Microsoft

Virtual Desktop Infrastructure

A deployment guide for education

January 2014

Table of contents

Windows 8

Virtual Desktop Infrastructure

A deployment guide for education

One of the challenges for educational institutions is managing the wide diversity of devices and user types. Given such diversity, establishing and maintaining a standardized technology learning platform can be difficult. Although it may be possible to purchase new devices running the Windows 8.1 operating system or upgrade existing devices to Windows 8.1, other institution-owned devices may be unable to run Windows 8.1 (such as older hardware or devices running Apple iOS or Google Android).

In addition, Bring Your Own Device (BYOD) initiatives are increasingly popular in institutions because they allow faculty to use their devices to perform administrative roles aid with curriculum. BYOD initiatives also allow students to use their devices (in and out of the classroom) as a part of the educational process. BYOD initiatives help institutions by reducing the up-front cost of devices while allowing faculty and students to take advantage of technology for education.

However, BYOD initiatives can create problems for IT pros who support the faculty and students. It is almost certain that the devices will have broad diversity. Although it may be possible that the faculty or students may have devices running the Windows 8.1 operating system, other personally owned devices may be unable to run Windows 8.1 (such as older hardware or devices running iOS or Android).

You can address these challenges by using Virtual Desktop Infrastructure (VDI) powered by the Windows Server 2012 R2 or Windows MultiPoint Server 2012 operating system. With VDI in

NOTE

Although many of the topics discussed in this guide are applicable to VDI in Windows Server 2012 R2, Windows Server 2012, or Windows MultiPoint Server 2012, this guide focuses on VDI in Windows Server 2012 R2. For more information about Windows MultiPoint Server 2012 planning and deployment, see the topic "Windows MultiPoint Server 2012" at http://technet.microsoft.com/library/jj916259.aspx and other Windows MultiPoint Server 2012 resources listed in this guide.

Windows 8

Windows Server 2012 R2 or Windows MultiPoint Server 2012, users can remotely run Windows 8.1 apps as though they were running on their local device, including video clips, movies, streaming video, and other graphically intensive applications. Users can also directly access USB devices connected to their device (such as smart card readers, USB flash drives, or scanners) from within VDI.

The following is a list of assumptions about the institutionally-owned devices described in this guide:

- The devices may or may not be domain-joined.
- Users log on to their device by using an institution-issued account (and possible have an associated Microsoft account) instead of using their own Windows account.
- Windows 8.1 Enterprise can be deployed on the devices (if desired).
- Windows-based devices that need to support Microsoft RemoteFX will be running Windows Vista or later operating systems.
- Devices running operating systems other than Windows (such as iOS or Android) will require an app that supports the Remote Desktop Protocol (RDP) and RemoteFX.

The following is a list of assumptions about the personally owned devices described in this guide:

- The devices are not domain joined.
- Users log on to their device by using their own Windows account (and possible Microsoft account) instead of an institution-issued account.
- None of the devices will be running Windows 8.1 Enterprise.
- Windows-based devices that need to support RemoteFX will be running Windows Vista or later.
- Devices running operating systems other than Windows (such as iOS or Android) will require an app that supports the RDP or RemoteFX.

Choosing a VDI deployment scenario

Windows Server 2012 R2 offers the following deployment scenarios:

- **Virtual machine (VM)–based** In this scenario, Windows 8.1 VMs run in a HyperV infrastructure. You use Remote Desktop Services to provide users remote connectivity to the VMs. You can use the VM-based deployment scenario with pooled or personal VM collections. For more information about the VM-based deployment scenario and pooled and personal VM collections, see the section "Virtual machine–based desktop deployment" on page 6.

- **Session-based** In this scenario, remote users connect to Remote Desktop Services in Windows Server 2012 R2 and run their application in Windows Server 2012 R2 sessions. Only Remote Desktop Services is required for this scenario. For more information about the session-based deployment scenario, see the section "Session-based desktop deployment" on page 10.

Figure 1 provides a high-level comparison of the VDI deployment scenarios in Windows Server 2012 R2. Use the information in Figure 1 to identify the high-level differences between the VM and session-based desktop deployment scenarios.

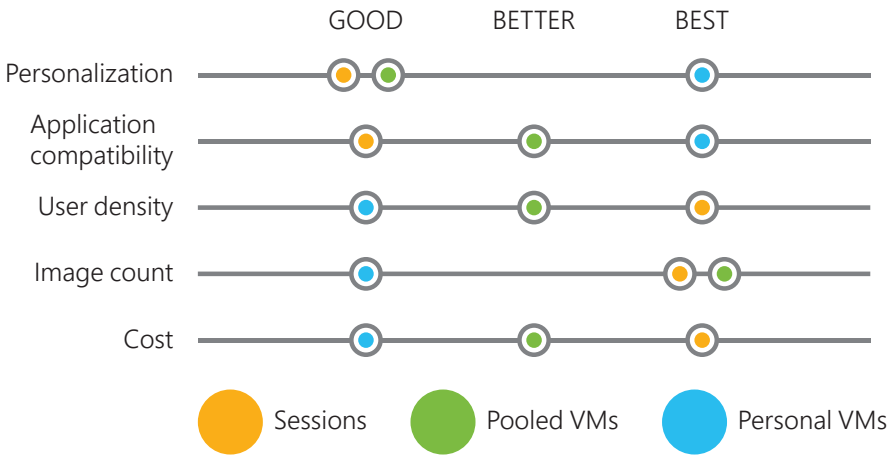

FIGURE 1 High-level comparison of VDI desktop deployment scenarios

Table 1 provide a more detailed comparison of the VDI desktop deployment scenarios and Windows MultiPoint Server 2012. Use the information in this table to choose the right combination of VDI deployment solutions for your institution. You can use any combination of these scenarios to create a comprehensive VDI deployment solution.

TABLE 1 Detailed Comparison of VDI Desktop Deployment Scenarios and Windows MultiPoint Server 2012

	Session-based desktop deployment	Windows MultiPoint Server 2012	VM-based desktop deployment
User operating system experience	Windows Server 2012 R2	Windows 8.1	Windows 8.1
Support for full-fidelity video, with coverage for all media types and highly synchronized audio, rich media support, Microsoft Silverlight, 3D graphics, and Windows Aero	Microsoft RemoteFX	Requires direct video–connected stations, USB zero client–connected stations, USB-over-Ethernet zero clients, or RDP–over-LAN with RemoteFX	Requires RemoteFX
Directly connect the VDI session to client USB devices	• Standard RDP connection provides limited support of USB device • RemoteFX required for broader support of USB devices	• Standard RDP connection provides limited support of USB device • Direct video–connected stations, USB zero client–connected stations, USB-over-Ethernet zero clients, or RDP-over-LAN with RemoteFX required for broader support of USB devices	• Standard RDP connection provides limited support of USB device • RemoteFX required for broader support of USB devices

	Session-based desktop deployment	Windows MultiPoint Server 2012	VM-based desktop deployment
Supported client devices	Any device that supports RDP or RemoteFX (including Windows Thin PC)	Supports the following: • Direct video–connected stations • USB zero client–connected stations • USB-over-Ethernet zero clients • Any device that supports RDP or RemoteFX	Any device that supports RDP or RemoteFX (including Windows Thin PC)
Scaling	As many as hundreds of users for each server, but multiple servers can be added to scale to higher numbers	As many as 20 users	Up to hundreds of users for each server, but multiple servers can be added to scale to higher numbers
High availability	Supports load balancing and clustering of resources	Unavailable	Supports load balancing and clustering of resources

Additional resources:

- "HP Client Virtualization SMB Reference Architecture for Windows Server 2012" at http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA4-3901ENW&cc=us&lc=en

Virtual machine–based desktop deployment

Figure 2 illustrates the high-level components in a VM-based desktop deployment. You can run these components all on one server or on even more servers to provide additional scaling and high availability.

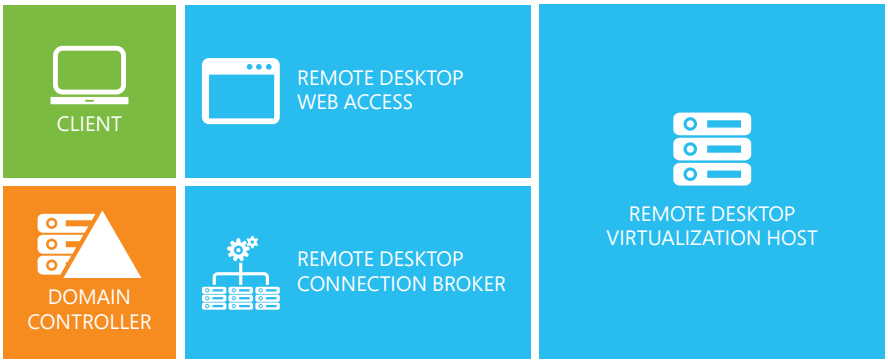

FIGURE 2 Components in a VM-based desktop deployment

The following is a description of the components in a typical VM-based desktop deployment:

- **Remote Desktop Connection Broker** This role service manages connections between the clients and the VMs running on the Remote Desktop Virtualization Host.
- **Remote Desktop Virtualization Host** This role service integrates with HyperV to provide VMs. It uses the Remote Desktop Connection Broker role service to determine the VM to which the user is redirected.
- **Remote Desktop Web Access** This role service enables users to access VMs through a web browser.
- **Client** The client provides access to the remote desktop. it can be a traditional device running the Remote Desktop Client in Windows, an app that supports RDP and RemoteFX, a thin or zero client that supports RDP (such as Windows Thin PC), or a RemoteFX-enabled device. For institution-owned devices, the client device may or may not be a member of an Active

Directory domain. For personally owned devices, the client will not be a member of the Active Directory Domain Services (AD DS) domain.

- **Domain controller and other network infrastructure services** These services include AD DS, Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and routing.

Windows Server 2012 R2 introduces the concept of *virtual desktop collections.* A virtual desktop collection consists of one or more virtual desktops used in a VDI deployment scenario. You can choose to deploy pooled or personal collections with the method you select, depending on your environment and preferences, as described in Table 2.

TABLE 2 Comparison of Pooled and Personal Virtual Desktop Collections

	Pooled	Personal
Changes are made to	Transient virtual hard disk	VM virtual hard disk
Changes saved after session ends	No (except for user profile changes)	Yes
VM instances	Single VM master image that all users in the collection share	Separate VM instances created from a mater VM for each user
Number of images to manage	One master image	An image for each user (after the VM instance is created)
Infrastructure services	• Managed network • Remote Desktop Services • HyperV	• Managed network • Remote Desktop Services • HyperV
Network connectivity	• Support standard Remote Desktop Services by using low-bandwidth connections • RemoteFX connection requires medium- to high-bandwidth connections (depending on content being displayed)	• Support standard Remote Desktop Services by using low-bandwidth connections • RemoteFX connection requires medium- to high-bandwidth connections (depending on content being displayed)
Storage requirements	• Storage for master image and transient virtual hard disks • Storage for each User Profile Disk (if used)	Requires separate VM storage for each user; if the average storage for the master VM is 100 GB and there are 100 users, 10 TB of storage will be required

	Pooled	Personal
Manageability	Only one image to manage, so use stand-alone image-management tools; changes to the master image are reflected the next time a session is initiated	Manage by using technologies and products such as Group Policy, Windows Server Update Services, or Microsoft System Center 2012 R2 Configuration Manager
User flexibility	• Users cannot install apps • Users cannot be an administrator on their VM	• Users can install apps • Users can be an administrator on their VM
User profile storage	• Transient virtual hard disk (VHD; user profile changes are lost) • User Profile Disk (user profile changes are retained)	Stored and retained in the VM VHDs
User, operating system, and app configuration management	• Roaming Profiles • Folder Redirection • Microsoft User Experience Virtualization (UE-V) • Microsoft Application Virtualization (App-V) • User Profile Disk	• Roaming Profiles • Folder Redirection • UE-V • App-V • Locally stored on VM

You can deploy both pooled and personal collections as:

- **Managed** This deployment option lets Remote Desktop Services automatically manage the virtual desktops within the collection.
- **Unmanaged** This deployment option lets you manually manage the virtual desktops within the collection.

The high-level steps for deploying VM-based desktop deployment are:

1. Deploy Windows Server 2012 R2 on the Remote Desktop Connection Broker server.
2. Deploy Windows Server 2012 R2 on the Remote Desktop Web Access server.
3. Deploy Windows Server 2012 R2 on the Remote Desktop Virtualization Host server.
4. Ensure that all servers are members of the same AD DS domain.

5. On the Remote Desktop Connection Broker server, use Server Manager to add all the servers to the server pool.

6. On the Remote Desktop Connection Broker server, use Server Manager to install the following role services for the Remote Desktop Services Installation server role:

    - Remote Desktop Connection Broker
    - Remote Desktop Web Access
    - Remote Desktop Virtualization Host

7. Add the virtual desktop template to the Remote Desktop Virtualization Host server.

8. If deploying a pooled collection, create a network shared folder in which to store the User Profile Disk (typically on the Remote Desktop Connection Broker server).

9. Create the collection (pooled for a pooled collection or personal for a personal collection).

10. Verify that the virtual desktop collection works correctly.

NOTE

Although you are running Server Manager on the Remote Desktop Connection Broker server, Server Manager prompts you for the names of the servers running the other Remote Desktop Services role services.

Additional resources:

- "Test Lab Guide: Virtual Desktop Infrastructure Standard Deployment" at http://technet.microsoft.com/en-us/library/hh831541.aspx
- "Test Lab Guide: Managed Pooled Virtual Desktop Collections" at http://technet.microsoft.com/en-us/library/hh831663.aspx
- "Test Lab Guide: Unmanaged Pooled Virtual Desktop Collections" at http://technet.microsoft.com/en-us/library/hh831618.aspx
- "Windows 8/Windows Server 2012: Pooled Virtual Desktop Infrastructure" at http://blogs.technet.com/b/askperf/archive/2012/10/31/windows-8-windows-server-2012-pooled-virtual-desktop-infrastructure.aspx

Session-based desktop deployment

Figure 3 illustrates the high-level components in a session-based desktop deployment. You can run all of these components on one server or on even more servers to provide additional scaling and high availability.

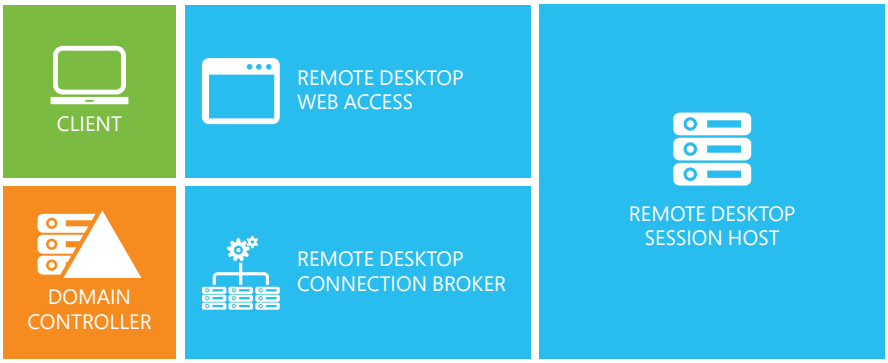

FIGURE 3 Components in a session-based desktop deployment

The following list provides a description of the components in a typical session-based desktop deployment:

- **Remote Desktop Connection Broker** This role service manages connections between the clients and the remote desktop sessions running on the Remote Desktop Session Host.
- **Remote Desktop Session Host** This role service runs RemoteApp programs or session-based virtual desktops. This role servers is ultimately where the users connect to run programs, save files, and use other resources. It uses the Remote Desktop Connection Broker role service to determine the remote desktop session to which the user is redirected.
- **Remote Desktop Web Access** This role service enables users to access the remote desktop sessions through a web browser.
- **Client** The client provides access to the remote desktop. it can be a traditional device running the Remote Desktop Client in Windows, an app that supports RDP and RemoteFX, a thin or zero client that supports RDP (such as Windows Thin PC), or a RemoteFX-enabled device. For institution-owned devices, the

client device may or may not be a member of an AD DS domain. For personally owned devices, the client will not be a member of an AD DS domain.

- **Domain controller and other network infrastructure services** These services include AD DS, DHCP, DNS, and routing.

The high-level steps for deploying session-based desktop deployment are:

1. Deploy Windows Server 2012 R2 on the Remote Desktop Connection Broker server.
2. Deploy Windows Server 2012 R2 on the Remote Desktop Web Access server.
3. Deploy Windows Server 2012 R2 on the Remote Desktop Session Host server.
4. Ensure that all servers are members of the same AD DS domain.
5. On the Remote Desktop Connection Broker server, use Server Manager to add all of the servers to the server pool.
6. On the Remote Desktop Connection Broker server, use Server Manager to install the following role services for the Remote Desktop Services Installation server role:
   - Remote Desktop Connection Broker
   - Remote Desktop Web Access
   - Remote Desktop Session Host
7. Create a network shared folder in which to store the User Profile Disk (typically on the Remote Desktop Connection Broker server).
8. Create the session collection.
9. Verify that the session collection works correctly.

NOTE

Although you are running Server Manager on the Remote Desktop Connection Broker server, Server Manager prompts you for the names of the servers running the other Remote Desktop Services role services.

Additional resources:

- "Test Lab Guide: Remote Desktop Services Session Virtualization Standard Deployment" at http://technet.microsoft.com/en-us/library/hh831610.aspx
- "Test Lab Guide: Remote Desktop Services Session Virtualization Quick Start" at http://technet.microsoft.com/en-us/library/hh831754.aspx
- "Windows 8/Windows Server 2012: Remote Desktop Management Server" at http://blogs.technet.com/b/askperf/archive/2012/10/30/windows-8-windows-server-2012-remote-desktop-management-server.aspx
- "Virtualization: VDI made easy" at http://technet.microsoft.com/en-us/magazine/jj992579.aspx

Windows MultiPoint Server 2012

Windows MultiPoint Server 2012 enables multiple users to share one computer and provides a low-cost alternative to traditional computing scenarios in which each user has their own computer. Windows MultiPoint Server 2012 also provides an easy management solution for Windows MultiPoint Server 2012 system administration called *MultiPoint Manager* and an easy management solution for day-to-day administration called *MultiPoint Dashboard*.

Windows MultiPoint Server 2012 is available in Standard and Premium versions. Use the information in Table 3 to select the appropriate versions for your educational institution.

	Standard	Premium
Number of simultaneously connected stations	10	20
Can be joined to a domain?	No	Yes
Virtualization support as a host or guest operating system?	No	Yes

TABLE 3 Comparison of Windows MultiPoint Server 2012 Standard and Premium

Windows MultiPoint Server 2012 can only be deploy on a single computer. You can scale Windows MultiPoint Server 2012 only through the addition of Windows MultiPoint Server 2012 instances: It has no inherent high availability. However, you could run virtualized instances of Windows MultiPoint Server 2012 on highly available HyperV clusters.

The user endpoints that connect to the computer running Windows MultiPoint Server 2012 are called *stations*. Windows MultiPoint Server 2012 supports the following station types:

- **Direct video–connected stations** The computer running Windows MultiPoint Server 2012 can contain multiple video cards, each of which can have one or more video ports. This allows you to plug monitors for multiple stations directly into

the computer. Keyboards and mouse devices are connected through USB hubs associated with each monitor. Use a combination of all of these technologies to create a direct video–connected station.

- **USB zero client–connected stations** USB zero client–connected stations use the USB zero client as a station USB hub (also referred to as a *multifunction USB hub with video*). These stations connect to the Windows MultiPoint Server 2012 instance through a USB cable and typically support a video monitor, a mouse, a keyboard (PS/2 or USB), audio, and additional USB devices.

- **USB-over-Ethernet zero client–connected stations** USB-over-Ethernet zero clients are a variation of USB zero client–connected stations that send USB over LAN to the Windows MultiPoint Server 2012 instance. These clients function similarly to USB zero client–connected stations but are not limited by USB cable length maximums. USB-over-Ethernet zero clients are not traditional thin clients, and they appear as virtual USB devices on the Windows MultiPoint Server 2012 system.

- **RDP-over-LAN–connected stations** These stations include traditional thin clients or other devices running a full operating system that support RDP.

> **NOTE**
>
> Personally owned devices can only use RDP-over-LAN connected station types. Institution-owned devices can use any stationed type as applicable.

Additional resources:

- "Deploying Windows MultiPoint Server 2012" at http://technet.microsoft.com/en-us/library/jj916399.aspx

- "Planning a Windows MultiPoint Server 2012 Deployment" at http://technet.microsoft.com/en-us/library/jj916408.aspx

- "Differences between Product Versions: Standard versus Premium" at http://technet.microsoft.com/en-us/library/jj916405.aspx

- "MultiPoint Server Stations" at http://technet.microsoft.com/en-us/library/jj916411.aspx

Preparing the infrastructure for VDI

Before you deploy VDI in your institution, you must prepare the appropriate infrastructure. Table 4 lists the VDI infrastructure components and provides an overview of the preparation that may be necessary for each component. In some instances, no infrastructure remediation may be necessary.

TABLE 4 VDI Infrastructure Components and Preparation Steps

Component	Preparation steps
Network	The following factors affect whether the network infrastructure is able to support the VDI session traffic between VDI clients and the VDI servers: • Placement of the VDI servers can directly affect the available network requirements (as described in the section "Placing VDI servers" on page 17). • The larger the number of VDI clients simultaneously accessing the VDI infrastructure, the greater the network bandwidth that is required. • Type of client traffic—for example, graphically intensive VDI sessions require more network bandwidth than less graphically intensive sessions.
Storage	The primary consideration for planning storage are: • Pooled collections require sufficient storage for the transitional hard disks and the User Profile Disk for each VDI session. • Personal collections require sufficient storage for each VHD for each VDI session.

Component	Preparation steps
Client devices	Each user who accesses the VDI infrastructure requires a device that supports the appropriate clients. Users who will access: • VM- or session-based desktop deployment scenarios require devices that support RDP or RemoteFX • Windows MultiPoint Server 2012 require one of the supported Windows MultiPoint Server 2012 stations Some of these devices can be software-based clients (such as the Remote Desktop Client in Windows operating systems or apps for other operating systems) or hardware-based clients (such as RemoteFX devices, thin clients, or zero clients). For more information about the client devices that can be used in these VDI solutions, see the following sections in this guide: • "Windows MultiPoint Server 2012" on page 13 • "Connecting users to VDI sessions" on page 25

You can approximate the actual requirements for each component in Table 4 on page 15 by verifying the resource requirements in a lab environment. For example, you could approximate the network bandwidth requirement by configuring a test environment and measuring the network traffic a limited number of VDI sessions performing typical tasks generate. Then, you could extrapolate the actual requirement by multiplying the measured network traffic in the lab by the number of simultaneous VDI sessions.

Placing VDI servers

Table 5 compares the centralized and decentralized placement strategies for VDI servers. You can use any combination of these strategies to place your VDI servers.

TABLE 5 Comparison of Centralized and Decentralized Placement of VDI Servers

	Centralized	Decentralized
Scenario	Centralized IT data center.	Placement in classrooms, labs, or near VDI client locations.
Management	Requires less effort because there are fewer servers to manage.	Requires more effort because there are more servers to manage.
High availability	Higher concentration of user VDI sessions makes implementing high-availability technologies (such as load balancing or Windows failover clustering) more cost-effective.	Lower concentration of user VDI sessions makes implementing high-availability technologies less effective.
Scaling	Higher concentration of user VDI sessions can offset the costs required for scaling. You can add servers or system resources to increase scaling capability.	Lower concentration of user VDI sessions may not be able to offset costs required for scaling. For example, adding a server to a classroom with an existing server would effectively double the costs.
Efficient use of system resources	User VDI sessions can be distributed (load balanced) across multiple servers, which results in the servers being more equally utilized.	Some VDI servers may be underutilized, while others are overutilized, with no way to share resources among servers.
Network traffic	Higher available network bandwidth is required on the institution's network backbone to support VDI sessions.	Traffic is more localized and has less impact on the institution's network backbone.

Building virtual desktop templates

VDI VM-based desktop deployment scenarios require a *virtual desktop template*. A virtual desktop template has all the normal settings of a VM (such as memory, networking, and VHD settings). When a new user connects to the VDI, the VDI creates a virtual desktop VM based on the virtual desktop template.

To create your virtual desktop template, use HyperV Manager with the recommendations listed in Table 6.

TABLE 6 Virtual Desktop Template Configuration Setting Recommendations

Setting	Description
Memory	Depending on the apps your users will be running, you may need to increase this value. Measure the memory users require by determining the memory consumed on a physical device while running the apps. You can configure the virtual desktop template to use static or dynamic memory. Microsoft recommends that you configure the virtual desktop template to use at least 1,024 MB.
Network	Configure the virtual network adapter to connect to: • A virtual switch in HyperV on the Remote Desktop Virtualization Host. The HyperV virtual switch must connect to your institution's intranet so that the VDI sessions can connect to resources on your intranet and the Internet. • The domain specified during the configuration process. This is required because the instances of the VM template are automatically joined to the domain when they are created.
VHDs	Only one VHD is supported. The VHD: • Must contain a Windows 8.1 image that you have configured to a generalized state by using the Windows System Preparation Tool (Sysprep) • Can be configured as a differencing disk • Can contain more than one partition but only one Windows operating system image
Snapshots	The virtual desktop template can have one or more snapshots but the current (Now) state of the virtual desktop template. This allows you to manage the template more efficiently. You can take snapshot of the template just prior to running Sysprep so that it is easy to restore the template to a beginning state, change the configuration, take another snapshot, and then run Sysprep again on the updated version of the template.

Remote Desktop Services exports the virtual desktop template during the virtual desktop collection creation process. The export process creates a copy of the virtual desktop template, including all of the configuration settings made in Table 6 on page 18. This allows you manage the virtual desktop template while users are connected to their VDI sessions.

NOTE

Two or more virtual desktop collections can share the same virtual desktop template.

Additional resources:

- "Single Image Management for Virtual Desktop Collections in Windows Server 2012" at http://blogs.msdn.com/b/rds/archive/2012/10/29/single-image-management-for-virtual-desktop-collections-in-windows-server-2012.aspx
- "Test Lab Guide: Managed Pooled Virtual Desktop Collections" at http://technet.microsoft.com/en-us/library/hh831663.aspx
- "Test Lab Guide: Unmanaged Pooled Virtual Desktop Collections" at http://technet.microsoft.com/en-us/library/hh831618.aspx
- "Setting up a new Remote Desktop Services deployment using Windows PowerShell" at http://blogs.msdn.com/b/rds/archive/2012/07/18/setting-up-a-new-remote-desktop-services-deployment-using-windows-powershell.aspx

Client licensing for VDI

Microsoft licenses client access to VDI sessions through Windows Virtual Desktop Access (VDA). Windows VDA is a device-based subscription that licenses Windows 8.1 for virtual desktops by access device:

- **Devices covered by Microsoft Software Assurance** Virtual desktop access rights are a benefit of Software Assurance. Devices covered under Software Assurance have access to a VDI desktop at no additional charge.

  Table 7 list the Windows 8.1 VDI licensing options based on the operating system running on the device used as a VDI client.

- **Devices not covered by Software Assurance** These devices (such as thin clients) must purchase a Windows VDA license for each device to access a VDI desktop, regardless of the operating system running on the device. This includes personally owned devices.

INFO

The licensing listed in this table applies only to institution-owned devices. All personally owned devices require a Windows VDA subscription.

TABLE 7 Windows VDA Licensing Options

Client OS	VDA license options
Windows 8.1 Pro	Windows VDA license and free upgrade to Windows 8.1 Enterprise included
Windows RT	Windows VDA license included when the device is associated with a primary device covered by Software Assurance (for example, the primary device is running Windows 8.1 Enterprise and is covered by Software Assurance)
Windows 7	Windows VDA license and free upgrade to Windows 8.1 Enterprise
Windows Vista	Windows VDA license included; licensed to use Windows Thin PC as an RDP and RemoteFX client on these devices
Windows XP	Windows VDA license included; licensed to use Windows Thin PC as an RDP and RemoteFX client on these devices
Android	Must purchase a Windows VDA license for each device

Windows 8

Client OS	VDA license options
iOS	Must purchase a Windows VDA license for each device

Additional resources:

- "Microsoft VDI and Windows VDA Frequently Asked Questions" at http://download.microsoft.com/download/1/1/4/114A45DD-A1F7-4910-81FD-6CAF401077D0/Microsoft%20VDI%20and%20VDA%20FAQ%20v3%200.pdf
- "Volume Licensing—Microsoft Software Assurance " at http://www.microsoft.com/licensing/software-assurance/default.aspx
- "Microsoft Licensing for the Consumerization of IT" at http://www.microsoft.com/licensing/about-licensing/briefs/consumerization-it.aspx
- "Microsoft Licensing for the Consumerization of IT—Academic Licensing Scenarios" at http://www.microsoft.com/licensing/about-licensing/briefs/consumerization-it-academic.aspx
- "Licensing Windows desktop operating system for use with virtual machines" at http://download.microsoft.com/download/3/D/4/3D42BDC2-6725-4B29-B75A-A5B04179958B/Licensing_Windows_Desktop_OS_for_Virtual_Machines.pdf

Using Volume Activation

You must provide Windows 8.1 license activation for the VMs used in VDI scenarios. The following is a list of the Microsoft Volume Activation technologies available for Windows 8.1 and a brief description of each:

- **Active Directory-Based Activation (ADBA)** ADBA is a role service that allows you to use AD DS to store activation objects, which can further simplify the task of maintaining Volume Activation services for a network. With ADBA, no additional host server is needed, and activation requests are processed during computer startup. ADBA works only for domain-joined devices running Windows 8.1.
- **Key Management Service (KMS)** The KMS role service allows organizations to activate systems within their network from a server on which a KMS host has been installed. With KMS, you can complete activations on your local network, eliminating the need for individual computers to connect to Microsoft for product activation. KMS does not require a dedicated system, and it can be cohosted on a system that provides other services. By default, volume editions of Windows 8.1 connect to a system that hosts the KMS service to request activation. No action is required from the user.

Table 8 lists the Volume Activation technologies and the information necessary for selecting the appropriate technologies for your institution. You can use any combination of these technologies to design a complete Volume Activation solution.

INFO

For information about licensing the clients used to access your VDI, see the section "Client licensing for VDI" on page 20.

NOTE

Although you can perform Volume Activation by using Multiple Activation Keys (MAKs), Microsoft does not recommend MAKs for VDI because they cannot be dynamically applied to VMs based on VDI demands. Use ADBA or KMS, instead.

TABLE 8 Volume Activation Technology Selection

	ADBA	KMS
Domain joined	Yes	Yes
Devices must connect to the network at least once every 180 days	Yes	Yes

Windows 8

	ADBA	KMS
Supports Volume Activation of Microsoft Office	Yes (Microsoft Office 2013 only, not Microsoft Office 365 or previous versions of Office)	Yes
Requires Volume Activation services in Windows Server 2012 R2	Yes	No
Microsoft Volume Licensing information is stored in AD DS	Yes	No
Infrastructure	AD DS	AD DS KMS server

ADBA and KMS are both role services in the Volume Activation Services server role in Windows Server 2012 R2. KMS is also available in prior versions of Windows Server. You can use Server Manager or Windows PowerShell cmdlets to install and configure these role services.

You can centrally manage Windows, Office, and other Microsoft products' volume and retail activation processes by using the Volume Activation Management Tool (VAMT), which is included in the Windows Assessment and Deployment Kit.

NOTE

You can use the same Volume Activation infrastructure to manage VDI activation and activation for your other Windows 8.1, Windows 7, Windows Server 2012 R2, and Windows Server 2008 R2 operating systems.

Additional resources:

- "Volume Activation Overview" at http://technet.microsoft.com/library/hh831612.aspx
- "Installing Volume Activation Services Role in Windows Server 2012 to setup a KMS Host" at http://blogs.technet.com/b/askcore/archive/2013/03/14/installing-volume-activation-services-role-in-windows-server-2012-to-setup-a-kms-host.aspx
- "Test Lab Guide: Demonstrate Volume Activation Services" at http://technet.microsoft.com/library/hh831794.aspx
- "Volume Activation" in *Windows 8 deployment planning: A guide for education* at http://www.microsoft.com/download/details.aspx?id=39682
- "Volume Activation Management Tool (VAMT) Overview" at http://technet.microsoft.com/library/hh824953.aspx
- "Volume Licensing" at http://www.microsoft.com/licensing/about-licensing/windows8.aspx
- "Introduction to VAMT" at http://technet.microsoft.com/library/hh825141.aspx
- *Volume Licensing Guide for Windows 8.1 and Windows RT 8.1* at http://download.microsoft.com/download/9/4/3/9439A928-A0D1-44C2-A099-26A59AE0543B/Windows_8-1_Licensing_Guide.pdf
- "Microsoft Licensing for the Consumerization of IT—Academic Licensing Scenarios" at http://www.microsoft.com/licensing/about-licensing/briefs/consumerization-it-academic.aspx
- "Volume activation methods in Office 2013" at http://technet.microsoft.com/library/jj219430.aspx

Connecting users to VDI sessions

Users need access to their VDI sessions through their institution-owned devices. Connections for VDI sessions go:

- **Directly to Windows MultiPoint Server 2012 for all Windows MultiPoint Server 2012 clients** Windows Multipoint Server 2012 supports four types of connections:
  - Direct video–connected stations
  - USB zero client–connected stations
  - USB-over-Ethernet zero client–connected stations
  - RDP-enabled devices

  Of these connections, only RDP-enabled devices are able to connect over remote access connections (such as a virtual private network [VPN] or Microsoft DirectAccess). The other connection types will not function properly over WAN-speed connections.

  Institution-owned devices can use any combination of connection types as appropriate. Personally owned devices can only act as RDP-enabled devices.

  For more information about how to select the right Windows MultiPoint Server 2012 client, see the topic "MultiPoint Server Stations" at http://technet.microsoft.com/en-us/library/jj916411.aspx.

- **Through Remote Desktop Session Broker for all session-based and VM-based VDI sessions** The Remote Desktop Session Broker supports the following RDP clients:
  - **Remote Desktop Client** This RDP client is included in full Windows operating systems (such as Windows 8.1, Windows 7, or Windows Vista). Select this client when the client device runs Windows 8.1, Windows 8, Windows 7, or Windows Vista.

NOTE

RemoteFX is only supported on Windows Vista and later operating systems. The Windows XP operating system supports only a standard RDP client connection and does not support the enhanced features in RemoteFX.

- **Remote Desktop Web Access** This client allows users to establish VDI connections through a web browser (such as Internet Explorer). No client software need be installed on the target device. Select this RDP client when you cannot install the Remote Desktop Client on the client device or the client device is running an operating system other than Windows 8 .1, Windows 8, Windows 7, or Windows Vista.

- **Window Thin PC** This operating system includes the Remote Desktop Client and can be installed on older devices that are unable to support Windows 8 .1, Windows 8, Windows 7, or Windows Vista. For example, you could install Windows Thin PC on a device that has sufficient resources to support Windows XP only. Windows Thin PC is provided as a part of Software Assurance. Select this method when the client device has insufficient system resources to run Windows 8.1, Windows 8, Windows 7, or Windows Vista.

- **Thin client devices** These types of devices are provided by Microsoft partners and have the RDP imbedded in their firmware. These devices typically have little or no capability to perform any local processing but do support USB devices. Select these types of devices when users need access to VDI sessions only and do not need to perform any local processing.

- **RemoteFX devices** These devices are provided by Microsoft partners and run a superset of the RDP that also includes support for RemoteFX. Select these devices when you need to support enhanced multimedia.

- **Partner products** Many Microsoft partners and software vendors create RDP clients for other client devices (such as iOS or Android devices). These products enable these devices to connect to VDI by using RDP or RemoteFX. Select this method when you need to support specific types of client devices.

All clients that support RPD and RemoteFX can function over remote access connections (such as a VPN or DirectAccess), but RemoteFX connections typically require higher available bandwidth than a standard RDP connection.

Additional resources:

- "Remote Desktop Protocol" at http://msdn.microsoft.com/en-us/library/windows/desktop/aa383015(v=vs.85).aspx

Storing user and application settings

When users connect to VDI, they need to have the same user experience they would if they were using a physical device. Users also require access to Windows Store apps and desktop applications that they use for administration or curriculum.

One challenge is that in many instances, users have a physical device running Windows in addition to their VDI session. This means they need their user experience and apps to follow them between their physical devices running Windows and their VDI sessions.

After a user ends their VDI session, by default, user and application settings in their VDI session is:

- **Saved for personal collections in VM-based desktop deployment** Although user and application settings are saved for this type of VDI session, they are saved only on the VHDs associated with the VDI session. This can create problems if the user also uses a physical device or a separate VDI infrastructure within the educational institution (for example, a student accesses one VDI infrastructure for a physics class and another, separate VDI infrastructure for a computer graphics class).
- **Saved for pooled collections in VM-based desktop deployment with a User Profile Disk** This type of VDI session has the same problems as personal collection sessions. User and application settings are saved on the User Profile Disk, which is unique to a specific VDI infrastructure and will not be available to other VDI infrastructures or physical devices.
- **Saved for session-based deployment with a User Profile Disk** This type of VDI session has the same problems as personal and pooled collection sessions. User and application settings are saved on the User Profile Disk, which is unique to a specific VDI infrastructure and will not be available to other VDI infrastructures or physical devices.

NOTE

User and application settings cannot follow physical devices that are not domain joined, that run a Windows operating system prior to Windows 7, or that run another operating system (such as iOS or Android).

- **Lost for all other types of VDI sessions** These types of VDI sessions include session-based VDI without a User Profile Disk, personal collections in VM-based desktop deployment without a User Profile Disk, and Windows MultiPoint Server 2012 sessions. When the user ends the VDI session, all the changes they made to their user profile and applications are discarded.

You can use any combination of the following technologies to help ensure that user experience and apps follow users between their VDI sessions and physical devices (if the devices are domain joined and the user logs on by using their institution-issued credentials):

- **Windows Folder Redirection** The Folder Redirection feature in Windows 8.1 redirects the path of a known folder (such as the Documents, Pictures, or Video folder in a user profile) to a new location manually or by using Group Policy. The new location can be a folder on the local device or a directory on a file share. Users interact with files in the redirected folder as if they still existed on the local drive.

- **Windows Roaming User Profiles** The Roaming User Profiles feature in Windows 8.1 redirects user profiles to a file share so that users receive the same operating system and application settings on multiple computers. When a user logs on to a computer by using an account that is set up with a file share as the profile path, the user's profile is downloaded to the local computer and merged with the local profile (if present). When the user logs out of the computer, the local copy of their profile, including any changes, is merged with the server copy of the profile.

- **UE-V** UE-V is an enterprise-scale user state virtualization solution that keeps users' experience with them. UE-V provides users the choice of changing their device and keeping their experience so that they do not have to reconfigure applications each time they log on to different Windows 8.1 VDI sessions. UE-V integrates with the Folder Redirection feature in Windows 8.1 to help make user folders accessible from multiple physical or virtual devices. UE-V supports desktop applications that are deployed using different methods (such as locally installed apps, App-V sequenced applications, or Remote Desktop applications).

- **App-V** App-V virtualizes desktop applications so that they become centrally managed services deployed to a virtualized desktop application environment on devices without using traditional installation methods (known as *application sequencing*). The sequenced desktop applications run in their own self-contained virtual environment and are isolated from each other, which eliminates application conflicts but allows desktop applications to interact with the VM.

Remember that user experience and apps follow users for VDI sessions and not to their institution-owned or personally owned devices (unless an institution-owned device is domain joined and the user logs on by using their institution-issued credentials).

Additional resources:

- "Device roaming" in *Windows 8.1 deployment planning: A guide for education* at http://www.microsoft.com/download/details.aspx?id=39682

Running Windows Store and sideloaded apps

One benefit of running Windows 8.1 in VDI is the ability to run Windows Store apps. Table 9 lists the support for Windows Store and sideloaded apps in VDI.

TABLE 9 Support for Windows Store and Sideloaded Apps in VDI

Scenario	Support
Personal VM-based desktop deployment	Windows Store and sideloaded apps are installed and run as they would be on a physical device.

Pooled VM-based desktop deployment	• Sideloaded apps require that user state be persisted by using any combination of the following methods:
	  • User Profile Disk
	  • Folder Redirection
	  • UE-V
	• Windows Store apps are unsupported.

Session-based desktop deployment	• Sideloaded apps require that user state be persisted by using any combination of the following methods:
	  • User Profile Disk
	  • Folder Redirection
	  • UE-V
	• Windows Store apps are unsupported.

RemoteApp	Windows Store and sideloaded apps are unsupported.

Additional resources:

- *Windows Store apps: A deployment guide for education* at http://www.microsoft.com/download/details.aspx?id=39685

Managing VDI

Table 10 lists the technologies available for managing your VDI. You can select any combination of these technologies to design a complete VDI management solution. Each technology is discussed in a subsequent section.

TABLE 10 VDI Management Technology Selection

	Group Policy	Windows PowerShell	System Center 2012 R2 Configuration Manager	Windows Intune
Control Windows Store access	Yes	No	Yes	Yes
Control installation of apps	Yes (with AppLocker, which requires Windows 8.1 Enterprise)	No	Yes (in conjunction with Group Policy and AppLocker, which requires Windows 8.1 Enterprise)	No
Operating system setting management	Yes	Yes	Yes	Yes
User setting management	Yes	Yes	Yes	Yes
App setting management	Yes (if registry based)	App specific	Yes, but scripting may be required	Yes, but scripting may be required
Centralized administration model	Yes	No	Yes	Yes
On or off premises	On premises	On premises	On premises	Off premises
On-premises infrastructure	AD DS	None	Managed networks System Center 2012 R2 Configuration Manager	None

	Group Policy	Windows PowerShell	System Center 2012 R2 Configuration Manager	Windows Intune
VDI sessions must be domain joined	Yes	No	No, but challenges exist for native support; Windows Intune integration is recommended for nondomain-joined VDI sessions	No
Supports self-service model for software and updates	No	No	Yes	Yes
Supports push model for software and updates	Yes	Yes	Yes	Yes
Can be used to create enterprise app store	No	No	Yes	Yes
User interaction	IT pro does back-end configuration User performs no actions	IT pro performs all tasks	IT pro does back-end configuration User has no interaction for push model and limited interaction for self-service model	IT pro does back-end configuration User has no interaction for push model and limited interaction for self-service model
Provided with Windows 8.1	No	Yes	No	No
Provides unified solution for the entire software life cycle, including installation, updates, supersedence, and removal	No	No	Yes	Yes
Can be used for operating system deployment	No	No	Yes	No

	Group Policy	Windows PowerShell	System Center 2012 R2 Configuration Manager	Windows Intune
Requires additional cost	Yes (if AD DS is not already installed)	No	Yes (if no System Center Configuration Manager infrastructure is installed)	Yes (subscription model)
Manage institution-owned devices	Yes (if domain joined)	Yes	Yes	Yes
Manage personally owned devices	No (as are typically not domain joined)	Yes	Yes (through Microsoft Exchange ActiveSync connector or Windows Intune integration)	Yes

You can manage Windows Store apps and desktop applications in VDI by using any technology used to manage Windows Store apps and desktop applications on physical devices. For more information about Windows Store app and desktop application management, see *Windows Store apps: A deployment guide for education* at http://www.microsoft.com/download/details.aspx?id=39685 and *Windows 8.1 deployment planning: A guide for education* at http://www.microsoft.com/download/details.aspx?id=39682.

Group Policy

You can use Group Policy to manage user, Windows operating system, and application settings for the VDI infrastructure and VDI sessions. Ultimately, you can use Group Policy to manage any configuration settings stored in the Windows registry. Microsoft provides built-in Group Policy templates for most common configuration settings. In addition, you can create custom Group Policy templates that allow you to manage configuration settings that the built-in templates do not provide. You can also use Group Policy to control Windows Store access and the installation and running of apps on devices (when

NOTE

Personally owned devices are typically not domain joined and as such cannot be managed through Group Policy. Institution-owned devices that are domain joined can be managed by using Group Policy.

used in conjunction with AppLocker). You can also use Group Policy to manage Remote Desktop Services, Remote Desktop Client, and RemoteFX configuration.

Additional resources:

- "Group Policy" at http://technet.microsoft.com/windowsserver/bb310732.aspx
- "Managing Client Access to the Windows Store" at http://technet.microsoft.com/en-us/library/hh832040.aspx

Windows PowerShell

You can perform many common Windows 8.1 administrative tasks by using Windows PowerShell cmdlets, including Windows Store app management and operating system configuration. You can also use Windows PowerShell to manage the Windows Server 2012 R2 server roles and role services. You can use Windows PowerShell interactively or to create scripts that can be run to perform more complex tasks for the VDI infrastructure and VDI sessions.

Additional resources:

- "Windows PowerShell" at http://technet.microsoft.com/library/bb978526.aspx

System Center 2012 R2 Configuration Manager

System Center 2012 R2 Configuration Manager automates the ongoing management of the VMs, the Windows Server 2012 R2 server roles and role service, client devices, and the other infrastructure services (such as AD DS or DHCP). You can use System Center 2012 R2 Configuration Manager to automate the following management tasks for the VDI infrastructure and sessions:

- Deploy Windows Store app and desktop applications
- Deploy software updates and hotfixes
- Help ensure compliance with established configuration baselines.
- Provide virus and malware protection
- Inventory hardware and software assets
- Provide remote helpdesk support for users

- Provide comprehensive reporting on the current status of all hardware assets, software assets, software deployment status, compliance status, software update status, and other reports

System Center 2012 R2 Configuration Manager provides a unified console for managing VDI and can optionally integrate with Windows Intune to help you manage devices that are not connected to the educational institution's intranet. Institution-owned devices can be managed by using System Center 2012 R2 Configuration Manager. Personally owned devices are typically not domain joined and cannot be managed by using System Center 2012 R2 Configuration Manager only, but personally owned devices can be managed by using System Center 2012 R2 Configuration Manager with the Exchange ActiveSync Connector or Windows Intune integration.

Additional resources:

- "System Center 2012 R2 Configuration Manager" at http://www.microsoft.com/en-us/server-cloud/system-center/configuration-manager-2012.aspx

Windows Intune

Windows Intune is an off-premises, cloud-based management solution that provides device management, software installation, and software update management. Windows Intune can integrate with System Center 2012 R2 Configuration Manager to provide a unified management solution for the VDI infrastructure and VDI. You can use Windows Intune to manage institution-owned or personally owned devices.

Additional resources:

- "Windows Intune" at http://www.microsoft.com/en-us/windows/windowsintune/pc-management.aspx

Windows 8