VCP5-DT – Architecture Planning Guide Notes

**Chapter 1 - Introduction to VMware View**

- On LANs, the display is faster and smoother than traditional remote displays
- On WANs, the display protocol can compensate for an increase in latency or a reduction in bandwidth, ensuring that end users can remain productive regardless of network conditions

Location-based printing does require that you install print drivers in the virtual machine

View Persona Management to retain user settings and data between sessions even after the desktop has been refreshed or recomposed. **Replicate user profiles to a remote profile store (CIFS share) at configurable intervals**
Repurposing a legacy PC into a thin client desktop can extend the life of the hardware by three to five years
View Composer can then create a pool of linked clones from a specified parent virtual machine. This strategy reduces storage costs by up to **90** percent

You can configure VMware View to record events to a Microsoft SQL Server or Oracle database.
- End-user actions such as logging in and starting a desktop session.
- Administrator actions such as adding entitlements and creating desktop pools.
- Alerts that report system failures and errors.
- Statistical sampling such as recording the maximum number of users over a 24-hour period.

You can use **vdmadmin** to perform administration tasks that are not possible from within the View Administrator

**Chapter 2 - Planning a Rich User Experience**

**PCoIP** - You can use 3D applications such as Windows Aero themes or Google Earth, with a screen resolution of up to **1920 x 1200**
With this **non-hardware-accelerated graphics feature**, you can run DirectX 9 and OpenGL 2.1 applications without a physical graphics processing unit (GPU)
- If PCoIP, you can use up to **4 monitors** and adjust the resolution for each monitor separately, up to **2560 x 1600** resolutions per display. When 3D feature is enabled, up to 2 monitors are supported with a resolution of up to **1920x1200**
- You can **copy and paste** text and images between the local system and the desktop, up to **1MB**. Supported file formats include text, images, and RTF
For users outside the corporate firewall, you can use this protocol with View security servers or with your company's **VPN**

**RDP -** With RDP 6, you can use multiple monitors in span mode. **RDP 7** has true multiple monitor support, for up to **16 monitors**
*You can **copy and paste** text and **system objects** such as folders and files between the local system and the View desktop

**Using View Persona Management to Retain User Data and Settings**

View Persona Management retains changes that users make to their profiles. User profiles comprise a variety of user-generated information
- User-specific data and desktop settings
- Application data and settings
- Windows registry entries configured by user applications
View Persona Management requires storage on a CIFS share equal or greater than the size of the user's local profile

**Minimizing Logon and Logoff Times**

View takes recent changes in the profile on the View desktop and copies them to the remote repository at regular intervals. **The default is every 10 minutes**. In contrast, Windows roaming profiles wait until logoff time and copy all changes to the server at logoff

With View Persona Management, if you provision desktops with VMware ThinApp applications, the ThinApp sandbox data can also be stored in the user profile. This data can roam with the user but does not significantly affect logon times. This strategy provides better protection against data loss or corruption

**Configuration Options**

You can configure View personas at several levels:
- Single View desktop, desktop pool, OU, all View desktops in your deployment

To configure a remote repository to store personas:
- You can use either a network share or an existing Active Directory user profile path that you configured for Windows roaming profiles.

(EQ) The **network share can be a folder on a server**, a **network-attached storage (NAS) device**, or a network server. To support a large View deployment, you can configure separate repositories for different desktop pools

**Limitations**

View Persona Management has the following limitations and restrictions:
- You must have a **View license** that includes the View Personal Management component.
- View Persona Management operates **only on virtual machines**. It does not operate on physical computers or Microsoft Terminal Servers.
- View Persona Management **requires a CIFS** (Common Internet File System) share.
- You **cannot** use View Persona Management with desktops that run in **local mode**.
- A user cannot access the same profile if the user switches between desktops that have v1 user profiles and v2 user profiles. However, redirected folders can be shared between v1 and v2 profiles. Windows XP uses v1 profiles. Windows Vista and Windows 7 use v2 profiles

**Benefits of Using View Desktops in Local Mode**

If a network connection is present on the client system, the desktop that is checked out continues to communicate with View Connection Server to provide policy updates, and ensure that locally cached authentication criteria is current. By default, contact is attempted **every 5 minutes**

Checking out a View desktop that uses virtual hardware version 8 is not supported. In vSphere 5 environment, user version 7 for local mode deployment

You cannot copy and paste text or system objects such as files and folders between the local system and the View desktop

USB redirection is not supported on Windows 2000 systems or for View desktops sourced from Microsoft Terminal Servers

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

Although MMR is not supported on Windows 7 virtual desktops, if the Windows 7 desktop has 1GB of RAM and 2 virtual CPUs, you can use PCoIP to play 480p- and 720p-formatted videos at native resolutions. For 1080p, you might need to make the window smaller than full screen size

Wyse MMR port, **9427** by default, must be added as a firewall exception in the View desktop. Use WMP 10 or later on both client machines and view desktops

**Chapter 3 - Managing Desktop Pools from a Central Location**

When you create a linked-clone pool, you can also optionally configure a separate, **disposable virtual disk** to store the guest operating system's paging and temp files that are generated during user sessions

View Composer uses a base image, or parent virtual machine, and creates a pool of up to **512** linked-clone virtual machines

Using disposable disks can save storage space **by slowing the growth of linked clones** and reducing the space used by powered off virtual machines

**Chapter 4 - Architecture Design Elements and Planning Guidelines**

On linked-clone virtual machines, the page file and temporary files can be redirected to a separate virtual disk that is deleted when the virtual machines are powered off – Disposable file redirection

**RAM Sizing Impact on Storage**

***.Windows page file -** C:\pagefile.sys - On linked-clone virtual machines, the page file and temporary files can be redirected to a separate virtual disk that is deleted when the virtual machines are powered off
***.Windows hibernate file for laptops -** You can safely **delete** this file because it is not needed in View deployments

**ESX/ESXi swap file - .**vswp extension - is created if you reserve less than 100 percent of a virtual machine's RAM
**ESX/ESXi suspend file -** .vmss extension, is created if you set the desktop pool logoff policy so that the virtual desktop is suspended when the end user logs off

To use the new 3D rendering feature, available with View 5.0, you must allocate between **64MB and 128MB** of VRAM for each Windows 7 View desktop
RAM Sizing - 1GB for Windows XP desktops and 32-bit Windows Vista and Windows 7 desktops and 2GB for 64-bit Windows 7 desktops

**Stateful** desktop image have data in the operating system image itself that must be preserved, maintained, and backed up
**Stateless** desktop images by using View Composer and creating floating-assignment pools of linkedclone virtual machines

**Desktop Virtual Machine Configuration for Windows XP**
OS - 32-bit Windows XP (with the latest service pack)
RAM - 1GB (512MB low end, 2GB high end)
Virtual CPU - 1
System disk - 16GB (8GB low end, 40GB high end)
User data capacity (as a persistent disk) - 5GB (starting point)
Virtual SCSI adapter type - LSI Logic Parallel (not the default)
Virtual network adapter - Flexible (the default)

**Desktop Virtual Machine Configuration for Vista**
OS - 32-bit Windows Vista (with the latest service pack)
RAM - 1GB
Virtual CPU - 1
System disk - 20GB (standard)
User data capacity (as a persistent disk) - 5GB (starting point)
Virtual SCSI adapter type - LSI Logic Parallel (the default)
Virtual network adapter - VMXNET 3

**Desktop Virtual Machine Configuration for Windows 7**
OS - 32-bit Windows 7 (with the latest service pack)
RAM - 1GB
Virtual CPU - 1
System disk - 20GB (slightly less than standard)
User data capacity (as a persistent disk) - 5GB (starting point)
Virtual SCSI adapter type - LSI Logic SAS (the default)
Virtual network adapter - VMXNET 3

**vCenter and View Composer Virtual Machine Configuration and Desktop Pool Maximums**
*View Composer can **create and provision up to 1,000 desktops** per pool if you are using vSphere 4.1 or later
*View Composer can also **perform a recompose operation on up to 1,000** desktops at a time

OS - 64-bit Windows Server 2008 R2 Enterprise
RAM - 4 GB
Virtual CPU - 2
System disk - 40GB
Virtual SCSI adapter type - LSI Logic SAS (the default for Windows Server 2008)
Virtual network adapter - E1000 (the default)
Maximum View Composer pool size - 1,000 desktops

**View Connection Server Maximums and Virtual Machine Configuration**
OS - 64-bit Windows Server 2008 R2
RAM - 10GB
Virtual CPU - 4
System disk - 40GB
Virtual SCSI adapter type - LSI Logic SAS (the default for Windows Server 2008)
Virtual network adapter - E1000 (the default)
1 NIC - 1 Gigabit

*A group of replicated View Connection Server instances across a WAN due to the communication traffic needed between the grouped instances

**Connection Servers per Deployment Connection Type Maximum Simultaneous Connections**
1 Connection Server **Direct connection, RDP or PCoIP; Tunneled connection, RDP; PCoIP Secure Gateway connection** - **2,000**
7 Connection Servers (5 + 2 spares) **Direct connection, RDP or PCoIP** - **10,000**
1 Connection Server Unified Access to **physical PCs** - **100**
1 Connection Server Unified Access to **terminal servers – 200**

***.PCoIP Secure Gateway** connections are required if you use security servers for PCoIP connections from outside the corporate network. **Tunneled connections** are required if you use security servers for RDP connections from outside the corporate network and for USB and multimedia redirection (MMR) acceleration with a PCoIP Secure Gateway connection

**View Transfer Server Configuration**
OS - 64-bit Windows Server 2008 R2
RAM - 4GB
Virtual CPU - 2
System disk - 20GB
Virtual SCSI adapter type - LSI Logic Parallel (not the default, which is SAS)
Virtual network adapter - E1000 (the default)
1 NIC - 1 Gigabit

*.Each Transfer Server instance can theoretically accommodate **60 concurrent** disk operations
*.VMware tested **20 concurrent** disk operations, such as 20 clients downloading a local desktop at the same time, over a 1GB per second network connection

You can control which encryption algorithms are advertised by the PCoIP endpoint during session negotiation. By default, both **Salsa20-256round12** and **AES-128-GCM** algorithms are available

The cluster configuration is also important because each View desktop pool must be associated with a vCenter resource pool

---

**Chapter 5 - Planning for Security Features**
**Direct Client Connections**
The hardware implementation of PCoIP uses both AES and IP Security (IPsec)

*Policies, such as restricting permitted hours to log in and setting the expiration date for passwords, are also handled through existing Active Directory Operational procedures

Smart card authentication is supported by the Windows-based View Client and View Client with Local Mode only. It is **not** supported by View Administrator
Client connections that use smart card authentication must be SSL enabled. Administrators can enable SSL for client connections by setting a global parameter in View Administrator
To use smart cards with local desktops, 1024-bit or 2048-bit key size during smart card enrollment

Administrators 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

*Cached credentials - If the user then attempts to connect to a security server or a View Connection Server instance without first establishing a **VPN connection**, the user is prompted for credentials, and the Log in as Current User feature does not work
**Restricting View Desktop Access – Tagging**
Connection Servers and Desktop Pools

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

You can use a security server to provide an additional layer of security between the Internet and your internal network
As of View 4.6, security servers include a PCoIP Secure Gateway component so that clients that use the PCoIP display protocol can use a security server rather than a VPN

**Firewalls for DMZ-Based Security Servers**
Front End -> External Clients to reach View Security Servers
Back End -> View Security Servers to reach View Connection Servers

**Front End Firewall Rules** – HTTP 80, HTTPS 443, PCoIP 4172 TCP & 4172 UDP both directions
**Back End Firewall Rules** – HTTP 80, HTTPS 443, *.AJP13 8009, JMS 4001, RDP 3389, PCoIP 4172 TCP & 4172 UDP both directions
If **USB Redirection** is used – 32111 (TCP), **MMR** – 9427 (TCP)

SOAP - TCP port 80 or 443
Security servers use port 8009 to transmit AJP13-forwarded Web traffic to View Connection Server instances
*AJP13 is used in a security server configuration only

**View Connection Server Intercommunication –** Port 4100 JMSIR

**PCoIP Secure Gateway**
When you enable the PCoIP Secure Gateway component, PCoIP traffic is forwarded by a security server to View desktops

**VMware View LDAP**
View LDAP contains entries that represent each View desktop, each accessible View desktop, multiple View desktops that are managed together, and View component configuration settings.
View LDAP also includes a set of View plug-in DLLs to provide automation and notification services for other VMware View components.

**View Messaging**
View messaging component provides the messaging router for communication between View Connection Server components and between View Agent and View Connection Server – Port 4001 JMS

**Ports Opened During View Connection Server Installation**

| | | |
|---|---|---|
| JMS | TCP 4001 in | Standard and replica |
| JMSIR | TCP 4100 in | Standard and replica |
| AJP13 | TCP 8009 in | Standard and replica |
| HTTP | TCP 80 in | Standard, replica, and security server |
| HTTPS | TCP 443 in | Standard, replica, and security server |
| PCoIP | TCP 4172 in;<br>UDP 4172<br>Both directions | Standard, replica, and security server |

**TCP Ports Opened During View Agent Installation**

| | |
|---|---|
| RDP | 3389 |
| USB redirection | 32111 |
| MMR | 9427 |
| PCoIP | 4172 (TCP and UDP) |

**View Client with Local Mode** data is downloaded and uploaded through **port 902**. If you intend to use View Client with Local Mode, **port 902** must be accessible to your ESX/ESXi host