Designing the Logical Structure for Windows Server AD DS

Updated: April 26, 2012

Applies To: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012

Active Directory Domain Services (AD DS) in the Windows Server operating system enables organizations to create a scalable, secure, and manageable infrastructure for user and resource management. It also enables them to support directory-enabled applications.

A well-designed Active Directory logical structure provides the following benefits:

- Simplified management of Microsoft® Windows®–based networks that contain large numbers of objects
- A consolidated domain structure and reduced administration costs
- The ability to delegate administrative control over resources, as appropriate
- Reduced impact on network bandwidth
- Simplified resource sharing
- Optimal search performance
- Low total cost of ownership

A well-designed Active Directory logical structure facilitates the efficient integration of such features as Group Policy; desktop lockdown; software distribution; and user, group, workstation, and server administration into your system. In addition, a carefully designed logical structure facilitates the integration of Microsoft and non-Microsoft applications and services, such as Microsoft Exchange Server, public key infrastructure (PKI), and a domain-based distributed file system (DFS).

When you design an Active Directory logical structure before you deploy AD DS, you can optimize your deployment process to best take advantage of Windows Server 2008 Active Directory features. To design the Active Directory logical structure, your design team first identifies the requirements for your organization and, based on this information, decides where to place the forest and domain boundaries. Then, the design team decides how to configure the Domain Name System (DNS) environment to meet the needs of the forest. Finally, the design team identifies the organizational unit (OU) structure that is required to delegate the management of resources in your organization

Understanding the Active Directory Logical Model

Updated: April 26, 2012

Applies To: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012

Designing your logical structure for Active Directory Domain Services (AD DS) involves defining the relationships between the containers in your directory. These relationships might be based on administrative requirements, such as delegation of authority, or they might be defined by operational requirements, such as the need to control replication.

Before you design your Active Directory logical structure, it is important to understand the Active Directory logical model. AD DS is a distributed database that stores and manages information about network resources as well as application-specific data from directory-enabled applications. AD DS allows administrators to organize elements of a network (such as users, computers, and devices) into a hierarchical containment structure. The top-level container is the forest. Within forests are domains, and within domains are organizational units (OUs). This is called the logical model because it is independent of the physical aspects of the deployment, such as the number of domain controllers required within each domain and network topology.

Active Directory forest

A forest is a collection of one or more Active Directory domains that share a common logical structure, directory schema (class and attribute definitions), directory configuration (site and replication information), and global catalog (forest-wide search capabilities). Domains in the same forest are automatically linked with two-way, transitive trust relationships.

Active Directory domain

A domain is a partition in an Active Directory forest. Partitioning data enables organizations to replicate data only to where it is needed. In this way, the directory can scale globally over a network that has limited available bandwidth. In addition, the domain supports a number of other core functions related to administration, including:

- Network-wide user identity. Domains allow user identities to be created once and referenced on any computer joined to the forest in which the domain is located. Domain controllers that make up a domain are used to store user accounts and user credentials (such as passwords or certificates) securely.

- Authentication. Domain controllers provide authentication services for users and supply additional authorization data such as user group memberships, which can be used to control access to resources on the network.

- Trust relationships. Domains can extend authentication services to users in domains outside their own forest by means of trusts.

- Replication. The domain defines a partition of the directory that contains sufficient data to provide domain services and then replicates it between the domain controllers. In this way, all domain controllers are peers in a domain and are managed as a unit.

Active Directory organizational units

OUs can be used to form a hierarchy of containers within a domain. OUs are used to group objects for administrative purposes such as the application of Group Policy or delegation of authority. Control (over an OU and the objects within it) is determined by the access control lists (ACLs) on the OU and on the objects in the OU. To facilitate the management of large numbers of objects, AD DS supports the concept of delegation of authority. By means of delegation, owners can transfer full or limited administrative control over objects to other users or groups. Delegation is important because it helps to distribute the management of large numbers of objects across a number of people who are trusted to perform management tasks.

Identifying the Deployment Project Participants

Updated: April 26, 2012

Applies To: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012

The first step in establishing a deployment project for Active Directory Domain Service (AD DS) is to establish the design and deployment project teams that will be responsible for managing the design phase and deployment phase of the Active Directory project cycle. In addition, you must identify the individuals and groups who will be responsible for owning and maintaining the directory after the deployment is completed.

- Defining project-specific roles

- Establishing owners and administrators

- Building project teams

Defining project-specific roles

An important step in establishing the project teams is to identify the individuals who are to hold project-specific roles. These include the executive sponsor, the project architect, and the project manager. These individuals are responsible for running the Active Directory deployment project.

After you appoint the project architect and project manager, these individuals establish channels of communication throughout the organization, build project schedules, and identify the individuals who will be members of the project teams, beginning with the various owners.

Executive sponsor

Deploying an infrastructure such as AD DS can have a wide-ranging impact on an organization. For this reason, it is important to have an executive sponsor who understands the business value of the deployment, supports the project at the executive level, and can help resolve conflicts across the organization.

Project architect

Each Active Directory deployment project requires a project architect to manage the Active Directory design and deployment decision-making process. The architect provides technical expertise to assist with the process of designing and deploying AD DS.

Note

If no existing personnel in your organization have directory design experience, you might want to hire an outside consultant who is an expert in Active Directory design and deployment.

The responsibilities of the Active Directory project architect include the following:

- Owning the Active Directory design
- Understanding and recording the rationale for key design decisions
- Ensuring that the design meets the business needs of the organization
- Establishing consensus between design, deployment, and operations teams
- Understanding the needs of AD DS–integrated applications

The final Active Directory design must reflect a combination of business goals and technical decisions. Therefore, the project architect must review design decisions to ensure that they align with business goals.

Project manager

The project manager facilitates cooperation across business units and between technology management groups. Ideally, the Active Directory deployment project manager is someone from within the organization who is familiar with both the operational policies of the IT group and the design requirements for the groups that are preparing to deploy AD DS. The project manager oversees the entire deployment project, beginning with design and continuing through implementation, and makes sure that the project stays on schedule and within budget. The responsibilities of the project manager include the following:

- Providing basic project planning such as scheduling and budgeting
- Driving progress on the Active Directory design and deployment project
- Ensuring that the appropriate individuals are involved in each part of the design process
- Serving as single point of contact for the Active Directory deployment project
- Establishing communication between design, deployment, and operations teams
- Establishing and maintaining communication with the executive sponsor throughout the deployment project

Establishing owners and administrators

In an Active Directory deployment project, individuals who are owners are held accountable by management to make sure that deployment tasks are completed and that Active Directory design specifications meet the needs of the organization. Owners do not necessarily have access to or manipulate the directory infrastructure directly. Administrators are the individuals responsible for completing the required deployment tasks. Administrators have the network access and permissions necessary to manipulate the directory and its infrastructure.

The role of the owner is strategic and managerial. Owners are responsible for communicating to administrators the tasks required for the implementation of the Active Directory design such as the creation of new domain controllers within the forest. The administrators are responsible for implementing the design on the network according to the design specifications.

In large organizations, different individuals fill owner and administrator roles; however, in some small organizations, the same individual might act as both the owner and the administrator.

Service and data owners

Managing AD DS on a daily basis involves two types of owners:

- Service owners who are responsible for planning and long-term maintenance of the Active Directory infrastructure and for ensuring that the directory continues to function and that the goals established in service level agreements are maintained
- Data owners who are responsible for the maintenance of the information stored in the directory. This includes user and computer account management and management of local resources such as member servers and workstations.

It is important to identify the Active Directory service and data owners early so that they can participate in as much of the design process as possible. Because the service and data owners are responsible for the long-term maintenance of the directory after the deployment project is finished, it is important for these individuals to provide input regarding organizational needs and to be familiar with how and why certain design decisions are made. Service owners include the forest owner, the Active Directory Domain Naming System (DNS) owner, and the site topology owner. Data owners include organizational unit (OU) owners.

Service and data administrators

The operation of AD DS involves two types of administrators: service administrators and data administrators. Service administrators implement policy decisions made by service owners and handle the day-to-day tasks associated with maintaining the directory service and infrastructure. This includes managing the domain controllers that are hosting the directory service, managing other network services such as DNS that are required for AD DS, controlling the configuration of forest-wide settings, and ensuring that the directory is always available.

Service administrators are also responsible for completing ongoing Active Directory deployment tasks that are required after the initial Windows Server 2008 Active Directory deployment process is complete. For example, as demands on the directory increase, service administrators create additional domain controllers and establish or remove trusts between domains, as needed. For this reason, the Active Directory deployment team needs to include service administrators.

You must be careful to assign service administrator roles only to trusted individuals in the organization. Because these individuals have the ability to modify the system files on domain controllers, they can change the behavior of AD DS. You must ensure that the service administrators in your organization are individuals who are familiar with the operational and security policies that are in place on your network and who understand the need to enforce those policies.

Data administrators are users within a domain who are responsible both for maintaining data that is stored in AD DS such as user and group accounts and for maintaining computers that are members of their domain. Data administrators control subsets of objects within the directory and have no control over the installation or configuration of the directory service.

Data administrator accounts are not provided by default. After the design team determines how resources are to be managed for the organization, domain owners must create data administrator accounts and delegate them the appropriate permissions based on the set of objects for which the administrators are to be responsible.

It is best to limit the number of service administrators in your organization to the minimum number required to ensure that the infrastructure continues to function. The majority of administrative work can be completed by data administrators. Service administrators require a much wider skill set because they are responsible for maintaining the directory and the infrastructure that supports it. Data administrators only require the skills necessary to manage their portion of the directory. Dividing work assignments in this way results in cost savings for the organization because only a small number of administrators need to be trained to operate and maintain the entire directory and its infrastructure.

For example, a service administrator needs to understand how to add a domain to a forest. This includes how to install the software to convert a server into a domain controller and how to manipulate the DNS environment so that the domain controller can be merged seamlessly into the Active Directory environment. A data administrator only needs to know how to manage the specific data that they are responsible for such as the creation of new user accounts for new employees in their department.

Deploying AD DS requires coordination and communication between many different groups involved in the operation of the network infrastructure. These groups should appoint service and data owners who are responsible for representing the various groups during the design and deployment process.

Once the deployment project is complete, these service and data owners continue to be responsible for the portion of the infrastructure managed by their group. In an Active Directory environment, these owners are the forest owner, the DNS for AD DS owner, the site topology owner, and the OU owner. The roles of these service and data owners are explained in the following sections.

Forest owner

The forest owner is typically a senior information technology (IT) manager in the organization who is responsible for the Active Directory deployment process and who is ultimately accountable for maintaining service delivery within the forest after the deployment is complete. The forest owner assigns individuals to fill the other ownership roles by identifying key personnel within the organization who are able to contribute necessary information about

network infrastructure and administrative needs. The forest owner is responsible for the following:

- Deployment of the forest root domain to create the forest
- Deployment of the first domain controller in each domain to create the domains required for the forest
- Memberships of the service administrator groups in all domains of the forest
- Creation of the design of the OU structure for each domain in the forest
- Delegation of administrative authority to OU owners
- Changes to the schema
- Changes to forest-wide configuration settings
- Implementation of certain Group Policy policy settings, including domain user account policies such as fine-grained password and account lockout policy
- Business policy settings that apply to domain controllers
- Any other Group Policy settings that are applied at the domain level

The forest owner has authority over the entire forest. It is the forest owner's responsibility to set Group Policy and business policies and to select the individuals who are service administrators. The forest owner is a service owner.

DNS for AD DS owner

The DNS for AD DS owner is an individual who has a thorough understanding of the existing DNS infrastructure and the existing namespace of the organization.

The DNS for AD DS owner is responsible for the following:

- Serving as a liaison between the design team and the IT group that currently owns the DNS infrastructure
- Providing the information about the existing DNS namespace of the organization to assist in the creation of the new Active Directory namespace
- Working with the deployment team to make sure that the new DNS infrastructure is deployed according to the specifications of the design team and that it is working properly
- Managing the DNS for AD DS infrastructure, including the DNS Server service and DNS data

The DNS for AD DS owner is a service owner.

Site topology owner

The site topology owner is familiar with the physical structure of the organization network, including mapping of individual subnets, routers, and network areas that are connected by means of slow links. The site topology owner is responsible for the following:

- Understanding the physical network topology and how it affects AD DS
- Understanding how the Active Directory deployment will impact the network
- Determining the Active Directory logical sites that need to be created
- Updating site objects for domain controllers when a subnet is added, modified, or removed
- Creating site links, site link bridges, and manual connection objects

The site topology owner is a service owner.

OU owner

The OU owner is responsible for managing data stored in the directory. This individual needs to be familiar with the operational and security policies that are in place on the network. OU owners can perform only those tasks that have been delegated to them by the service administrators, and they can perform only those tasks on the OUs to which they are assigned. Tasks that might be assigned to the OU owner include the following:

- Performing all account management tasks within their assigned OU
- Managing workstations and member servers that are members of their assigned OU
- Delegating authority to local administrators within their assigned OU

The OU owner is a data owner.

Building project teams

Active Directory project teams are temporary groups that are responsible for completing Active Directory design and deployment tasks. When the Active Directory deployment project is complete, the owners assume responsibility for the directory, and the project teams can disband.

The size of the project teams varies according to the size of the organization. In small organizations, a single person can cover multiple areas of responsibility on a project team and be involved in more than one phase of the deployment. Large organizations might require larger teams with different individuals or even different teams covering the different areas of responsibility. The size of the teams is not important as long as all areas of responsibility are assigned, and the design goals of the organization are met.

Identifying potential forest owners

Identify the groups within your organization that own and control the resources necessary to provide directory services to users on the network. These groups are considered potential forest owners.

The separation of service and data administration in AD DS makes it possible for the infrastructure IT group (or groups) of an organization to manage the directory service while local administrators in each group manage the data that belongs to their own groups. Potential forest owners have the required authority over the network infrastructure to deploy and support AD DS.

For organizations that have one centralized infrastructure IT group, the IT group is generally the forest owner and, therefore, the potential forest owner for any future deployments. Organizations that include a number of independent infrastructure IT groups have a number of potential forest owners. If your organization already has an Active Directory infrastructure in place, any current forest owners are also potential forest owners for new deployments.

Select one of the potential forest owners to act as the forest owner for each forest that you are considering for deployment. These potential forest owners are responsible for working with the design team to determine whether or not their forest will actually be deployed or if an alternate course of action (such as joining another existing forest) is a better use of the available resources and still meets their needs. The forest owner (or owners) in your organization are members of the Active Directory design team.

Establishing a design team

The Active Directory design team is responsible for gathering all the information needed to make decisions about the Active Directory logical structure design.

The responsibilities of the design team include the following:

- Determining how many forests and domains are required and what the relationships are between the forests and domains

- Working with data owners to ensure that the design meets their security and administrative requirements
- Working with the current network administrators to ensure that the current network infrastructure supports the design and that the design will not adversely affect existing applications deployed on the network
- Working with representatives of the security group of the organization to ensure that the design meets established security policies
- Designing OU structures that permit appropriate levels of protection and the proper delegation of authority to the data owners
- Working with the deployment team to test the design in a lab environment to ensure that it functions as planned and modifying the design as needed to address any problems that occur
- Creating a site topology design that meets the replication requirements of the forest while preventing overload of available bandwidth. For more information about designing the site topology, see Designing the Site Topology for Windows Server 2008 AD DS.
- Working with the deployment team to ensure that the design is implemented correctly

The design team includes the following members:

- Potential forest owners
- Project architect
- Project manager
- Individuals who are responsible for establishing and maintaining security policies on the network

During the logical structure design process, the design team identifies the other owners. These individuals must start participating in the design process as soon as they are identified. After the deployment project is handed off to the deployment team, the design team is responsible for overseeing the deployment process to ensure that the design is implemented correctly. The design team also makes changes to the design based on feedback from testing.

Establishing a deployment team

The Active Directory deployment team is responsible for testing and implementing the Active Directory logical structure design. This involves the following tasks:

- Establishing a test environment that sufficiently emulates the production environment

- Testing the design by implementing the proposed forest and domain structure in a lab environment to verify that it meets the goals of each role owner
- Developing and testing any migration scenarios proposed by the design in a lab environment
- Making sure that each owner signs off on the testing process to ensure that the correct design features are being tested
- Testing the deployment operation in a pilot environment

When the design and testing tasks are complete, the deployment team performs the following tasks:

- Creates the forests and domains according to the Active Directory logical structure design
- Creates the sites and site link objects as needed based on the site topology design
- Ensures that the DNS infrastructure is configured to support AD DS and that any new namespaces are integrated into the existing namespace of the organization

The Active Directory deployment team includes the following members:

- Forest owner
- DNS for AD DS owner
- Site topology owner
- OU owners

The deployment team works with the service and data administrators during the deployment phase to ensure that members of the operations team are familiar with the new design. This helps to ensure a smooth transition of ownership when the deployment operation is completed. At the completion of the deployment process, the responsibility for maintaining the new Active Directory environment passes to the operations team.

Documenting the design and deployment teams

Document the names and contact information for the people who will participate in the design and deployment of AD DS. Identify who will be responsible for each role on the design and deployment teams. Initially, this list includes the potential forest owners, the project manager, and the project architect. When you determine the number of forests that you will deploy, you might need to create new design teams for additional forests. Note that you will need to update your documentation as team memberships change and as you identify the various Active Directory owners during the design process. For a worksheet to assist you in documenting the design and deployment teams for each forest, download

Job_Aids_Designing_and_Deploying_Directory_and_Security_Services.zip from Job Aids for Windows Server 2003 Deployment Kit (http://go.microsoft.com/fwlink/?LinkID=102558) and open "Design and Deployment Team Information" (DSSLOGI_1.doc).

Creating a Forest Design

Updated: April 26, 2012

Applies To: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012

Creating a forest design involves first identifying the groups within your organization that have the resources available to host an Active Directory forest and then defining your forest design requirements. Finally, you need to determine the number of forests that you require to meet the needs of your organization.

After you map all your design requirements to forest models and select the forest model that meets the needs of your organization, document the proposed forest design. Include in your documentation the name of the group for which the forest is designed, the contact information for the forest owner, the type of forest for each forest that you include, and the requirements that each forest is designed to meet. This documentation will help the design team both to ensure that all the appropriate people are involved in the design process and to clarify the scope of the deployment project.

For a worksheet to assist you in documenting the proposed forest design, download Job_Aids_Designing_and_Deploying_Directory_and_Security_Services.zip from Job Aids for Windows Server 2003 Deployment Kit (http://go.microsoft.com/fwlink/?LinkID=102558) and open "Forest Design" (DSSLOGI_3.doc).

Identifying Forest Design Requirements

Updated: April 26, 2012

Applies To: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012

To create a forest design for your organization, you must identify the business requirements that your directory structure needs to accommodate. This involves determining how much autonomy the groups in your organization need to manage their network resources and whether or not each group needs to isolate their resources on the network from other groups.

Active Directory Domain Services (AD DS) enables you to design a directory infrastructure that accommodates multiple groups within an organization that have unique management requirements and to achieve structural and operational independence between groups as needed.

Groups in your organization might have some of the following types of requirements:

- **Organizational structure requirements**. Parts of an organization might participate in a shared infrastructure to save costs but require the ability to operate independently from the rest of the organization. For example, a research group within a large organization might need to maintain control over all of their own research data.

- **Operational requirements**. One part of an organization might place unique constraints on the directory service configuration, availability, or security, or use applications that place unique constraints on the directory. For example, individual business units within an organization might deploy directory-enabled applications that modify the directory schema that are not deployed by other business units. Because the directory schema is shared between all the domains in the forest, creating multiple forests is one solution for such a scenario. Other examples are found in the following organizations and scenarios:

    - Military organizations

    - Hosting scenarios

    - Organizations that maintain a directory that is available both internally and externally (such as those that are publicly accessible by users on the Internet)

- **Legal requirements**. Some organizations have legal requirements to operate in a specific way, for example, restricting access to certain information as specified in a business contract. Some organizations have security requirements to operate on isolated internal networks. Failure to meet these requirements can result in loss of the contract and possibly legal action.

Part of identifying your forest design requirements involves identifying the degree to which groups in your organization can trust the potential forest owners and their service administrators and identifying the autonomy and isolation requirements for each group in your organization.

The design team must document the isolation and autonomy requirements for service and data administration for each group in the organization that intends to use AD DS. The team must also note any areas of limited connectivity that might affect the deployment of AD DS.

The design team must document the isolation and autonomy requirements for service and data administration for each group in the organization that intends to use AD DS. The team must also note any areas of limited connectivity that might affect the deployment of AD DS. For a worksheet to assist you in documenting the regions you identified, download Job_Aids_Designing_and_Deploying_Directory_and_Security_Services.zip from Job Aids for Windows Server 2003 Deployment Kit (http://go.microsoft.com/fwlink/?LinkID=102558) and open "Forest Design Requirements" (DSSLOGI_2.doc).

Service Administrator Scope of Authority

Updated: April 26, 2012

Applies To: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012

If you choose to participate in an Active Directory forest, you must trust the forest owner and the service administrators. The forest owners are responsible for selecting and managing the service administrators; therefore, when you trust a forest owner, you also trust the service administrators that the forest owner manages. These service administrators have access to all of the resources in the forest. Before making the decision to participate in a forest, it is important to understand that the forest owner and the service administrators will have full access to your data. You cannot prevent this access.

All service administrators in a forest have full control over all data and services on all computers in the forest. Service administrators have the capability to do the following:

- Correct errors on access control lists (ACLs) of objects. This enables the service administrator to read, modify, or delete objects regardless of the ACLs that are set on those objects.

- Modify the system software on a domain controller to bypass normal security checks. This enables the service administrator to view or manipulate any object in the domain, regardless of the ACL on the object.

- Use the Restricted Groups security policy to grant to any user or group administrative access to any computer joined to the domain. In this way, service administrators can obtain control of any computer joined to the domain regardless of the intentions of the computer owner.

- Reset passwords or change group memberships for users.

- Gain access to other domains in the forest by modifying the system software on a domain controller. Service administrators can affect the operation of any domain in the forest, view or manipulate forest configuration data, view or manipulate data stored in any domain, and view or manipulate data stored on any computer joined to the forest.

For this reason, groups that store data in organizational units (OUs) in the forest and that join computers to a forest must trust the service administrators. For a group to join a forest, it must choose to trust all service administrators in the forest. This involves ensuring that:

- The forest owner can be trusted to act in the interests of the group and does not have reason to act maliciously against the group.

- The forest owner appropriately restricts physical access to domain controllers. Domain controllers within a forest cannot be isolated from one another. It is possible for an attacker who has physical access to a single domain controller to make offline changes to the directory database and, by doing so, interfere with the operation of any domain in the forest, view or manipulate data stored anywhere in the forest, and view or manipulate data stored on any computer joined to the forest. For this reason, physical access to domain controllers must be restricted to trusted personnel.

- You understand and accept the potential risk that trusted service administrators can be coerced into compromising the security of the system.

Some groups might determine that the collaborative and cost-saving benefits of participating in a shared infrastructure outweigh the risks that service administrators will misuse or will be coerced into misusing their authority. These groups can share a forest and use OUs to delegate authority. However, other groups might not accept this risk because the consequences of a compromise in security are too severe. These groups require separate forests.

Autonomy vs. Isolation

Updated: April 26, 2012

Applies To: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012

You can design your Active Directory logical structure to achieve either of the following:

- **Autonomy**. Involves independent but not exclusive control of a resource. When you achieve autonomy, administrators have the authority to manage resources independently; however, administrators with greater authority exist who also have control over those resources and can take control away if necessary. You can design your Active Directory logical structure to achieve the following types of autonomy:
    - **Service autonomy**. This type of autonomy involves control over all or part of service management.
    - **Data autonomy**. This type of autonomy involves control over all or part of the data stored in the directory or on member computers joined to the directory.
- **Isolation**. Involves independent and exclusive control of a resource. When you achieve isolation, administrators have the authority to manage a resource independently, and no other administrator can take away control of the resource. You can design your Active Directory logical structure to achieve the following types of isolation:
    - **Service isolation**. Prevents administrators (other than those administrators who are specifically designated to control service management) from controlling or interfering with service management.
    - **Data isolation**. Prevents administrators (other than those administrators who are specifically designated to control or view data) from controlling or viewing a subset of data in the directory or on member computers joined to the directory.

Administrators who require only autonomy accept that other administrators who have equal or greater administrative authority have equal or greater control over service or data management. Administrators who require isolation have exclusive control over service or data management. Creating a design to achieve autonomy is generally less expensive than creating a design to achieve isolation.

In Active Directory Domain Services (AD DS), administrators can delegate both service administration and data administration to achieve either autonomy or isolation between organizations. The combination of service management, data management, autonomy, and isolation requirements of an organization impact the Active Directory containers that are used to delegate administration.

Isolation and autonomy requirements

The number of forests that you need to deploy is based on the autonomy and isolation requirements of each group within your organization. To identify your forest design requirements, you must identify the autonomy and isolation requirements for all groups in your organization. Specifically, you must identify the need for data isolation, data autonomy, service isolation, and service autonomy. You must also identify areas of limited connectivity in your organization.

Data isolation

Data isolation involves exclusive control over data by the group or organization that owns the data. It is important to note that service administrators have the ability to take control of a resource away from data administrators. And data administrators do not have the ability to prevent service administrators from accessing the resources that they control. Therefore, you cannot achieve data isolation when another group within the organization is responsible for service administration. If a group requires data isolation, that group must also assume responsibility for service administration.

Because data stored in AD DS and on computers joined to AD DS cannot be isolated from service administrators, the only way for a group within an organization to achieve complete data isolation is to create a separate forest for that data. Organizations for which the consequences of an attack by malicious software or by a coerced service administrator are substantial might choose to create a separate forest to achieve data isolation. Legal requirements typically create a need for this type of data isolation. For example:

- A financial institution is required by law to limit access to data that belongs to clients in a particular jurisdiction to users, computers, and administrators located in that jurisdiction. Although the institution trusts service administrators that work outside the protected area, if the access limitation is violated, the institution will no longer be able to do business in that jurisdiction. Therefore, the financial institution must isolate data from service administrators outside that jurisdiction. Note that encryption is not always an alternative to this solution. Encryption might not protect data from service administrators.

- A defense contractor is required by law to limit access to project data to a specified set of users. Although the contractor trusts service administrators who control computer systems related to other projects, a violation of this access limitation will cause the contractor to lose business.

Note

If you have a data isolation requirement, you must decide if you need to isolate your data from service administrators or from data administrators and ordinary users. If your isolation requirement is based on isolation from data administrators and ordinary users, you can use access control lists (ACLs) to isolate the data. For the purposes of this design process, isolation from data administrators and ordinary users is not considered a data isolation requirement.

Data autonomy

Data autonomy involves the ability of a group or organization to manage its own data, including making administrative decisions about the data and performing any required administrative tasks without the need for approval from another authority.

Data autonomy does not prevent service administrators in the forest from accessing the data. For example, a research group within a large organization might want to be able to manage their project-specific data themselves but not need to secure the data from other administrators in the forest.

Service isolation

Service isolation involves exclusive control of the Active Directory infrastructure. Groups that require service isolation require that no administrator outside of the group can interfere with the operation of the directory service.

Operational or legal requirements typically create a need for service isolation. For example:

- A manufacturing company has a critical application that controls equipment on the factory floor. Interruptions in the service on other parts of the network of the organization cannot be allowed to interfere with the operation of the factory floor.
- A hosting company provides service to multiple clients. Each client requires service isolation so that any service interruption that affects one client does not affect the other clients.

Service autonomy

Service autonomy involves the ability to manage the infrastructure without a requirement for exclusive control; for example, when a group wants to make changes to the infrastructure (such as adding or removing domains, modifying the Domain Name System (DNS) namespace, or modifying the schema) without the approval of the forest owner.

Service autonomy might be required within an organization for a group that wants to be able to control the service level of AD DS (by adding and removing domain controllers, as needed) or for a group that needs to be able to install directory-enabled applications that require schema extensions.

Limited connectivity

If a group within your organization owns networks that are separated by devices that restrict or limit connectivity between networks (such as firewalls and Network Address Translation (NAT) devices), this can impact your forest design. When you identify your forest design requirements, be sure to note the locations where you have limited network connectivity. This information is required to enable you to make decisions regarding the forest design.