Microsoft

Identity and Access

Windows Server 2012

Table of contents

Copyright information

Identity and access enhancements in Windows Server 2012

Today's organizations need the flexibility to respond rapidly to new opportunities. They also need to give workers access to data and information—across varied networks, devices, and applications—while still keeping costs down. Innovations that meet these needs—such as virtualization, multitenancy, and cloud-based applications—help organizations maximize existing infrastructure investments, while exploring new services, improving management, and increasing availability.

While some factors—such as hybrid cloud implementations, a mobile workforce, and increased work with third-party business partners—add flexibility and reduce costs, they also lead to a more porous network perimeter. When organizations move more and more resources into the cloud, and grant network access to mobile workers and business partners outside the firewall, managing security, identity, and access control becomes a greater challenge. Adding to this challenge are increasingly stringent regulatory requirements, such as Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and Sarbanes-Oxley Act of 2002 (SOX), both of which increase the cost of compliance.

New and enhanced capabilities in Windows Server 2012 help organizations meet these challenges by making it easier and less costly to ensure secure access to valuable digital assets and comply with regulations. These identity and access improvements include:

- **Dynamic Access Control.** A new feature that enables automated information governance on file servers for compliance with business and regulatory requirements.
- **Active Directory Domain Services.** Storing directory data and managing communication between users and domains is improved by making it easier to deploy and virtualize domain services both locally and remotely, as well as simplifying management tasks.
- **DirectAccess**. Always-available connectivity to the corporate network now includes simplified deployment, a streamlined management experience, and improved scalability and performance.

This paper provides an introduction to these Windows Server 2012 identity and access technologies for IT professionals.

Protecting digital assets with previous versions of Windows Server

A major obstacle faced by IT professionals today is the sheer volume of repetitive work that needs to be done, particularly when large deployments of physical or virtual desktops are involved. Manual work is not only time-consuming, but it makes systems less secure by introducing many opportunities for errors and misconfiguration. In previous versions of Windows Server, Microsoft helped reduce this type of work.

For example, Windows Server 2008 R2 included the following improvements:

- **File Classification Infrastructure.** This new infrastructure for classifying files by tagging them enabled IT professionals to more easily manage unstructured data in files based on their organizational value.
- **Active Directory Domain Services.** As part of the Information Protection Solution, Active Directory Domain Services was improved to make domain controllers easier to deploy, both on-premises and in the cloud.
- **System Management and Security.** The Windows PowerShell 2.0 command-line interface enabled IT professionals to automate many common tasks involved in deploying and managing desktops.

Protecting digital assets with Windows Server 2012

With Windows Server 2012, Microsoft builds on these previous improvements by making it even easier to configure, manage, and monitor users, resources, and devices to improve security and automate auditing. In addition, Windows Server 2012 includes the following new and enhanced identity, access and data protection features:

- **Dynamic Access Control** gives you the ability to automatically control and audit access to files in file shares across your organization based on the characteristics of both the files and the users requesting access to them. It uses claims to achieve this high degree of access control specificity. Claims, contained in security tokens, consist of assertions about a user or device, such as name or type, department, or security clearance, for example. You can employ user claims, device claims, and file classification tags to centrally control and audit access to files, as well as use Rights Management Services (RMS) to protect information in files across your organization.
- **Active Directory Domain Services** is important in new hybrid cloud infrastructures because it supports the increased need for security, compliance, and access control. Furthermore, unlike many competing cloud services, which require users to have a separate set of credentials hosted with the provider, Active Directory Domain Services provides continuity between your on-premises and cloud resources so that users only need a single set of credentials no matter where the resources are located. A new deployment wizard and support for cloning virtual domain controllers makes Active Directory Domain Services easier to virtualize and simpler to deploy, both locally and remotely. The introduction of Active Directory Domain Services and Windows PowerShell 3.0 integration, and the ability to capture and record command-line syntax as you perform tasks in the Service Manager interface, improves automation of manual tasks. Other new features include desktop activation support using Active Directory Domain Services and Group Managed Service Accounts.
- **DirectAccess** allows nearly any user who has an Internet connection to more securely access corporate resources, such as email servers, shared folders, or internal websites, with the experience of being easily connected to the corporate network. Windows Server 2012 offers a new, unified management experience, allowing administrators to configure DirectAccess and legacy virtual private network (VPN) connections from one location. Other enhancements simplify deployment, and improve performance and scalability.

The remaining sections in this paper describe these new features in more detail.

Dynamic Access Control

Dynamic Access Control in Windows Server 2012 gives IT professionals new ways to control access to file data and monitor regulatory compliance. It provides next-generation authorization and auditing controls, along with classification capabilities that let you apply information governance to the unstructured data on file servers.

Until now, file security was handled at the file and folder level. IT professionals had little control over the way security was handled by users day to day. However, by using Dynamic Access Control, you can restrict access to sensitive files regardless of user actions by establishing and enforcing file security policy at the domain level, which is then enforced across all Windows Server 2012 file servers. For instance, if a development engineer accidentally posts confidential files to a publicly shared folder, those files can still be protected from access by unauthorized users.

In addition, security auditing is now more powerful than ever, and audit tools make it easier to prove compliance with regulatory standards, such as the requirement that access to Health and Biomedical Information (HBI) is appropriately guarded and regularly monitored.

Windows Server 2012 provides the following new and enhanced ways to control access to your files while providing authorized users the resources they need:

- **Classify.** Automatic and manual file classification using an improved file classification infrastructure. There are several methods to manually or automatically apply classification tags to files on file servers across the organization.
- **Control.** Central access control for information governance. You can control access to classified files by applying central access policies (CAPs). CAPs is a new feature of Active Directory that enables you to define and enforce very specific requirements for granting access to classified files. For example, you can define which users can have access to files that contain health information within the organization by using claims that might include employment status (such as full-time or contractor) or access method (such as managed computer or guest). You can even require two-factor authentication, such as that provided by smartcards. Central access control functionality includes the ability to provide automated assisted access-denied remediation when users have problems gaining access to files and shares.
- **Audit.** File access auditing for forensic analysis and compliance. You can audit access to files by using central audit policies, for example, to identify who gained (or tried to gain) access to highly sensitive information.
- **Protect.** Classification-based encryption. You can apply protection by using automatic RMS encryption for sensitive documents. For example, you can configure Dynamic Access Control to automatically apply RMS protection to all documents that contain HIPAA information. This feature requires a previously provisioned RMS environment.

Dynamic Access Control can provide these classification, control, audit, and protection capabilities because it is built on top of the following technologies:

- A new Windows authorization and audit engine that can process conditional expressions and central policies
- Kerberos support for user claims and device claims within Active Directory Domain Services

- Improvements to the File Classification Infrastructure
- RMS extensibility support so that partners can provide solutions that encrypt third-party files

You can use the Dynamic Access Control application programming interface (API) to extend these technologies and create custom classification tools, audit software, and more.

Classification

The first step in establishing file access policies that are more secure is to identify the files, and then classify them by applying tags to group files based on the information they contain. In Windows Server 2012, files are tagged in one of four ways:

- **By location.** When a file is stored on a file server, it inherits the tags from its parent folder. Folder tags are specified by the folder owner.
- **Manually.** Users and administrators can manually apply tags through the Windows 8 operating system File Explorer interface, or use data entry applications to apply them.
- **Automatically.** Automatic classification processes in Windows Server 2012 can automatically tag files, depending on the content of the file. This method is useful for applying tags to large numbers of files.
- **By application API.** Applications can use APIs to tag files that they manage. For example, tags can be specified by line-of-business (LOB) applications that store information on file servers, or by data management applications.

Control access

Controlling access to files is enforced by central access policies—sets of authorization policies that you centrally manage in Active Directory Domain Services, and deploy to file servers using Group Policy. You can use CAPs to comply with both organizational and regulatory requirements. CAPs help you to create more complete access policies by pairing information about files in the form of file tags with user and device claims.

In earlier versions of Windows Server, claims were used only by Active Directory Federation Services to authorize users in one domain to use applications in different, federated domains based on attributes submitted to Active Directory Federation Services. In Dynamic Access Control, the functionality of claims is essentially the same. In both cases, a claim consists of one or more statements (for example, name, identity, key, group, privilege, or capability) made about a user or device. These statements are contained in a security token that is issued and signed by a trusted partner or entity (such as Active Directory Domain Services) and used for authorizing that user or device to access a resource. You can create claim properties, either manually by using the Active Directory management tools or by using an identity management tool. In the case of Dynamic Access Control, the token is issued by Active Directory Domain Services and the resource to be accessed is a file.

In Dynamic Access Control, claims can be combined into logical policies that enable fine-grained control over arbitrarily-defined subsets of files. The following are two examples of situations where you might want to apply such policies:

- To obtain access to high-business-impact (HBI) information, a user might be required to be a full-time employee. In this scenario, you would have to do the following:
    - Identify and tag the files that contain HBI information.

    - Identify the full-time employees in your organization.
    - Create a central access policy that applies to all files that contain HBI on all file servers across the organization.
- To enforce an organization-wide requirement to restrict access to personally identifiable information (PII) in files so that only the file owner and members of the human resources (HR) department are allowed to view it, you might implement a policy that applies to all PII files independent of their location. In this scenario, you would have to do the following:
    - Identify and classify (tag) the files that contain PII.
    - Identify the group of HR members that are allowed to view PII information.
    - Create a CAP that applies to all files that contain PII on all file servers across the organization.

The motivation to deploy and enforce an authorization policy can arise for different reasons and from multiple levels of the organization. The following are some examples:

- **Organization-wide authorization policy.** Most commonly initiated from the information security office, this type of authorization policy arises from compliance or another high-level requirement that is relevant across the organization. For example, HBI files should be accessed by full-time employees only.
- **Departmental authorization policy.** Various departments in an organization may have special data-handling requirements that they want to enforce. For example, the finance department might want to limit access to finance servers for the finance employees.
- **Specific data-management policy.** This type of policy usually arises from compliance and organizational requirements for protecting information that is being managed, such as to prevent modification or deletion of files that are under retention or files that are under electronic discovery (eDiscovery).
- **Need-to-know policy.** This type of policy is typically used in conjunction with the policy types mentioned earlier. The following are two examples:
    - Vendors should be able to access and edit only those files that relate to a project that they are working on.
    - In financial institutions, information barriers are important so that analysts do not access brokerage information and brokers do not access analysis information.

The structure of central access policies

CAPs stored in Active Directory Domain Services act as security umbrellas that an organization applies across its file servers. These policies supplement—but do not replace—the local access policy, or discretionary access control list (DACL), applied to files and folders. For example, if a local DACL allows access to a specific user, but a CAP that is applied to the file denies access to the same user, the user cannot access the file. The reverse also applies: if a CAP allows access to a user but the local DACL denies it, the user cannot access the file. File access is only possible when permitted by both local DACLs and CAPs.

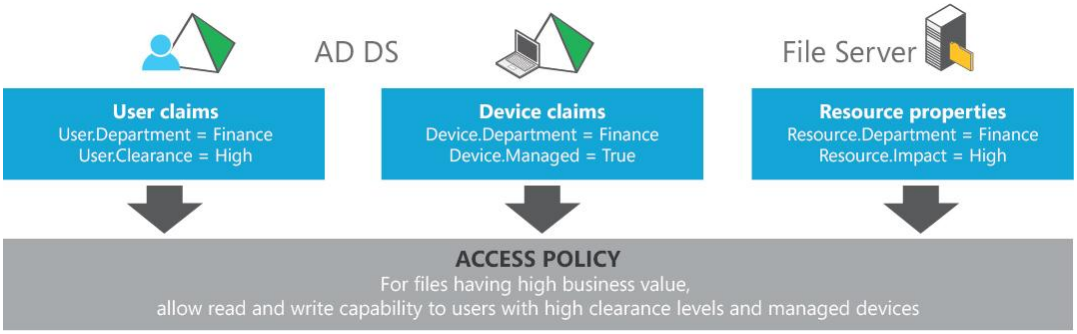
A CAP can contain many rules—each of which are evaluated and deployed as part of an overall CAP. Each rule contained in the CAP has the following logical parts:

- **Applicability.** This is a condition that defines which files the rule applies to. For example, the condition can define all files tagged as containing personal information.

- **Access conditions.** This is a list of one or more access control entries (ACEs) that define who can access the data, such as allow read and write access if the user has a high clearance level and their device is a managed device.

Figure 1 shows the components of a CAP rule, and how they can be combined to create very explicit data access policies.

Figure 1: CAP components



Central access policies and file servers

Figure 2 shows the interrelationships between Active Directory Domain Services, where CAPs, user claims, and property definitions are defined and stored; the file server, where these policies are applied; and the user, who is trying to gain access to a file on the file server.

Figure 2: CAP structure

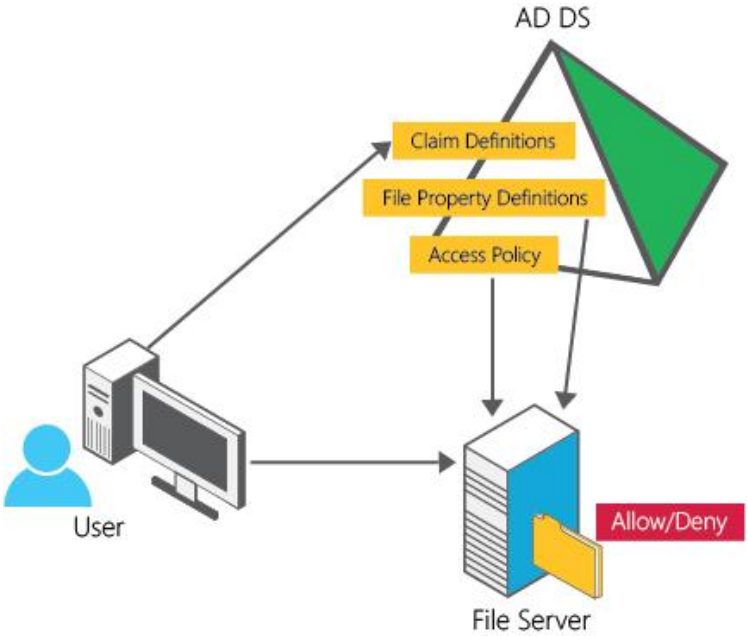
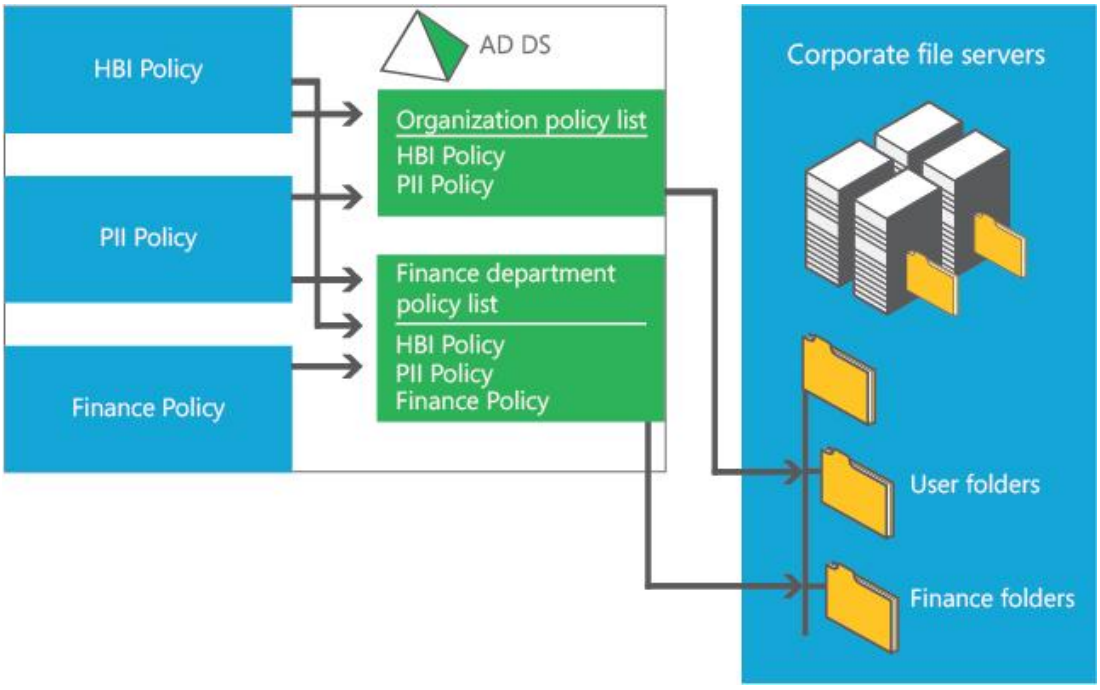


Figure 3 shows how you can combine different rules (blue boxes) into a CAP (green boxes) that can then be applied to shares on file servers across the organization.

Figure 3: Combining multiple policies into policy lists and applying them to resources



Policy staging

When you want to change a policy, Microsoft Windows 2012 lets you test a proposed policy that runs parallel to the current policy so that you can identify the consequences of the new policy without enforcing it. This feature, which is known as policy staging, lets you measure the effects of a new policy in the production environment.

When policy staging is enabled, Windows Server 2012 continues to use the current policy to authorize user access to files. However, if the access allowed by the proposed policy differs from that of the current policy, the system logs an event with the details. You can use the logged events to determine whether the policy has to be changed or is ready to be deployed.

Access-denied remediation

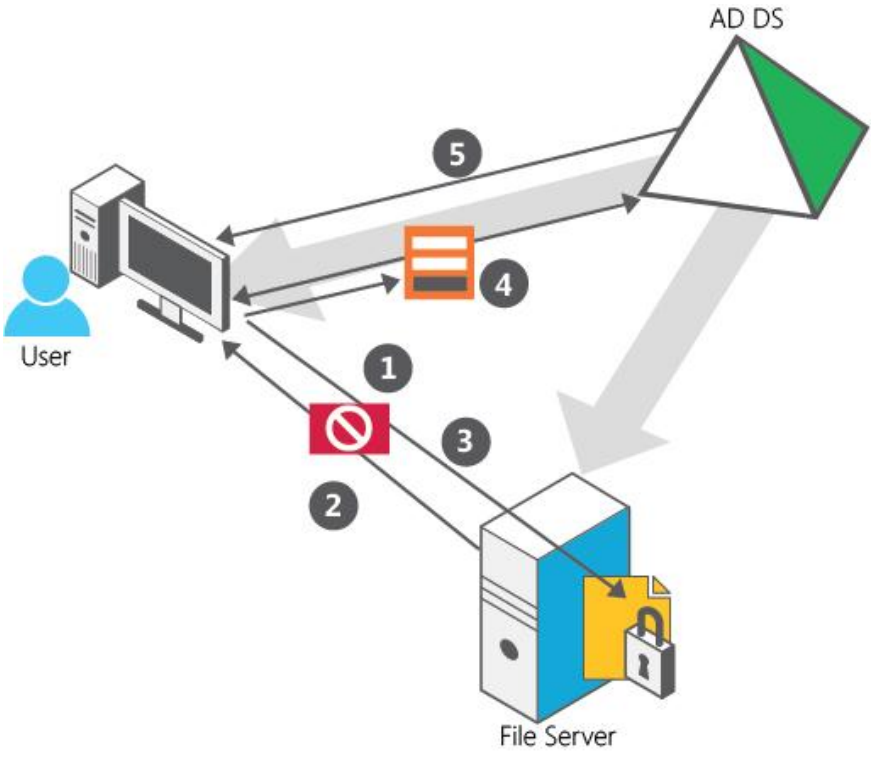
Of course, denying access is only part of an effective central access control strategy, and sometimes access must be granted after at first being denied. Today, when access is denied, the user does not receive additional information on how to get access. This causes a lot of pain for both users and help desk or IT administrators. To mitigate this problem, assisted access-denied remediation in Windows Server 2012 enables you to provide the user with additional information and the opportunity to send an access request email message to the appropriate owner. Access-denied remediation reduces the need for manual intervention by providing the following three different processes for granting users access to resources:

- **Self-remediation.** If users can determine what the issue is and correct the problem so that they can get the requested access, the impact on the organization is low, and minimal special exceptions are needed in the organization policy. Windows Server 2012 helps you to author a general access-denied message to help users self-remediate when access is denied. This message can include URLs to direct the users to self-remediation websites provided by the organization.

- **Remediation by the file owner.** Windows Server 2012 enables you to create a distribution list of file or folder owners so that users can directly connect with them to request access. This resembles the Microsoft SharePoint model, where the share owner receives a user's request for access to a file. Remediation can range from adding user rights to the appropriate file or folder to editing share permissions. For example, if a local DACL on a file allows access to a specific user but a CAP restricts access to the same user, the user will be unable to gain access to the file. In Windows Server 2012 when a user requests access to a file or a folder, an email message with the request details is sent to the file owner. When additional help is required, the file owner can in turn forward this information to the appropriate IT administrator.
- **Remediation by help desk and file server administrators.** When the user cannot self-remediate an access problem and the file owner cannot help, the issue can be corrected manually by the help desk or file server administrator. This is the most costly and time-consuming remediation. Windows Server 2012 provides a UI to view the effective permissions for users on a file or a folder so that it is easier to troubleshoot access issues.

Figure 4 shows the series of events involved in access-denied remediation.

Figure 4: Access-denied remediation



Access denied remediation provides a user access to a file when it has been initially denied:

1. The user attempts to read a file.
2. The server returns an "access denied" error message because the user has not been assigned the appropriate claims.
3. On a computer running Windows 8, Windows retrieves the access information from the File Server Resource Manager on the file server, and presents a message with the access remediation options, which may include a link for requesting access.
4. When the user has satisfied the access requirements (for example, by signing a non-disclosure agreement, or providing other authentication) the user's claims are updated.
5. The user can access the file.

Security auditing

Security auditing of file access is one of the most powerful tools to help maintain the security of an organization. A key goal of security auditing is regulatory compliance. For example, industry standards such as SOX, HIPAA, and Payment Card Industry (PCI) require organizations to follow a strict set of rules related to data security and privacy. Security audits help establish the presence or absence of such policies and thereby prove compliance or noncompliance with these standards. Additionally, security audits help detect anomalous behavior, identify and reduce gaps in security policy, and deter irresponsible behavior by creating a trail of user activity that can be used for forensic analysis. Audit policy requirements typically arise from three levels:

- **Information security.** File access audit trails are frequently used for forensic analysis and intrusion detection. The ability to monitor specified events regarding access to high-value information lets organizations significantly improve their response time and investigation accuracy.
- **Organizational policy.** For example, organizations regulated by PCI standards can have a central policy to monitor access to all files that are marked as containing credit card information and PII, or organizations may want to monitor all unauthorized attempts to view information about their projects.
- **Departmental policy.** For example, the finance department may require that the ability to modify certain finance documents (for example, a quarterly earnings report) be restricted to the finance department, and thus want to monitor all other attempts to change these documents. Additionally, the compliance department may want to monitor all changes to central policies and policy constructs such as user, computer, and resource attributes.

One of the biggest considerations for security audits is the cost of collecting, storing, and analyzing audit events. If the audit policies are too broad, the volume of audit events that are collected increases, making it more time-consuming and expensive to identify the most important audit events. However, if the audit policies are too narrow, you risk missing important events.

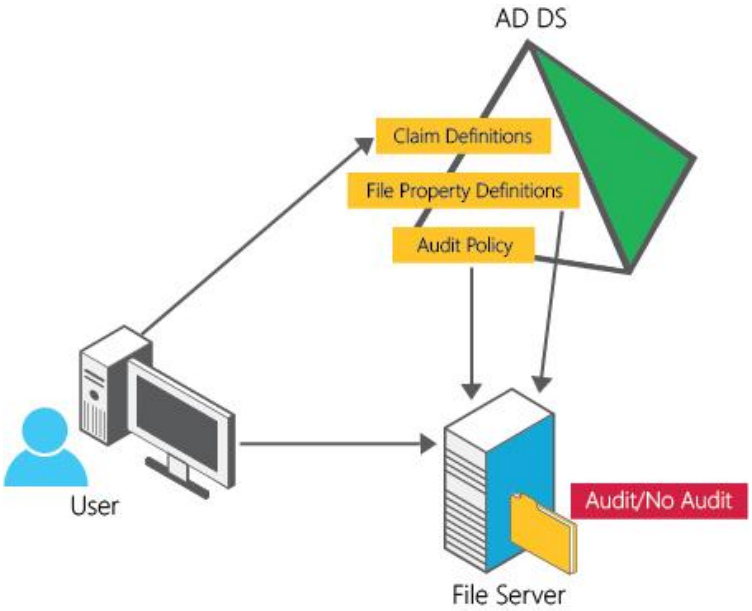
With Windows Server 2012, you can author audit policies by combining claims and resource properties (file tags). This leads to audit policies that are richer, more selective, and easier to manage by reducing the number of potential audit events to those most relevant to your auditing requirements. It enables scenarios that until now were either impossible, or too difficult to implement. The following are examples of such audit policies:

- Audit everyone who does *not* have a high security clearance and yet tries to access an HBI document. In this example, "high security clearance" is a claim, and "HBI" is a file tag. The audit policy triggers an event when a user who does not have a high security clearance tries to gain access to an HBI document.
- Audit all vendors when they try to access documents related to projects that they are not working on. In this example, the user's claims include an employment status of "vendor" as well as a list of projects the user is authorized to work on. In addition, each file in the organization to which a vendor could potentially have access was tagged to identify its associated project. The audit policy triggers an event if a vendor tries to access a project file, and none of the projects in the vendor's claim list matches the file's project tag.

To view and query audit events you can use familiar tools such as Event Viewer on the local server or Microsoft System Center Operations Manager Audit Collection Service across multiple servers. The Dynamic Access Control API also provides support for integrating DAC audit events into third- party audit software consoles. These tools help you to answer such questions as, "Who is accessing my HBI data?" or "Was there an unauthorized attempt to access sensitive data?"

Figure 5 shows the file-access auditing workflow and the interrelationships between Active Directory, where claim types and resource properties are created; Group Policy, where the audit policies are defined and stored; the file server, where policies and resource properties are applied as file tags; and the user, who is trying to access information on the file server.

Figure 5: Central auditing workflow



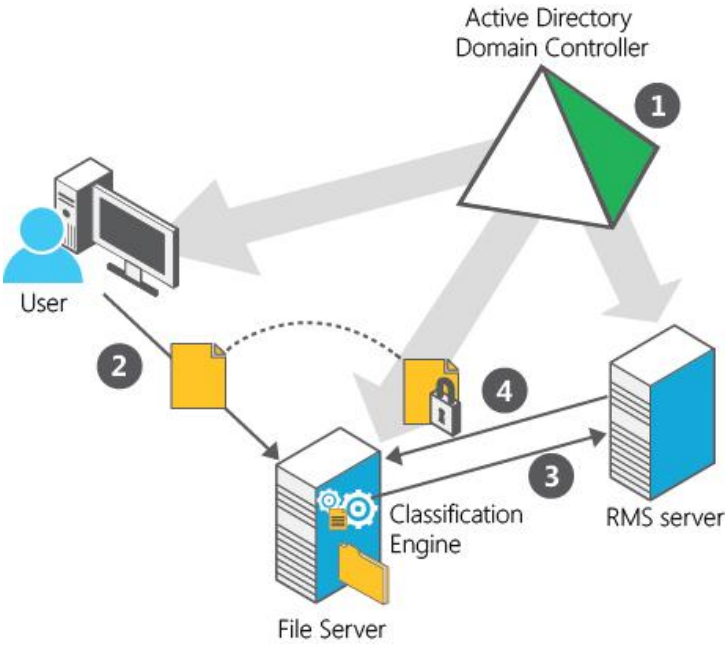
Protection

Protecting sensitive information involves reducing risk for the organization. Various regulations, such as HIPAA or Payment Card Industry Data Security Standard (PCI-DSS), require encryption of information, and there are many business reasons to also encrypt sensitive information. However, encryption is expensive and can adversely affect productivity. Therefore, organizations usually have different approaches and priorities for it.

To support this scenario, Windows Server 2012 lets you automatically encrypt sensitive Microsoft Office files based on their classification. This is done through automatic file management of tasks that are running on the server, and that start RMS protection for sensitive Microsoft Office documents a few seconds after the file is identified as being a sensitive file on the file server (continuous file management tasks).

RMS encryption provides another layer of protection for files. If a person with access to a sensitive file inadvertently sends that file out through email, the file is still protected by the RMS encryption. Nearly any user who wants to gain access to the file must first authenticate to an RMS server to receive the decryption key. This process is illustrated in Figure 6.

Figure 6: Classification-based RMS protection



Dynamic Access Control allows sensitive information to be automatically protected using Active Directory RMS:

1. A rule is created to automatically apply RMS protection to nearly any file that contains the word "confidential."
2. A user creates a file with the word "confidential" in the text and saves it.
3. The RMS Dynamic Access Control classification engine, following rules set in the CAP, discovers the document with the word "confidential," and initiates RMS protection accordingly.
4. The RMS template and encryption are applied to the document on the file server, and it is classified and encrypted.

Note that support for third-party file formats is available through third-party vendors. Also be aware that if a file is RMS-protected, data management features such as search- or content-based classification are no longer available for that file.

Active Directory Domain Services

Active Directory has been at the center of IT infrastructure for more than 10 years, and its features, adoption, and business value have grown with each new release. Today, most Active Directory infrastructure remains on-premises, but the trend toward cloud computing is creating the need to deploy Active Directory in the cloud as well.

New hybrid infrastructures are emerging, and Active Directory Domain Services must support the needs of new and unique deployment models that include services hosted entirely in the cloud, services that consist of both cloud and on-premises components, and services that remain exclusively on-premises. These new hybrid models further increase the importance of security and compliance, and compound the already complex and time-consuming exercise of ensuring that access to information and services is appropriately audited, and accurately expresses the intent of the organization.

Active Directory Domain Services in Windows Server 2012 addresses these emerging needs with features that help you more quickly and easily deploy domain controllers both on-premises and in the cloud, audit and authorize access to files, and perform administrative tasks at scale—either locally or remotely—through consistent graphical and scripted management interfaces. Active Directory Domain Services in Windows Server 2012 improvements include the following:

- Simpler on-premises deployment, which replaces DCpromo with a new, streamlined domain controller configuration wizard that is integrated with Server Manager and built on Windows PowerShell 3.0.
- More rapid deployment of virtual domain controllers through cloning.
- Better support for public and private cloud implementations through safer virtualization of domain controllers.
- A consistent graphical and scripted management interface that enables you to perform tasks in the Active Directory Administrative Center and automatically generate the syntax required to fully automate the task in Windows PowerShell 3.0.
- Functionality that uses Active Directory to simplify client activations.
- Group Managed Services Accounts for groups of servers such as server clusters that share their identity and service principal name.

Using these features, you can effectively and efficiently deploy and manage Active Directory Domain Services over multiple servers, locally and around the globe.

Simplified deployment

The new Active Directory Domain Services configuration wizard in Windows Server 2012 integrates all the required steps to deploy new domain controllers into a single graphical interface. It requires only one organization-level credential, and can prepare the forest or domain by remotely targeting the appropriate operations master role holders. It conducts extensive prerequisite validation tests that minimize the opportunity for errors that might have otherwise blocked or slowed the installation. The wizard is built on

Windows PowerShell 3.0, and is integrated with Server Manager. It can configure multiple servers and remotely deploy domain controllers, resulting in a deployment experience that is simpler, more consistent, and less time-consuming.

The Active Directory Domain Services configuration wizard includes the following features:

- **Adprep integration into the Active Directory Domain Services deployment process.** This reduces the time that is required to deploy Active Directory Domain Services, and reduces the chances for errors that might block domain controller promotion.
- **Remote execution against multiple servers.** This greatly reduces the probability of administrative errors and the overall time required for deployment, especially when you deploy multiple domain controllers across global countries/regions and domains.
- **Prerequisite validation.** This identifies potential errors before the deployment begins. You can correct error conditions before they occur without the concerns that result from a partially complete upgrade.
- **Configuration pages grouped in a sequence that mirror the requirements of the most common promotion options**, with related options grouped in fewer wizard pages. This provides better context for making installation choices, and reduces the number of steps and time that is required to complete domain controller installation.
- **Options that were specified in the wizard are exported into a Windows PowerShell script.** This simplifies the process of automating later Active Directory Domain Services installations through automatically generated Windows PowerShell scripts.

Deployment with cloning

With earlier versions of Windows Server, administrators found that deploying virtualized replica domain controllers was as labor-intensive as deploying physical domain controllers. In theory, this should not be the case because virtualization brings the possibility of cloning domain controllers, instead of performing all deployment steps separately for each one. Domain controllers within the same domain/forest are nearly identical, except for name, IP address, and so on. Therefore virtualization should be fairly easy. With earlier versions of Windows Server, however, deployment still involved many (redundant) steps.

With Windows Server 2012, you can deploy replica virtual domain controllers by "cloning" existing virtual domain controllers. This significantly reduces the number of steps and time involved by eliminating repetitive deployment tasks and also lets you fully deploy additional domain controllers that are authorized and configured for cloning by the Active Directory domain administrator.

Safer virtualization of domain controllers

Active Directory Domain Services has been successfully virtualized for several years, but features present in most hypervisors can invalidate strong assumptions made by the Active Directory replication algorithms—primarily, the assumption that the logical clocks used by domain controllers to determine relative levels of convergence only go forward in time. Windows Server 2012 includes improvements that enable virtual domain controllers to detect when snapshots are applied to a virtual machine or a virtual machine is copied, causing the domain controller clock to go backward in time.

This new functionality is made possible by a virtual domain controller that uses a unique ID exposed by the hypervisor, called the virtual machine GenerationID. The virtual machine GenerationID changes when

the virtual machine experiences an event that affects its position in time. The virtual machine GenerationID is exposed to the virtual machine's address space within its Basic Input Output System (BIOS), and is made available to its operating system and applications through a Windows Server 2012 driver.

During startup, and before completing any transactions, a Windows Server 2012 virtual domain controller compares the current value of the virtual machine GenerationID against the value that it stored in the directory. A mismatch is interpreted as a "rollback" event, and the domain controller uses safeguards in Active Directory Domain Services that are new to Windows Server 2012. The safeguards enable the virtual domain controller to converge with other domain controllers and also prevent it from creating duplicate security principals.

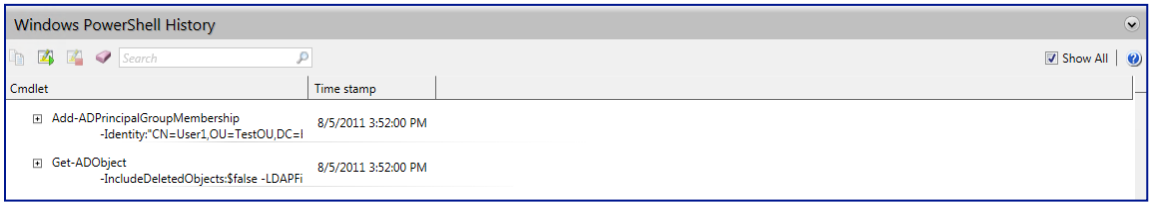
For Windows Server 2012 virtual domain controllers to gain this extra level of protection, the virtual domain controller must be hosted on a virtual machine GenerationID–aware hypervisor such as Windows Server 2012 Hyper-V.

Windows PowerShell script generation

The Windows PowerShell cmdlets for Active Directory are a set of tools that help you to manipulate and query Active Directory Domain Services by using Windows PowerShell commands, and to create scripts that automate common administrative tasks. The Active Directory Administrative Center uses these cmdlets to query and modify Active Directory Domain Services according to the actions that are performed within the Active Directory Administrative Center UI.

In Windows Server 2012, the Windows PowerShell History viewer in the Active Directory Administrative Center, as shown in the following figure, lets an administrator view the Windows PowerShell commands as they execute in real time. For example, when you create a new fine-grained password policy, the Active Directory Administrative Center displays the equivalent Windows PowerShell commands in the Windows PowerShell History viewer task pane. You can then use those commands to automate the process by creating a Windows PowerShell script.

Figure 7: Windows Server 2012 Windows PowerShell History viewer



By combining scripts with scheduled tasks, you can automate everyday administrative duties that were previously completed manually. Because the cmdlets and required syntax are created for you, very little experience with Windows PowerShell is required. Because the Windows PowerShell commands are the same as the ones executed by the Active Directory Administrative Center, they should replicate their original function exactly.

Active Directory for client activation

Client licensing is an additional labor-intensive task that can be eased with the improved Active Directory functionality in Windows Server 2012. With earlier versions of Windows Server, volume licensing for Windows and Office required Key Management Service (KMS) servers. These entail several drawbacks:

- They require remote procedure call (RPC) network traffic, which some organizations want to disable.
- Additional training is necessary.
- The turnkey solution only covers approximately 90 percent of deployments.
- There is no graphical administration console, so the process is more complex than it needs to be.
- KMS does not support any kind of authentication, because the Microsoft Software License terms prohibit the customer from connecting the KMS server to any external network.
- Access to the service means that anyone can be activated.

This situation is improved in Windows Server 2012 because it helps leverage your existing Active Directory infrastructure to help you activate clients. No additional computers are required, and no RPC is needed. The activation uses Lightweight Directory Access Protocol (LDAP) exclusively and includes support for read-only domain controllers (RODCs).

In this activation process, the only data written back to the directory is what's required for the installation and service. Activating the initial customer-specific volume license key (CSVLK) requires the following:

- One-time contact with Microsoft Activation Services over the Internet (identical to retail activation).
- A key entered using volume activation server role or the command line.
- Repetition of the activation process for additional forests (by default, up to six times).

Another benefit of Active Directory integration is that the activation object is maintained in the configuration partition. This represents proof-of-purchase, and means that the activated computers can be a member of any domain in the forest. And, perhaps most important, with Active Directory activation integration, all computers that are running Windows 8 will automatically activate. This represents a significant workflow improvement over earlier versions of Windows Server, and is achieved by using additional resources that are provided in Active Directory.

Group-managed service accounts

Managed service accounts (MSAs) were a new type of account introduced in Windows Server 2008 R2 and Windows 7 to enhance the service isolation and manageability of network applications such as Microsoft SQL Server and Exchange Server. They eliminate the need for an administrator to manually administer the service principal name (SPN) and credentials for domain-level service accounts.

Until now, however, this feature has not been available for server groups, such as clusters, that share their identity and service principal name. This creates a problem for IT administrators.

When a client connects to a service hosted on a server farm using network load balancing (NLB) or some other method where all the servers appear to be the same service to the client, authentication protocols supporting mutual authentication, such as Kerberos, cannot be used unless all the instances of the

services use the same principal (which means that they use the same passwords/keys to prove their identity). Service administrators find managing this to be difficult.

When a client connects to a shared service it cannot know in advance which instance it will connect to, so the authentication must succeed regardless of the host. This requires that each instance of the server use the same security principal. Today, services have four principals to choose from, each with their own issue: computer, virtual, managed service, or user.

Computer, MSA, or virtual accounts cannot be shared across multiple systems. This only leaves the option of using a user account for services on server farms. Because user accounts do not have password management, each organization then has to create a solution to update keys for the service in Active Directory, and distribute the keys to all instances of the services. This is expensive and problematic.

By creating a group MSA, services or service administrators do not have to manage password synchronization between service instances. The group MSA supports credential reset, hosts that are kept offline for some time, and seamless management of member host group management for all instances of a service.

- You can deploy single-identity server farms/clusters on Windows Server 2012 to which domain clients can authenticate without knowing which instance of a server farm/cluster they are connecting.
- You can configure services by using Service Control Manager to use a shared domain identity that automatically manages passwords.
- As soon as the group MSA is created, a domain administrator can delegate management of the group MSA to a service administrator.
- You can deploy single identity server farms/clusters on Windows Server 2012 servers running Windows 8 for identities in mixed-mode domains.

DirectAccess and remote access

Windows Server 2012 provides an integrated remote access solution that is easier to deploy and manage when compared to earlier versions that relied on multiple tools and consoles. Employees can gain access to corporate network resources while they work remotely, and IT administrators can manage corporate computers in Active Directory that are located outside the internal network. Windows Server 2012 accomplishes this by integrating two existing remote access technologies: DirectAccess for automatic, transparent connectivity, and traditional virtual private networks (VPNs) for compatibility.

DirectAccess was introduced in Windows 7 and Windows Server 2008 R2 to help remote users to more securely access shared resources, websites, and applications on an internal network without connecting to a VPN. DirectAccess establishes bidirectional connectivity with an organization's corporate network every time a DirectAccess-enabled computer is connected to the Internet. Users never have to think about connecting to the corporate network, and IT administrators can manage remote computers outside the office, even when the computers are not connected to the VPN. Windows Server 2012 continues to offer

this transparent connection to the corporate network, with improvements around deployment, management, performance, and scalability. Remote access improvements in Windows Server 2012 include:

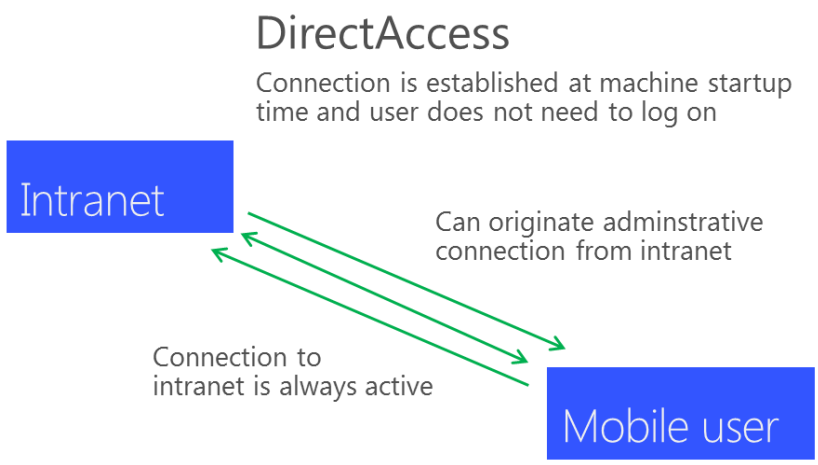
- **Integrated remote access:** DirectAccess and VPN can be configured together in the Remote Access Management console by using a single wizard. The new role allows easier migration of Windows 7 Routing and Remote Access service (RRAS) and DirectAccess deployments.
- **Cross-premises connectivity.** Windows Server 2012 provides a highly cloud-optimized operating system. VPN site-to-site functionality in remote access provides cross-premises connectivity between enterprises and hosting service providers, including Azure.
- **Improved management experience:** By using the new Remote Access Management console, you can configure, manage, and monitor multiple DirectAccess and VPN remote access servers in a single location. The console provides a dashboard that allows you to view information about server and client activity.
- **Simplified deployment:** In simple deployments, you can configure DirectAccess without being required to set up a certificate infrastructure. DirectAccess clients can now authenticate themselves by using only Active Directory credentials; no computer certificate is required.
- **New deployment scenarios.** Remote access in Windows Server 2012 includes integrated deployment for several scenarios that required manual configuration in Windows Server 2008 R2. These include force tunneling (which sends all traffic through the DirectAccess connection), Network Access Protection (NAP) compliance, support for locating the nearest remote access server from DirectAccess clients in different geographical locations, and deploying DirectAccess for only remote management.
- **Improved scalability:** Remote access in Windows Server 2012 offers several scalability improvements than support more users while providing better performance and lower costs. These include support for network load balancing, better performance in virtualized environments, and underlying platform improvements.

Integrated remote access

With **DirectAccess**, users who have an Internet connection can more securely access corporate resources, such as email servers, shared folders, or internal websites, with the experience of being easily connected to the corporate network.

DirectAccess transparently connects client computers to the internal network whenever the computer connects to the Internet, even before the user logs on, as shown in the following figure. This transparent, automatic connectivity means that access is provided without additional steps or configuration required by the user.

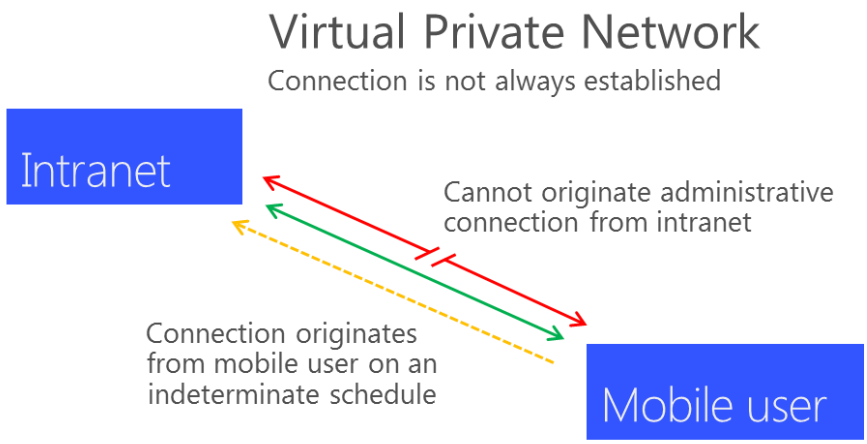
Figure 8: DirectAccess connection architecture



DirectAccess also lets you easily monitor connections and remotely manage DirectAccess client computers on the Internet.

At the same time, RRAS provides traditional client VPN connectivity for unmanaged client computers, such as computers running client operating systems earlier than Windows 7. In addition, RRAS site-to-site VPN provides connectivity between VPN servers, as shown in the following figure.

Figure 9: VPN connection architecture



The remote access server role in Windows Server 2012 integrates DirectAccess and RRAS VPN. You can configure DirectAccess and VPNs together in the Remote Access Management console by using a single wizard. You also can configure other RRAS features by using the legacy RRAS management console. The new role allows easier migration of Windows 7 RRAS and DirectAccess deployments, and it provides new features and improvements.

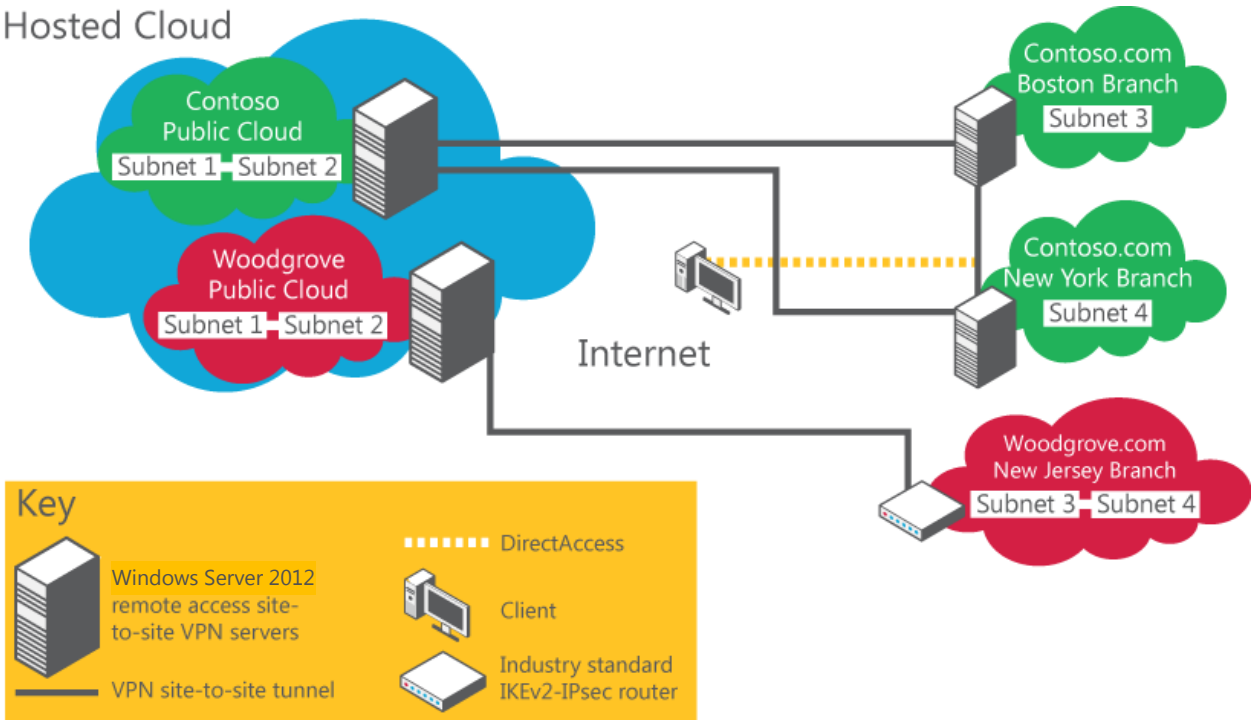
Cross-premises connectivity

Windows Server 2012 provides an operating system that is highly optimized for the cloud. VPN site-to-site functionality in remote access provides cross-premises connectivity between enterprises and hosting service providers. Cross-premises connectivity enables organizations to connect to private subnetworks in a hosted cloud network. It also enables connectivity between geographically separate enterprise locations.

With cross-premises connectivity, you can use existing networking equipment to connect to hosting providers by using the industry standard Internet Key Exchange version 2 (IKEv2) and IP security (IPsec) protocol.

Figure 10 demonstrates how these two organizations implement cross-premises deployments by using Windows Server 2012.

Figure 10: Example of a cross-premises deployment



The following steps describe the procedures that Contoso and Woodgrove use for the cross-premises deployment shown in Figure 10:

1. Contoso.com and Woodgrove.com offload some of their enterprise infrastructure in a hosted cloud.
2. The hosting provider provides private clouds for each organization.
3. In the hosted cloud, virtual machines running Windows Server 2012 are configured as remote access servers running site-to-site VPN.
4. In each hosted private cloud, a cluster of two or more remote access servers is deployed to provide continuous availability and failover.
5. Contoso.com has two branch office locations. In each location, a Windows Server 2012 remote access server is deployed to provide a cross-premises connectivity solution to the hosted cloud and between the branch offices.
6. The Contoso.com branch office computers running the unified remote access server role in Windows Server 2012 are also configured as DirectAccess servers in a multisite deployment. DirectAccess clients can access any resource in the Contoso.com public cloud or Contoso.com branch offices from nearly any location on the Internet.
7. Woodgrove.com can use existing routers to connect to the hosted cloud because cross-premises functionality in Windows Server 2012 complies with IKEv2 and IPsec standards.

Improved management experience

By using the new Remote Access Management console, you can configure, manage, and monitor multiple DirectAccess and VPN remote access servers in a single location. The console provides a dashboard that allows you to view information about server and client activity. You can also generate reports for additional, more detailed information. Operations status provides comprehensive monitoring information about specific server components. Event logs and tracing help diagnose specific issues. By using client monitoring, you can see detailed views of connected users and computers, and you can even monitor which resources the clients are accessing. Accounting data can be logged to a local database or a Remote Authentication Dial-In User Service (RADIUS) server.

In addition to the Remote Access Management console, you can use Windows PowerShell command-line interface tools and automated scripts for remote access setup, configuration, management, monitoring, and troubleshooting.

On client computers, users can access the Network Connectivity Assistant application, integrated with Windows Network Connection Manager, to see a concise view of the DirectAccess connection status and links to corporate help resources, diagnostics tools, and troubleshooting information. Users can also enter one-time password (OTP) credentials if OTP authentication for DirectAccess is configured.

Easier deployment

The enhanced installation and configuration design in Windows Server 2012 allows you to set up a working deployment without changing your internal networking infrastructure. In simple deployments, you can configure DirectAccess without setting up a certificate infrastructure. DirectAccess clients can now authenticate themselves by using only Active Directory credentials; no computer certificate is required. In

addition, you can choose to use a self-signed certificate created automatically by DirectAccess for IP-HTTPS and for authentication of the network location server.

To further simplify deployment, DirectAccess in Windows Server 2012 supports access to internal servers that are running IPv4 only. An IPv6 infrastructure is not required for DirectAccess deployment.

Improved deployment scenarios

The remote access server role in Windows Server 2012 includes additional enhancements, including integrated deployment for several scenarios.

- With Windows Server 2012, you can now configure a DirectAccess server with two network adapters at the network edge or behind an edge device, or with a single network adapter running behind a firewall or network address translation device. The ability to use a single adapter removes the requirement to have dedicated public IPv4 addresses for DirectAccess deployment. With this configuration, clients connect to the DirectAccess server by using IP-HTTPS.
- In Windows Server 2012, you can configure remote access servers in a multisite deployment that allows users in dispersed geographical locations to connect to the multisite entry point closest to them. You can distribute and balance traffic across the multisite deployment by using an external global load balancer. To support fault tolerance, redundancy, and scalability, DirectAccess servers can now be deployed in a cluster configuration that uses Windows load balancer or an external hardware load balancer.
- DirectAccess in Windows Server 2012 adds support for two-factor authentication that uses an one-time password (OTP). For two-factor smart card authentication; Windows Server 2012 supports the use of Trusted Platform Module (TPM)-based virtual smart card capabilities that are available in Windows 8. The TPM of client computers can act as a virtual smart card for two-factor authentication, which reduces the overhead and costs incurred in smart card deployment.
- Windows Server 2012 also introduces the ability of computers to join an Active Directory domain and receive domain settings remotely via the Internet. By using this capability, you will find that deployment of new computers in remote offices and provisioning of client settings to DirectAccess clients is easier. You can configure client computers running Windows 8, Windows 7, and Windows Server 2008 R2 as DirectAccess clients. Clients running Windows 8 have access to all DirectAccess features, and they have an improved experience when connecting from behind a proxy server that requires authentication. Clients not running Windows 8 have the following limitations:
    - They must download and install the DirectAccess Connectivity Assistant tool.
    - They require a computer certificate for authentication.
    - In a multisite deployment, they must be configured to always connect through the same entry point.

Scalability improvements

Remote access offers several scalability improvements, including support for more users with better performance and lower costs:

- You can cluster multiple remote access servers for load balancing, continuous availability, and failover. Cluster traffic can be load-balanced by using NLB or a third-party load balancer. Servers can be added to or removed from the cluster with few interruptions to the connections in progress.
- The remote access server role takes advantage of Single Root I/O Virtualization (SR-IOV) for improved I/O performance when running on a virtual machine. In addition, remote access improves the overall scalability of the server host with support for IPsec hardware offload capabilities, available on many server interface cards that perform packet encryption and decryption in hardware.
- Optimization improvements in IP-HTTPS use the encryption that IPsec provides. This optimization, combined with the removal of the Secure Sockets Layer (SSL) encryption requirement, increases scalability and performance.

With the new DirectAccess and remote access enhancements, you can easily provide more secure remote access connections for your users, as well as log reports for monitoring and troubleshooting those connections. The new features in Windows Server 2012 support deployments in dispersed geographical locations, improved scalability with continuous availability, and improved performance in virtualized environments.

Summary

Identity and access control are two areas that require critical attention from IT professionals, particularly when you move to virtualized and private or public cloud environments. Windows Server 2012 makes these tasks easier by offering simple but powerful new and enhanced features to provide intelligent, auditable security; easier deployment and management of Active Directory Domain Services; and secure, always-on connectivity to the corporate resources.

For more information, see the Windows Server 2012 website at: http://www.microsoft.com/windowsserver2012/.

List of charts, tables, and figures