Trust Technologies: Domain and Forest Trusts

By Archiveddocs

Archived: 2026-04-05 19:54:28 UTC

Applies To: Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2

Trust Technologies

By default, all users in a specific Windows domain can be authenticated to resources contained within that domain. In this way, a domain can provide its users with secured access to all resources in that domain. To expand that access to include resources beyond the boundaries of a single domain, you need to use trust relationships. Trust relationships provide a mechanism for one domain to allow access to resources based on the logon authentications of another domain.

Trust Concepts

Trusts in Microsoft Windows NT version 4.0 differ from trusts in the Microsoft Windows 2000 and Windows Server 2003 operating systems. In domains that have domain controllers running Windows NT 4.0 Server and earlier, trusts are limited to two domains, and the trust relationship is one-way (only one of the two domains trusts the other domain) and nontransitive (does not extend to any other domains trusted by the two domains). With domains that have domain controllers running Windows Server 2003 or Windows 2000 Server, all trusts created within a forest are two-way (both domains trust each other) and transitive (extends to all domains in the forest). Domains that have domain controllers running Windows 2000 Server or Windows Server 2003 (domains that use the Active Directory directory service) are also referred to as Active Directory domains.

To understand trust technology, you should be familiar with basic trust concepts including the nature and purpose of trust relationships, the role of trusted authorities, the variety of trust paths, and trust transitivity.

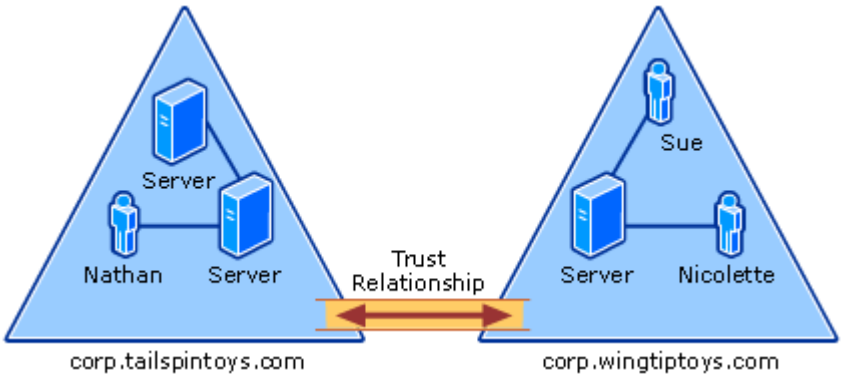
Trust Relationships

A trust relationship (also called a trust) is a logical relationship established between domains to allow authentication and authorization to shared resources. The authentication process verifies the identity of the user, and the authorization process determines what the user is permitted to do on a computer system or network. Once a user requesting access to a resource computer in another domain has been authenticated by the resource domain, the resource computer compares the user’s credentials to the permissions assigned within its security descriptor to help determine the user’s level of authorization to that resource. A security descriptor contains access control lists (ACLs) that identify the users and groups that are assigned or denied access permissions on a resource.

In its simplest form, a trust acts as a technological drawbridge, by either allowing or disallowing authentication traffic to flow between two or more domains. When a trust relationship is created between two domains, traffic is

allowed over the bridge, permitting the sharing of resources between them, as shown in the following illustration.

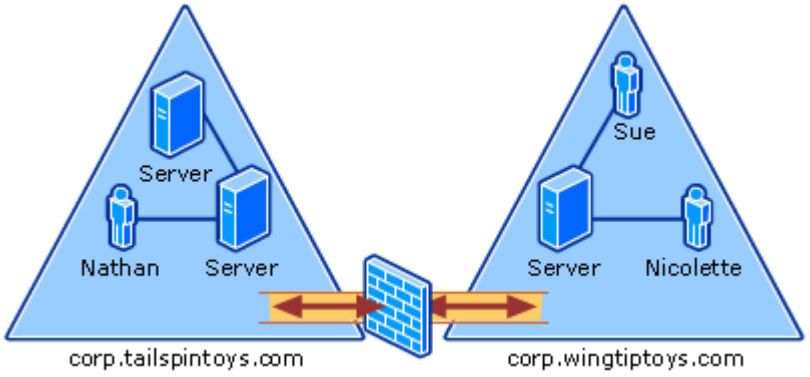
Simple Trust Relationship



The domain where the user account requesting access is located is referred to as the trusted domain. The domain that contains a shared resource that a user account is trying to access is referred to as the trusting domain.

Severing a trust removes the bridge through which authentication traffic flows, and removes all relationships to any trusted authorities located in the other domain. When this occurs, no authentication traffic originating from a user in the formerly trusted domain can cross over to the formerly trusting domain; it is no longer possible to share information across domain boundaries, as is shown in the following figure.

Severed Trust Relationship



Active Directory domains do not unconditionally accept credentials coming from other domains; they accept credentials only from trusted authorities. In Active Directory, domain controllers act as trusted authorities for all security principals located in their domain and all security principals located within trusted domains, as long as a valid trust is present between those domains.

A trusted authority, in Active Directory, is analogous to a certificate granting agency that distributes certificates by which a sub agency can verify its authenticity. For example, when a passport is issued by a passport authority in one country (a domain controller in a trusted domain), customs officials physically located in another country (domain controllers in a trusting domain), trust the authority that issued the passport, therefore they trust the validity of the passport.

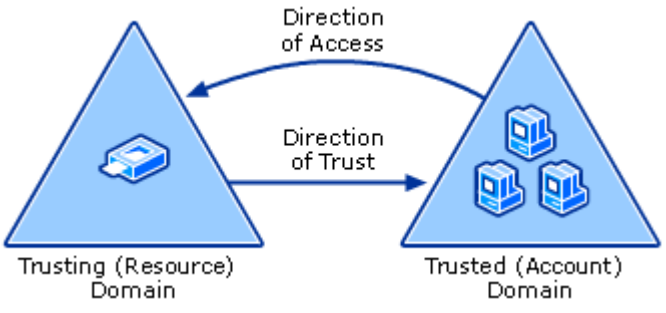
Conversely, a company might create a specific means by which to identify employees, such as employee badges issued by its various departments (domains). The manufacturing department (domain controllers in a trusting domain) might trust identification badges issued by the sales department (domain controllers in a trusted domain) for important transactions, but other companies (domains or forests that do not have a trust relationship with that company or its departments) would not trust them because they do not inherently trust the authority that issued them.

In Windows NT 4.0 or Active Directory domains, domain administrators act as the chief executive officer of the certificate granting agency by defining the policy regarding what external authorities (domains) are trusted in their domain. For example, a domain administrator in a trusting domain first identifies which other domains should be trusted to access shared resources in the domain. The administrator then establishes the trust relationships that provide a path by which authentication requests from trusted domains can travel and be verified. In this way, trusts define for each domain which authentication requests are valid. For more information about trust paths, see “Trust Paths” later in this overview.

Trust Paths

The direction that a trust is assigned determines the trust path used for authentication. A trust path is defined by the series of trust relationships that authentication requests must follow between domains. Before a user can access a resource in another domain, the security system on domain controllers running Windows NT 4.0, Windows 2000 Server, and Windows Server 2003 must determine whether the trusting domain (the domain containing the resource the user is trying to access) has a trust relationship with the trusted domain (the user’s logon domain). To determine this, the security system computes the trust path between a domain controller in the trusting domain and a domain controller in the trusted domain. All domain trust relationships have only two domains: the trusting domain and the trusted domain. In the following figure, the trust path is indicated by arrows showing a one-way direction of trust and the direction of access:

Trust Path in a One-Way Trust



One-Way Trust

A one-way trust is a unidirectional authentication path created between two domains (trust flows in one direction, and access flows in the other). This means that in a one-way trust between a trusted domain and a trusting domain, users or computers in the trusted domain can access resources in the trusting domain. However, users in the trusting domain cannot access resources in the trusted domain. Some one-way trusts can be either nontransitive or transitive, depending on the type of trust being created.

Two-Way Trust

A two-way trust can be thought of as a combination of two, opposite-facing one-way trusts, so that, the trusting and trusted domains both trust each other (trust and access flow in both directions). This means that authentication requests can be passed between the two domains in both directions. Some two-way relationships can be either nontransitive or transitive depending on the type of trust being created. All domain trusts in an Active Directory forest are two-way, transitive trusts. When a new child domain is created, a two-way, transitive trust is automatically created between the new child domain and the parent domain.

Trust Transitivity

Transitivity determines whether a trust can be extended beyond the two domains between which it was formed. A transitive trust extends trust relationships to other domains; a nontransitive trust does not extend trust relationships to other domains. Each time you create a new domain in a forest, a two-way, transitive trust relationship is automatically created between the new domain and its parent domain. If child domains are added to the new domain, the trust path flows upward through the domain hierarchy, extending the initial trust path created between the new domain and its parent.

Transitive trust relationships thus flow upward through a domain tree as it is formed, creating transitive trusts between all domains in the domain tree. A domain tree can therefore be defined as a hierarchical structure of one or more domains, connected by transitive, bidirectional trusts, that forms a contiguous namespace. Multiple domain trees can belong to a single forest.

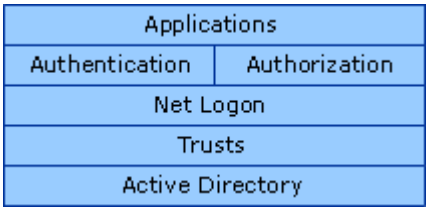
Authentication requests follow these extended trust paths, so accounts from any domain in the forest can be authenticated by any other domain in the forest. Consequently, with a single logon process, accounts with the proper permissions can access resources in any domain in the forest.

With a nontransitive trust, the flow is restricted to the two domains in the trust relationship and does not extend to any other domains in the forest. A nontransitive trust can be either a two-way trust or a one-way trust.

Trust Architecture

The architecture of trusts includes various interdependent technologies and processes that, when implemented together, provide cross domain resource sharing. These technologies include authentication, authorization, the Net Logon service and Active Directory, which all rely on DNS or Windows Internet Name Service (WINS) to locate domain service records. The following figure shows the various technologies that make up the trust architecture.

Trust Architecture



Active Directory provides the foundation for trust relationships by supplying a central management system through which domain administrators can grant access to trusted authorities in other domains. Trusts then provide the mechanism through which authentication traffic between domains or forests must travel to obtain authorization for a given shared resource. Authentication and authorization are the security enforcement mechanisms within this resource access management environment.

The authentication process and the Net Logon service provide pass-through validation of credentials for users or distributed applications located in other domains, and rely on either the NTLM or Kerberos version 5 authentication protocol to transport all trust related traffic. Applications can use these protocols to securely and seamlessly integrate with the Active Directory user store for authentication, and can also use these protocols to secure application data.

Trust Components

The various components of trust technologies and the related components that are an important part of the Windows Server 2003 security architecture determine how trusts function. The following table provides a summary view of these components.

Trust Technologies and Related Components

Related components	Description
Security Identifiers (SIDs)	The Windows security model identifies account objects such as users, groups, computers, and domains by SIDs. SIDs are domain-unique values, built when the user or group is created, or when the computer or trust is registered with the domain. The components of a SID follow a hierarchical convention: A SID contains parts that identify the revision number, the authority — such as the domain — that issued the SID, and a variable number of sub authority or relative identifier (RID) values that uniquely identify the security principal relative to the issuing authority.
Access Tokens and Authentication	An essential component of the Windows-based trust model is authentication, which involves identifying the user to the local or trusted domain by presenting credentials, usually in the form of a user name and password. Assuming these credentials are acceptable, the system creates an access token for the user that contains the SID of the user (the primary SID), and the SIDs of all the local and domain groups of which the user is a member. Every process the user creates, for example by running an application, carries the user’s access token.

Security Descriptors and Authorization	Once authenticated, the user can attempt to gain access to resources from any domain in the forest by using the Active Directory authorization process. This process determines what a user is permitted to do on a resource by using the access token to determine whether and at what level to grant the user access to system resources. The counterpart of the user's access token is the security descriptor attached to resources such as files or printers. A security descriptor contains a discretionary access control list (DACL), which consists of a list of access control entries (ACEs). Each ACE consists of a SID that identifies a security principal, together with an indicator of the specific access on that resource that is granted or denied to that security principal.
SIDHistory	In Active Directory, domain migration or restructuring across trusts is made considerably easier by an attribute on Active Directory security principals called SIDHistory. SIDHistory stores the former SIDs of moved objects such as users and security groups. When a user is moved, the SIDHistory attribute of the user object is updated with the former SID. When the user then logs on to the system, the system retrieves the entries in the user object and the user's SIDHistory and adds them to the user access token. In this way SIDHistory ensures that migrated users can continue to access resources located in a trusting (resource) domain, even though the user's new domain does not have a trust relationship with the resource domain.
SID Filtering	SID filtering prevents domains from accepting SIDs with domain SIDs from outside the sender's domain. Applying SID filtering to trusts can prevent malicious users who have domain administrator level access in the trusted domain from granting, to themselves or other user accounts in their domain, elevated user rights in the trusting domain.

Trust Deployment Scenarios

There are three scenarios in Active Directory in which specific types of trusts can be used to help accommodate different resource sharing needs of an organization. These include using trusts within a forest (intra-forest trusts), using trusts across forests (inter-forest trusts), and using trusts to collaborate with Kerberos realms.

Intra-Forest Trusts

Intra-forest trusts are transitive trusts that can be used only within a single forest, and include tree-root, parent-child, and shortcut trusts.

Tree-root trusts

By default, two-way, transitive trusts are automatically created when a new domain is added to a domain tree or forest root domain by using the Active Directory Installation Wizard. When a new domain tree is created in an

existing forest, a new tree-root trust is established.

Parent-child trusts

When a new child domain is added to an existing domain tree, a new parent and child trust is established. Authentication requests made from subordinate domains flow upward through their parent to the trusting domain.

Shortcut trusts

You can use shortcut trusts to improve user logon times between two domains that are located in two separate domain trees within the same forest. Authentication requests must first travel a trust path between domain trees, and in a complex forest this can take time. Using shortcut trusts helps to speed up authentication in this situation.

Inter-Forest Trusts

Inter-forest trusts can be nontransitive or transitive, depending on the type of inter-forest trust used, and can only be created between domains located in different forests or realms. Inter-forest trust types include external trusts and forest trusts; both of these trust types must be manually created.

External trusts

External trusts are nontransitive and can be created between Active Directory domains in different forests or between an Active Directory domain and a Windows NT 4.0 domain.

Forest trusts

With Windows Server 2003 forests, you can link two different forests to create a one-way or two-way transitive trust relationship. A two-way forest trust is used to form a transitive trust relationship between every domain in both forests. Forest trusts can be created only between two Windows Server 2003 forests and cannot be implicitly extended to a third forest.

Kerberos Realm Trusts

A realm trust can be established between any non-Windows-based operating system Kerberos version 5 realm and a Windows 2000 Server or Windows Server 2003 domain. This trust relationship allows cross-platform interoperability with security services based on other Kerberos version 5 implementations, such as that from the Massachusetts Institute of Technology. Realm trusts can be manually switched back and forth between nontransitive and transitive by using the Netdom.exe tool. Realm trusts can be either one-way or two-way.
