Enabling the modern workstyle

Access virtually anywhere, from any device

If you are an office worker in today's accelerated business world, you need to be able to access your applications and data from any device – your personal computer, mobile computer, tablet computer, or other mobile device. And if you are an IT person involved in supporting such an environment, you want to be able to implement such capabilities easily and without hassles or additional costs.

Improvements in several Windows Server 2012 features now make it simple to deploy, configure, and maintain an IT infrastructure that can meet the needs of the modern workstyle. Remote access is now an integrated solution that you can use to deploy DirectAccess and traditional virtual private network (VPN) solutions quickly. Enhancements to Remote Desktop Services now make it easier than ever to deploy both session-based desktops and virtual desktops and to manage your RemoteApp programs centrally. User-Device Affinity now makes it possible for you to map roaming users to specific computers and devices. BranchCache has been enhanced to improve performance and make better use of expensive wide area network (WAN) bandwidth. And Branch Office Direct Printing enables branch office users to get their print jobs done faster while putting less strain on the WAN.

Unified remote access

Today's enterprises face an increasingly porous perimeter for their IT infrastructures. With a larger portion of their workforce being mobile and needing access to mobile data, enterprises are presented with new security challenges to address. Cloud computing promises to help resolve some of these issues, but the reality is that most organizations will deploy a hybrid cloud model that combines traditional datacenter computing with hosted cloud services.

Providing remote access to corporate network resources in a secure, efficient, and cost-effective way is essential for today's businesses. The previous version of Windows Server supported a number of different options for implementing remote access, including:

- Point-to-Point Tunneling Protocol (PPTP) VPN connections.
- Layer 2 Transport Protocol over IPsec (L2TP/IPsec) VPN connections.

- Secure Sockets Layer (SSL) encrypted Hypertext Transfer Protocol (HTTP) VPN.
- Connections using the Secure Socket Tunneling Protocol (SSTP).
- VPN Reconnect, which uses Internet Protocol Security (IPsec) Tunnel Mode with Internet Key Exchange version 2 (IKEv2).
- DirectAccess, which uses a combination of Public Key Infrastructure (PKI), IPsec, SSL, and Internet Protocol version 6 (IPv6).

Implementing remote access could be complex in the previous version of Windows Server because different tools were often needed to deploy and manage these different solutions. For example, the Remote Access and Routing (RRAS) component was used for implementing VPN solutions, whereas DirectAccess was configured separately using other tools.

Beginning with Windows Server 2012, however, the process of deploying a remote access solution has been greatly simplified by integrating both DirectAccess and VPN functionality into a single Remote Access server role. In addition, functionality for managing remote access solutions based on both DirectAccess and VPN has now been unified and integrated into the new Server Manager. The result is that Windows Server 2012 now provides you with an integrated remote access solution that is easy to deploy and manage. Note that some advanced RRAS features, such as routing, are configured using the legacy Routing and Remote Management console.

Simplified DirectAccess

If remote client devices can be always connected, users can work more productively. Devices that are always connected are also more easily managed, which helps improve compliance and reduce support costs. DirectAccess, first introduced in Windows Server 2008 R2 and supported by client devices running Windows 7, helps address these needs by giving users the experience of being seamlessly connected to their corporate network whenever they have Internet access. DirectAccess does this by allowing users to access corpnet resources such as shared folders, websites, and applications remotely, in a secure manner, without the need of first establishing a VPN connection. DirectAccess does this by automatically establishing bidirectional connectivity between the user's device and the corporate network every time the user's device connects to the Internet.

DirectAccess alleviates the frustration that remote users often experience when using traditional VPNs. For example, connecting to a VPN usually takes several steps, during which the user needs to wait for authentication to occur.

And if the corporate network has Network Access Protection (NAP) implemented for checking the health of computers before allowing them to connect to the corporate network, establishing a VPN connection could sometimes take several minutes or longer depending on the remediation require, or the length of time of the user's last established the VPN connection. VPN connections can also be problematic for environments that filter out VPN traffic, and Internet performance can be slow for the user if both intranet and Internet traffic route through the VPN connection. Finally, any time users lose their Internet connection, they have to reestablish the connection from scratch.

DirectAccess solves all these problems. For example, unlike a traditional VPN connection, DirectAccess connectivity is established even before users log on so that they never have to think about connecting resources on the corporate network or waiting for a health check to complete. DirectAccess can also separate intranet traffic from Internet traffic to reduce unnecessary traffic on the corporate network. Because communications to the Internet do not have to travel to the corporate network and back to the Internet, as they typically do when using a traditional VPN connection, DirectAccess does not slow down Internet access for users.

Finally, DirectAccess allows administrators to manage remote computers outside the office even when the computers are not connected via a VPN. This also means that remote computers are always fully managed by Group Policy, which helps ensure that they are secure at all times.

In Windows Server 2008 R2, implementing DirectAccess was a fairly complex task and required performing a large number of steps, including some command-line tasks that needed to be performed both on the server and on the clients. With Windows Server 2012, however, deploying and configuring DirectAccess servers and clients is greatly simplified. In addition, DirectAccess and traditional VPN remote access can coexist on the same server, making it possible to deploy hybrid remote access solutions that meet any business need. Finally, the Remote Access role can be installed and configured on a Server Core installation.

DirectAccess enhancements

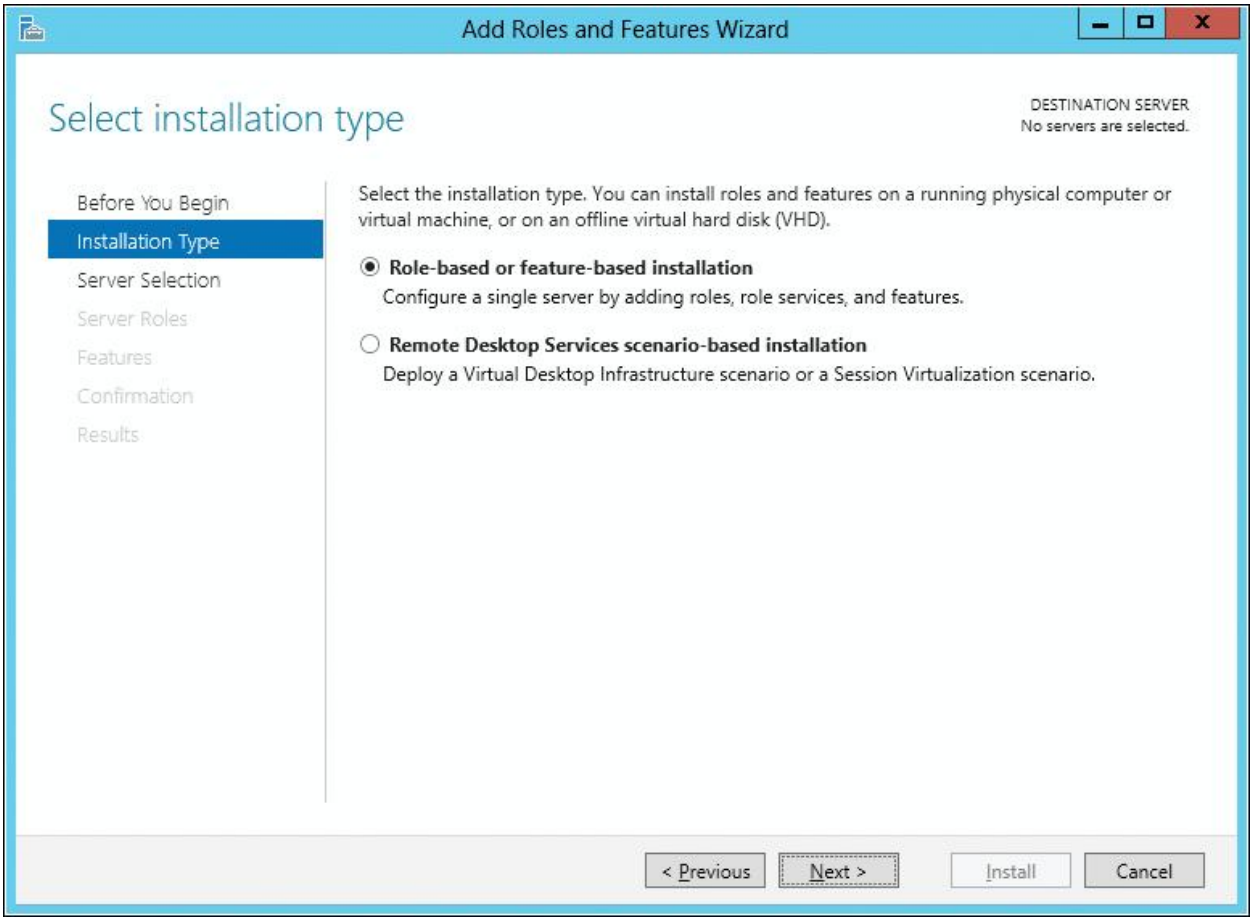
Besides simplified deployment and unified management, DirectAccess has been enhanced in other ways in Windows Server 2012. For example:

- You can implement DirectAccess on a server that has only one network adapter. If you do this, IP-HTTPS will be used for client connections because it enables DirectAccess clients to connect to internal IPv4 resources when other IPv4 transition technologies such as Teredo cannot be used. IP-HTTPS is implemented in Windows Server 2012 using NULL encryption, which removes redundant SSL encryption during client communications to improve performance.
- You can access a DirectAccess server running behind an edge device such as a firewall or network address translation (NAT) router, which eliminates the need to have dedicated public IPv4 addresses for DirectAccess. Note that deploying DirectAccess in an edge configuration still requires two network adapters, one connected directly to the Internet and the other to your internal network. Note also that the NAT device must be configured to allow traffic to and from the Remote Access server.
- DirectAccess clients and servers no longer need to belong to the same domain but can belong to any domains that trust each other.
- In Windows Server 2008 R2, clients had to be connected to the corporate network in order to join a domain or receive domain settings. With Windows Server 2012 however, clients can join a domain and receive domain settings remotely from the Internet.
- In Windows Server 2008 R2, DirectAccess always required establishing two IPsec connections between the client and the server; in Windows Server 2012 only one IPsec connection is required.
- In Windows Server 2008 R2, DirectAccess supported both IPsec authentication and two-factor authentication by using smart cards; Windows Server 2012 adds support for two-factor authentication using a one-time password (OTP) in order to provide interoperability with OTP solutions from third-party vendors. In addition, DirectAccess can now use the Trusted Platform Module (TPM)–based virtual smart card capabilities available in Windows Server 2012, whereby the TPM of clients functions as a virtual smart card for two-factor authentication. This new approach eliminates the overhead and costs incurred by smart card deployment.

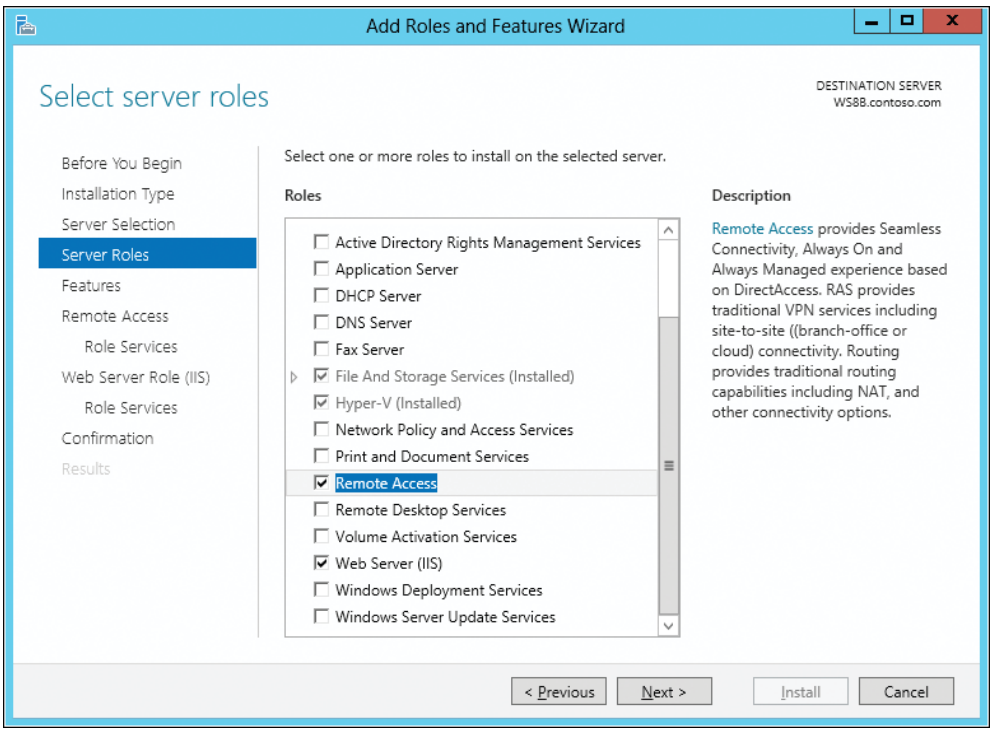
Deploying remote access

To see unified remote access at work, let's walk through the initial steps of deploying a DirectAccess solution. Although we've used the UI for performing the steps described below, you can also use Windows PowerShell. You can also deploy the Remote Access role on a Windows Server Core installation of Windows Server 2012.

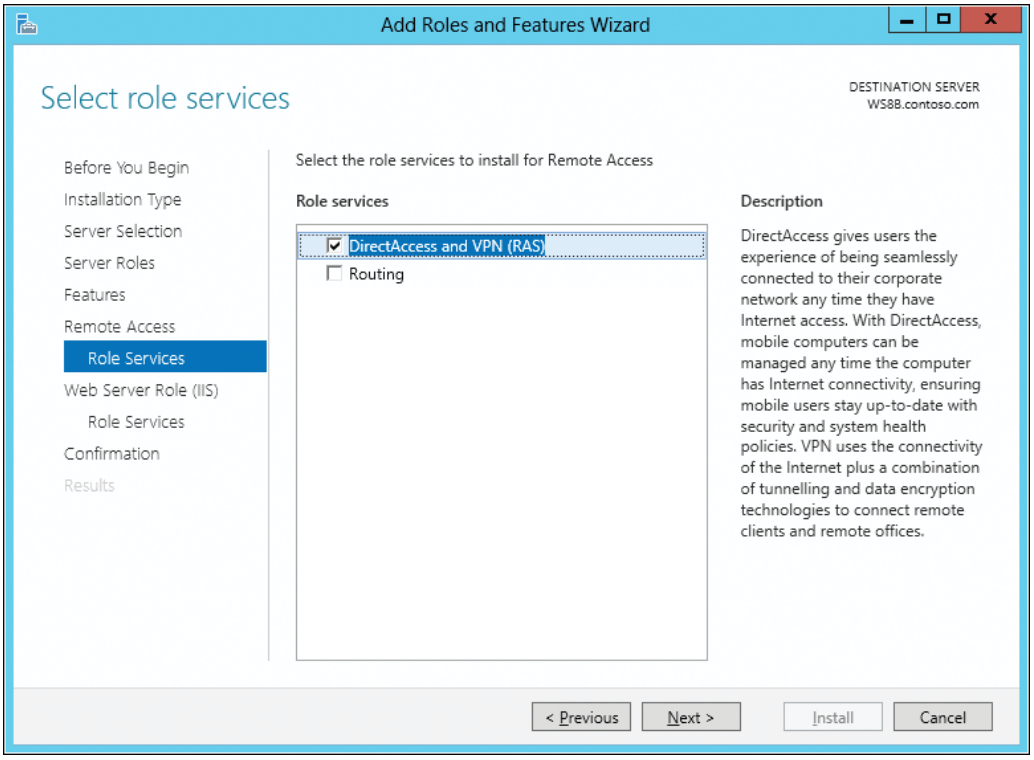
After making sure that all the requirements have been met for deploying a DirectAccess solution (for example, by making sure your server is domain-joined and has at least one network adapter), you can start the Add Roles And Features Wizard from Server Manager. Then, on the Select Installation Type page, begin by selecting the Role-based Or Feature-based Installation option, as shown here:



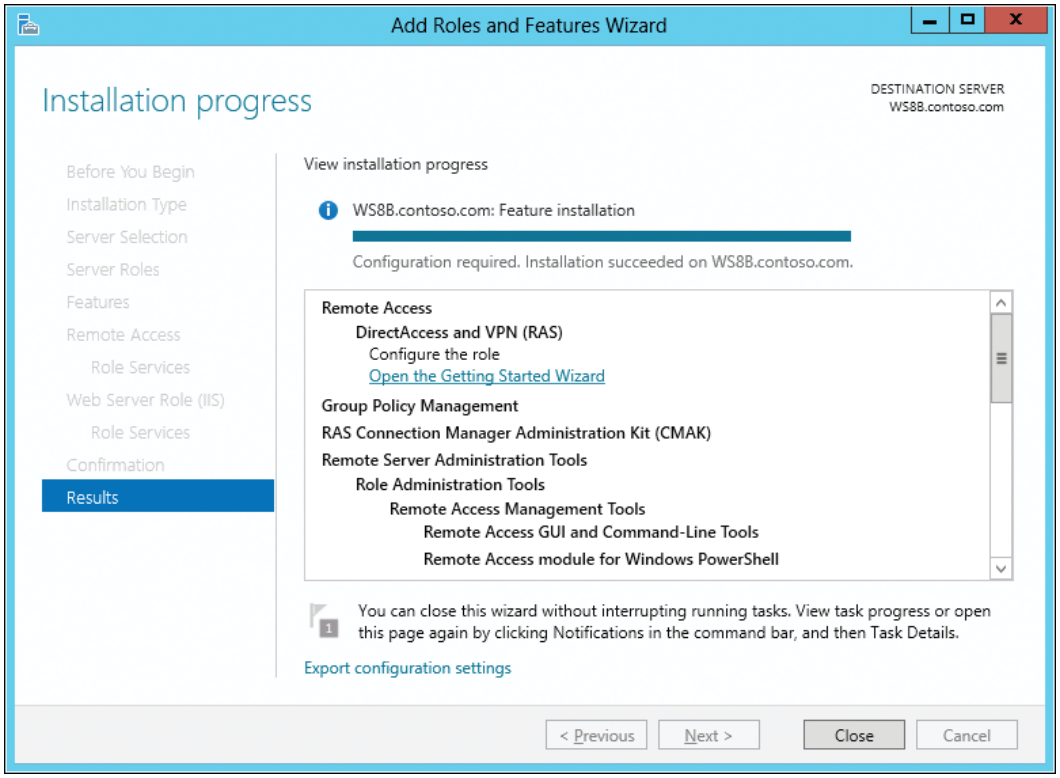
After choosing the server(s) you want to install remote access functionality on, select the Remote Access role on the Select Server Roles page:



On the Select Role Services page, select the DirectAccess And VPN (RAS) option, as shown here:

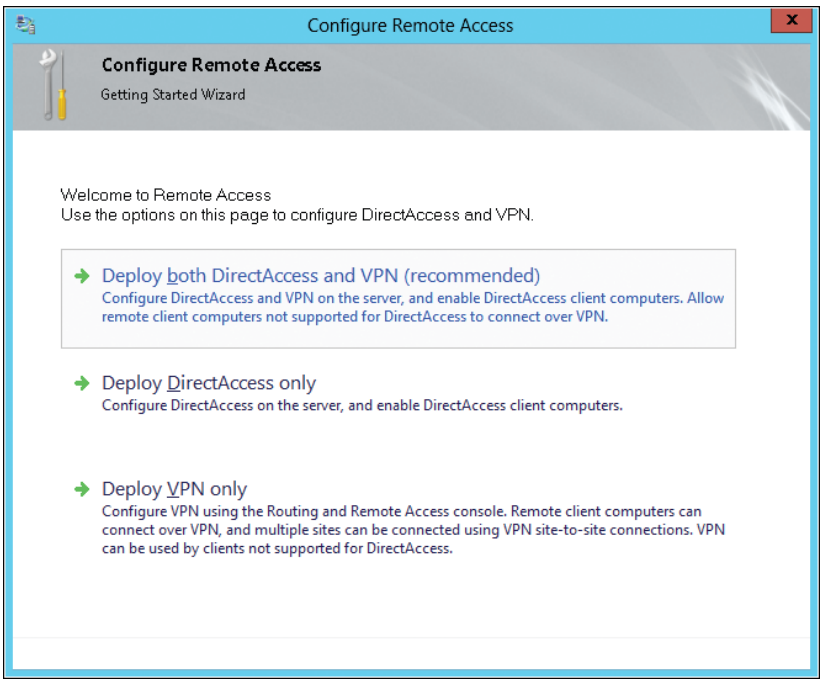


Continue through the wizard to install the Remote Access server role. Once this is finished, click the Open The Getting Started Wizard link on the Installation Progress page shown here to begin configuring remote access:



Windows Server 2012 presents you with three options for configuring remote access:

- Deploying both DirectAccess and VPN server functionality so that DirectAccess can be used for clients running Windows 7 or later while the VPN server can be used so that clients that don't support DirectAccess can connect to your corporate network via VPN
- Deploying only DirectAccess, which you might choose if all your clients are running Windows 7 or later
- Deploying only a VPN server, which you might use if you've invested heavily in third-party VPN client software and you want to continue using these investments Let's choose the recommended option by selecting the Deploy Both DirectAccess And VPN option:

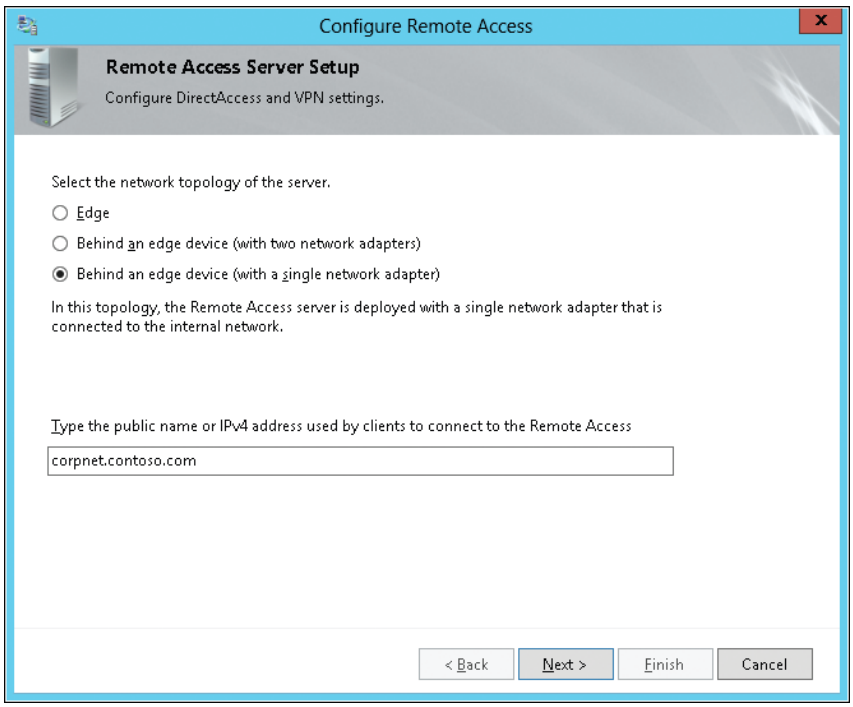


On the Remote Access Server Setup page of the Configure Remote Access wizard, you now choose the network topology that best describes where your DirectAccess server is located.

The three options available are:

- Edge, which requires that the server have two network interfaces, one connected to the public Internet and one to the internal network.
- Behind An Edge Device (With Two Network Adapters), which again requires that a server has two network interfaces with the DirectAccess server being located behind a NAT device.
- Behind An Edge Device (Single Network Adapter), which only requires the server (located behind a NAT device) to have one network interface connected to the internal network.

Because the server used in this walkthrough has only one network adapter and is located behind a NAT inside, we'll choose the third option listed here. We'll also specify Corpnet. contoso.com as the Domain Name System (DNS) name to which the DirectAccess clients will connect:



Note that if the server has two network interfaces, with one connected to the Internet, the Configure Remote Access wizard will detect this and configure the two interfaces as needed.

When you are ready to finish running the Configure Remote Access wizard, you will be presented with a web-based report of the configuration changes that the wizard will make before you apply them to your environment. For example, performing the steps previously described in this walkthrough will result in the following changes:

- A new GPO called DirectAccess Server Settings will be created for your DirectAccess server.
- A new GPO called DirectAccess Client Settings will be created for your DirectAccess clients.
- DirectAccess settings will be applied to all mobile computers in the CONTOSO\Domain Computers security group.
- A default web probe will be created to verify internal network connectivity.
- A connection name called Workplace Connection will be created on DirectAccess clients.
- The remote access server has DirectAccess configured to use Corpnet.contoso.com as the public name to which remote clients connect.
- The network adapter connected to the Internet (via the NAT device) will be identified by name.

- Configuration settings for your VPN server will also be summarized; for example, how VPN client address assignment will occur (via DHCP server) and how VPN clients will be authenticated (using Windows authentication).
- The certificate used to authenticate the network location server deployed on the Remote Access server, which in the above walkthrough was CN=DirectAccess-NLS. contoso.com, is identified.

Configuring and managing remote access

Deploying the Remote Access server role also installs some tools for configuring and managing remote access in your environment. These tools include:

- The Remote Access Management Console (see Figure 5-1), which can be started from Server Manager.
- The Remote Access module for Windows PowerShell.

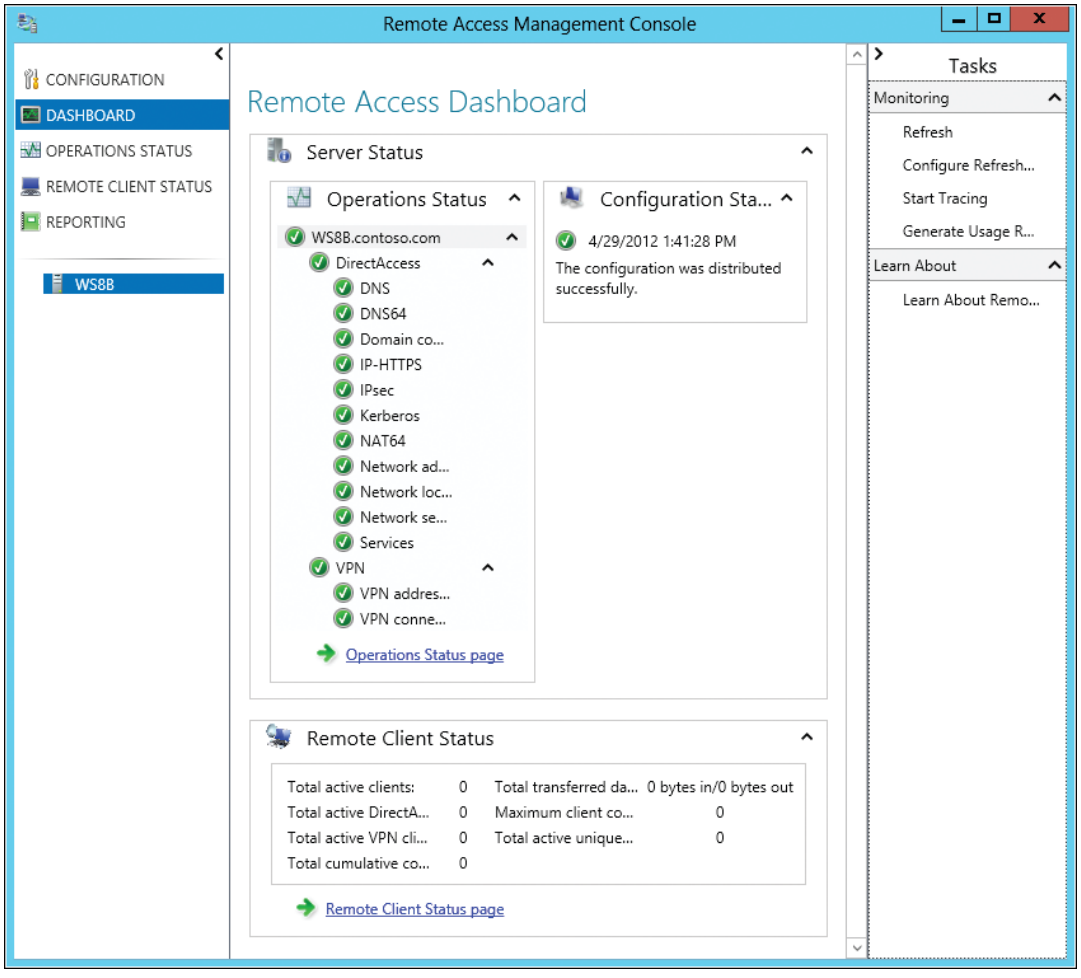


FIGURE 5-1 – The Remote Access Management Console is integrated into Server Manager

In addition to allowing you to monitor the operational status of your remote access servers and clients, the Remote Access Management Console enables you to perform an additional configuration of your remote access environment (see Figure 5-2).

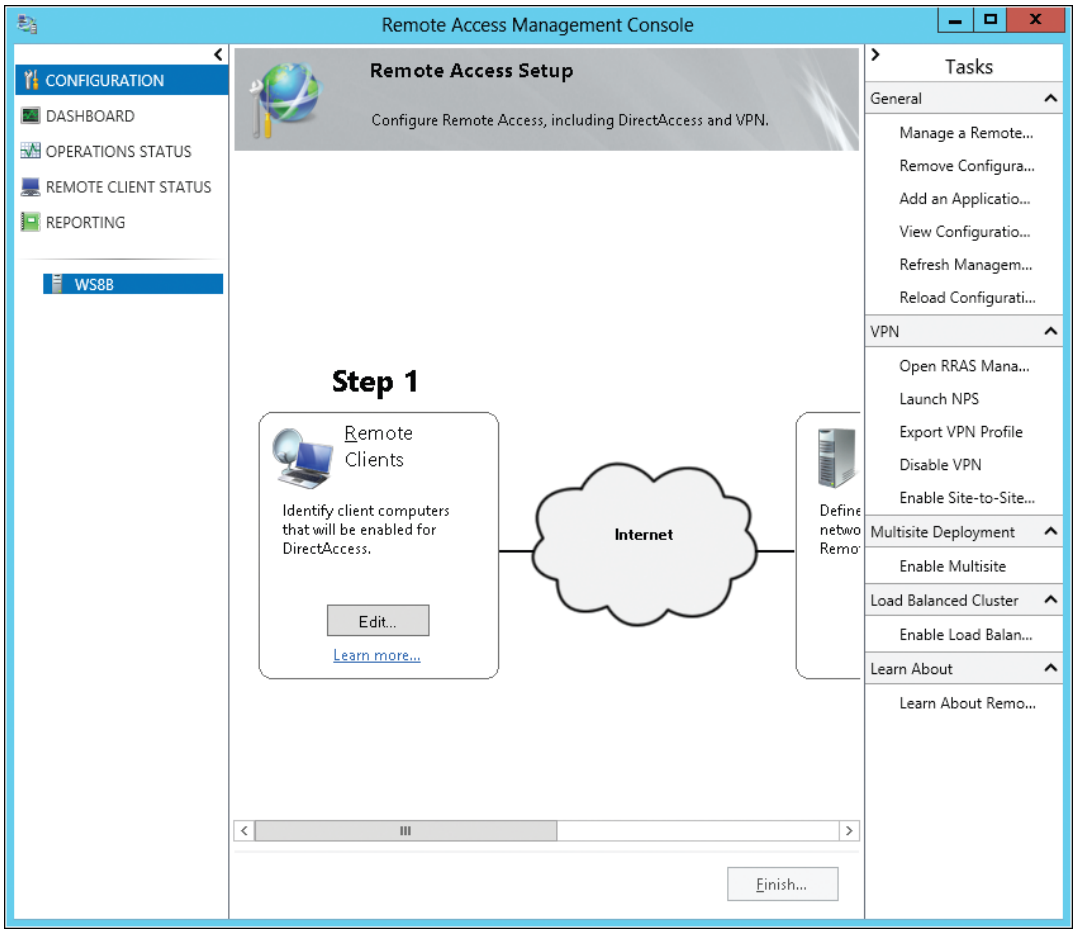


FIGURE 5-2 – Using the Remote Access Management Console to perform additional configuration of a remote access environment.

The Configuration page of the Remote Access Management Console lets you perform additional configuration if needed (or initial configuration if desired) in four areas:

- **Step 1**: **Remote Clients**. Lets you select between two DirectAccess scenarios:
  - Deploying full DirectAccess for client access and remote management so that remote users can access resources on the internal network and their computers can be managed by policy.

    - Deploying DirectAccess for remote management only so that the computers of remote users can be managed by policy but the users cannot access resources on the internal network.
    - You can also select which group or groups of computers will be enabled for DirectAccess (by default, the Domain Computers group), choose whether to enable DirectAccess for mobile computers only (enabled by default), and choose whether to use force tunneling so that DirectAccess clients connect to both the internal network and the Internet via the Remote Access server (disabled by default).
- **Step 2**: **Remote Access Server**. Lets you configure the network topology of the Remote Access server (but only if not previously configured), the public name or IPv4 address used by clients to connect to the server, which network adapter is for the internal network, which certificate to use to authenticate IP-HTTPS connections, how user authentication is performed, whether to enable clients running Windows 7 to connect via DirectAccess, and how your VPN server assigns IP addresses and performs authentication
- **Step 3**: **Infrastructure Servers**. Lets you configure the name of your network location server for DirectAccess clients, DNS settings for remote access, and other settings
- **Step 4**: **Application Servers.** Lets you specify whether to extend IPsec authentication and encryption to selected application servers on your internal network

Simplified VDI deployment

Virtual desktop infrastructure (VDI) is an emerging alternative to the traditional PC-based desktop computing paradigm. With the VDI approach, users access secure, centrally managed virtual desktops running on virtualization hosts located in the datacenter. Instead of having a standard PC to work with, VDI users typically have less costly thin clients that have no hard drive and only minimal processing power.

A typical environment where the VDI approach can provide benefits might be a call center where users work in shifts using a shared pool of client devices. In such a scenario, VDI can provide greater flexibility, more security, and lower hardware costs than providing each user with his or her own PC. The VDI approach can also bring benefits to organizations that frequently work with contractors because it eliminates the need to provide contractors with PCs and

helps ensure that corporate intellectual property remains safely in the datacenter. A help desk also benefits from the VDI approach because it's easier to re-initialize failed virtual machines remotely than with standard PCs.

Although implementing a VDI solution may be less expensive than provisioning PCs to users, VDI can have some drawbacks. The server hardware for virtualization hosts running virtual desktops must be powerful enough to provide the level of performance that users have come to expect from using desktop PCs. Networking hardware must also be fast enough to ensure that it doesn't become a performance bottleneck. And in the past, deploying and managing virtual desktops using previous Windows Server versions has been more complex than deploying and managing PCs because it requires deploying RDS with Hyper-V in your environment.

Windows Server 2012, however, eliminates the last of these drawbacks by simplifying the process by which virtual desktops are deployed and managed. The result is that VDI can now be a viable option to consider even for smaller companies who are looking for efficiencies that can lead to cost savings for their organization.

Deployment types and scenarios

Windows Server 2012 introduces a new approach to deploying the Remote Desktop Services server role based on the type of scenario you want to set up in your environment:

- Session virtualization Lets remote users connect to sessions running on a Remote Desktop Session Host to access session-based desktop and RemoteApp programs.
- VDI Lets remote users connect to virtual desktops running on a Remote Desktop Virtualization Host to access applications installed on these virtual desktops (and also RemoteApp programs if session virtualization is also deployed).

Whichever RDS scenario you choose to deploy, Windows Server 2012 gives you two options for how you can deploy it:

- **Quick Start.** This option deploys all the RDS role services required on a single Computer using mostly the default options and is intended mainly for test environments.

- **Standard deployment.** This option provides you with more flexibility concerning how you deploy different RDS role services to different servers and is intended for production environments.

RDS enhancements

Besides enabling scenario-based deployment of RDS role services like Remote Desktop Session Host, Remote Desktop Virtualization Host, Remote Desktop Connection Broker, and Remote Desktop Web Access, RDS in Windows Server 2012 includes other enhancements such as:

- A unified administration experience that allows you to manage your RDS-based infrastructure directly from Server Manager.
- Centralized resource publishing that makes it easier to deploy and manage RemoteApp programs for both session virtualization and VDI environments.
- A rich user experience using the latest version of Remote Desktop Protocol (RDP), including support for RemoteFX over WAN.
- USB Redirection, for enhanced device remoting for both session virtualization and VDI environments.
- User profile disks that let you preserve user personalization settings across collections of sessions or pooled virtual desktops.
- The ability to automate deployment of pooled virtual desktops by using a virtual desktop template.
- Support for using network shares for storing personal virtual desktops.
- Support for Storage Migration between host machines when using pooled virtual desktops.

Virtual desktops and collections

A virtual desktop is a virtual machine running on a Hyper-V host that users can connect to remotely using RDS. A collection consists of one or more virtual desktops used in a VDI deployment scenario. Virtual desktops can either be managed or unmanaged:

- **Managed collections.** These can be created from an existing virtual machine that has been sysprepped so it can be used as a template for creating other virtual desktops in the collection.

- **Unmanaged collections.** These can be created from an existing set of virtual desktops, which you then add to the collection.

Virtual desktops can also be pooled or personal:

- **Pooled virtual desktops.** This type allows the user to log on to any virtual desktop in the pool and get the same experience. Any customizations performed by the user on the virtual desktop are saved in a dedicated user profile disk.
- **Personal virtual desktops.** This type permanently assigns a separate virtual desktop to each user account. Each time the user logs on, he or she gets the same virtual desktop, which can be customized as desired, with customizations being saved within the virtual desktop itself.

Table 5-1 summarizes some of the differences between pooled and personal virtual desktops when they are configured as managed virtual desktops, whereas Table 5-2 lists similar kinds of differences between them when they are configured as unmanaged virtual desktops.

TABLE 5-1 – Comparison of pooled and personal managed virtual desktops

Capability	Pooled?	Personal?
New virtual desktop creation based on virtual desktop template	+	+
Re-create virtual desktop based on virtual desktop template	+	
Store user settings on a user profile disk	+	
Permanent user assignment to the virtual desktop		+
Administrative access on the virtual desktop		+

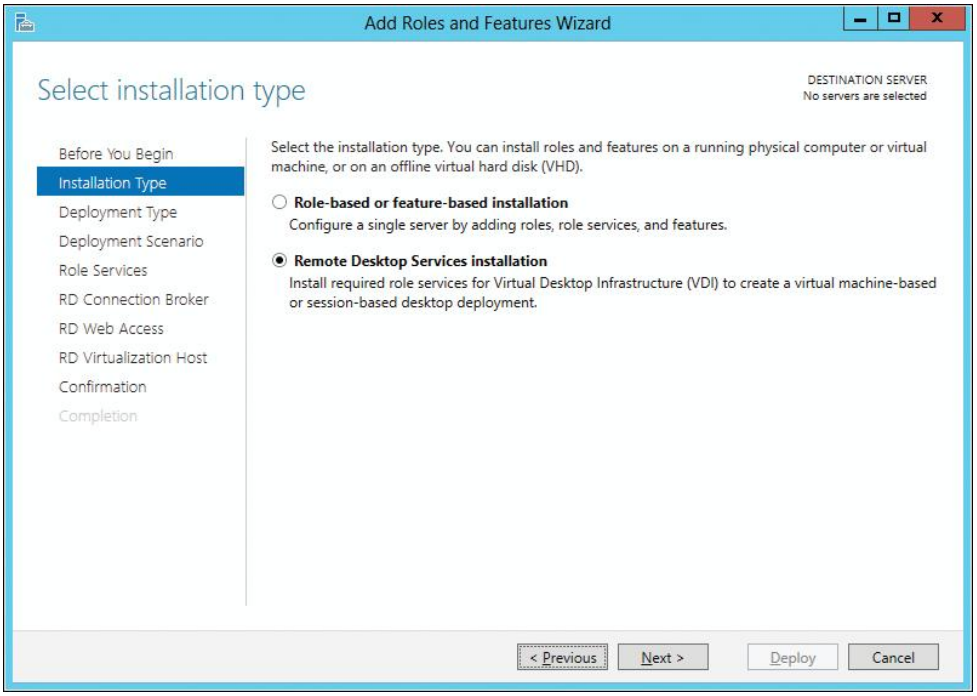
TABLE 5-2 – Comparison of pooled and personal unmanaged virtual desktops

Capability	Pooled?	Personal?
New virtual desktop creation based on virtual desktop template		
Re-create virtual desktop based on virtual desktop template		
Store user settings on a user profile disk	+	
Permanent user assignment to the virtual desktop		+

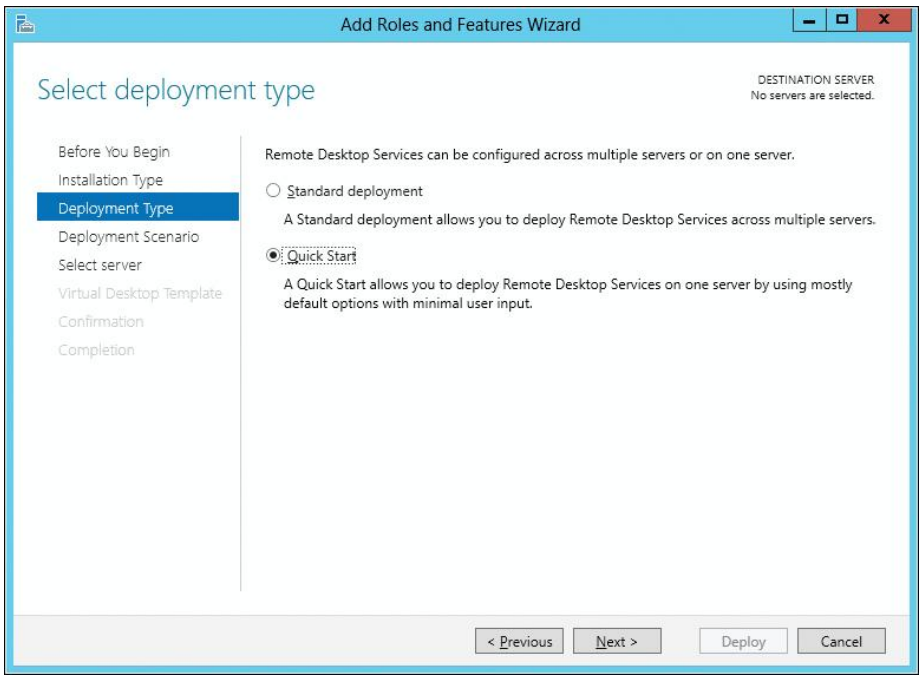
Administrative access on the virtual desktop		+

Deploying VDI

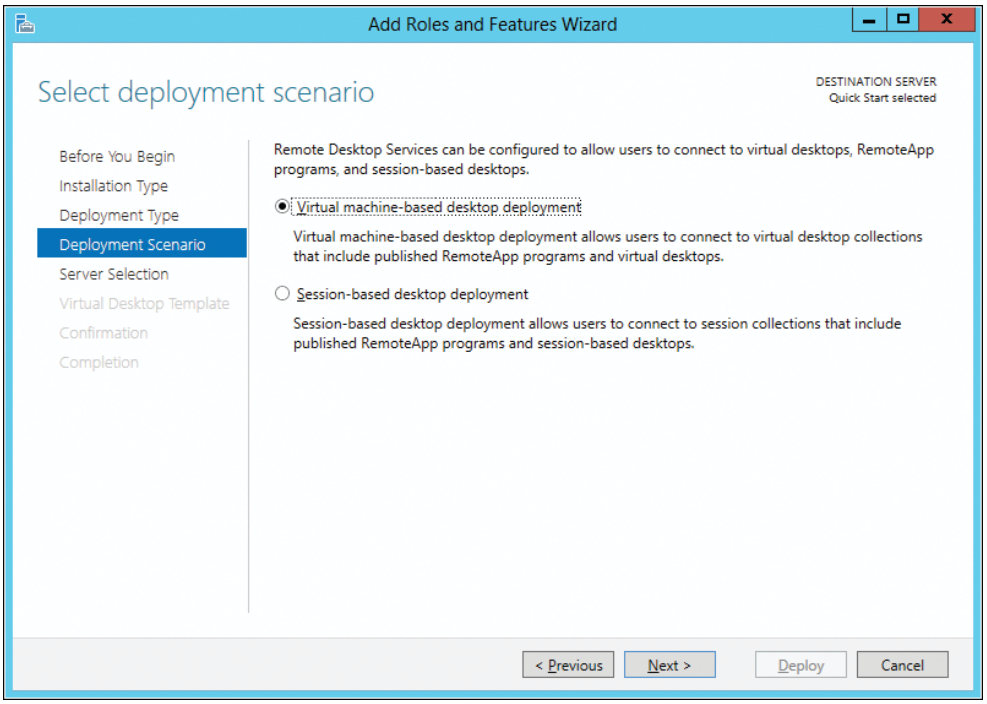
To see simplified VDI deployment at work, let's walk through the initial steps of deploying a Quick Start VDI deployment. Begin by starting the Add Roles And Features Wizard from Server Manager. Then on the Select Installation Type page, begin by selecting the Remote Desktop Services Scenario-based Installation option, as shown here:



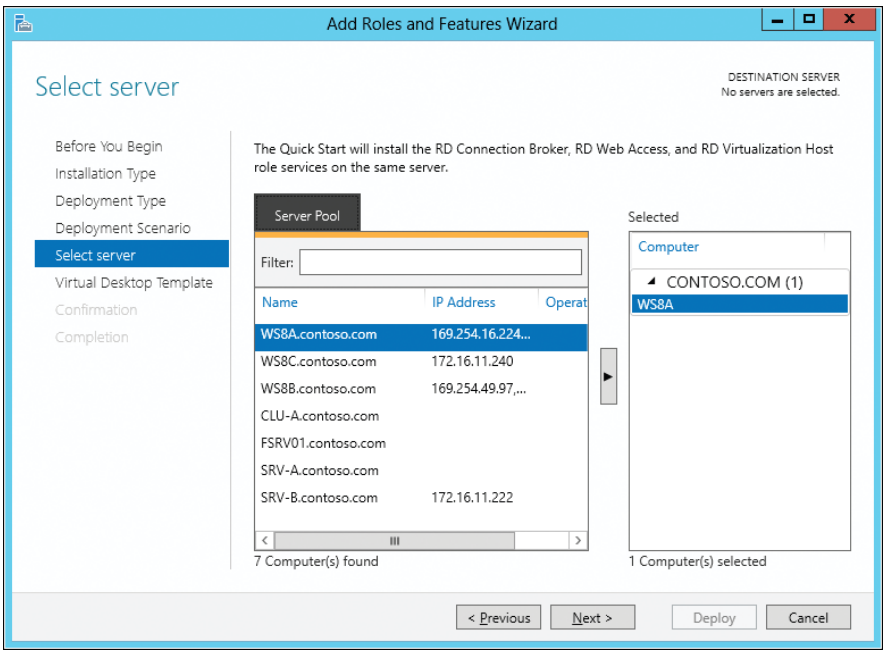
Select the Quick Start option on the Select Deployment Type page:



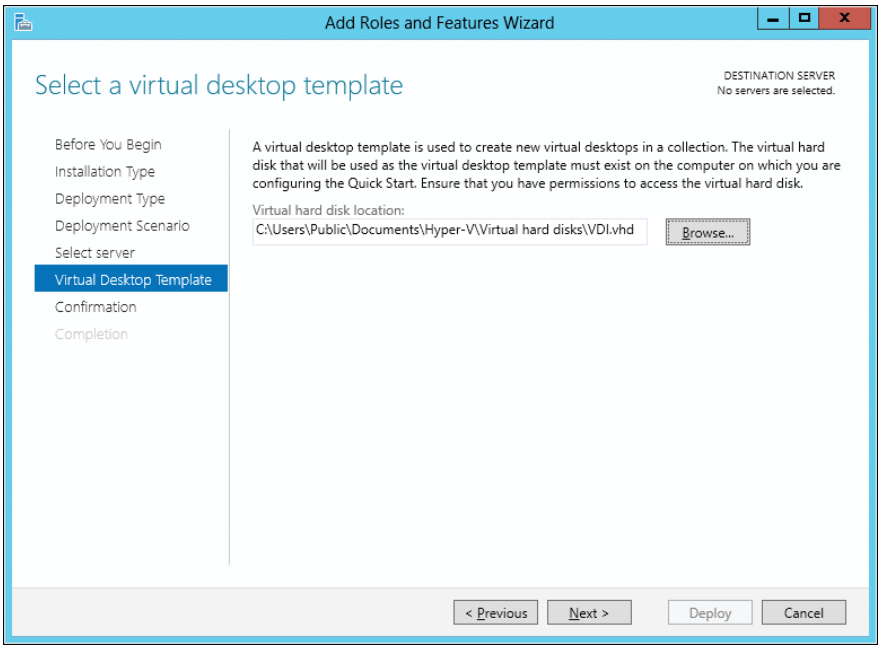
On the Select Deployment Scenario page of the wizard, choose the Virtual Desktop Infrastructure option:



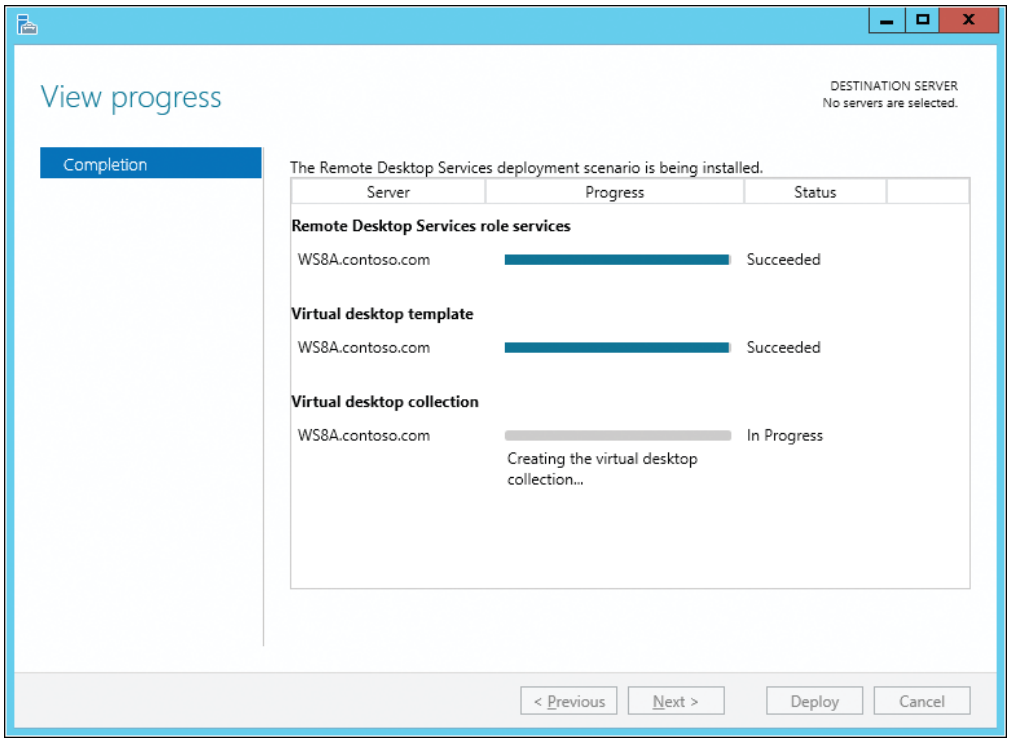
Select a server from your server pool for deploying RDS role services onto:



A compatibility check will be performed at this point to ensure that the selected server meets all the requirements for implementing the selected deployment scenario. If no compatibility issues are detected, the next wizard page appears, which prompts you to select a virtual disk template (a .vhd or .vhdx file) on which a VDI-capable client operating system like Windows 8 or Windows 7 has been installed, along with any locally installed applications needed on the virtual desktop. The Windows installation on this VHD must have been prepared by running sysprep /generalize on it so that it can function as a reference image for adding new virtual desktops to your collection.



Completing the wizard and clicking Deploy begins the process of deploying your VDI environment. Three RDS role services (Connection Broker, RD Virtualization Host, and RD Web Access) are first installed on the selected server, which is then restarted to complete installation of these role services. A virtual desktop template is then created from the previously specified VHD file, and a new pooled virtual desktop collection named QuickVMCollection is created with two pooled virtual desktops based on the virtual desktop template:



The VDI deployment process also creates a new Hyper-V network switch named RDS Virtual and assigns the pooled virtual desktops to that switch.

Managing VDI

Once the Quick Start VDI deployment process is finished, you can manage your VDI environment by using the Remote Desktop Services option that now appears in Server Manager. For example, the Overview page of the Remote Desktop Services option provides you with visual information concerning your RDS infrastructure, virtualization hosts, and collections (see Figure 5-3). You can use the Remote Desktop Services option in Server Manager to configure your RDS role services, manage your virtualization hosts, create new collections, and perform other VDI-related tasks.

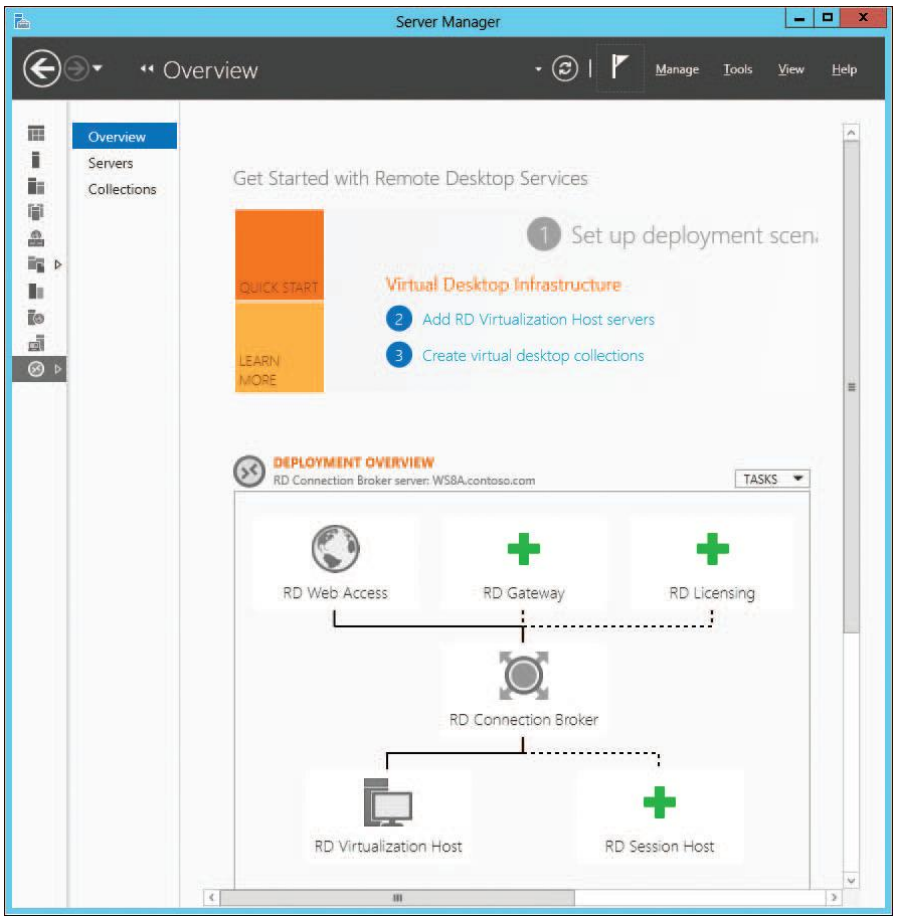


FIGURE 5-3 – The Remote Desktop Services option in Server Manager.

User-Device Affinity

Previous versions of the Windows platform have included three features for supporting roaming users, namely **roaming user profiles** (RUPs), **Folder Redirection** (FR), and Offline Files. What was missing was a way of associating each user profile with specific computers or devices. Windows Server 2012 and Windows 8 now provide such functionality in the form of User-Device Affinity, which lets you map a user to a limited set of computers where RUP or FR is used. As a result, administrators can control on which computers RUPs and offline files are stored.

User-Device Affinity benefits organizations by enabling new types of scenarios. For example, you could configure the environment so the user's data and settings can be roamed between the user's desktop PC and his or her laptop but cannot be roamed to any other computers. That way, for example, when the user logs on to a shared computer in the public foyer of the building, there is no

danger that the user's personal or corporate data will be left behind on the computer.

Configuring User-Device Affinity

User-Device Affinity can be implemented using Group Policy by configuring the Evaluate User Device Affinity Configuration For Roaming Profiles And Folder Redirection policy setting found under System\User State Technologies. When you enable this policy setting, you can select from three possible configuration options:

- Apply To Neither Roaming Profiles Nor Folder Redirection Disables the primary computer check when logging on.
- Apply To Roaming Profiles And Folder Redirection Only Roams the user profile and applies FR only when logging on to primary computers.
- Apply To Roaming Profiles Only Roams the user profile when logging on to primary computers, and always applies FR.

Enhanced BranchCache

BranchCache was first introduced in Windows Server 2008 R2 and Windows 7 as a way of caching content from file and web servers on a WAN locally at branch offices. When another client at the branch office requests the same content, the client downloads it from the local cache instead of downloading it across the WAN. By deploying BranchCache, you can increase the network responsiveness of centralized applications that are being accessed from remote offices, with the result that branch office users have an experience similar to being directly connected to the central office.

BranchCache has been enhanced in Windows Server 2012 and Windows 8 in a number of different ways. For example:

- The requirement of having a GPO for each branch office has been removed to simplify the deployment of BranchCache.
- BranchCache is tightly integrated with the File Server role and can use the new Data Deduplication capabilities of Windows Server 2012 to provide faster download times and reduced bandwidth consumption over the WAN.
- When identical content exists in a file or multiple files on either the content server or hosted cache server, BranchCache stores only a single instance of the

content and clients at branch offices download only a single instance of duplicated content. The results are more efficient use of disk storage and savings in WAN bandwidth.

- BranchOffice provides improved performance and reduced bandwidth usage by performing offline calculations that ensure content information is ready for the first client that requests it.
- New tools are included in Windows Server 2012 that allow you to preload cachable content onto your hosted cache servers even before the content is first requested by clients.
- Cached content is encrypted by default to make it more secure.
- Windows PowerShell can be used to manage your BranchCache environment, which enables automation that makes it simpler to deploy BranchCache in cloud computing environments.

Branch Office Direct Printing

Branch Office Direct Printing is a new feature of Windows Server 2012 that enables print jobs from a branch office to be redirected to local printers without the requirement of first having them sent to a print server on the network. As a result, when a print job is initiated from a branch office, the printer configuration and drivers are still accessed from the print server if needed, but the print job itself is sent directly to the local printer at the branch office.

Implementing this feature has several benefits, including reducing printing time at branch offices and making more efficient use of costly WAN bandwidth. In addition, cost can be reduced because you no longer need to deploy costly WAN optimization appliances at branch offices specifically for printing purposes.

Full Windows experience

Today's users expect and demand the full Windows experience, even when they work in virtual environments. Windows Server 2012 delivers this experience better than ever before with enhancements to RemoteFX, USB redirection, and the new User Profile Disks feature. This section introduces these new features and enhancements.

RemoteFX enhancements

RemoteFX was first introduced in Windows Server 2008 R2 as a way of delivering a full Windows experience over the RDP across a wide variety of client devices. RemoteFX is part of the Remote Desktop Services role service and is intended mainly for use in VDI environments to support applications that use rich media, including 3-D rendering. RemoteFX uses two capabilities for providing remote users with a rich desktop environment similar to the local desktop environment that PC users enjoy:

- Host side rendering Allows graphics to be rendered on the host instead of the client by utilizing the capabilities of a RemoteFX-capable graphics processing unit (GPU) on the host. Once rendered on the host, graphics are delivered to the client over RDP in an adaptive manner as compressed bitmap images. In addition, multiple GPU cards are now supported on Windows Server 2012 as well as using a software GPU.
- GPU Virtualization Exposes a virtual graphics device to a virtual machine running on a RemoteFX-capable host and allows multiple virtual desktops to share the single GPU on the host.

RemoteFX can benefit organizations by enabling flexible work scenarios like hot-desking and working from home. By making the virtual desktop experience similar to that of traditional PCs, RemoteFX can make VDI a more feasible solution for organizations who want increased data security and simplified management of the desktop environment.

RemoteFX has been enhanced in Windows Server 2012 in a number of different ways, including the following:

- RemoteFX is integrated throughout the RDS role services instead of being installed as its own separate role service and is installed automatically whenever the Remote Desktop Virtualization Host role service is installed.
- The performance when delivering streaming media content over RDP has been greatly improved.
- RemoteFX can dynamically adapt to changing network conditions by using multiple codecs to optimize how content is delivered.
- RemoteFX can choose between Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) to optimize performance when sending RDP traffic over the WAN (this is called RemoteFX for WAN).
- Support for multi-touch gestures and manipulations in remote sessions is included.

- Improved multimonitor support over RDP, which allows a virtual machine to support up to four monitors regardless of their resolution, is available.
- There is now the ability to use VMConnect to manage virtual machines that have the RemoteFX 3D Video Adapter installed in them. (In the previous version of Windows Server, you had to use a Remote Desktop connection to manage the virtual machines.)

Configuring RemoteFX

To use RemoteFX, the host machine must:

- Support hardware-assisted virtualization and data execution prevention (DEP).
- Have at least one GPU listed as supporting RemoteFX in the Windows Server Catalog.
- Have a CPU that supports Second Level Address Translation (SLAT). Note that Intel refers to SLAT as Extended Page Tables (EPT), whereas AMD refers to SLAT as Nested Page Tables (NPT).

To configure a Windows Server 2012 host to use RemoteFX, you can use the new GPU management interface in the Hyper-V settings of the host (see Figure 5-4). This interface lets you select from a list of available GPUs on the host that are RemoteFX-capable (if any) and then enable or disable RemoteFX functionality for the selected GPU. The interface also shows the details concerning each RemoteFX-capable GPU on the host.

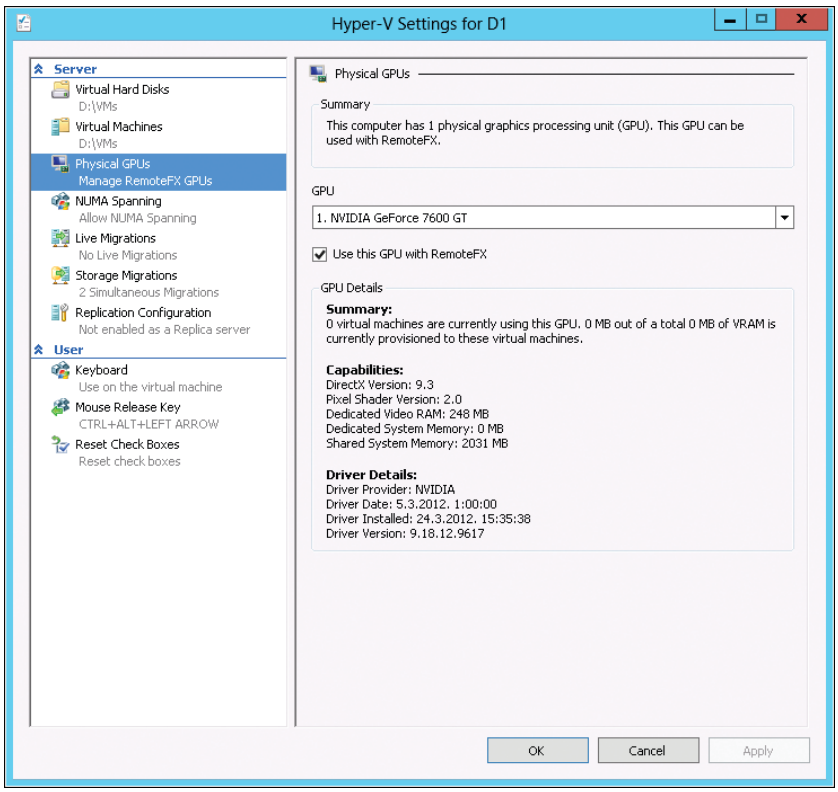


FIGURE 5-4 – Configuring RemoteFX on a Hyper-V host running Windows Server 2012

Enhanced USB redirection

USB redirection in RemoteFX is an important ingredient in establishing parity of experience between virtual desktops and traditional PCs. USB redirection was first introduced in Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1 to support RemoteFX VDI scenarios. USB redirection occurs at the port protocol level and enables redirection of a wide variety of different types of universal serial bus (USB) devices, including printers, scanners, webcams, Voice over Internet Protocol (VoIP) headsets, and biometric devices. USB redirection does not require hardware drivers to be installed on the virtual machines. Instead, the necessary drivers are installed on the host.

In Windows 7 SP1 and Windows Server 2008 R2 SP1, RemoteFX USB redirection was supported only within virtual desktops running Remote Desktop Virtualization Host. New in Windows Server 2012 and Windows 8 is support for USB redirection for Remote Desktop Session Host. This enables new kinds of scenarios where RemoteFX can bring a richer desktop experience for businesses that implement session virtualization solutions.

Other enhancements to USB redirection in Windows Server 2012 include the following:

- USB redirection for Remote Desktop Virtualization Host no longer requires installing the RemoteFX 3D Video Adapter on the virtual machine.
- USB redirection for Remote Desktop Session Host is isolated to the session in which the device is being redirected. This means that users in one session will not be able to access USB devices redirected in a different session.

User Profile Disks

Preserving the user state is important in both session virtualization and VDI environments. Users who have worked in traditional PC environments are used to being able to personalize their desktop environment and applications by configuring settings such as desktop backgrounds, desktop shortcuts, application settings, and other customizations. When these same users encounter session virtualization or VDI environments, they expect the same personalization capabilities that traditional PCs provide.

In previous versions of Windows Server, preserving user state information for sessions and virtual desktops required using Windows roaming technologies like RUPs and FR. This approach had certain limitations, however. For one thing, implementing RUP and FR adds more complexity to deploying RDS for session virtualization or VDI. And for VDI deployments in particular, RUP/FR restricted the solution to using personal virtual desktops because pooled virtual desktops did not support preserving user state with RUP/FR.

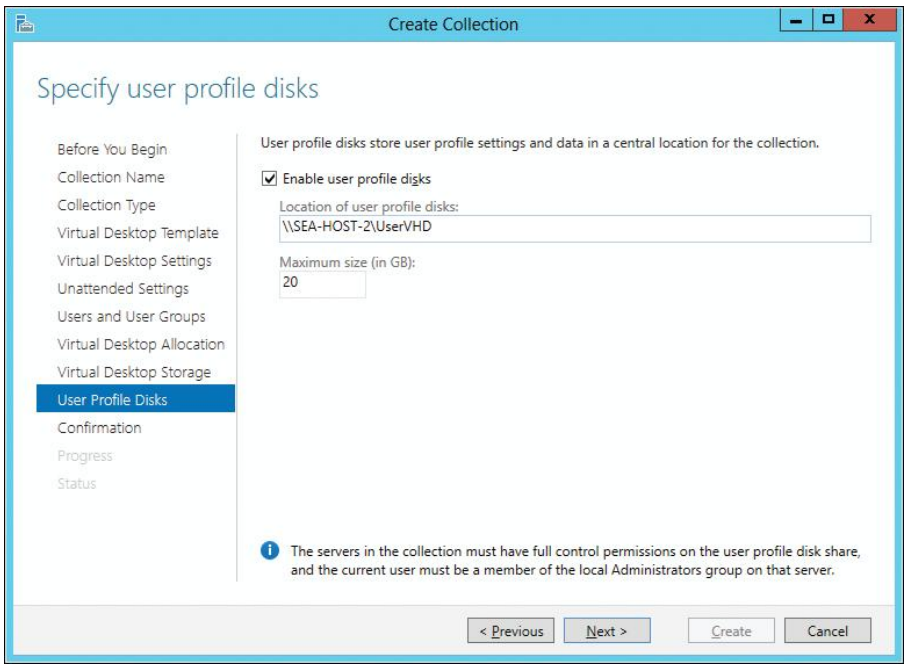
Other problems could arise when using RUP/FR with RDS in previous versions of Windows Server. For example, if the user's RUP was accidentally used outside the RDS environment, data could be lost, making the profile unusable. RUP/FR could also increase the time it takes for a user to log on to a session or virtual desktop. Finally, applications that were poorly designed and didn't write user data and settings to the proper location might not function as expected when RUP/FR was used as a roaming solution.

Windows Server 2012 solves these problems with the introduction of User Profile Disks, which store user data and settings for sessions and virtual desktops in a separate VHD file that can be stored on a network share.

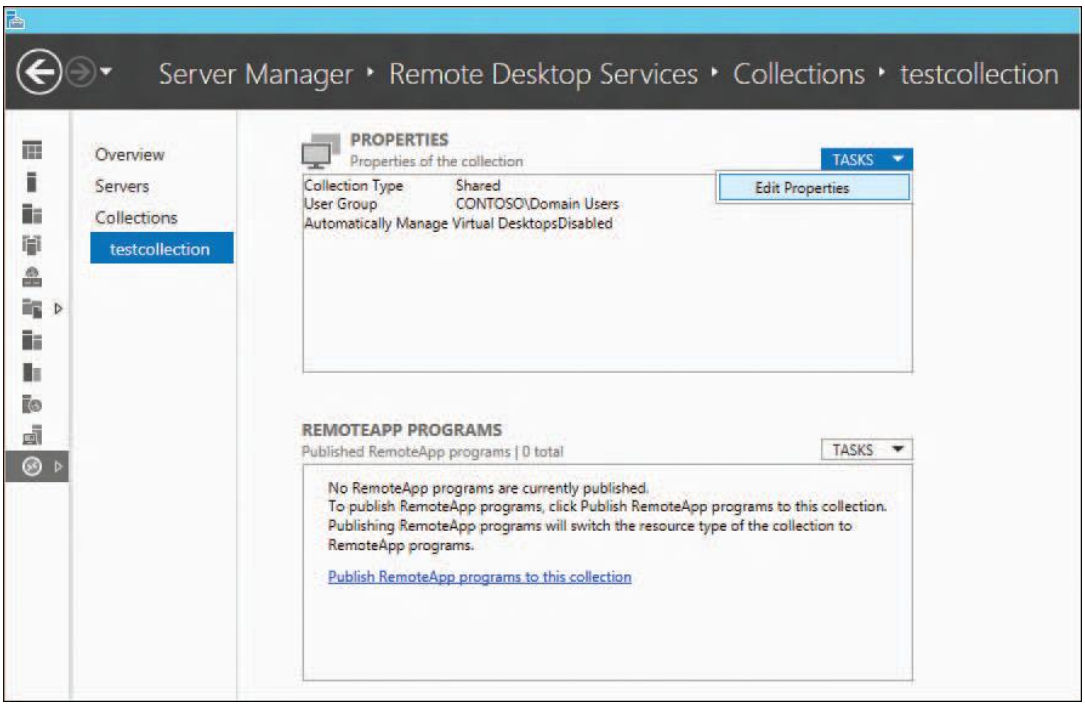
Configuring User Profile Disks

Configuring a user profile disk for a virtual desktop collection is done when you create the collection. Before you do this however, you need to create a server message block (SMB) file share where your user profile disk will be stored on the network and configure permissions on the file share so the computer account of your host has at least write access.

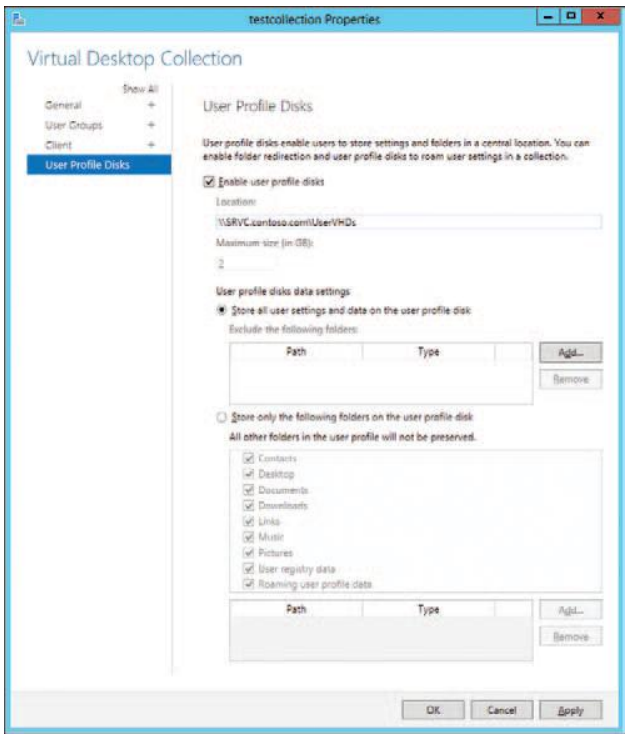
Begin by starting the Create Collection wizard by clicking Create Virtual Desktop Collections on the Overview page of the Remote Desktop Services section of Server Manager. Then on the Specify User Profile Disks page of the Create Collection wizard, make sure Enable User Profile Disks is selected and type the Universal Naming Convention (UNC) path to the file share where you'll store your user profile disks on the network:



Once your new collection has been created, you can further configure your user profile disk settings by selecting the collection on the Collections page of the Remote Desktop Services section of Server Manager, clicking the Tasks control in the Properties area, and clicking Edit Properties:



On the Virtual Desktop Collection page of the properties of your collection, you can customize how your user profile disk will be used. By default, all user profile data and settings are stored on the user profile disk, but you can configure these settings by selecting folders that should be excluded from being stored on your user profile disk. Alternatively, you can configure which specific types of items should be stored on your user profile disk; for example, only the user's Documents folder and user registry data:



Enhanced security and compliance

Security and compliance are two areas that have been significantly extended in Windows Server 2012. Dynamic Access Control now allows centralized control of access and auditing functions. BitLocker Drive Encryption has been enhanced to make it easier to deploy, manage, and use. And implementing Domain Name System Security Extensions (DNSSEC) to safeguard name resolution traffic can now be performed using either user interface (UI) wizards or Windows PowerShell. This concluding section covers these new features and enhancements.

Dynamic Access Control

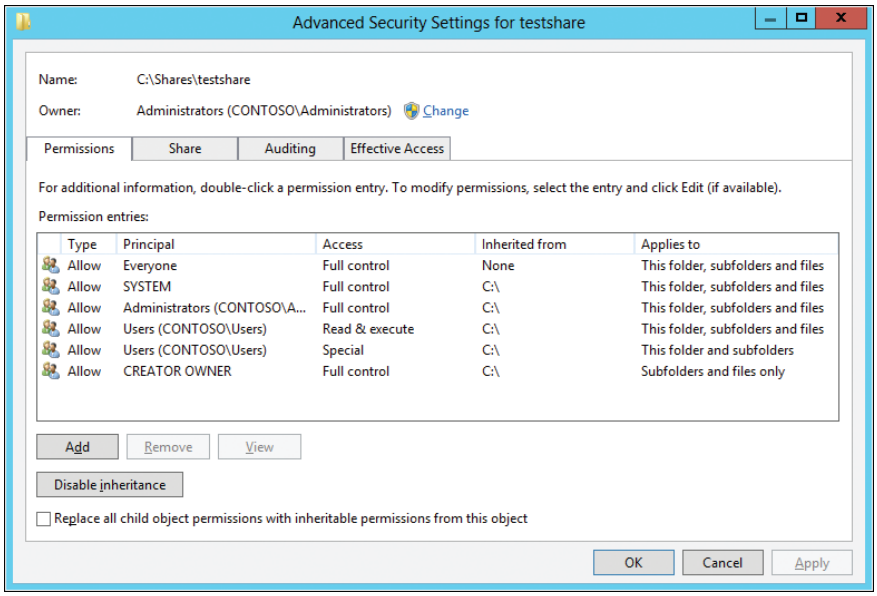
Controlling access and ensuring compliance are essential components of IT systems in today's business environment. Windows Server 2012 includes enhancements that provide improved authorization for file servers to control and audit who is able to access data on them. These enhancements are described under the umbrella name of Dynamic Access Control and enable automatic and manual classification of files, central access policies for controlling access to files, central audit policies for identifying who accessed files, and the application of Rights Management Services (RMS) protection to safeguard sensitive information.

Dynamic Access Control is enabled in Windows Server 2012 through the following new features:

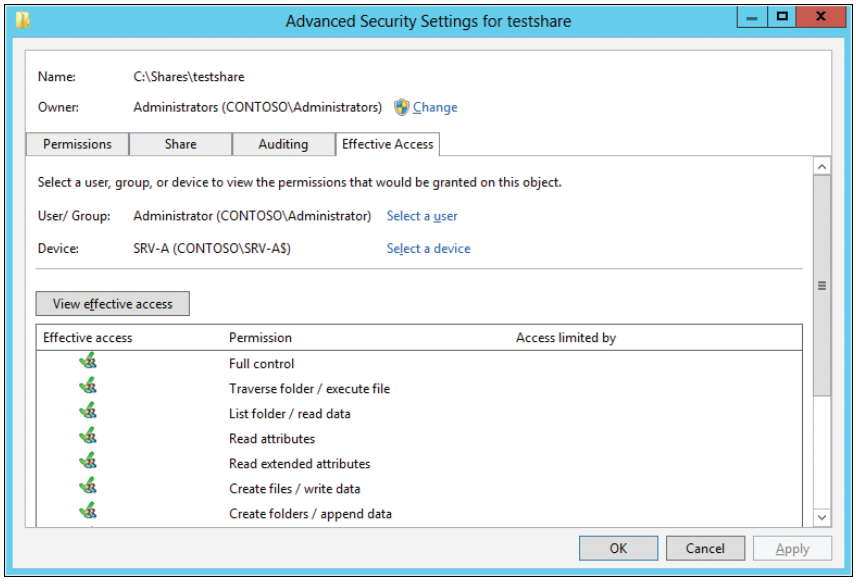
- A new authorization and audit engine that supports central policies and can process conditional expressions.
- A redesigned Advanced Security Settings Editor that simplifies configuration of auditing and determination of effective access.
- Kerberos authentication support for user and device claims.
- Enhancements to the File Classification Infrastructure (FCI) introduced previously in Windows Server 2008 R2.
- RMS extensibility to allow partners to provide solutions for applying Windows Server-based RMS to non-Microsoft file types.

Implementing Dynamic Access Control in your environment requires careful planning and the performing of a number of steps that include configuring Active Directory, setting up a file classification scheme, and more.

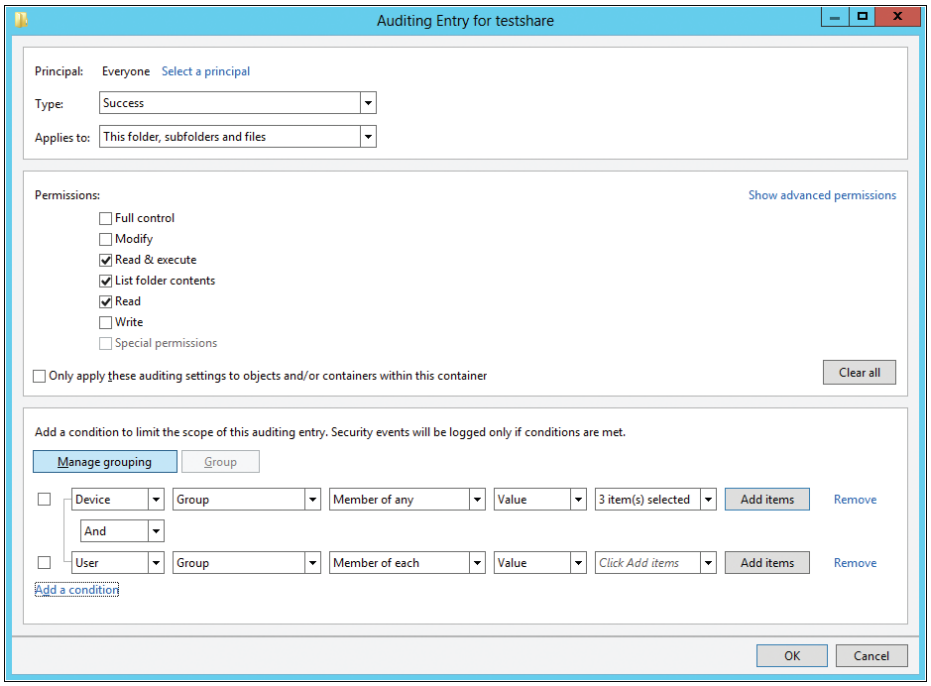
Just to give you a taste, however, let's look briefly at the redesigned Advanced Security Settings Editor that simplifies the configuration of auditing and determination of effective access. As in previous versions of Windows, the advanced permissions for a file or folder can be opened from the Security tab of the Properties dialog box for the file or folder. As you can see here, the Permissions tab of the Advanced Security Settings Editor in Windows Server 2012 and Windows 8 looks fairly similar to the one in previous versions of Windows:



However, the Effective Permissions tab of the Advanced Security Settings Editor in earlier versions of Windows has been replaced with a tab named Effective Access, which lets you choose not only the user or group being used for accessing the file or folder, but also the device:



The Auditing tab of the Advanced Security Settings Editor in earlier versions of Windows has been completely redesigned and now allows you to add auditing entries such as the one shown below that can include conditions to limit their scope:



BitLocker enhancements

BitLocker Drive Encryption is a data protection feature first introduced in Windows Vista and Windows Server 2008. BitLocker encrypts entire disk volumes to help safeguard sensitive business data from theft, loss, or inappropriate decommissioning of computers.

BitLocker has been enhanced in several ways in Windows Server 2012 and Windows 8:

- It's now easy to provision BitLocker before deploying the operating system onto systems. This can be done either from the Windows Preinstallation Environment (WinPE) or by using Microsoft Deployment Toolkit (MDT) 2012 to deploy your Windows installation.
- The process of encrypting a volume with BitLocker can occur more rapidly in Windows Server 2012 and Windows 8 by choosing to encrypt only the used disk space instead of both used and unused disk space, as was the only option in previous versions of Windows (see Figure 5-5).

- Standard users can change their BitLocker personal identification number (PIN) or password for the operating system volume or the BitLocker password for fixed data volumes. This change makes it easier to manage BitLocker-enabled clients because it means that users can choose PINs and passwords that are easier for them to remember.
- A new feature called BitLocker Network Unlock allows a network-based key protector to be used for automatically unlocking BitLocker-protected operating system volumes on domain-joined computers when these computers are restarted. This can be useful when you need to perform maintenance on computers and the tasks that you need to perform require a restart to be applied.
- BitLocker supports a new kind of enhanced storage device called Encrypted Hard Drive, which offers the ability to encrypt each block on the physical drive and not just volumes on the drive.
- BitLocker can now be used for failover clusters and cluster shared volumes.

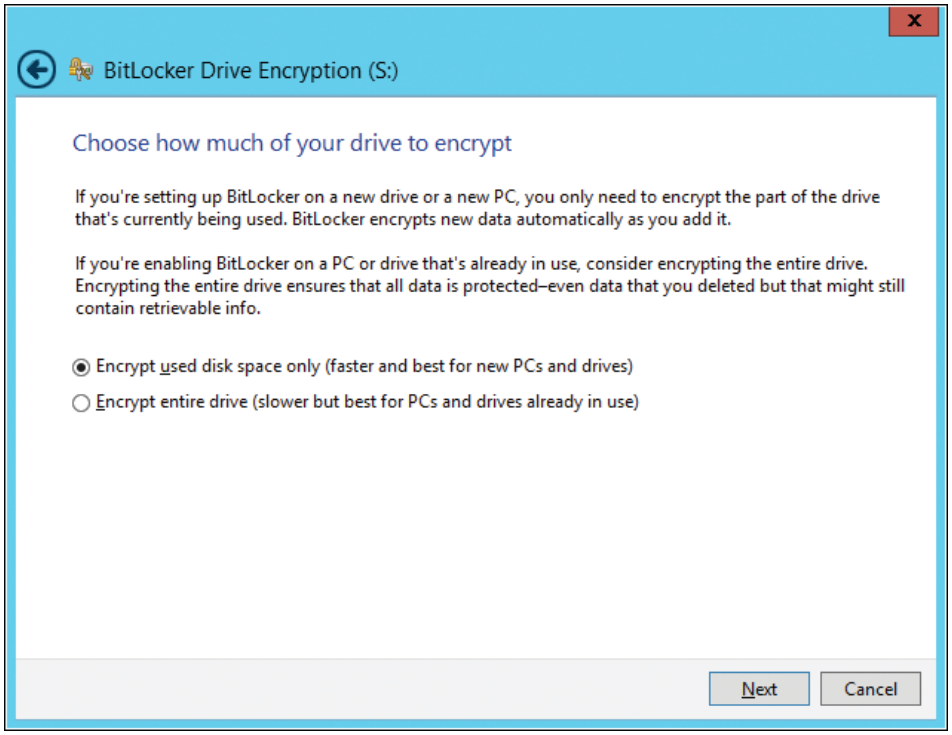


FIGURE 5-5 – Encrypting only used disk space when enabling BitLocker on a volume

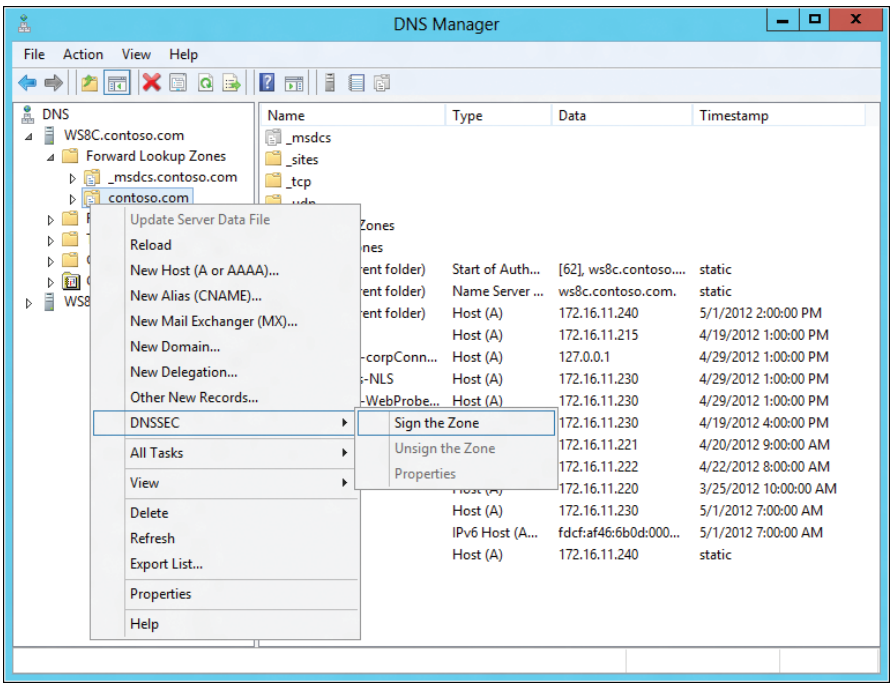
DNSSEC

Domain Name System Security Extensions (DNSSEC) is a suite of extensions that adds security to the DNS protocol. DNSSEC enables all the records in a DNS zone to be cryptographically signed and provides origin authority, data integrity, and authenticated denial of existence. DNSSEC is important because it allows DNS servers and resolvers to trust DNS responses by using digital signatures for validation to ensure that the responses they return have not been modified or tampered with in any way.

DNSSEC functionality was first included in the DNS Server role of Windows Server 2008 R2 and has been significantly enhanced in Windows Server 2012. The following are a few of the enhancements included in DNSSEC on Windows Server 2012:

- Support for Active Directory–integrated DNS scenarios, including DNS dynamic Updates in DNSSEC signed zones.
- Support for updated DNSSEC standards, including NSEC3 and RSA/SHA-2 and validation of records signed with updated DNSSEC standards (NSEC3, RSA/SHA-2).
- Automated trust anchor distribution through Active Directory with easy extraction of the root trust anchor and automated trust anchor rollover support per RFC 5011.
- An updated user interface with deployment and management wizards.
- Windows PowerShell support for configuring and managing DNSSEC.

Configuring DNSSEC on your DNS servers can now be done with the DNS Manager console. Simply right-click a zone and select Sign The Zone under the DNSSEC menu option:



This opens the Zone Signing Wizard, and by following the prompts, you can select the Key Master for the zone, configure a Key Signing Key (KSK) used for signing other keys, configure a Zone Signing Key (ZSK) used for signing the zone data, configure Next Secure (NSEC) resource records to provide authenticated denial of existence, configure distribution of Trust Anchors (TAs) and rollover keys, and configure values for DNSSEC signing and polling: