desktop or pool or if it is in the Pending Uninstall state

*You can add and remove applications from a ThinApp template. You can also delete a ThinApp template

*You cannot edit the share path of an application repository in ViewAdministrator

5. Monitoring and Troubleshooting ThinApp Applications in View Administrator

View Administrator logs events that are related to ThinApp application management to the Events and Reporting database. You can view these events on the **Events** tab in View Administrator

Cannot Register an Application Repository

- Problem - The View Connection Server host cannot access the network share that hosts the application repository. The network share path that you typed in the **Share path** text box might be incorrect

- Solution - The network share that hosts the application repository is in a domain that is not accessible from the View Connection Server host, or the network share permissions have not been set up properly

Cannot Add ThinApp Applications to View Administrator

- **Problem** - Either the application packages are not in MSI format or the View Connection Server host cannot access the directories in the network share

- **Solution** - Verify that the application packages in the application repository are in MSI format

ThinApp Application Is Not Installed (Solution - Retry Install\Force Clear Assignment)

Not enough disk space on the desktop

*. Network was lost between the View Connection Server host and the desktop or between the View Connection Server host and the application repository

Application was not accessible in the network share

Application was previously installed or the directory or file already exists on the desktop

ThinApp Application Is Not Uninstalled (Solution - Retry Uninstall)

ThinApp application was busy when View Administrator tried to uninstall it.

*Network connectivity was lost between the View Connection Server host and the desktop

MSI Package Is Invalid

- The MSI file is corrupted
- The MSI file was not created with ThinApp
- The MSI file was created or repackaged with an unsupported version of ThinApp. You must use ThinApp version 4.6 or later

Chapter 14 - Managing Local Desktops

1. Benefits of Using View Desktops in Local Mode (use dedicated assignment)

The local View desktop can automatically use up to two CPUs available on the local system, and you can configure the local desktop to use up to four CPUs

The data on each local system is encrypted with AES 128-bit encryption (default). But you can configure 192-bit or 256-bit encryption

*Verify that the **Local Mode** policy is set to **Allow** for the desktop pool.

*If you want desktops to run only in local mode so that users must always check out the desktop, set the **Remote Mode** policy to **Deny**

IMPORTANT: You cannot check out a desktop if when you logged in, you used the **Log in as current user** feature. You must close View Client, start it again, and clear the **Log in as current user** check box

For local mode View desktop uses NAT so that it shares the IP and MAC addresses of the local computer

*SSL for local mode operations such as checking out and checking in desktops or for replicating data back to the datacenter, View TS requires additional vCPU

*You might also need more processing power if you turn on **compression for replication** operations. Automatic replication - default is for **every 12 hours**

Deduplication & compression features reduce the amount of network bandwidth

2. Managing View Transfer Server

When all View Transfer Server instances are in maintenance mode, you can **migrate** the Transfer Server repository

In a WAN environment with high network latency, you can enhance transfer performance by increasing the sizes of TCP send and receive windows (640 KB)

In 2K8, 640 KB is set automatically. In 2K3, change windows registry to 640 KB

View TS synchronizes local desktops with the corresponding desktops in the datacenter by replicating **user-generated changes** to the datacenter

View TS **distributes common system data** from the datacenter to local clients

3. Managing the Transfer Server Repository

View TS repository is required for checking out linked-clone desktops to run in local mode

You do not use View Composer linked clones in local mode, you do not have to configure a View TS repository

When you run linked-clone desktops in the datacenter, the linked clones share access to one base image

*When you run a linked-clone desktop in local mode, a copy of the base image must reside with the linked-clone desktop on the local computer

*As a best practice, to enhance the security of access to the TS repository, make sure that you restrict network access for the repository to **View administrators**

4. Managing Data Transfers

User deferred replication - The deferment period is two hours

5. Configure Security and Optimization for Local Desktop Operations

You use deduplication and compression to optimize data transfers

6. Configuring Endpoint Resource Usage

Memory Allocation	**Windows XP Guests**	**Windows 7 and Vista**
Minimum	512MB	1GB
Best effort	512MB + (Available/2)	1GB + (Available/2)
Maximum	2GB	4GB

7. Configuring an HTTP Cache to Provision Local Desktops Over a WAN

HTTP cache, the base image is stored in the proxy server's cache when the first user checks out a desktop. When subsequent users check out desktops, the base image is transferred over the LAN within the local office (**useProxyForTransfer)**

To complete a check-out operation, View Transfer Server still must transfer each user's linked-clone OS disk and persistent disk from the datacenter over the WAN, but these disks are a fraction of the size of the base image

8. Configuring the Heartbeat Interval for Local Desktop Client Computers

Client computers that host local desktops send heartbeat messages to View Connection Server at regular intervals to read the status of their checked-out desktops. The default heartbeat interval for all client computers is **five** minutes

9. Manually Downloading a Local Desktop to a Location with Poor Network Connections

You must remove the read-only attribute on the package files and give the user **Full control** privilege on the directory and all the files it contains

10. Troubleshooting View Transfer Server and Local Desktop Operations

***Problem -** The check-out can fail when the operation is approximately 10% complete

Cause - This problem can occur because View Transfer Server is running on an ESX host that does not have access to the datastores where the desktops reside

***Problem -** You might see an error message such as, Cannot access local desktop--desktop corrupted

Cause - If you change the encryption key cipher for a local desktop, or if you delete the desktop from its pool and create a new one, View Connection Server uses a new authentication key to generate a new configuration file

***Problem** - Virtual Disk of a Local Desktop Needs Repair

Cause - The problem can occur if you disconnect or power off the client computer while the virtual machine image is being updated

***Problem** - Recover Data from a Local Desktop

Solution – Use vdmadmin –V (Use this only if you cannot recover the data in a local desktop by any other method)

Chapter 15 - Maintaining View Components

1. Backing Up and Restoring View Configuration Data

Back up your **View Manager** and **View Composer** configuration data

NOTE: The vdmexport tool backs up the View LDAP data only. This tool does not back up View Composer database information

*vdmexport needs Administrators or Administrators (Read only) role

*vdmimport needs Administrators role

Use the **SviConfig restoredata** command to restore View Composer database data

2. Monitor View Components

Monitoring using the View Administrator Dashboard

*Green up arrow - component has no problems

*Red down arrow - component is unavailable or not functioning

*Yellow double arrow - component is in a warning state

*Question mark - status of a component is unknown

3. Monitor Desktop Status

Desktop Status - Preparing; Problem Desktops; Prepared for use

4. Understanding View Manager Services

View CS - 8 Services, Security Server - 4 Services, View TS - 4 Services

5. Add Licenses to VMware View

6. Update General User Information from Active Directory

Updates View Manager with the current user information that is stored in AD and updates name, phone, email, user name and default Windows domain of View users

7. Migrating View Composer with an Existing Database

To use an existing View Composer database, you must migrate the RSA key container between computers.

You migrate the RSA key container by using the ASP.NET IIS registration tool provided with Microsoft .NET Framework

8. Update the Certificates on a View CS Instance or Security Server

When you receive updated server SSL certificates or intermediate certificates, you import the certificates into a new keystore file and update the **locked.properties** file on each View CS or security server host to use the new keystore file

*Server certificates expire after 12 months

*Root and intermediate certificates expire after 5 or 10 years

Chapter 16 - Troubleshooting View Components

1. Monitor Events in View Manager

You might need to take some action if you see messages that are associated with Audit Failure, Error, or Warning events

2. Collecting Diagnostic Information for VMware View

Collect Diagnostic Information for View Composer Using the Support Script

Syntax: cscript ".\svi-support.wsf /zip"

Collect Diagnostic Information for View Connection Server Using the Support Tool (Select logging level to 2 - debug level of logging, normal 1 is the default)

3. Troubleshooting Desktop Pool Creation Problems

Pool Creation Fails if Customization Specifications Cannot Be Found

Provisioning error occurred for Machine Machine_Name: Customization failed for Machine

Solution - Verify that you have sufficient permissions to access the customization specifications, and to create a pool

If the customization specification no longer exists because it has been renamed or deleted, choose a different specification

Pool Creation Fails Because of a Permissions Problem

You do not have the correct permissions to create a pool

You do not have the correct permissions to access the templates

You do not have the correct permissions to access the ESX/ESXi host, ESX/ESXi cluster, or datacenter

Pool Provisioning Fails Due to a Configuration Problem

A template is not accessible.

The name of a template has been changed in vCenter.

A template has been moved to a different folder in vCenter.

A virtual machine image has been moved between ESX/ESXi hosts or been deleted

Pool Provisioning Fails Due to a View Connection Server Instance Being Unable to Connect to vCenter

The Web service on the vCenter Server has stopped

There are networking problems between the View Connection Server host and the vCenter Server

The port numbers and login details for vCenter or View Composer have changed

Pool Provisioning Fails Due to Datastore Problem

Verify that you have sufficient permissions to access the selected datastore.

Verify whether the disk on which the datastore is configured is full.

If the disk is full or the space is reserved, free up space on the disk, rebalance the available datastores, or migrate the datastore to a larger disk

Pool Provisioning Fails Due to vCenter Being Overloaded

In View Administrator, reduce the maximum number of concurrent provisioning and power operations for vCenter

Configure additional vCenter Servers

Virtual Machines Are Stuck in the Provisioning State

The most likely cause of this problem is that you restarted the View Connection Server instance during a cloning operation

Virtual Machines Are Stuck in the Customizing State

The most likely cause of this problem is that there is not enough disk space to start the VM. A VM must start before customization can take place

9. Troubleshooting USB Redirection Problems

USB redirection is not supported for Windows 2003 or Windows 2008 systems or for View desktops that are managed by Microsoft Terminal Services

Solution – Use PCoIP instead of RDP; Global Policy -> USB Redirection to allow;

10. Troubleshooting QuickPrep Customization Problems

The script times out

The script path refers to a script that requires an interpreter

The account under which the script runs does not have sufficient permission to execute a script task

11. Windows XP Linked Clones Fail to Join the Domain

View Composer agent initialization state error (18): Failed to join the domain (waited 565 seconds)

Apply the Windows Server 2008 RODC compatibility update for Windows XP

Chapter 17 - Using the vdmadmin Command

You can use the vdmadmin command line on a View Connection Server instance

You must run the vdmadmin command as a user who is in the **Administrators** role

-A	Administers the information that a View Agent records in its log files Overrides the IP address reported by a View Agent
-C	Sets the name for a View Connection Server group
-F	Updates the Foreign Security Principals (FSPs) in Active Directory for all users or for specified users
-H	Displays health information about View Manager Services
-I	Generates reports about View Manager Operation
-L	Assigns a dedicated desktop to a user or removes an assignment
-M	Displays information about a virtual machine or physical computer
-N	Configures the domains that a View Connection Server instance or group makes available to View Clients
-O	Displays the desktops that are assigned to users who are no longer entitled to those desktops
-P	Displays the user policies that are associated with the desktops of unentitled users
-Q	Configures the account in Active Directory account and View Manager configuration of a client device in kiosk mode
-R	Reports the first user who accessed a desktop

-S	Removes a configuration entry for a View Connection Server instance from the configuration of View Manager
-T	Sets the split limit for View Transfer Server packages
-U	Displays information about a user including their desktop entitlements and ThinApp assignments and Administrator roles
-V	Allows data to be recovered from a local desktop by decrypting its virtual machine
-X	Detects and resolves duplicated LDAP entries on replicated View Connection Server instances

Chapter 18 - Setting up Clients in Kiosk Mode

View Manager uses the **Flexible Authentication** feature in VMware View 4.5 and later to authenticate a client device in kiosk mode rather than the end user

You can configure a View Connection Server instance to authenticate clients that identify themselves by their **MAC address** or by a **user name** that starts with the characters **"custom-"** or with an alternate prefix string that you have defined in ADAM

To display the MAC Addresses of Client Devices - **(wswc –printEnvironmentInfo)**

*On both Windows and Linux clients, human interface devices (HIDs) and smart card readers are not forwarded by default in Kiosk Clients

Do not use a specified name with more than one client device

Chapter 19 - Running View Client from the Command Line

Use **wswc** command to run the View Client for Windows from the command line

-unattended - Runs View Client in a non-interactive mode that is suitable for clients in kiosk mode

You can define default settings for the View Client in the Windows registry instead of specifying these settings on the command line