Vendor: VMware

Exam Code: VCP510-DT

Exam Name: VMware Certified Professional 5 - Desktop

Version: Demo

QUESTION 1
Which two steps are part of the View Composer installation process? (Choose two.)

A. select the Enable View Composer checkbox in the View Administrator
B. install the View Composer on the vCenter Server system
C. register View Composer service on the Windows system
D. configure ODBC connection to the View Composer database

Correct Answer: BD
Explanation

Explanation/Reference:
Explanation:
Explanation:
- Ab Version 5.1 nicht mehr zwingend auf dem vCenter
- braucht eine DB (Oracle oder SQL-Server) inkl. ODBC-DSN

QUESTION 2
The View Composer Database stores information about which three components and connections? (Choose three.)

A. Active Directory Connections
B. View Connection Broker Connections
C. Replicas created by the View Composer
D. Disposable data disk created by View Composer
E. Linked-clone desktops deployed by View Composer

Correct Answer: ACE
Explanation

Explanation/Reference:
Explanation:

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

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

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

QUESTION 3
Which two platforms are supported by VMware View Composer in a VMware View 5 environment? (Choose two.)

A. VMware vCenter 4.0 Update 3 running on Windows Server 2008 R2
B. VMware vCenter 4.1 Update 1 running on Windows XP Pro 64-bit
C. VMware vCenter 4.1 Update 1 running on Windows Server 2003 64-bit
D. VMware vCenter 5.0 running on Windows Server 2008 R2

Correct Answer: AD

Explanation

Explanation/Reference:

QUESTION 4
What are three supported Database Servers for VMware View Composer in a VMware View 5 environment? (Choose three.)

A. Microsoft SQL Server 2005 Express with vCenter Server 4.1 U1
B. Microsoft SQL Server 2005 Express with vCenter Server 5.0
C. Microsoft SQL Server 2005 SP3 Standard with vCenter Server 5.0
D. Microsoft SQL Server 2008 R2 Express with vCenter 4.0 U3
E. Microsoft SQL Server 2008 R2 Express with vCenter Server 5.0

Correct Answer: ACE
Explanation

Explanation/Reference:
Explanation:

Table 1-4. Supported Database Servers for View Composer

Database	vCenter Server 5.0 and later	vCenter Server 4.1 U1 and later	vCenter Server 4.0 U3 and later
Microsoft SQL Server 2005 Express	No	Yes	Yes
Microsoft SQL Server 2005 SP3 and later, Standard and Enterprise (32- and 64-bit)	Yes	Yes	Yes
Microsoft SQL Server 2008 R2 Express	Yes	No	No
Microsoft SQL Server 2008 SP1 and later, Standard and Enterprise (32- and 64-bit)	Yes	Yes	Yes
Oracle 10g Release 2	Yes	Yes	Yes
Oracle 11g Release 2, with Oracle 11.2.0.1 Patch 5	Yes	Yes	Yes

QUESTION 5
What is the proper syntax to use when adding a domain user to the View Composer configuration?

A. DOMAIN\USER
B. DOMAIN.COM\USER
C. OU=DOMAIN, CN=USER
D. USER@DOMAIN.COM

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 6
What are three required permissions that need to be assigned to the View Composer user account? (Choose three.)

A. Create User Accounts
B. Create Computer Objects
C. Delete Group Accounts
D. Delete Computer Objects
E. Write All Properties

Correct Answer: BDE
Explanation

Explanation/Reference:
Explanation:

2 Add the **Create Computer Objects**, **Delete Computer Objects**, and **Write All Properties** permissions to the account in the Active Directory container in which the linked-clone computer accounts are created or to which the linked-clone computer accounts are moved.

The following list shows all the required permissions for the user account, including permissions that are assigned by default:

- List Contents
- Read All Properties
- Write All Properties
- Read Permissions
- Create Computer Objects
- Delete Computer Objects

QUESTION 7
Which two operating systems are supported for the View Connection Server? (Choose two.)

A. Windows Server 2003 R2 64-bit Standard or Enterprise
B. Windows Server 2003 R2 32-bit Standard or Enterprise
C. Windows Server 2008 R2 32-bit Standard or Enterprise
D. Windows Server 2008 R2 64-bit Standard or Enterprise

Correct Answer: BD

Explanation

Explanation/Reference:

QUESTION 8
Which two ports must be opened in the firewall to enable communication between a Security Server and a Connection Server? (Choose two.)

A. 4001
B. 8443
C. 3389
D. 8009

Correct Answer: AD
Explanation

Explanation/Reference:
Explanation:

Table 5-2. Back-End Firewall Rules

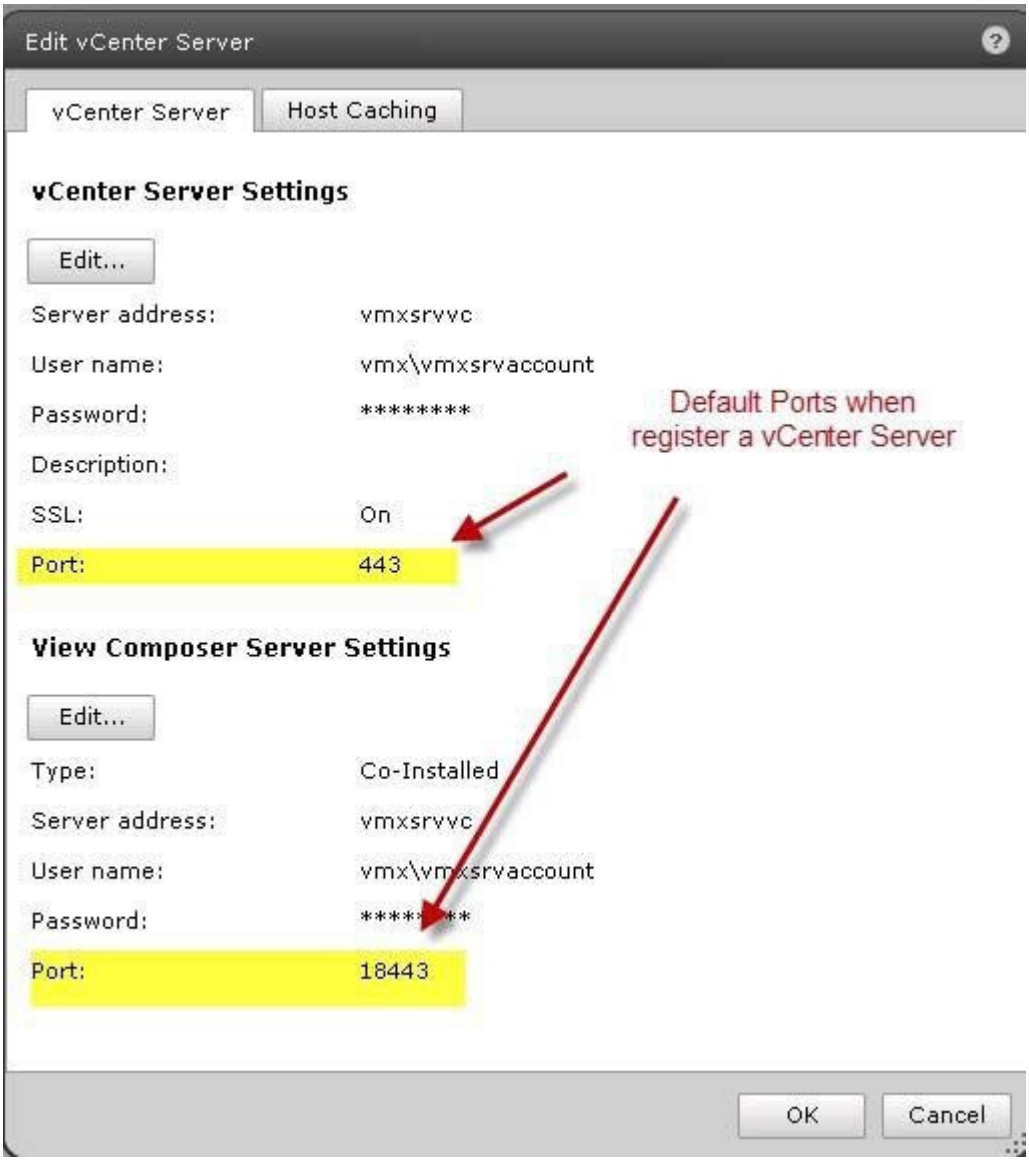
Source	Protocol	Port	Destination	Notes
Security server	HTTP	80	Transfer Server	Security servers can use port 80 to download View desktop data to local mode desktops from the Transfer Server and to replicate data to the Transfer Server.
Security server	HTTPS	443	Transfer Server	If you configure View Connection Server to use SSL for local mode operations and desktop provisioning, security servers use port 443 for downloads and replication between local mode desktops and the Transfer Server.
Security server	AJP13	8009	View Connection Server	Security servers use port 8009 to transmit AJP13-forwarded Web traffic to View Connection Server instances.
Security server	JMS	4001	View Connection Server	Security servers use port 4001 to transmit Java Message Service (JMS) traffic to View Connection Server instances.
Security server	RDP	3389	View desktop	Security servers use port 3389 to transmit RDP traffic to View desktops. NOTE For MMR, TCP port 9427 is used alongside RDP.
Security server	PCoIP	TCP 4172 UDP 4172	View desktop	Security servers use TCP port 4172 to transmit PCoIP traffic to View desktops, and security servers use UDP port 4172 to transmit PCoIP traffic in both directions.
Security Server	PCoIP or RDP	TCP 32111	View desktop	For USB redirection, TCP port 32111 is used alongside PCoIP or RDP from the client to the View desktop.

QUESTION 9
Which two ports must be opened in the firewall to enable communication between a View Connection Server and the vCenter Server running View Composer? (Choose two.)

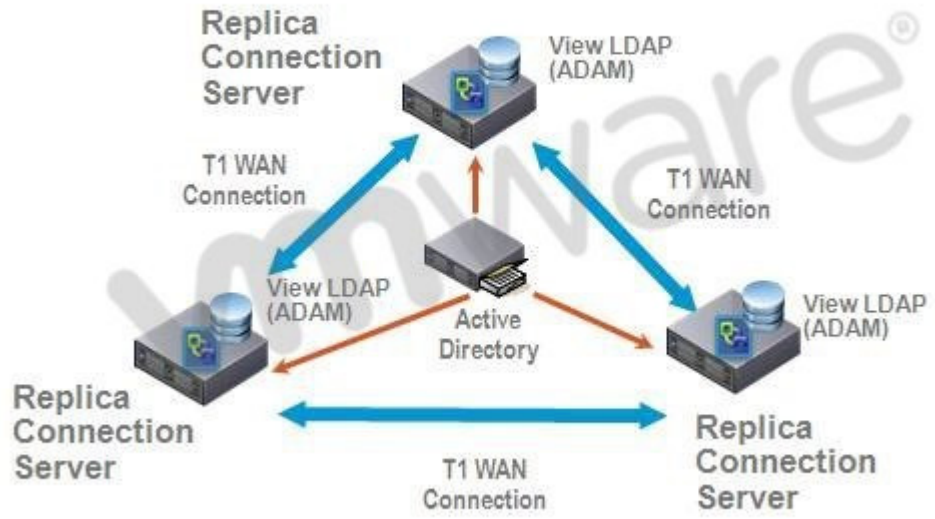
A. 18443
B. 443
C. 389
D. 4172

Correct Answer: AB
Explanation

Explanation/Reference:
Explanation:
389 LDAP, 4172 PCoIP



QUESTION 10
Click the Exhibit button.



A proposed configuration of three replica servers is shown.

What can result from this configuration?

A. Three replica servers can result in client connection problems.
B. Multiple connections to Active Directory can cause a performance problem.
C. Replication over WAN connections can cause inconsistencies in the LDAP database.
D. Multiple ADAM instances can cause a performance problem.

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 11
An administrator is preparing to install a View Connection Server 5.x for the first time.

Which two server prerequisites are required for a proper installation on Windows Server 2003? (Choose two.)

A. Configure a SSL certificate for use with the Connection Server.
B. Configure a static IP address on the server.
C. Configure a domain administrator account for installation.
D. Configure the firewall with the appropriate open ports.

Correct Answer: BD
Explanation

Explanation/Reference:
Explanation:
Explanation:
Only on Win 2008 R2 the setup configures Firewall
SSL certificate is not required, setup will install a self signed

QUESTION 12
An Administrator is upgrading to View Connection Server 5.x from a previous release.

Which component is omitted from installation automatically during an upgrade?

A. VMware Message Bus Component
B. VMware Script Host
C. VMware PCoIP Secure Gateway
D. VMware VDMDS

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 13
What is the minimum required level of privileges required to install the View Connection Server?

A. Domain User
B. Domain Administrator
C. Local Power User
D. Local Administrator

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 14
An administrator is adding a replicated instance of View Connection Server to the environment silently.

Which MSI property would be used to identify the instance being replicated?

A. ADAM_PRIMARY_INSTANCE
B. ADAM_PRIMARY_NAME
C. VDM_INSTANCE_NAME
D. VDM_SERVER_INSTANCE

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 15
Which two operating systems are supported for a View Transfer Server installation? (Choose two.)

A. Windows Server 2008 32-bit
B. Windows Server 2003 R2 SP2 32-bit
C. Windows Server 2003 SP2 64-bit
D. Windows Server 2008 R2 64-bit

Correct Answer: BD
Explanation

Explanation/Reference:

QUESTION 16

How many disks can a View Transfer Server concurrently transfer?

A. 15
B. 60
C. 4
D. 30

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 17
Which TCP port must be open on the firewall of the View Transfer Server?

A. 443
B. 21
C. 389
D. 4172

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 18
An administrator is creating a new virtual machine for use as a View Transfer Server.
Which SCSI controller should be selected?

A. Buslogic Parallel
B. LSI Logic Parallel
C. LSI Logic SAS
D. VMware Paravirtual

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:

View Transfer Server Configuration

You must install View Transfer Server on a virtual rather than a physical machine and the virtual machine must be managed by the same vCenter Server instance as the local desktops that it will manage. Table 4-8 lists the virtual machine specifications for a View Transfer Server instance.

Table 4-8. View Transfer Server Virtual Machine Example

Item	Example
Operating system	64-bit Windows Server 2008 R2
RAM	4GB
Virtual CPU	2
System disk capacity	20GB
Virtual SCSI adapter type	LSI Logic Parallel (not the default, which is SAS)
Virtual network adapter	E1000 (the default)
1 NIC	1 Gigabit

QUESTION 19
Which three items must be configured prior to installing a View Security Server? (Choose three.)

A. Connection Server
B. Security Server External URL
C. Security Server Firewall Exceptions
D. Security Server Pairing Password
E. Security Server Static IP address

Correct Answer: ACD
Explanation

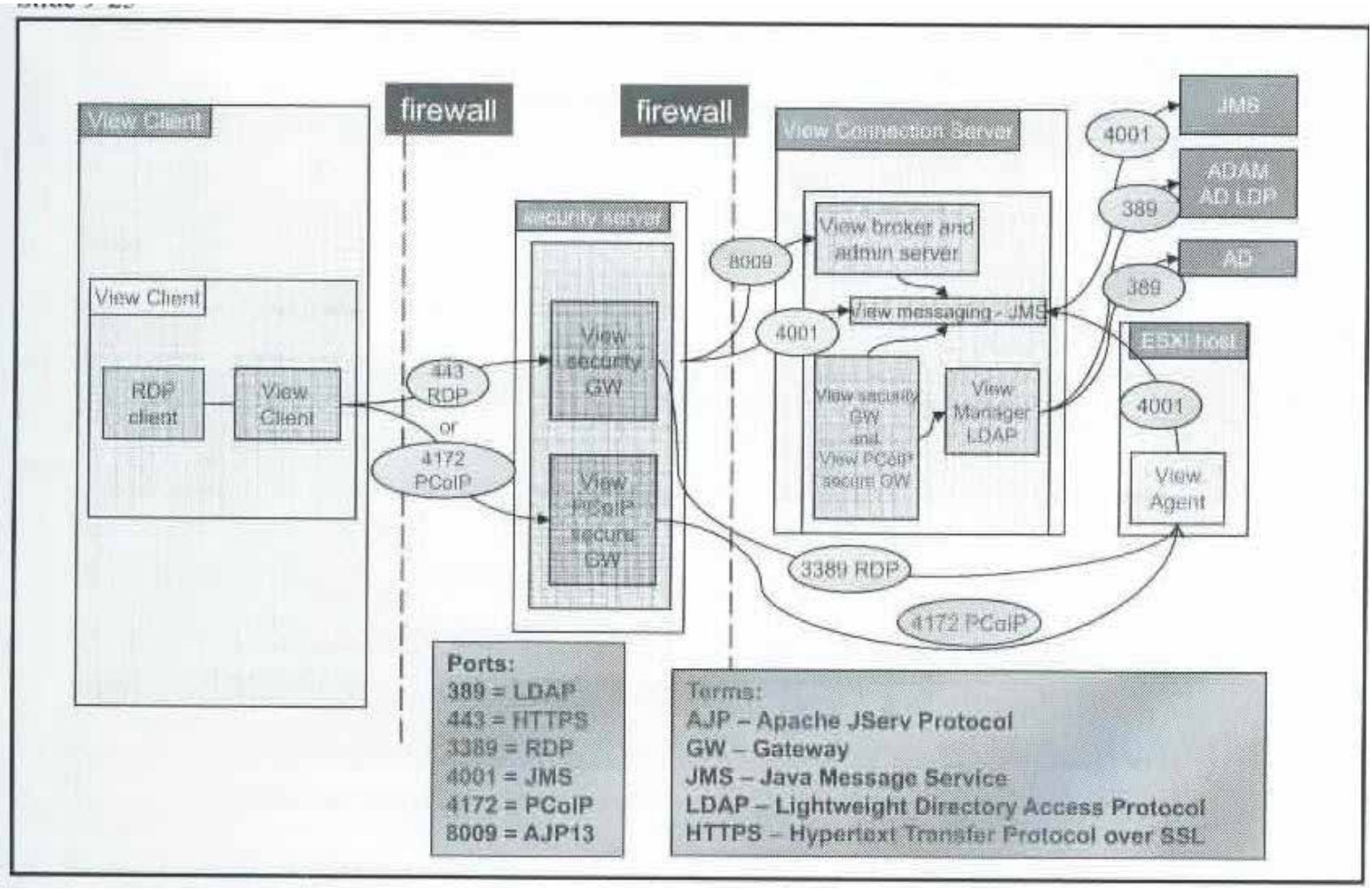
Explanation/Reference:

QUESTION 20
An administrator is installing a View Security Server on a Windows Server 2003 R2 system. Which three Windows Firewall ports must be pre-configured prior to installation to enable remote access? (Choose three.)

A. 443
B. 3389
C. 4001
D. 4172
E. 8009

Correct Answer: ABD
Explanation

Explanation/Reference:
Explanation:
Change from B/D to C/E b'c if you install a security server at least port 443 must be open from untrusted to the security server and from the DMZ to internal ports 4001 and 8009 RDP (3389) don't have to be opened, this is tunneled via 443



QUESTION 21
An administrator has installed the View Security Server and needs to verify all the services have started after the installation is complete.
Which three services should be started? (Choose three.)

A. VMware Message Bus Component
B. VMware View Framework Component
C. VMware View Security Gateway Component
D. VMware View Security Script
E. VMware View Security Server

Correct Answer: BCE
Explanation

Explanation/Reference:
Explanation:

Dienste auf einem Sicherheitsserver

Der Betrieb von View Manager hängt von verschiedenen Diensten ab, die auf einem Sicherheitsserver ausgeführt werden. Wenn Sie den Betrieb dieser Dienste anpassen möchten, müssen Sie sich zunächst mit ihnen vertraut machen.

Dienste auf einem Sicherheitsserver

Dienstname	Starttyp	Beschreibung
VMware View Security Server	Automatisch	Stellt Sicherheitsserverdienste bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion eines Sicherheitsservers ausgeführt werden. Wenn Sie diesen Dienst starten oder beenden, werden auch die Framework- und Sicherheits-Gateway-Dienste gestartet oder beendet.
VMware View-Framework-Komponente	Manuell	Stellt Dienste für Ereignisprotokollierung, Sicherheit und COM+-Framework bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion eines Sicherheitsservers ausgeführt werden.
VMware View, PCoIP Secure Gateway	Manuell	Stellt Dienste für ein PCoIP Secure Gateway bereit. Dieser Dienst muss ausgeführt werden, wenn die Clients die Verbindung zu einem Sicherheitsserver über ein PCoIP Secure Gateway herstellen.
VMware View-Sicherheits-Gateway-Komponente	Manuell	Stellt sichere Tunneldienste bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion eines Sicherheitsservers ausgeführt werden.

QUESTION 22
An administrator would like to add a View Security Server to add external access to the environment.
Which View component must be installed and configured prior to installation of the View Security Server?

A. View Agent Server
B. View Connection Server
C. View Replica Server
D. View Transfer Server

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 23
Which attribute is required when configuring a View Security Server Pairing Password?

A. Password complexity value
B. Password expiration value
C. Password length value
D. Password timeout value

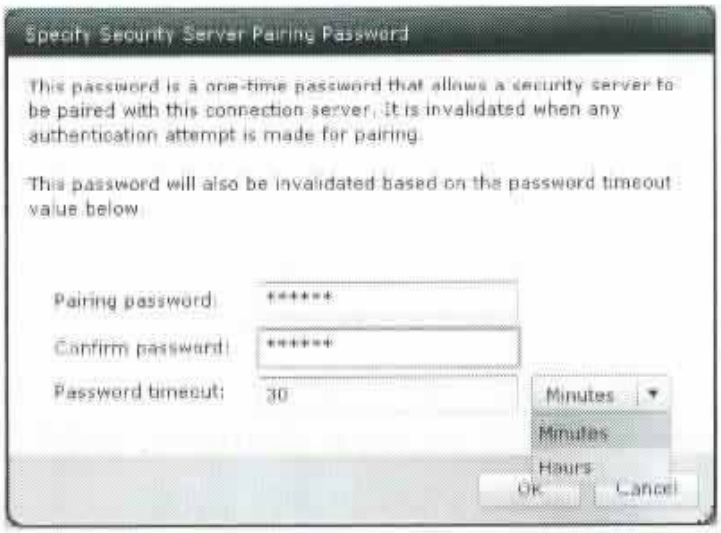
Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

A one-time password is required to complete the connection server pairing.

The password is created in View Administrator for the connection server that will be paired:

- Select **View Configuration** > **Servers** and select the appropriate connection server.
- Select **Specify Security Server Pairing Password** from **More Commands**.
- Enter the pairing password, which can be noncomplex.
- (Optional) Modify the expiration timeout.



Before you can install a security server, you must configure a security server pairing password. The installation wizard of View Connection Server prompts you for this password.

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

If you do not provide the security server pairing password to View Connection Server installation program before the password times out, the password becomes invalid. You will have to configure a new password.

The password is created in View Administrator for the connection server whose FQDN you entered in the previous installation wizard page. Password complexity rules are not enforced, because the password is a one-time password with a short lifetime. Ideally, the password is created when you reach this page in the installation sequence.

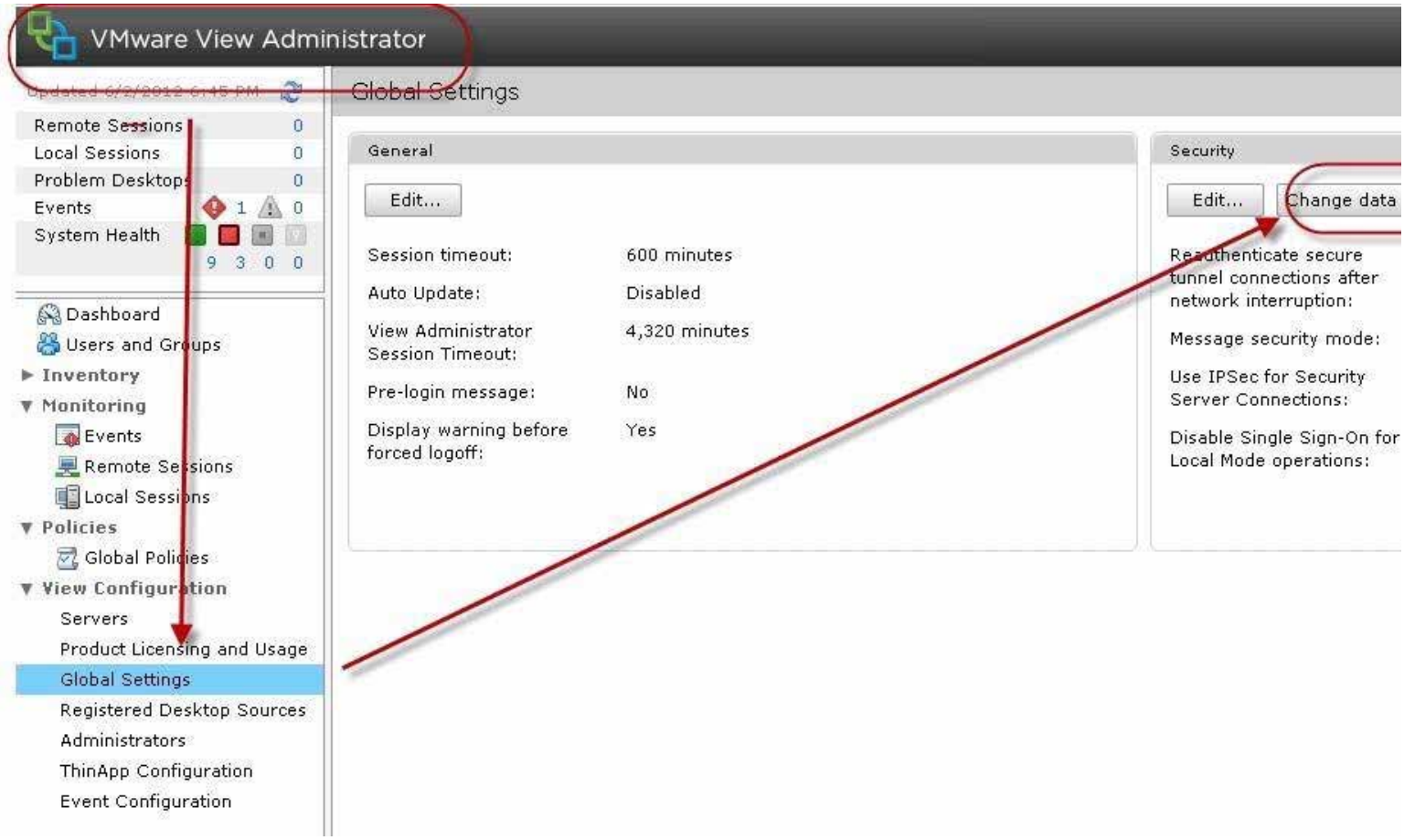
QUESTION 24
During an installation of Security Server, a message displays that the pairing password has expired.

Where must a new password be configured?

A. View Connection Server
B. Active Directory
C. View Administrator
D. View Security Server

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:



QUESTION 25
What is the minimum amount of memory required in order to install View Security Server on Windows Server 2003?

A. 1GB
B. 4GB
C. 2GB
D. 8GB

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:

Table 1-1. View Connection Server Hardware Requirements (Continued)

Hardware Component	Required	Recommended
Memory Windows Server 2008 64-bit	4GB RAM or higher	At least 10GB RAM for deployments of 50 or more View desktops
Memory Windows Server 2003 32-bit R2	2GB RAM or higher	6GB RAM for deployments of 50 or more View desktops, and enable Physical Address Extension (PAE) See the Microsoft KB article at http://support.microsoft.com/kb/283037.

These requirements also apply to replica and security server View Connection Server instances that you install for high availability or external access.

IMPORTANT The physical or virtual machine that hosts View Connection Server must use a static IP address.

QUESTION 26
An organization has a View Connection Server in DomainA. Users in DomainB need to access desktops on the existing connection server in DomainA.

What must the system administrator do in Active Directory to enable users from DomainB to access desktops in DomainA?

A. set up a Security Server to proxy the connection to DomainB
B. check the multidomain authentication box in the View Manager Server Settings
C. set up a one-way trust relationship from DomainB to DomainA
D. set up a two-way trust relationship between DomainA and DomainB

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 27
An organization requires a higher level of security for desktops that cannot be achieved with passwords alone. A certificate has been procured from a Certificate Authority, and smart cards have been purchased for the users.

Which three tasks must the desktop administrator perform to prepare Active Directory (AD)? (Choose three.)

A. add the user principal names to the Trusted Root Certification Authorities group
B. add the root certificate to the Enterprise NTAuth store in AD
C. add the root certificate to the Trusted Root Hierarchy in AD
D. add user principal names to the AD accounts of users
E. add the root certificate to the Trusted Root Certification Authorities group policy in AD

Correct Answer: BDE
Explanation

Explanation/Reference:
Explanation:

5. Prepare Active Directory for smart-card authentication. When you implement smart-card authentication, you must perform the following tasks in AD:

- Add the user principal names (UPNs) for smart card users.

  Smart-card logins rely on UPNs. So the AD accounts of users that use smart cards to authenticate in View must have valid UPNs.

- Add the root certificate to Enterprise NTAuth Store and Trusted Root Certification Authorities.

  If you use a CA to issue smart-card login or domain controller certificates, you must add the root certificate to the Enterprise NTAuth Store. The root certificate must also be added to the Trusted Root Certification Authorities group policy in AD.

- Add an intermediate certificate to the Intermediate Certification Authorities. If you use an intermediate certification authority to issue smart-card login and domain controller certificates, you must add the intermediate certificate to the Intermediate Certification Authorities group policy in AD.

QUESTION 28
An administrator creates a View Composer linked clone pool of Windows XP Desktops, and the operation fails to finish customizing the desktops. The error log below provides more detail.

2010-09-21 12:46:04,281 [836] INFO Guest - [Guest.cpp, 248] Attempting to join Test1 to the domain vmw-dc.local

f3 2010-09-21 12:46:04,562 [836] FATAL Guest - [Guest.cpp, 261] Domain join faileD. 1265 f3 2010-09-21 12:46:04,718 [836] FATAL CSvmGaService - [svmGaService.cpp, 116] Domain join failedError 1265 (0x4f1): The system detected a possible attempt to compromise security. Please ensure that you can contact the server that authenticated you.

What is the cause of the error?

A. Active Directory encryption levels
B. Active Directory group policy
C. Active Directory permissions
D. Active Directory root certificate

Correct Answer: A
Explanation

Explanation/Reference:
Explanation:

View Composer linked clones fail to finish customizing

3 Ratings

Details

- You cannot deploy linked clones.
- Linked clones cannot join the domain.
- View Administrator displays this error message:

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

- You see these errors in the View Composer log:

```
[1700] INFO SvmGa - [svmGa.cpp, 654] Domain join failed with 18
[1776] FATAL VolumesReady - [VolumesReady.cpp, 129] Joining Domain failed for 1 times.
[836] INFO CSvmGaService - [svmGaService.cpp, 256] Successfully parsed the policy and disk
signatures
[836] DEBUG CSvmGaService - [svmGaService.cpp, 113] Joining domain
[836] INFO Guest - [Guest.cpp, 248] Attempting to join Test1 to the domain vmw-dc.local
[836] FATAL Guest - [Guest.cpp, 261] Domain join failed: 1265
[836] FATAL CSvmGaService - [svmGaService.cpp, 116] Domain join failedError 1265 (0x4f1):
The system detected a possible attempt to compromise security. Please ensure that you can
contact the server that authenticated you.
```

For information on the location of View Composer log files, see Location of VMware View log files (1027744).

Note: This article applies only to View Manager 4.5. If you see this error in View Manager 4.6 and later, see:

- Provisioning linked clone desktops fail with the error: View Composer agent initialization state error (18): Failed to join the domain (1027087)
- Provisioning the View desktop pool fails with the error: View Composer agent initialization state error (18): Failed to join the domain (waited nnn seconds) (2006879)

Solution

This issue is caused by the default behavior of a Windows Server 2008/2008 R2 domain controller. In the default domain group side, there are NETLOGON service settings and the default is to prohibit the use of older versions of encryption protocol to connect.

To resolve this issue, allow the use of older encryption protocols:

1. Log in to your Active Directory (AD) domain controller.
2. Click **Start > Run**, type gpmc.msc, and click OK. This launches the Group Policy Management console.
3. In the console tree, navigate to **Domains** > **Current Domain Name** > **Group Policy objects**.
4. Right-click **Default Domain Controller Policy** and click **Edit**.
5. In the Group Policy Management Editor window, navigate to **Computer Configuration > Administrative Templates: Policy definitions (ADMX files) retrieved from the local machine > System > Net Logon**.
6. Enable **Allow cryptography algorithms compatible with Windows NT 4.0**.
7. Exit the Group Policy Management console.
8. Open a command prompt.
9. Run the `gpupdate /force` command. This updates the group policies applied to this computer.
10. Take a snapshot of the parent virtual machine and create the linked-clone desktop pool again.

For more information regarding the NETLOGON service and Windows NT 4.0 Cryptography algorithms, see the Microsoft Knowledge Base article 942564.

QUESTION 29
The domain administrator account permissions are limited to one user in an organization. An account for View Composer is needed with the proper permissions. The user needs Write All Properties, Create Computer Objects, and Delete Computer Objects. Which three additional permissions are required? (Choose three.)

A. Delete Contents
B. Read Permissions
C. Create All Properties
D. List Contents
E. Read All Properties

Correct Answer: BDE
Explanation

Explanation/Reference:
Explanation:

2 Add the **Create Computer Objects**, **Delete Computer Objects**, and **Write All Properties** permissions to the account in the Active Directory container in which the linked-clone computer accounts are created or to which the linked-clone computer accounts are moved.

The following list shows all the required permissions for the user account, including permissions that are assigned by default:

- List Contents
- Read All Properties
- Write All Properties
- Read Permissions
- Create Computer Objects
- Delete Computer Objects

QUESTION 30
The security team has determined that the default setting for the connection ticket is too long and wants to shorten the period that the ticket is valid for authentication.

Which GPO needs to be configured and applied to the View environment?

A. vdm_common.adm
B. vdm_client.adm
C. vdm_server.adm
D. vdm_agent.adm

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

QUESTION 31
Which two View user management policies are handled by Active Directory? (Choose two.)

A. Manually disconnecting user sessions
B. Restricting access to specific Connection Servers
C. Restricting permitted hours to log in
D. Setting password expiration dates

Correct Answer: CD
Explanation

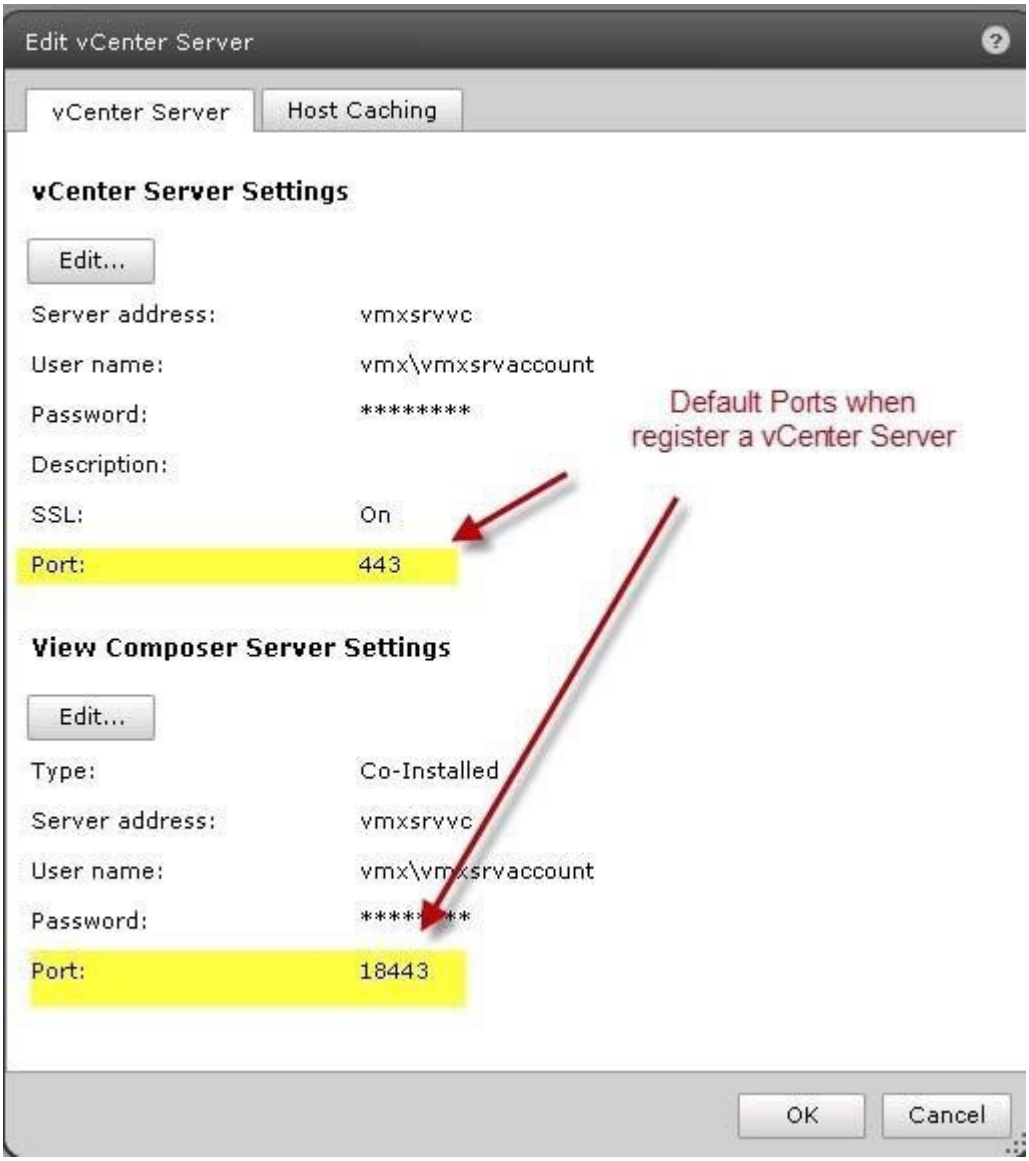
Explanation/Reference:

QUESTION 32
What is the default port number that View Composer uses to communicate with other View components?

A. 4001
B. 4100
C. 443
D. 18443

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:



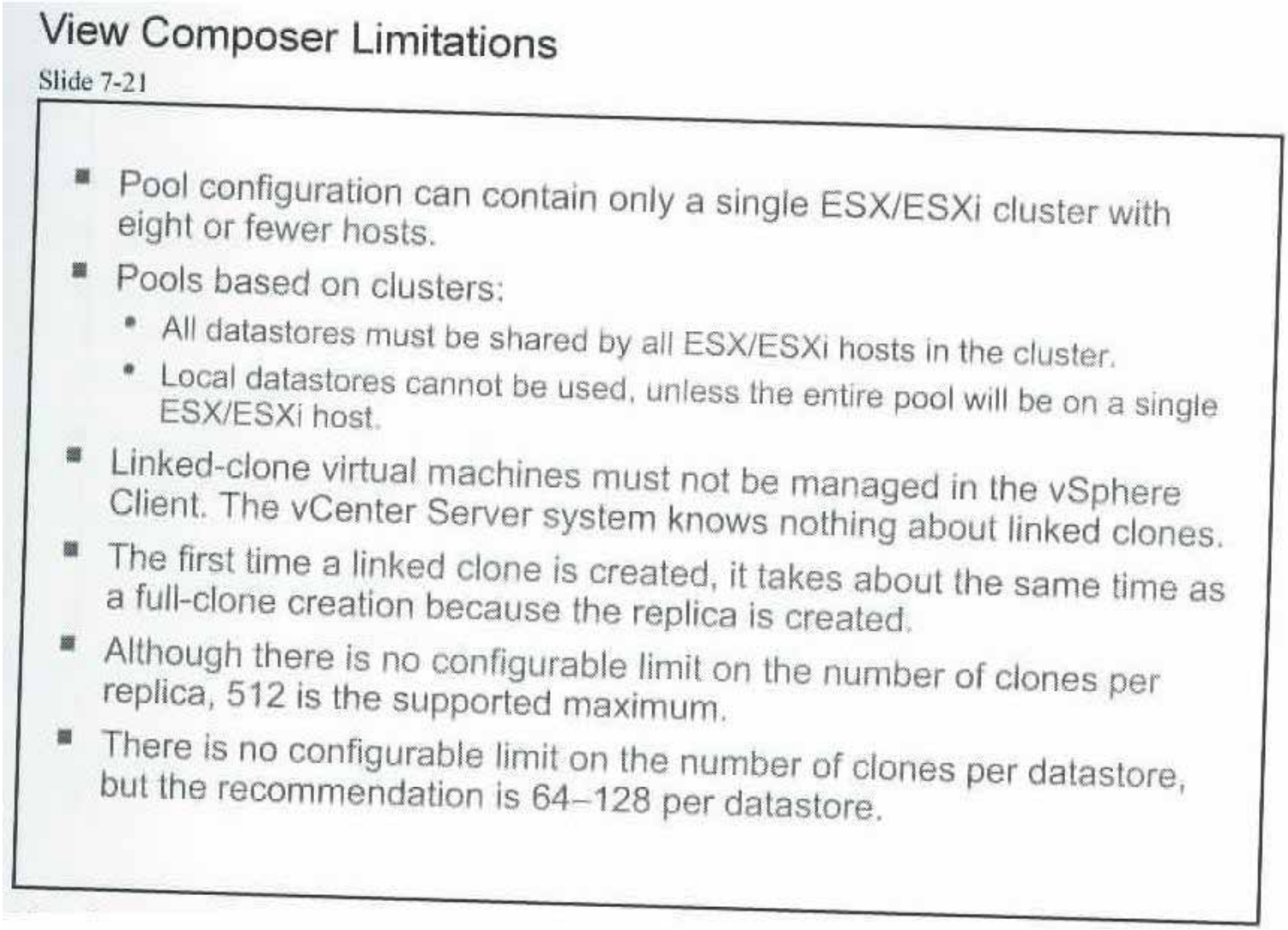
QUESTION 33
What is the maximum supported number of linked clone virtual machines View Composer can provision per pool?

A. 512

B. 1024
C. 128
D. 256

Correct Answer: A
Explanation

Explanation/Reference:
Explanation:

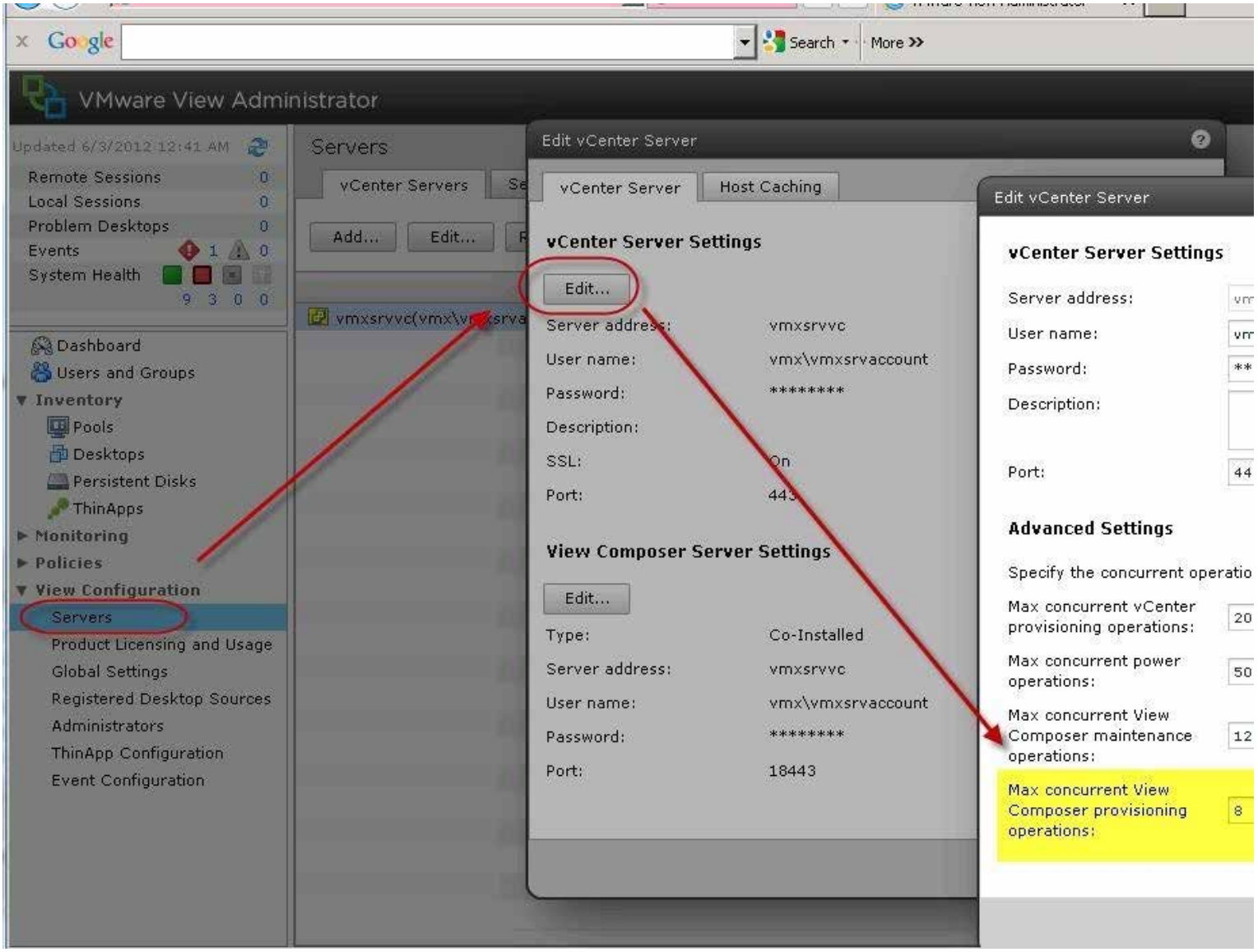


QUESTION 34
What is the default number of linked clone virtual machines that View Composer will recompose at one time?

A. 2
B. 8
C. 64
D. 128

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:



QUESTION 35
What is the maximum number of ESXi hosts in a vSphere cluster used by View Composer if using VMFS datastores?

A. 4
B. 8
C. 32
D. 16

Correct Answer: B
Explanation

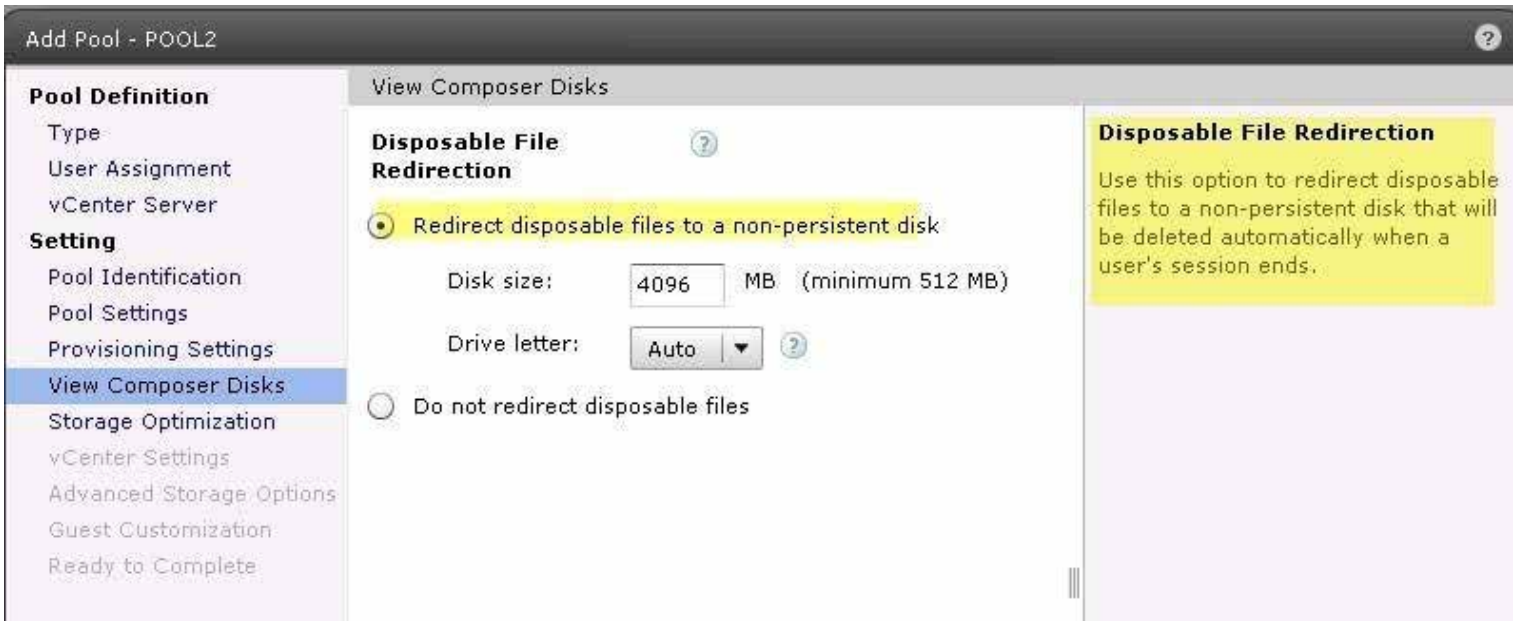
Explanation/Reference:
Explanation:
From http://myvirtualcloud.net/?p=3245
8 Hosts per Cluster when used with VMFS did not change This limit is hard-coded in View Composer; however it comes from a VMFS limitation on the number of hosts that can simultaneously read from a single VMDK. This VMDK in a VMware View environment with View Composer would be the Replica disk.

QUESTION 36
Which setting in View Composer can be used to reduce the storage footprint of a pool of virtual desktops?

A. redirect disposable files to a non-persistent disk
B. redirect temporary files to a non-persistent disk
C. redirect user profile data to a non-persistent disk
D. store Windows profile on a disposable disk

Correct Answer: A
Explanation

Explanation/Reference:
Explanation:



QUESTION 37
An administrator is creating a new account for use with View Composer.

What is the minimum security group to which the account must belong?

A. Domain Administrators
B. Domain Computers
C. Domain Users
D. Forest Administrators

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:

Create a User Account for View Composer

If you use View Composer, you must create a user account in Active Directory to use with View Composer. View Composer requires this account to join linked-clone desktops to your Active Directory domain.

To ensure security, you should create a separate user account to use with View Composer. By creating a separate account, you can guarantee that it does not have additional privileges that are defined for another purpose. You can give the account the minimum privileges that it needs to create and remove computer objects in a specified Active Directory container. For example, the View Composer account does not require domain administrator privileges.

Procedure

1 In Active Directory, create a user account in the same domain as your View Connection Server host or in a trusted domain.

2 Add the **Create Computer Objects**, **Delete Computer Objects**, and **Write All Properties** permissions to the account in the Active Directory container in which the linked-clone computer accounts are created or to which the linked-clone computer accounts are moved.

The following list shows all the required permissions for the user account, including permissions that are assigned by default:

- List Contents
- Read All Properties
- Write All Properties
- Read Permissions
- Create Computer Objects
- Delete Computer Objects

3 Make sure that the user account's permissions apply to the Active Directory container and to all child objects of the container.

What to do next

Specify the account in View Administrator when you configure View Composer for vCenter Server and when you configure and deploy linked-clone desktop pools.

QUESTION 38
An administrator is attempting to add a vCenter Server to View Administrator in order to add View Composer.

Which three prerequisites are necessary prior to adding the vCenter Server to View? (Choose three.)

A. Configure the View Pairing Password.
B. Install an SSL certificate on vCenter Server.
C. Install the View Connection Server product key.
D. Configure a vCenter Server user with correct permissions.
E. Configure a View Composer user with correct permissions.

Correct Answer: BCD
Explanation

Explanation/Reference:
Explanation:
A. Is necessary for Security Server, not for Composer C. There is no View Connection Server product key, View is licensed by concurrent

QUESTION 39
An administrator is receiving an error when trying to connect to View Composer from the View

Administrator. The environment has been upgraded from 4.0.x.

Why can the connection not be made?

A. The network port is no longer valid.
B. The View Composer service must be restarted.
C. An incorrect certificate was chosen during installation.
D. Security certificates cannot be migrated between versions.

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 40
An administrator is creating a new user for use with View Composer and needs to add the appropriate permissions.

Which three non-default permissions are required for the new account? (Choose three.)

A. Write All Properties
B. Read All Properties
C. Create All Child Objects
D. Delete Computer Objects
E. Create Computer Objects

Correct Answer: ADE
Explanation

Explanation/Reference:
Explanation:

2 Add the **Create Computer Objects**, **Delete Computer Objects**, and **Write All Properties** permissions to the account in the Active Directory container in which the linked-clone computer accounts are created or to which the linked-clone computer accounts are moved.

The following list shows all the required permissions for the user account, including permissions that are assigned by default:

- List Contents
- Read All Properties
- Write All Properties
- Read Permissions
- Create Computer Objects
- Delete Computer Objects

QUESTION 41
An IT company requires its field employees to use their View desktops in local mode only. The View administrator sets the Local Mode policy for the Field Employee pool to Allow, but notices that some users are not exclusively using local mode.

Which additional step should the administrator perform to ensure that field agents use local mode only?

A. set the Remote Mode View policy for the Field Agent pool to Deny

B. set the Local Mode policy for the Field Agent pool to Local Only
C. set the View Transfer Server to Local Only
D. ensure the users perform a rollback of the local View desktop to reset its state

Correct Answer: A
Explanation

Explanation/Reference:
Explanation:

View Policies

You can configure View policies to affect all client sessions, or you can apply them to affect specific desktops or users.

Table 8-1 describes each View policy setting.

Table 8-1. View Policies

Policy	Description
Multimedia redirection (MMR)	Determines whether MMR is enabled for client systems. MMR is a Microsoft DirectShow filter that forwards multimedia data from specific codecs on View desktops directly through a TCP socket to the client system. The data is then decoded directly on the client system, where it is played. The default value is **Allow**. If client systems have insufficient resources to handle local multimedia decoding, change the setting to **Deny**. MMR does not work correctly if the client system's video display hardware does not have overlay support.
USB Access	Determines whether desktops can use USB devices connected to the client system. The default value is **Allow**. To prevent the use of external devices for security reasons, change the setting to **Deny**.

Table 8-1. View Policies (Continued)

Policy	Description
Remote mode	Determines whether users can connect to and use desktops running on vCenter Server instances. If set to **Deny**, users must check out the desktop on their local computers and run the desktop only in local mode. Restricting users to running desktops only in local mode reduces the costs associated with CPU, memory, and network bandwidth requirements of running the desktop on a back-end server. The default value is **Allow**.
PCoIP hardware acceleration	Determines whether to enable hardware acceleration of the PCoIP display protocol and specifies the acceleration priority that is assigned to the PCoIP user session. This setting has an effect only if a PCoIP hardware acceleration device is present on the physical computer that hosts the desktop. The default value is **Allow** at **Medium** priority.

QUESTION 42
A View administrator needs to reduce the size of local mode desktop downloads.

Which connection server setting should be enabled?

A. use linked clones for local mode operations

B. use network optimization for local mode operations
C. use deduplication for local mode operations
D. use compression for local mode operations

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

You can reduce the amount of data that is sent over the network during transfer operations between the client computers and the datacenter. You use deduplication and compression to optimize data transfers. The two settings are:

- **Use deduplication for Local Mode operations** – Prevents redundant data from being sent from client computers to the datacenter. Deduplication operates on transfers from the client computer to the datacenter, including replications and desktop check-ins. Deduplication does not take place when desktops are checked out.

  With deduplication, the client computer detects identical blocks of data and sends a reference to the original block instead of sending the entire block again.

  Deduplication is valuable on slow networks because it saves network bandwidth. Deduplication adds to the CPU workload on the client computer when it checks for identical data blocks. Deduplication also increases the I/O workload on View Transfer Server when it reads duplicate blocks from disk. On fast networks, it might be more efficient to disable deduplication.

- **Use compression for Local Mode operations** – Compresses system-image and desktop files before sending them over the network. Like deduplication, compression saves bandwidth and speeds up transfers over slow networks. But View Transfer Server uses additional computing resources to compress files.

QUESTION 43
A newly created View Composer base image is unavailable for checkout in a local mode-enabled linked clone desktop pool.

Which task must be performed on the base image so that it is available for checkout?

A. convert the View Composer base image to a template in vCenter Server
B. publish the View Composer base image as a package in the Transfer Server repository
C. copy the View Composer base image to a Transfer Server via vCenter Server
D. publish the View Composer base image as a full virtual machine

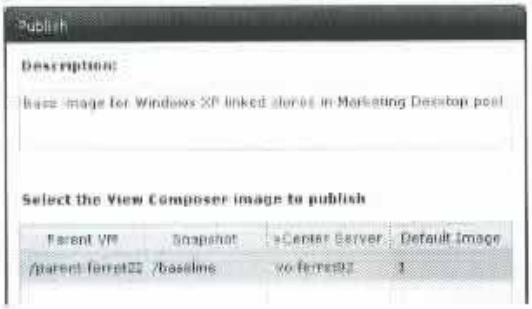
Correct Answer: B
Explanation

Explanation/Reference:
Explanation:

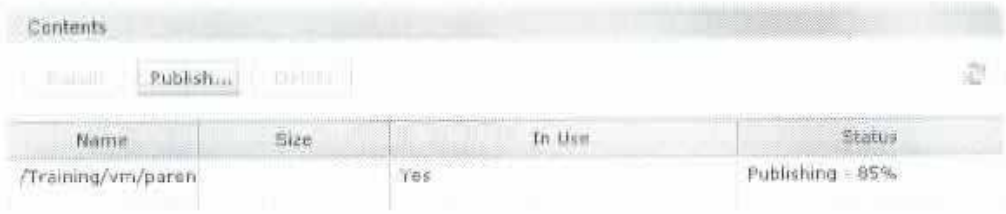
Publishing View Composer Base Images

Slide 8-20

1. In the **Contents** panel on the Transfer Server repository page, click **Publish**.
2. Enter a description and select the name of the parent virtual machine.



Publishing progress is displayed in the **Contents** panel.



Before a user can check out a linked-clone desktop, you must publish its View Composer base image as a package in the Transfer Server repository.

When a user checks out a linked-clone desktop, View Transfer Server downloads the clone's base-image package files from the Transfer Server repository to the local computer.

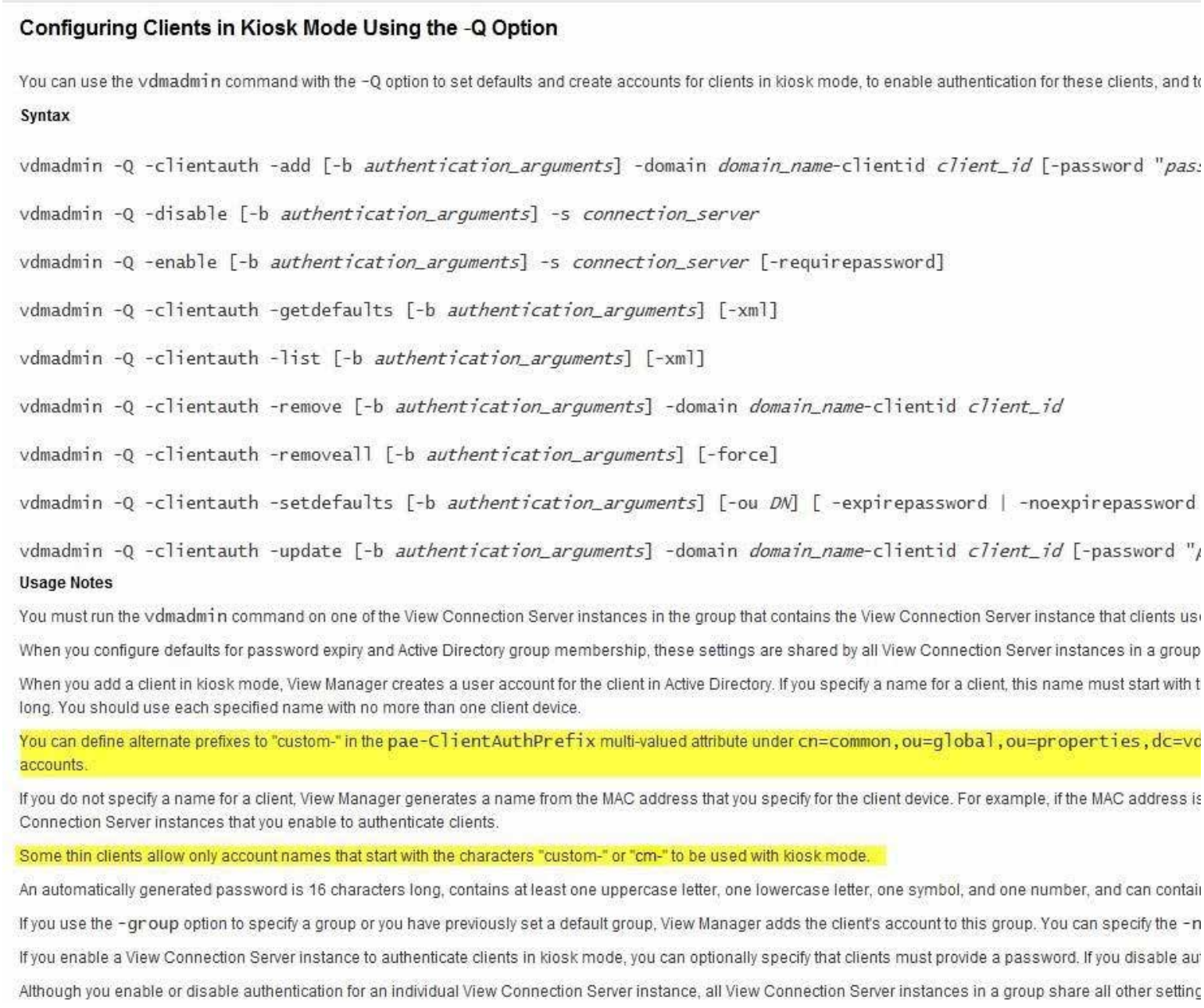
QUESTION 44
An administrator creates a kiosk mode desktop. The client device is unable to connect to the desktop.

Which action should the administrator take to resolve this issue?

A. activate kiosk mode for each View Connection Server
B. add the cm- or Custom- prefix to the AD account for the client device
C. enable kiosk mode on the desktop through View Administrator
D. create AD accounts for all users authorized to use the desktop

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:



Configuring Clients in Kiosk Mode Using the -Q Option

You can use the vdmadmin command with the -Q option to set defaults and create accounts for clients in kiosk mode, to enable authentication for these clients, and t

Syntax

```
vdmadmin -Q -clientauth -add [-b authentication_arguments] -domain domain_name-clientid client_id [-password "pas
vdmadmin -Q -disable [-b authentication_arguments] -s connection_server
vdmadmin -Q -enable [-b authentication_arguments] -s connection_server [-requirepassword]
vdmadmin -Q -clientauth -getdefaults [-b authentication_arguments] [-xml]
vdmadmin -Q -clientauth -list [-b authentication_arguments] [-xml]
vdmadmin -Q -clientauth -remove [-b authentication_arguments] -domain domain_name-clientid client_id
vdmadmin -Q -clientauth -removeall [-b authentication_arguments] [-force]
vdmadmin -Q -clientauth -setdefaults [-b authentication_arguments] [-ou DN] [ -expirepassword | -noexpirepassword
vdmadmin -Q -clientauth -update [-b authentication_arguments] -domain domain_name-clientid client_id [-password "
```

Usage Notes

You must run the vdmadmin command on one of the View Connection Server instances in the group that contains the View Connection Server instance that clients us

When you configure defaults for password expiry and Active Directory group membership, these settings are shared by all View Connection Server instances in a group

When you add a client in kiosk mode, View Manager creates a user account for the client in Active Directory. If you specify a name for a client, this name must start with t long. You should use each specified name with no more than one client device.

You can define alternate prefixes to "custom-" in the pae-ClientAuthPrefix multi-valued attribute under cn=common,ou=global,ou=properties,dc=vd accounts.

If you do not specify a name for a client, View Manager generates a name from the MAC address that you specify for the client device. For example, if the MAC address is Connection Server instances that you enable to authenticate clients.

Some thin clients allow only account names that start with the characters "custom-" or "cm-" to be used with kiosk mode.

An automatically generated password is 16 characters long, contains at least one uppercase letter, one lowercase letter, one symbol, and one number, and can contai

If you use the -group option to specify a group or you have previously set a default group, View Manager adds the client's account to this group. You can specify the -n

If you enable a View Connection Server instance to authenticate clients in kiosk mode, you can optionally specify that clients must provide a password. If you disable au

Although you enable or disable authentication for an individual View Connection Server instance, all View Connection Server instances in a group share all other setting

QUESTION 45
A View environment requires a thin client to automatically connect to a kiosk mode desktop without a password.

How can the administrator accomplish this?

A. configure the assigned desktop in Unsecured mode
B. add the thin client MAC address to the Kiosk folder on the View Connection Server

C. disable password checking from the View Administrator
D. set an automatically-generated password for the client account

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 46
A View administrator has received a request for a View desktop configured for kiosk mode.

Which three steps must a View administrator perform to accomplish this task? (Choose three.)

A. enable kiosk mode authentication from the Kiosk Mode tab under the View Administration Console
B. configure Active Directory to accept the kiosk mode accounts
C. enable authentication of clients in kiosk mode from the View desktops
D. configure kiosk mode service on the View desktop
E. configure the View Accounts to be used with kiosk mode from the View Administration Console

Correct Answer: BCE
Explanation

Explanation/Reference:
Explanation:

Procedure

1 Prepare Active Directory and View Manager for Clients in Kiosk Mode on page 350

You must configure Active Directory to accept the accounts that you create to authenticate client devices. Whenever you create a group, you must also entitle that group to the desktop pool that a client accesses. You can also prepare the desktop pool that the clients use.

2 Set Default Values for Clients in Kiosk Mode on page 351

You can use the `vdmadmin` command to set the default values for the organizational unit, password expiry, and group membership in Active Directory for clients in kiosk mode.

3 Display the MAC Addresses of Client Devices on page 352

If you want to create an account for a client that is based on its MAC address, you can use View Client to discover the MAC address of the client device.

4 Add Accounts for Clients in Kiosk Mode on page 353

You can use the `vdmadmin` command to add accounts for clients to the configuration of a View Connection Server group. After you add a client, it is available for use with a View Connection Server instance on which you have enabled authentication of clients. You can also update the configuration of clients, or remove their accounts from the system.

5 Enable Authentication of Clients in Kiosk Mode on page 354

You can use the `vdmadmin` command to enable authentication of clients that attempt to connect to their desktops via a View Connection Server instance.

6 Verify the Configuration of Clients in Kiosk Mode on page 355

You can use the `vdmadmin` command to display information about clients in kiosk mode and View Connection Server instances that are configured to authenticate such clients.

7 Connect to Desktops from Clients in Kiosk Mode on page 356

You can run View Client from the command line or use a script to connect a client to a remote session.

QUESTION 47
What are two requirements for creating a Kiosk Mode user in Active Directory? (Choose two.)

A. The name must be less than 21 characters long.
B. The name must match a local user on the Connection Server.
C. The name must reference the MAC address of the client device.
D. The name must start with a recognized prefix string.

Correct Answer: AD
Explanation

Explanation/Reference:
Explanation:

security server

Add Accounts for Clients in Kiosk Mode

You can use the `vdmadmin` command to add accounts for clients to the configuration of a View Connection Server group. After you add a client, it is available for use with a View Connection Server instance on which you have enabled authentication of clients. You can also update the configuration of clients, or remove their accounts from the system.

You must run the `vdmadmin` command on one of the View Connection Server instances in the group that contains the View Connection Server instance that clients will use to connect to their desktops.

When you add a client in kiosk mode, View Manager creates a user account for the client in Active Directory. If you specify a name for a client, this name must start with a recognized prefix string, such as "custom-", or with an alternate prefix string that you have defined in ADAM, and it cannot be more than 20 characters long. If you do not specify a name for a client, View Manager generates a name from the MAC address that you specify for the client device. For example, if the MAC address is 00:10:db:ee:76:80, the corresponding account name is cm-00_10_db_ee_76_80. You can only use these accounts with View Connection Server instances that you enable to authenticate clients.

IMPORTANT Do not use a specified name with more than one client device. Future releases might not support this configuration.

QUESTION 48
Which View feature is used to authenticate a Kiosk Mode connection by client device rather than end user?

A. Device Verification
B. Flexible Authentication
C. Kiosk Security
D. vShield Endpoint Security

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:
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. If you configure a client to have an automatically generated password, you can run View Client on the device without specifying a password. If you Configure an explicit password, you must specify this password to View Client. As you would usually run View Client from a script, and the password would appear in clear text, you should take precautions to make the script unreadable by unprivileged users.

QUESTION 49
A system administrator needs to create an application repository for ThinApp deployments from View Administrator.

Which two items are required in order to complete this task? (Choose two.)

A. Windows network share
B. ThinApp Distribution point
C. NFS datastore
D. ThinApp MSI files

Correct Answer: AD
Explanation

Explanation/Reference:

QUESTION 50
A system administrator has an existing ThinApp package that needs to be integrated with View for deployment.

When rebuilding the corresponding ThinApp package, which line does the system administrator need to add to the package.ini file to enable application streaming?

A. ThinAppStreaming=0
B. MSIStreaming=1
C. MSIStreaming=0
D. ThinAppStreaming=1

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:

Package Your Applications

You use the ThinApp Setup Capture wizard to capture and package your applications.

Prerequisites

- Download the ThinApp software from http://www.vmware.com/products/thinapp and install it on a clean computer. View supports ThinApp version 4.6 and later.
- Familiarize yourself with the ThinApp software requirements and application packaging instructions in the *ThinApp User's Guide*.

Procedure

1 Start the ThinApp Setup Capture wizard and follow the prompts in the wizard.

2 When the ThinApp Setup Capture wizard prompts you for a project location, select **Build MSI package**.

3 If you plan to stream the application to View desktops, set the MSIStreaming property to 1 in the `package.ini` file.

```
MSIStreaming=1
```

The ThinApp Setup Capture wizard encapsulates the application, all of the necessary components to run the application, and the application itself into an MSI package.

QUESTION 51
A system administrator has an existing ThinApp package that needs to be integrated with View 5.0 for deployment.

When rebuilding the corresponding ThinApp package, which line does the system administrator need to add to the package.ini file to enable full deployment of the application to view users?

A. MSIStreaming=1
B. ThinAppStreaming=1
C. MSIStreaming=0
D. ThinAppStreaming=0

Correct Answer: C

Explanation

Explanation/Reference:
Explanation:
Streaming means no Installation on Desktop, Application will be streamed. So a Full Installation is without Streaming

QUESTION 52
A ThinApp administrator needs to capture an application that leverages ODBC connections.

Which step should the administrator take during the ThinApp capture and build process to enable this functionality inside the ThinApp package?

A. configure the ODBC connections before starting the capture process
B. configure the ODBC connections during the capture process
C. configure the ODBC connections as an upgrade patch to a completed ThinApp application
D. configure the ODBC connections outside the capture process on the client workstations

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 53
A ThinApp administrator needs to capture an application that leverages .NET 2.0 as a prerequisite. The enterprise has standardized on .NET 2.0 on the corporate desktop image.

Which step should the administrator take during the ThinApp capture and build process to enable the ThinApp package to leverage the .NET 2.0 instance installed on the corporate desktop images?

A. Install .NET 2.0 as part of the ThinApp capture process
B. Install .NET 2.0 as an upgrade patch to a completed ThinApp application
C. Install .NET 2.0 as part of the capture workstation before starting the ThinApp capture process
D. Install .NET 2.0 outside the capture process on the client workstations

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 54
A View administrator needs to distribute ThinApp packages from a newly created ThinApp Repository. The corresponding ThinApp package has been set with the streaming option.

Which three ThinApp specific items will be stored inside the corresponding application repository? (Choose three.)

A. the ThinApp sandbox for the corresponding ThinApp package
B. the .EXE file for the corresponding ThinApp package
C. the .DAT file for the corresponding ThinApp package
D. the .MSI file containing the shortcut
E. a shortcut to the ThinApp package on the network share

Correct Answer: BCD
Explanation

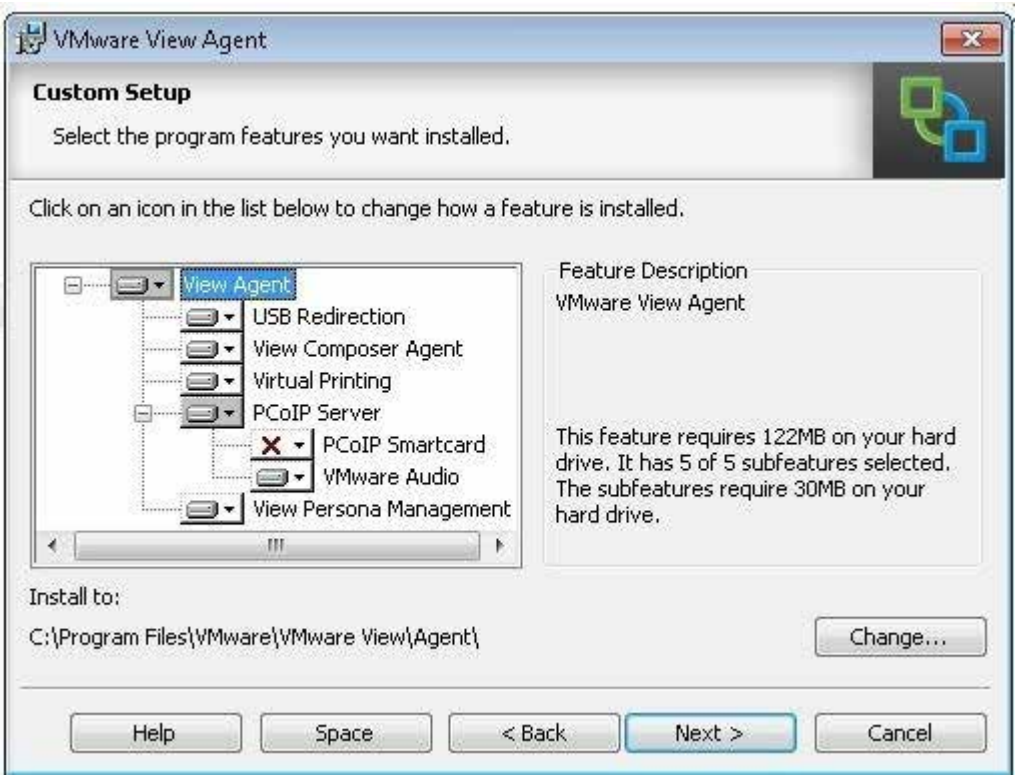
Explanation/Reference:

QUESTION 55
Which steps must a View administrator perform to configure View Persona Management with View desktops?

A. Install the View Agent with the View Persona Management setup option on the replica.
B. Install the View Agent with the View Persona Management setup option on the vCenter Server systems.
C. Install the View Agent with the View Persona Management setup option on the virtual machine that is used as a parent or template.
D. Install the View Agent on the virtual machine and enable the View Persona Management option on first boot.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:



QUESTION 56
In a View environment, users access both View and physical desktops. Users access their View desktops with View Persona Management and their standard desktops with Windows roaming profiles.

What is the recommended configuration?

A. Disable profile sharing in the persona management folder.
B. Enable profile sharing in the persona management folder.
C. Use different profiles for the two desktop types.
D. Use the same profile for the two desktop types.

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 57
View Persona Management has been installed and enabled on your virtual machines in your environment.

What is recommended for Persona Management backup?

A. Snapshot the Desktop and then backup the profile.
B. Set the Persona Management software to enable before backing up.
C. Enable the Persona Management plugin in the vStorage APIs for Data Protection.
D. Do not use backup software products like MozyPro or Windows Volume backup services.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

Additional Best Practices

You can also follow these recommendations:

- By default, many antivirus products do not scan offline files. For example, when a user logs in to a desktop, these anti-virus products do not scan user profile files that are not specified in the **Files and folders to preload** or **Windows roaming profiles synchronization** group policy setting. For many deployments, the default behavior is the best practice because it reduces the I/O required to download files during on-demand scans.

  If you do want to retrieve files from the remote repository and enable scanning of offline files, see the documentation for your antivirus product.
- It is highly recommended that you use standard practices to back up network shares on which View Persona Management stores the profile repository.

Note

Do not use backup software such as MozyPro or Windows Volume backup services with View Persona Management to back up user profiles on View desktops.

View Persona Management ensures that user profiles are backed up to the remote profile repository, eliminating the need for additional tools to back up user data on the desktops. In certain cases, tools such as MozyPro or Windows Volume backup services can interfere with View Persona Management and cause data loss or corruption.

- You can set View Persona Management policies to enhance performance when users start ThinApp applications. See Configuring User Profiles to Include ThinApp Sandbox Folders.
- If your users generate substantial persona data, and you plan to use refresh and recompose to manage dedicated-assignment, linked-clone desktops, configure your desktop pool to use separate View Composer persistent disks. Persistent disks can enhance the performance of View Persona Management. See Configuring View Composer Persistent Disks with View Persona Management.

QUESTION 58
A View deployment consists of ThinApp applications as well as other types of applications. The administrator wants to configure the user profiles to include the ThinApp sandbox folders.

Which action will meet this requirement?

A. Enable the Folders to background download group policy settings and add the user's files.
B. Enable the Folders to background download group policy settings and add the ThinApp sandbox folders.
C. Enable the Files and folders to preload group policy settings and add the ThinApp sandbox folders during the login.

D. Enable the Roam Local Settings folders to preload group policy settings and add the ThinApp sandbox folders

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:

Configuring User Profiles to Include ThinApp Sandbox Folders

View Persona Management maintains user settings that are associated with ThinApp applications by including ThinApp sandbox folders in user profiles. You can set View Persona Management policies to enhance performance when users start ThinApp applications.

View Persona Management preloads ThinApp sandbox folders and files in the local user profile when a user logs in. The ThinApp sandbox folders are created before a user can complete the log on. To enhance performance, View Persona Management does not download the ThinApp sandbox data during the login, although files are created on the local desktop with the same basic attributes and sizes as the ThinApp sandbox files in the user's remote profile.

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. See Roaming and Synchronization Group Policy Settings.

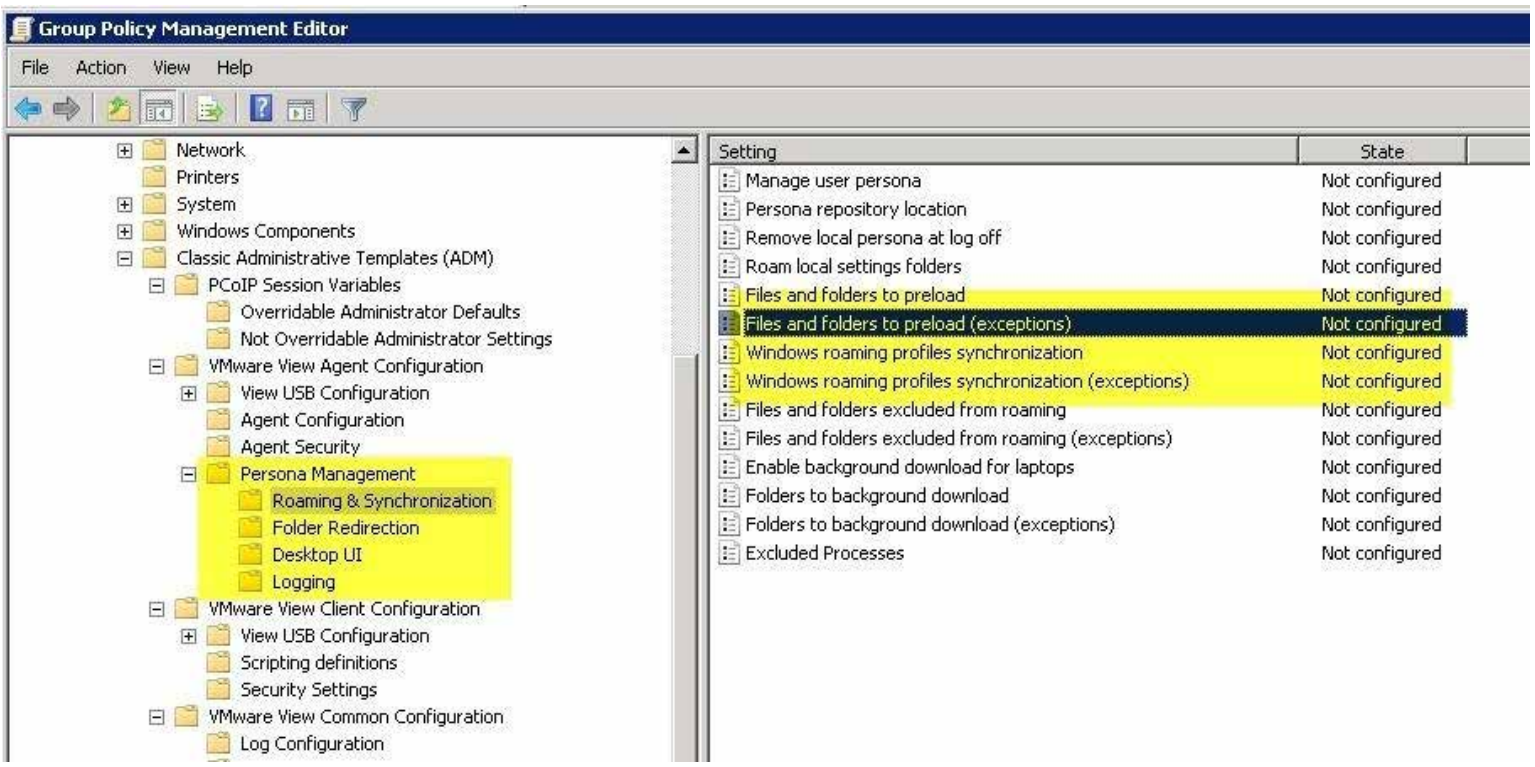
The actual ThinApp sandbox files can be large. With the **Folders to background download** setting, users do not have to wait for large files to download when they start an application. Also, users do not have to wait for the files to preload when they log in, as they might if you use the **Files and folders to preload** setting with large files.

QUESTION 59
What can an administrator specify within a user's persona that are managed by Windows roaming profiles functionality instead of View Persona Management?

A. ADM Template
B. Files and Folders
C. Network Share
D. Persona Repository

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:



QUESTION 60
Which two approaches can an administrator use to configure View Persona Management for one desktop pool? (Choose two.)

A. Add the View Persona Management Administrative (ADM) Template file to each desktop in the pool.
B. Add the View Persona Management Administrative (ADM) Template file to the virtual machine that is used to create the pool.
C. Add the View Persona Management Administrative (ADM) Template file to Active Directory and apply the group policy settings to the OU that contains the users in the pool.
D. Add the View Persona Management Administrative (ADM) Template file to Active Directory and apply the group policy settings to the OU that contains the desktops in the pool.

Correct Answer: BD
Explanation

Explanation/Reference:
Explanation:

Overview of Setting Up a View Persona Management Deployment

To set up a View desktop deployment with View Persona Management, you must perform several high-level tasks.

This sequence is recommended, although you can perform these tasks in a different sequence. For example, you can configure or reconfigure group policy settings in Active Directory after you deploy desktop pools.

1 Configure a remote repository to store user profiles.

You can configure a network share or use an existing Active Directory user profile path that you configured for Windows roaming profiles.

2 Install View Agent with the **View Persona Management** setup option on the virtual machines that you use to create desktop pools.

3 Add the View Persona Management Administrative (ADM) Template file to your Active Directory server or the Local Computer Policy configuration on the parent virtual machine.

To configure View Persona Management for your whole View deployment, add the ADM Template file to Active Directory.

To configure View Persona Management for one desktop pool, you can take these approaches:

- Add the ADM Template file to the virtual machine that you use to create the pool.
- Add the ADM Template file to Active Directory and apply the group policy settings to the OU that contains the desktops in the pool.

4 Enable View Persona Management by enabling the **Manage user persona** group policy setting.

5 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.

6 (Optional) Configure other group policy settings in Active Directory or the Local Computer Policy configuration.

7 Create desktop pools from the virtual machines on which you installed View Agent with the **View Persona Management** setup option.

QUESTION 61
A View administrator is instructed to use a network share to store the user profile repository for a View Persona Management deployment.

What are the two recommended locations for this network share? (Choose two.)

A. A shared folder on a local drive
B. A shared folder on a network server
C. A shared folder on an Active Directory server
D. A shared folder on a network-attached storage (NAS) device

Correct Answer: BD
Explanation

Explanation/Reference:

QUESTION 62
View Persona Management has been installed on the virtual machines in a View environment.

How often are changes in the local profile copied to the remote repository by default?

A. Every 5 minutes
B. Every 10 minutes
C. During login and every 10 minutes after login
D. An interval must be specified by the administrator

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:

View Persona Management minimizes the time it takes to log in to and log off of desktops. Login and logoff time can be a problem with Windows roaming profiles.

- 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.

QUESTION 63
View Persona Management has been installed and enabled on your virtual machines. The administrator wants to manage the View user personas.

Which statement is true?

A. The administrator can manage View user personas by logging into the remote repository.
B. The administrator can manage View user personas within the Folder view of the View Administrator.
C. The administrator cannot manage View user personas by adding the ADM Template file to Active Directory.
D. The administrator cannot manage View user personas by using the Windows roaming profiles functions.

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 64
A View administrator is configuring the events database.

Which two data repository configurations will allow users to monitor events in View Administrator? (Choose two.)

A. Oracle with SQL authentication
B. Microsoft SQL Server with Integrated Windows authentication
C. Microsoft SQL Server with SQL authentication
D. Oracle with Integrated Windows authentication

Correct Answer: AC
Explanation

Explanation/Reference:
Explanation:
SQL-Server Auth. is used, not Windows Auth.!

QUESTION 65
What is a prerequisite for configuring an events database?

A. The events database certificate must be created
B. An ODBC data source for the events database must exist
C. A prefix for the tables in the events database has been defined
D. The username and password of an administrator on View Administrator

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:

Add a Database and Database User for View Events

You create an event database by adding it to an existing database server. You can then use enterprise reporting software to analyze the events in the database.

The database server for the event database can reside on a View Connection Server host itself or on a dedicated server. Alternatively, you can use a suitable existing database server, such as a server that hosts a View Composer database.

NOTE You do not need to create an ODBC data source for this database.

QUESTION 66
Which two permissions are required by the Events Database user? (Choose two.)

A. Create Tables
B. Delete Views
C. Modify Tables
D. Read Views

Correct Answer: AD
Explanation

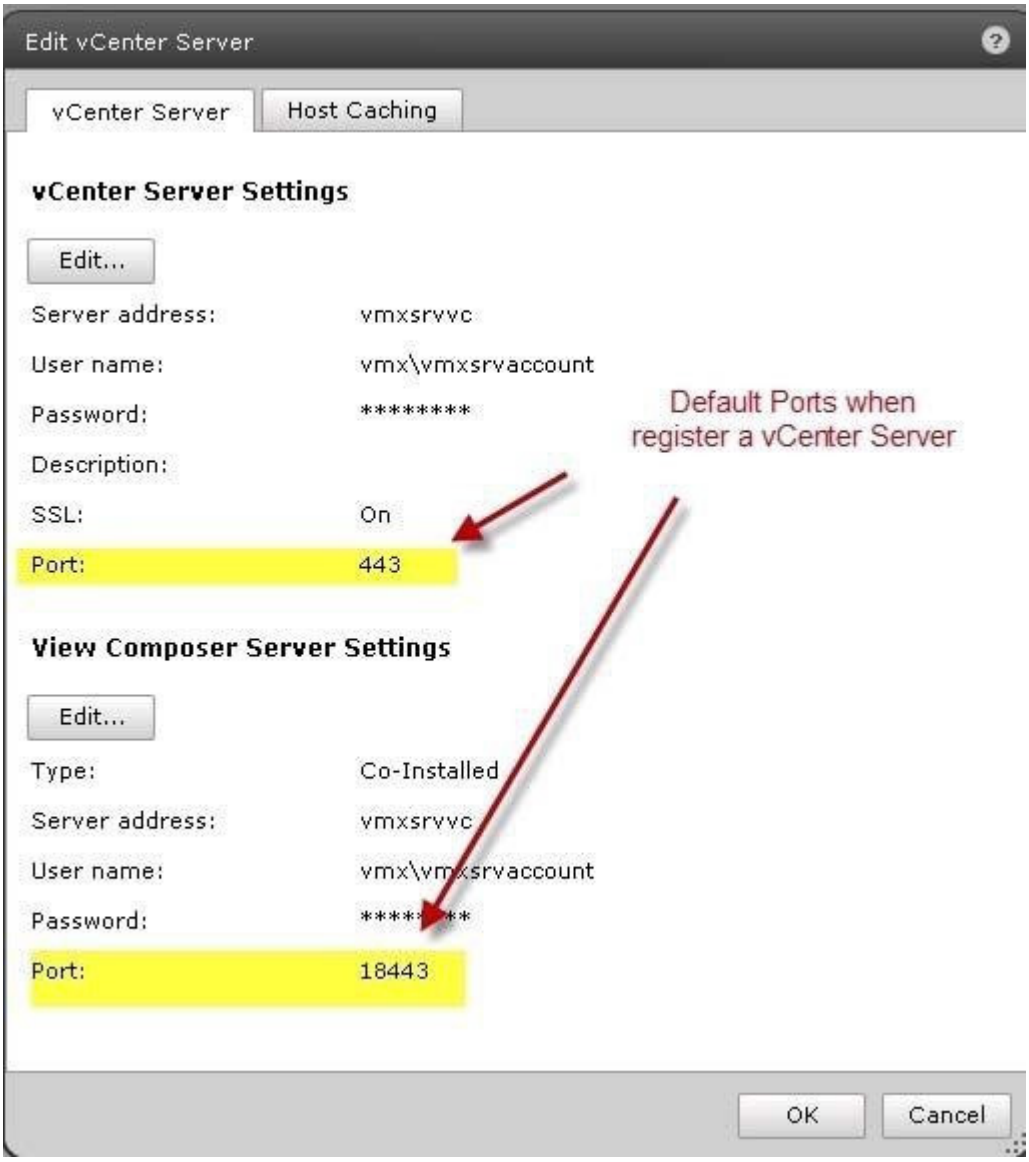
Explanation/Reference:

QUESTION 67
What is the default port number used by the View Composer when setting up the vCenter Server connection?

A. 443
B. 8080
C. 8443
D. 18443

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:



QUESTION 68
On which two objects can a View administrator apply a Tag? (Choose two.)

A. Connection Servers
B. Desktop Pools
C. Persistent Desktop
D. Security Servers

Correct Answer: AB
Explanation

Explanation/Reference:
Explanation:

Procedure

1 In View Administrator, select **Inventory** > **Pools**.

2 Select the pool that you want to assign a tag to.

Option	Action
Assign a tag to a new pool	Click **Add** to start the Add Pool wizard and define and identify the pool.
Assign a tag to an existing pool	Select the pool and click **Edit**.

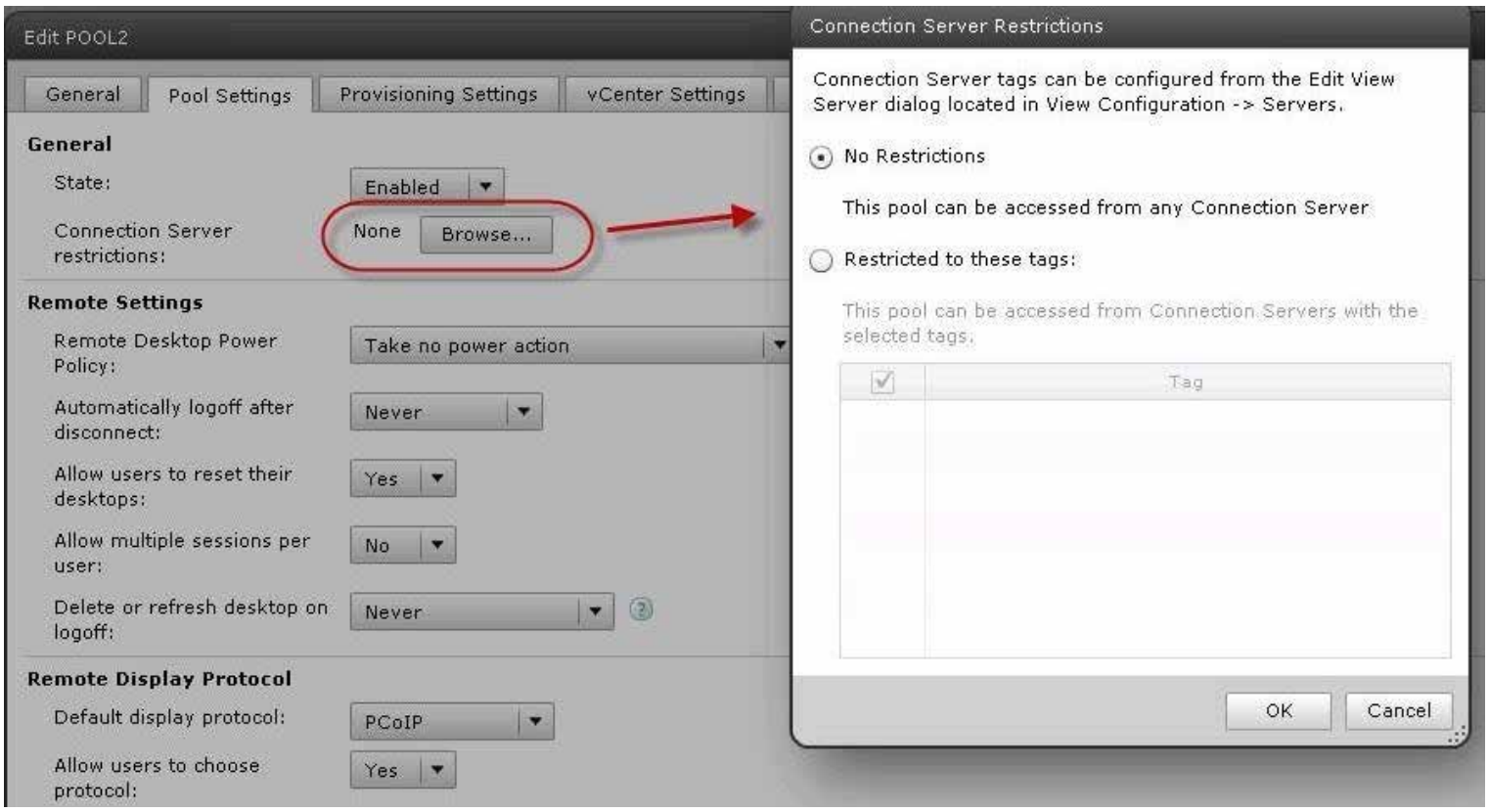
3 Go to the Pool Settings page.

Option	Action
Pool settings for a new pool	Click **Pool Settings** in the Add Pool wizard.
Pool settings for an existing pool	Select the **Pool Settings** tab.

4 Click **Browse** next to **Connection Server restrictions** and configure the View Connection Server instances that can access the desktop pool.

Option	Action
Make the pool accessible to any View Connection Server instance	Select **No Restrictions**.
Make the pool accessible only to View Connection Server instances that have those tags	Select **Restrict to these tags** and select one or more tags. You can use the check boxes to select multiple tags.

5 Click **OK** to save your changes.

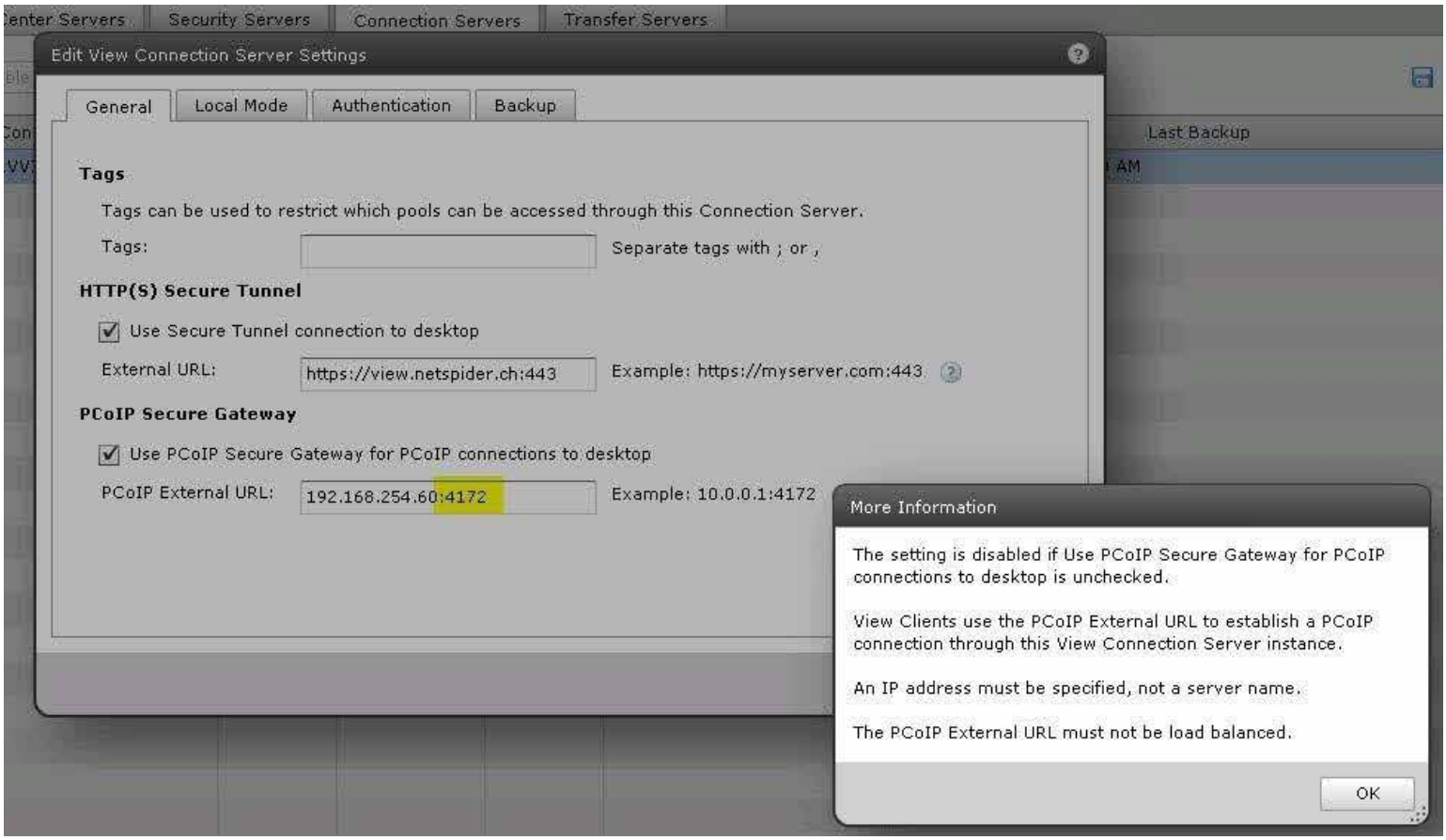


QUESTION 69
What is the default port used when an administrator configures the external URL for the PCoIP Secure Gateway?

A. 443
B. 3389
C. 4172
D. 8080

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:



QUESTION 70
Which three settings are configured under Global Settings on the View Connection Server administration page? (Choose three.)

A. USB access
B. Session Timeout
C. Pre-login message
D. PCoIP hardware acceleration
E. Re-authenticate secure tunnel connections after network interruption

Correct Answer: BCE
Explanation

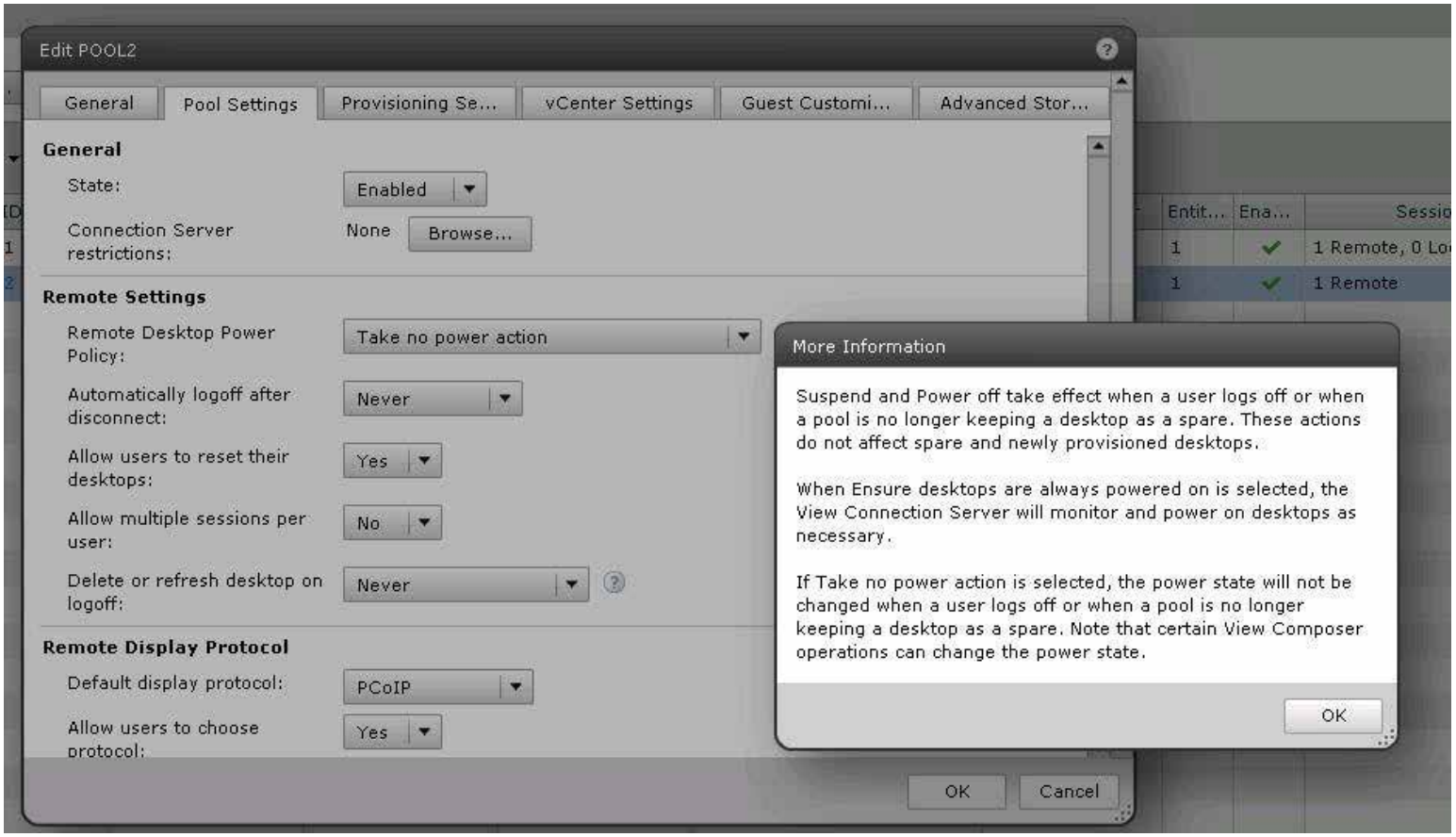
Explanation/Reference:
Explanation:

QUESTION 71
Session Timeout can be used in conjunction with which desktop/pool setting to help conserve ESXi host resources?

A. Desktop state
B. Remote desktop power policy
C. Allow users to reset their desktop
D. Refresh desktop OS

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:



QUESTION 72
When configured, which three Global settings help ensure the security of a View environment? (Choose three.)

A. Require SSL for client connections and View Administrator
B. Security Server Timeout
C. Session Timeout
D. Reauthenticate Secure VPN connections after network interruption
E. Require Security Server for client connections and View Administrator

Correct Answer: ACD
Explanation

Explanation/Reference:

QUESTION 73
Users have access to company confidential files and applications when using View internally. When users are connected from home, they are redirected to a different pool of desktops that have restricted applications and restricted network access.

Which feature in View enables this functionality?

A. Global Policies
B. vShield Endpoint

C. Security Servers
D. Tags

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

Restricting View Desktop Access

You can configure the restricted entitlements feature to restrict View desktop access based on the View Connection Server instance that users connect to when they select desktops.

With restricted entitlements, you assign one or more tags to a View Connection Server instance. Then, when configuring a desktop pool, you select the tags of the View Connection Server instances that you want to be able to access the desktop pool.

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.

QUESTION 74
A View environment for an enterprise has the following requirements for accessing USB devices:
All users can use USB devices with their virtual desktops except members of the finance group, who have sensitive data
There is one administrative assistant in the finance group that needs to transfer data using a USB device.

Which three actions should the administrator take to enable these requirements? (Choose three.)

A. set the View USB Access policy to Allow on the Global level
B. set the View USB Access policy to Deny for the Finance Desktop pool
C. set the View USB Access GPO for the View Agent on the Finance group desktops to deny USB access
D. set the View USB Access policy to Allow for the Administrative Assistant
E. set the View USB Access GPO for the View Agent for the administrative assistant user desktop to allow USB access

Correct Answer: ABD
Explanation

Explanation/Reference:
Explanation:

Setting Policies in View Administrator

You use View Administrator to configure policies for client sessions.

You can set these policies to affect specific users, specific desktop pools, or all client sessions users. 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.

User-level policies inherit settings from the equivalent desktop-pool policy settings. Similarly, pool-level policies inherit settings from the equivalent global policy settings. A pool-level policy setting takes precedence over the equivalent global policy setting. A user-level policy setting takes precedence over the equivalent global and pool-level policy settings.

Lower-level policy settings can be more or less restrictive than the equivalent higher-level settings. For example, if the global policy that specifies the amount of time a desktop can be checked out is set to 10 minutes and the equivalent pool-level policy is set to 5 minutes, you can set the equivalent user-level policy to 30 minutes for any user in the pool.

- Configure Global Policy Settings on page 138
  You can configure global policies to control the behavior of all client sessions users.
- Configure Policies for Desktop Pools on page 138
  You can configure desktop-level policies to affect specific desktop pools. Desktop-level policy settings take precedence over their equivalent global policy settings.
- Configure Policies for Desktop Users on page 139
  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.

QUESTION 75
The Finance Desktop pool has access to sensitive data. Enterprise security standards will not allow external access to this desktop. The enterprise has replica servers, one of which is paired with a security server to allow external access to desktops.

Which two actions would restrict external access to this pool? (Choose two.)

A. assign the tag named Finance to the security server
B. set a tag named Finance on the internal facing connection servers
C. assign the tag named Finance to the Finance Desktop pool
D. set a tag named Finance on the external facing connection servers

Correct Answer: BC
Explanation

Explanation/Reference:

QUESTION 76
Click the Exhibit button.

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

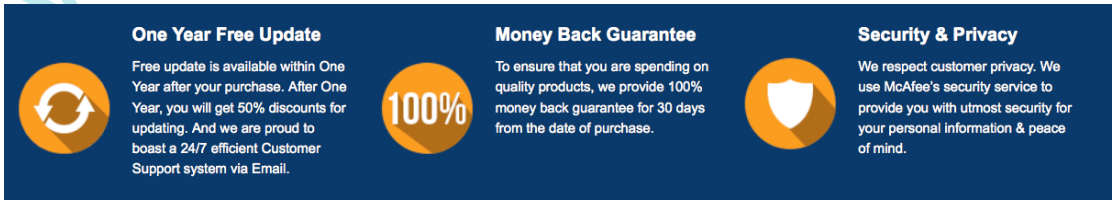
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.