DOMAIN TRUST ON WINDOWS SERVER

A domain trust is a relationship between domains which allows users of one domain to access services of other domain.

By default, users of a domain can have access to resources contained in that domain. i.e domain users can use domain resources like network printer, fax service and any network share. However, users of one domain cannot access resources of other domain.

By this way, a domain can provide its users with secured access to all resources in that domain. If all users accounts and services can be managed in a single large domain, then there is no problem.

However, there are needs to have multiple separate domains. This is because having multiple domains is a useful way to separate the scope of each domain administrator from other domain administrators. i.e:

Each domain **administrator** is responsible for setting up scope of **security policy** and account policy settings on domain users and domain resources. Thus both multiple domain and trusts between domains are needed.

Trust mechanism in windows

A domain trust (**trust relationship**) is a relationship between two domains to allow authentication and authorization to shared resources. In authentication process, verifies the user identity and in authorization process determines what the authenticated user is allowed to do on shared network resource on target computer.

For example: once the user is authenticated by the domain containing shared network resource, the target computer compares the user's credentials to the permissions assigned within its security descriptor table to help determine the user's level of authorization to the shared resource.

A **security descriptor table** contains access control lists (**ACLs**) that identify the users and groups that are assigned or **denied access** permissions on shared resource.

Trusts in Active Directory:

Domains that have domain controllers running **Windows 2000 Server** or **Windows Server 2003** used **Active Directory** service. **Windows NT** and earlier windows versions doesn't have active directory service support.

Trust Relationship types:

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.

The following are the domain trust relationship types characterized by the trust path used for authentication.

One-Way Trust

A one-way trust is a unidirectional trust between two domains. i.e in one-way trust between a trusted domain and a trusting domain, trusted domain users or computers can access resources in the trusting domain. However, the trusting domain users cannot access resources in the trusted domain.

Some one-way trusts can be either non-transitive or transitive, depending on the type of trust being created.

Two-Way Trust

A two-way trust is a bidirectional trust between two domains. i.e users of either domain can send authentication requests to other domain. 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** integrated 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. This is not true with domains not integrated with active directory service (**Windows NT** and earlier versions).

Trust Transitivity

Transitivity determines whether a trust between two domains can be extended beyond the two domains. A transitive trust extends trust relationships to other domains. Every time a domain created in a forest, a two-way transitive trust is created between the new domain and its parent domain automatically. 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. Therefore adomain tree can be defined as a hierarchical structure of one or more domains, connected by transitive, bidirectional trusts, that forms a contiguous namespace.

So with transitive trusts, user accounts of 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 happens.

Nontransitive trust

In this, The flow is restricted to the two domains in the trust relationship and nontransitive trust does not extend trust relationships to other domains in the forest. A nontransitive trust can be either a two-way trust or a one-way trust. By default, **Nontranstive Trusts** are not created. On must explicitly create those.

Various Trust Deployment methodologies

There are three trust deployment strategies that are used to accommodate the resource sharing needs of an enterprise. These are intra-forest, inter-forest and Kerberos realms based trusts.

Intra Forest Trusts

Intra-forest trusts are transitive trusts that can be used only within a single forest. i.e trust can't be created across multiple forests. Intra-forest trusts includes tree-root, parent-child, and shortcut trust relationships.

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. But when a new domain tree is created in an existing forest, then a new tree-root trust is established. tree-root trusts are two-way and transitive.

Parent-child trusts

A new parent and child trust is established when ever a new child domain is created in a domain tree. Trust flows from child domain to parent domain and goes upwards till domain tree.

Shortcut trusts

Shortcut trusts are the trusts established between two domain trees within the same forest. By Default, **Authentication** requests must first travel a trust path between domain trees, and in a complex forest this

can take time. Using shortcut trusts can create trust with domains in other domain trees. Thus authentication requests goes through shortcut trust which increases overall speed.

Inter Forest Trusts

Inter-forest trusts can be created between domains contained in different forests. Inter-forest trusts can be nontransitive or transitive. Inter-forest trusts include external trusts and forest trusts and both these trust types should be created explicitly.

External trusts

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

Forest trusts

Forest trust is a trust relationship between two forests. Forest trusts can be a one-way or two-way transitive.

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** or **Windows 2003** domain.

This trust relationship allows cross-platform interoperability with security services based on other **Kerberos version 5** implementations. Realm trusts can be either one-way or two-way.