Lesson 15: Configuring Trusts

MOAC 70-412: Configuring Advanced Windows Server 2012 Services

Microsoft Official Academic Course

WILEY

Overview

- Objective 5.2 – Configure trusts
  - Configure external, forest, shortcut, and realm trusts
  - Configure trust authentication
  - Configure SID Filtering
  - Configure name suffix routing

Configuring Trusts

Lesson 15: Configuring Trusts

Trusts

- ***Trusts*** are relationships between one Windows domain and another Windows domain or non-Microsoft Kerberos v5 realm.
- Trusts are created to allow users in one domain the ability to authenticate and then access resources on another domain, forest, or realm.

Trust Types

- Two types of trusts can exist in a forest and domain environment:
  - **Automatically generated** at forest/domain creation
  - **Manually created** after forest or domain creation, these trusts connect directly to domains and forests inside or outside the existing enterprise.

Automatically Generated Trusts

- When a new child domain or tree domain is created within the forest, a two-way trust with the root domain or the parent is created.
- These automatically generated trusts:
  - Are internal to a forest and are created automatically during domain creation.
  - Are transitive and can traverse trusts, domain to domain, up to the root domain throughout the forest, which allows users in one domain of the forest to authenticate to another domain in the forest.
  - Are all two-way trusts.

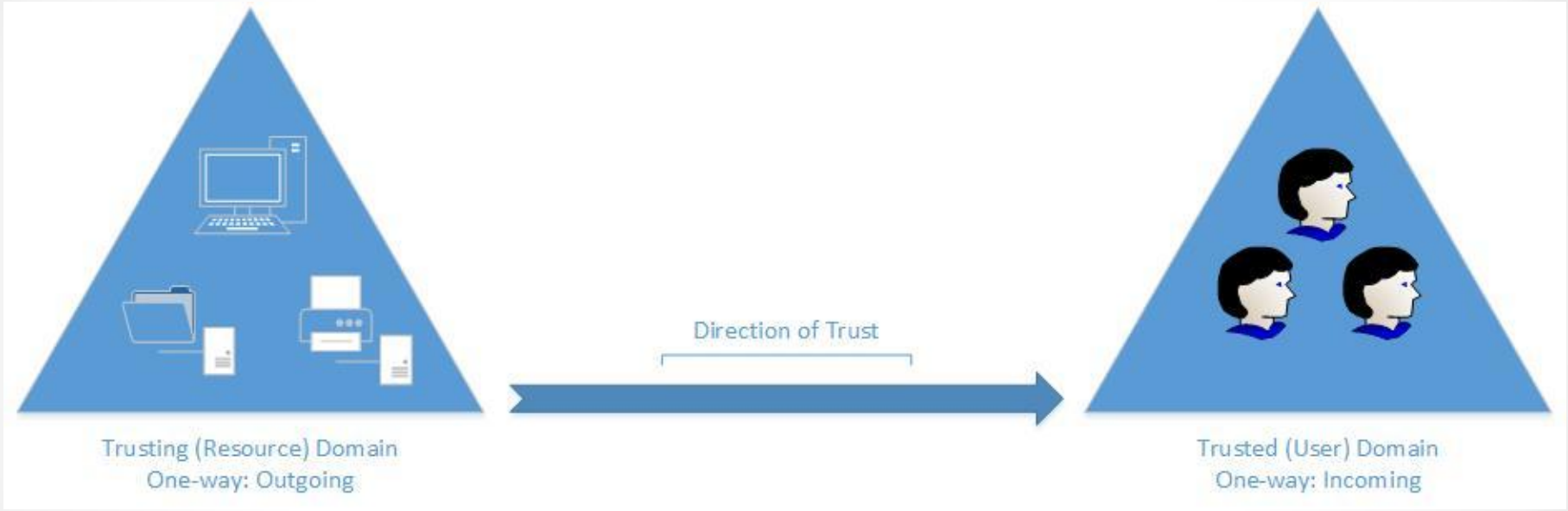
Manually Created Trusts

- Manually created trusts:
  - Can be created to connect two domains within the same forest to one other or to a forest or domain in a completely separate enterprise.
  - Can be one-way or two-way trusts.
  - Can be transitive or nontransitive in nature.
  - Four trusts can be created and configured manually: external trusts, forest trusts, shortcut trusts, and realm trusts.

Trust Direction

- Trust direction indicates the direction in which a trust is given.
- The ***trusting domain*** is giving trust to the ***trusted domain***.
- The trusted domain is "trusted" by the trusting domain.
- In a one-way trust, direction is from the trusting domain to the trusted domain.

One-Way Trust Direction



Trust Direction

- One-way incoming trust direction
- One-way outgoing trust direction
- Two-way trust

Transitivity

- Transitivity determines how far the trust relationship authentication requests can traverse existing trust authentication paths:
  - ***Transitive***
    - Trust authentication follows the flow of existing trust relationships that are part of the trusted domain.
    - If a transitive trust is created with an external forest, the authentication can traverse the path of the forest's existing trusts.
  - ***Nontransitive***
    - An explicit trust between two domains ignores any existing trusts in the external or internal domain or forest.
    - The domains in the trust only trust each other and will not traverse any existing or future trust paths of either domain.

Configuring DNS for Trusts

- For trusts to work properly, they need to be able to resolve the forest or domain names of each side of the trust.
- Through the use of name resolution, you can configure Domain Name System (DNS) to properly resolve authoritative zones in forests or domains that are part of the trust.
- To successfully configure name resolution with the other domains or forests in the trust, consider implementing one of the following DNS solutions:
  - Conditional forwarders in each domain or forest DNS in a Windows Server environment or non-Windows Server environment
  - Shared Root DNS Server solution
  - Secondary DNS zone to connect to DNS server in a Windows Server environment or non-Windows Server environment

Creating External Trusts

Lesson 15: Configuring Trusts

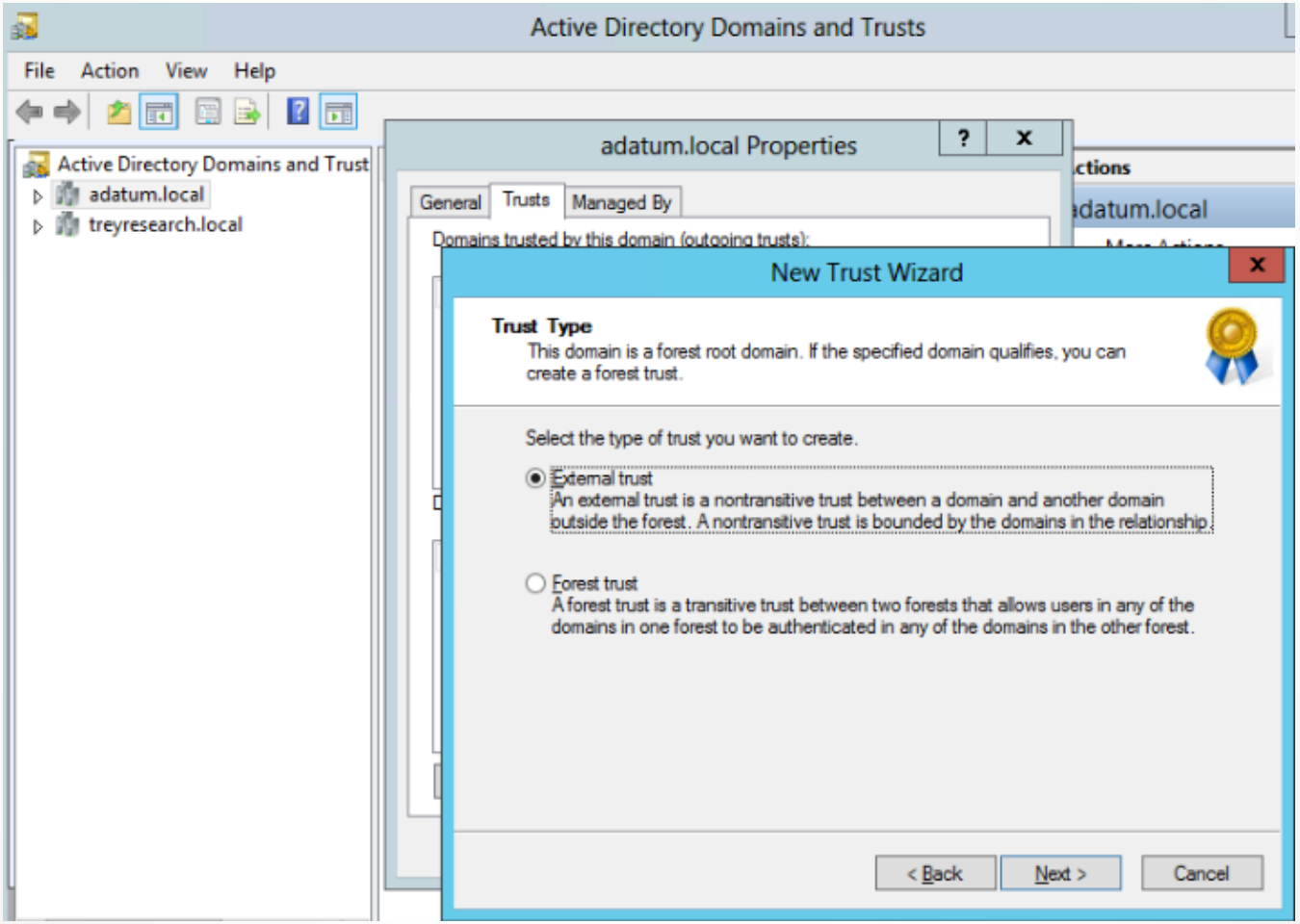
External Trust

- An ***external trust***
  - Is a one-way or two-way nontransitive trust between domains that are not in the same forest, and that are not already included in a forest trust.
  - Connects two domains in separate forests to allow users in the trusted domain the capability to authenticate and/or access resources in the trusting domain.
- Because external trusts are nontransitive, any existing trusts already in place with the trusting domain cannot be traversed by members of the external trust's trusted domain users.

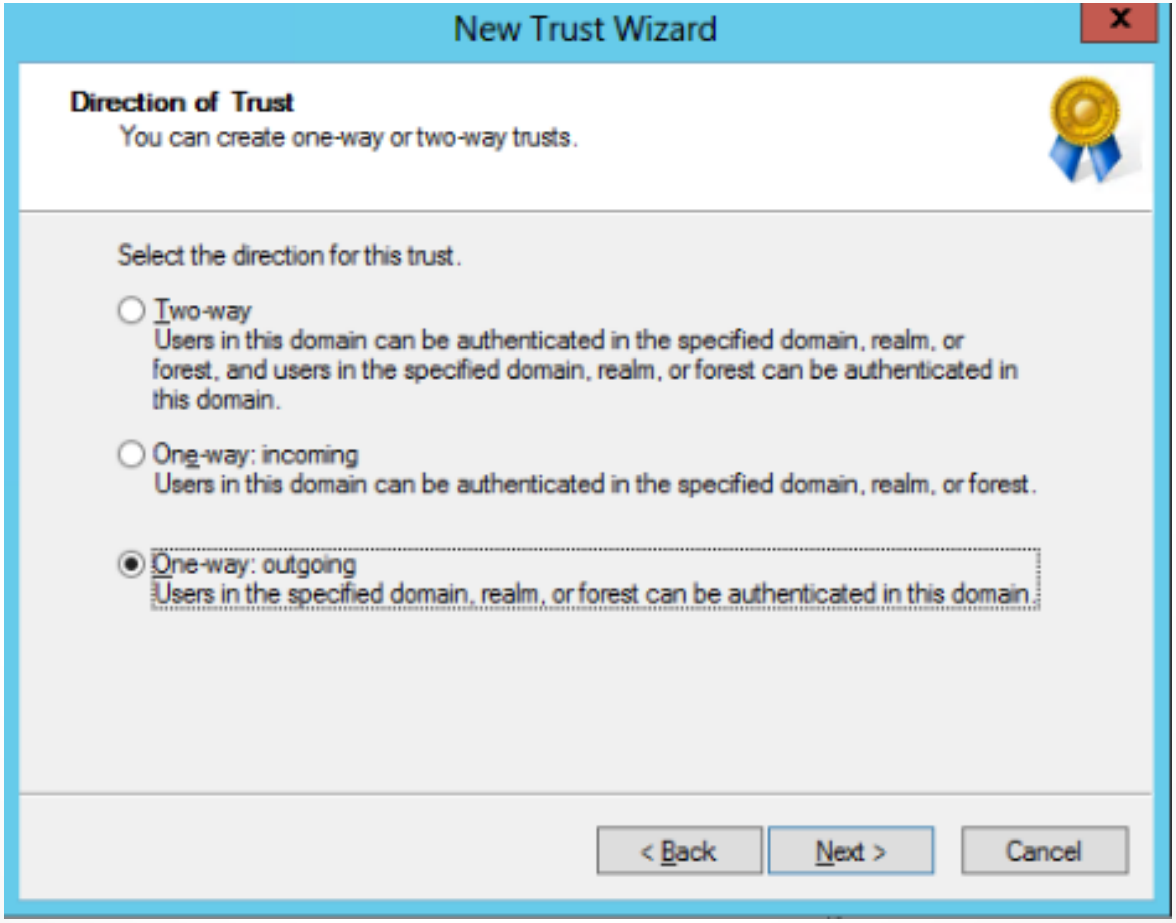
Creating External Trusts

- To accommodate external trusts, the trusting domain generates and stores, in AD DS, Foreign Security Principals for each security principal (Users, Computers, and Groups) of the trusted domain.
- This allows users of the trusted domain to become members of domain local groups in AD DS and to be added to Access Control Lists (ACL) of resources in the trusting domain.
- It is highly recommended to *not* modify the automatically generated Foreign Security Principals located in the trusting domain.

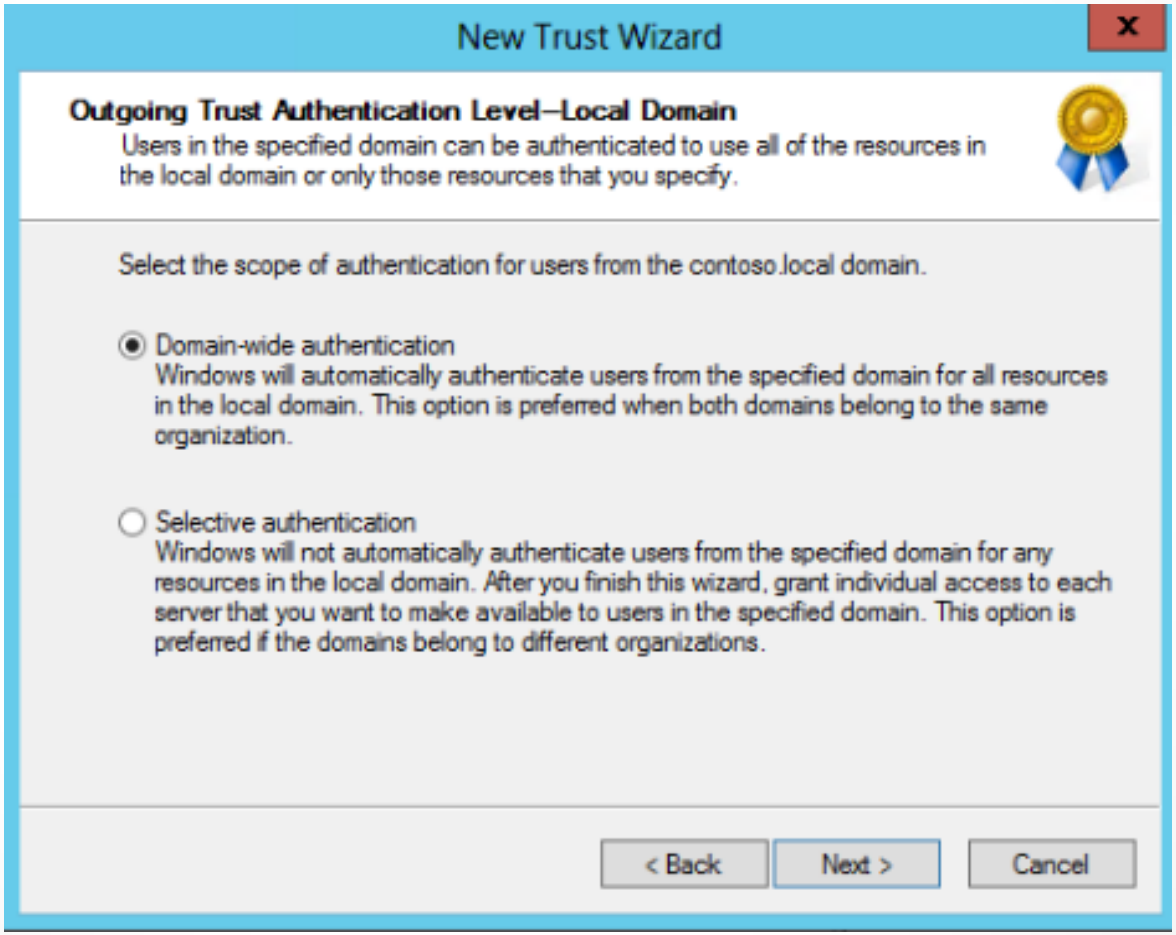
Creating External Trusts



Creating External Trusts



Creating External Trusts



Creating Forest Trusts

Lesson 15: Configuring Trusts

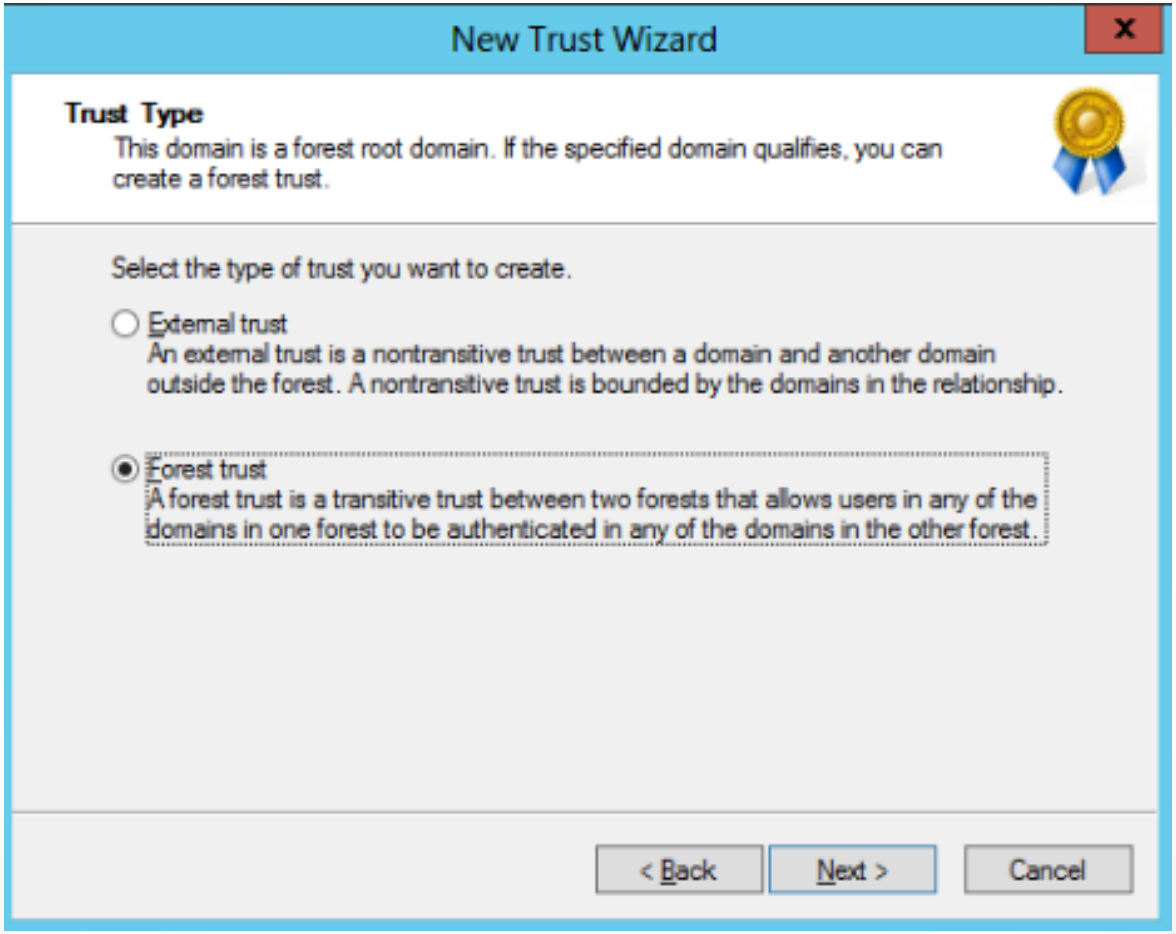
Creating Forest Trusts

- Forest trusts are implemented when users of an internal forest need to authenticate to and/or gain access to all resources of an external forest.
- When creating a forest trust, every domain within a forest has a two-way trust with one another from the forest root domain down; therefore, a forest trust is transitive to all domains within the trusting forest.
- Consider creating forest trusts in the following scenarios:
  - Integrating two forests during an acquisition or merger
  - Collaborating two businesses closely with one another
  - Combining all resources and users of a single company with multiple forests
  - Accessing an application provided by a service provider in a forest with another user forest

Creating Forest Trusts

- To create a forest trust, both domains of the trust must be the forest root domain and have a forest functional level of Windows Server 2003 or higher.
- The DNS infrastructure must be able to accommodate DNS requests between forests.
- You must be a member of the Domain Admins group, Enterprise Admins group, or have been delegated the authority with the appropriate permissions to create the trust.
- To create a two-way trust, you need an account in the external domain with the appropriate permissions or work closely with the other Domain Administrator or Enterprise Administrator to complete the two-way trust.

Creating Forest Trusts



Creating Shortcut Trusts

Lesson 15: Configuring Trusts

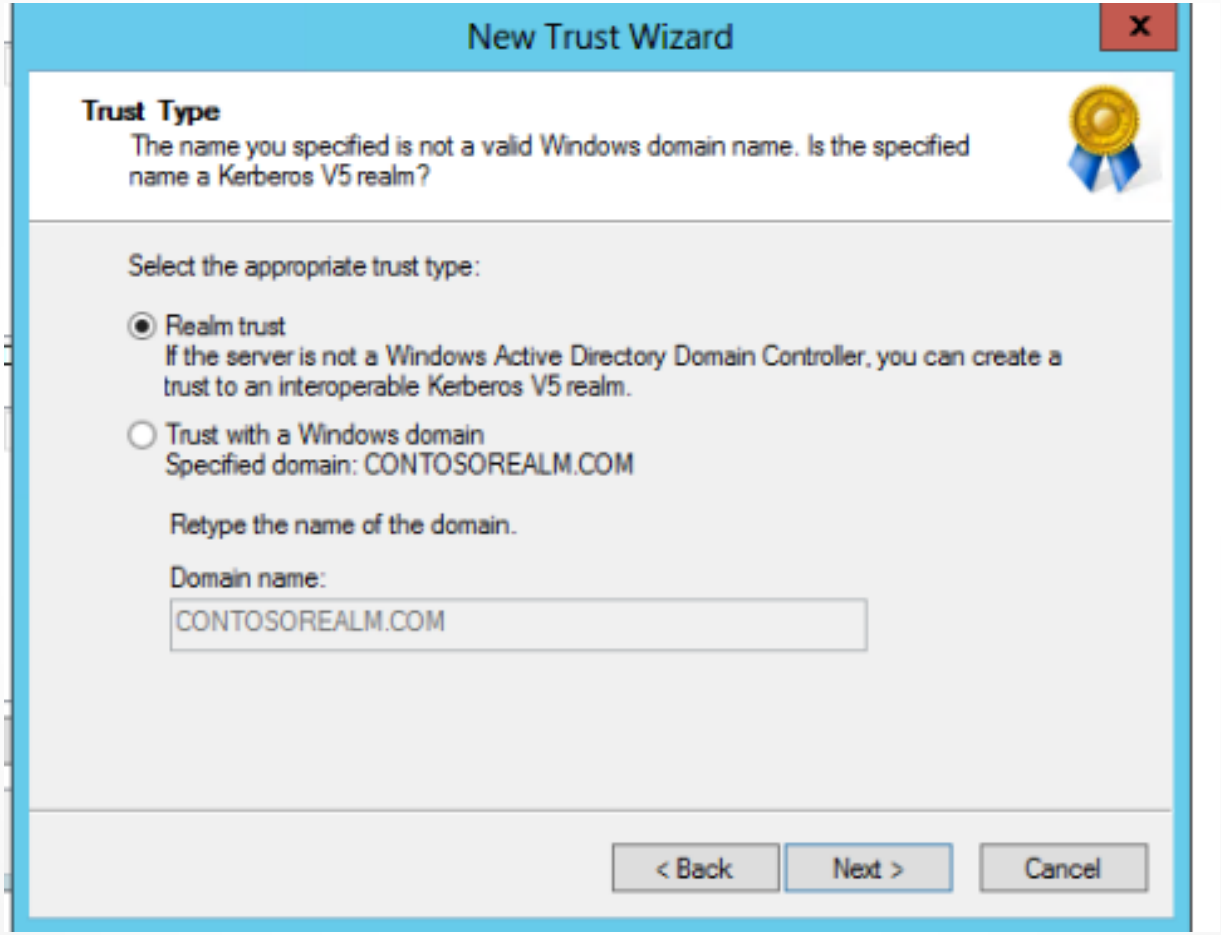
Shortcut Trusts

- A shortcut trust:
  - Is a one-way or two-way transitive trust between domains that are in the same forest.
  - Is primarily used to improve performance when authenticating to and accessing resources in an internal forest.
  - Can be one-way or two-way trusts; however, if only one, one-way trust is created, the authentication path will be optimized only for authentication to the trusting domain.
- If users of each domain are authenticating to one another's domain, create a two-way shortcut trust.

Creating Realm Trusts

- A realm trust
  - Is a one-way or two-way, transitive or nontransitive trust between an AD DS domain and a non-Microsoft Kerberos v5 realm.
  - Is used to allow users to authenticate and access resources in a non-Windows Kerberos v5 realm, or to allow users in a non-Windows Kerberos v5 realm access to resources in an AD DS domain.
- Because not all authentication domains and realms are Microsoft, this added benefit allows the non-Microsoft solutions interoperability with one another.

Creating Realm Trusts



Validating Trusts

Lesson 15: Configuring Trusts

Validating Trusts

- Existing trusts in an environment might need to be validated in the event of failure or problems between trusting and trusted domains.
- Validating trusts allows you to troubleshoot and reset trust relationships between trusts.
- You can validate a trust by using the Active Directory Domains and Trusts tool.
- Trusts between AD DS domains and forests can be validated.
- A realm trust cannot be validated.

Configuring Trust Authentication

Lesson 15: Configuring Trusts

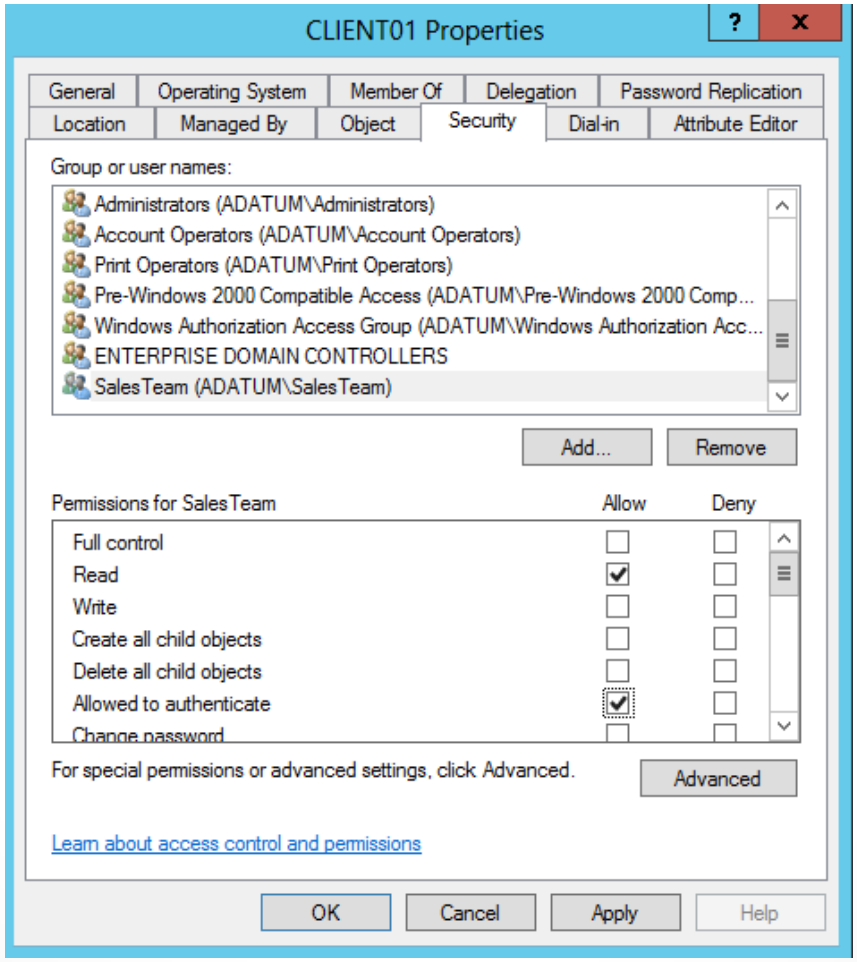
Trust Authentication

- Trust authentication defines how explicit the authentication and access to the trusting domain will be.
- There are three scopes of trust authentication: selective authentication, domain-wide authentication, and forest-wide authentication.
- Trust authentication is configured on external and forest trusts.

Selective Authentication

- ***Selective authentication*** allows explicit authentication and access to resources in an external trust or forest trust.
- In many cases, when you create an external trust or a forest trust, you will not want all users of the trusted domain to authenticate and access all resources in the trusting domain.
- By enabling selective authentication, you can prevent all users from having access, and you can then explicitly allow a security group or stand-alone user access to needed resources.
- The downside of implementing selective authentication is the administrative overhead involved to configure and maintain user access to resources.
- Each member server or computer account in the trusting domain that holds a required resource needs to be configured to allow authentication to the users in the trusted domain.

Selective Authentication



Domain-Wide Authentication

- In an external trust, ***domain-wide authentication*** allows unrestricted user access by users in the trusted domain to the resources in the trusting domain.
- After an external trust is created, all users in the trusted domain will be able to authenticate and access the resources in the trusting domain.

Forest-Wide Authentication

- ***Forest-wide authentication*** allows unrestricted user authentication and access by users in the trusted forest to the resources in the trusting forest.
- After forest trust creation, all users in the trusted forest will be able to authenticate and access the resources in the trusting forest.
- In a multi-domain forest, all users within each domain in the forest are able to authenticate and access resources in the trusting domain.

Configuring SID Filtering

Lesson 15: Configuring Trusts

SID Filtering

- SID Filtering protects trusting domains from malicious users.
- Malicious users might attempt to inject SIDs of an elevated user or group in the trusting domain to the sIDHistory of a user in the trusted domain.
- When SID Filtering is disabled, the malicious user can successfully inject the sIDHistory and gain privileged administrative access to resources in the trusting domain.
- It is best practice to keep SID Filtering enabled unless absolutely necessary.

Configuring Name Suffix Routing

Lesson 15: Configuring Trusts

Name Suffix Routing

- Name suffix routing manages how authentication requests are passed to each AD DS forest in a forest trust.
- When a forest trust is created, all unique suffixes are routed across the trust by default.
- This allows users in each forest the ability to authenticate to resources in the trusting forest through the means of a unique name suffix.
- Unique name suffixes must be unique to the forest and include the following suffixes:
  - User principal name (UPN)
  - Service principal name (SPN)
  - Domain Name System (DNS) name
  - Forest or domain tree name that is not a child to the tree

Lesson Summary

- The trusting domain holds the resources, and the trusted domain is where the users are that will authenticate and access the resources.
- There are four types of trusts that must be configured manually: external, forest, shortcut, and realm trusts.
- There are three types of configurable, trust authentication scopes: selective authentication, domain-wide authentication, and forest-wide authentication.
- There are benefits to keeping SID Filtering enabled and also certain conditions might require it to be disabled.

Lesson Summary

- Name suffix routing allows users from one domain or forest to authenticate to another domain or forest in a forest trust. There are also exclusions that can be created to prevent certain name suffixes from being routed. New name suffixes added after forest trust creation are disabled by default.