



IDENTITY WITH WINDOWS SERVER

20742 (55351AC)

Module 3: Advanced AD DS infrastructure management

Module overview

- Lesson 1: Overview of advanced AD DS deployments
- Lesson 2: Deploy a distributed AD DS environment
- Lesson 3: Configure AD DS trusts



Lesson 1: Overview of advanced AD DS deployments

Lesson 1 overview

- Overview of domain and forest boundaries
- Implementation of multiple domains and forests
- Deploy a DC in Azure virtual machine (VM)
- Manage objects in complex AD DS deployments

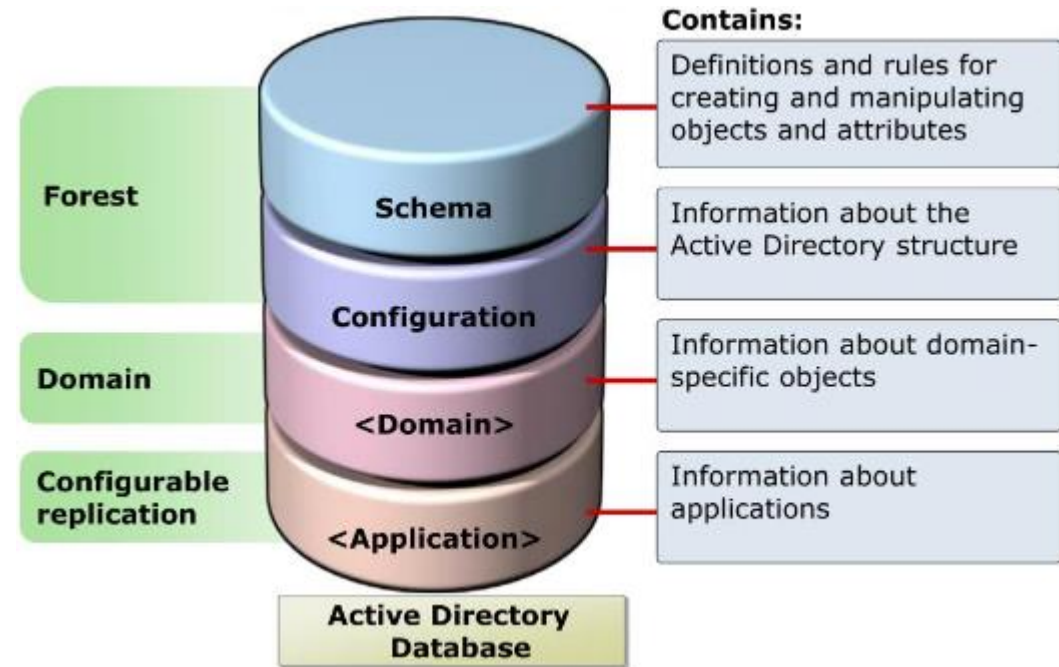
Overview of domain and forest boundaries

- Advanced AD DS deployments typically consist of multiple domains and forests.
- The choice between creating a domain in a new or an existing forest is commonly based on the differences between the domain and forest boundaries.

Domain boundaries	Forest boundaries
Domain naming context replication	Schema and configuration naming contexts replication
DNS zone replication (domain-wide)	DNS zone replication (forest-wide)
Delegated administration	Security isolation
Group Policy Object scoping	Global Catalog replication

Active Directory Partitions

- **Schema partition** - Replicates to all DCs in forest
- **Configuration partition** – Replications to all DCs in the forest
- **Domain partition** - Replicates to all DCs within a domain. The object portion becomes part of Global Catalog.
- **Application partition** - Example: AD integrated DNS, two application partitions for DNS zones
 - ForestDNSZones replicated to all DCs in the forest
 - DomainDNSZones replicated to all DCs in the domain
- NTDS.dit file



Implementation of multiple domains and forests

The recommended approach is to start your AD DS design with a single-domain forest.

Avoid creating additional domains/forests unless the required functionality cannot be accommodated by the existing design.

Common reasons for multiple domains	Common reasons for multiple forests
Bandwidth limitations	Bandwidth limitations
Distributed support/operational model	Security isolation
Separation of resource/user administration	Conflicting schema requirements
Separation of forest-level operations (empty root domain)	Regulatory/compliance requirements
	Extranet deployments
	Business mergers and divestitures

Deploy a DC in an Azure virtual machine (VM)

- Create a Microsoft Azure virtual network and a separate AD DS site.
 - AD DS authentication of cloud workloads
 - Disaster recovery
- Set up hybrid connectivity when extending on-premises AD DS.
- Assign a static IP at the platform level (not within the OS).
- Configure DNS server settings at the virtual network level:
 - Initially point to on-premise DNS
 - Set to an existing DNS server during promotion.
 - Set to the newly promoted DC after promotion.
- Disable caching for the disks hosting the AD DS database, logs, and SYSVOL.
- Avoid stopping/deallocating the Azure VM (use OS shutdown instead).

Manage objects in complex AD DS deployments

- User object management:
 - A workflow triggered by HR database updates.
 - Self-services for account unlock and password resets.
- Group object management:
 - Dynamic group membership tied to user object attributes.
 - Self-service for creating groups and managing their memberships.
- Certificate management:
 - Multiple CAs with cross-certifications and qualified subordination.
 - Consistent approach to template publishing, enrollment policies, and certificate revocation.
- Microsoft Identity Manager



Lesson 2: Deploy a distributed AD DS environment

Lesson 2 overview

- AD DS domain and forest functional levels
- Deploy new AD DS domains
- Demonstration: Install a DC in a new domain in an existing forest
- Upgrade and migrate AD DS domains
- Factors to consider when implementing complex AD DS environments

AD DS domain and forest functional levels

- Determine capabilities available in AD DS domains and forests.
- Determine the lowest OS version of AD DS DCs:
 - Does not restrict to the OS version supported on domain-joined computers.
 - Might affect the functionality available on domain-joined computers.
- Windows Server 2016 is the most recent OS associated with the domain and forest functional level updates.
- Windows Server 2022 DCs require, at minimum, Windows Server 2008 domain and forest functional level.
- Starting with Windows Server 2008 R2, it's possible to revert an update provided the optional features of the new version have not been activated.

AD DS domain functional levels (1 of 3)

OS version	Functionality
Windows 2000 Server	<ul style="list-style-type: none">• Universal groups and group nesting.• Conversion between security and distribution groups.• Introduction of the Security Identifier (SID)-History attribute.
Windows Server 2003	<ul style="list-style-type: none">• Support for renaming DCs.• Introduction of the lastLogonTimestamp attribute and inetOrgPerson object.• Customizable default location for new user and computer objects.• Support for constrained delegation.• Support for selective authentication.• Introduction of application partitions.
Windows Server 2008	<ul style="list-style-type: none">• Support of DFS-Replication for replication of SYSVOL.• Tracking additional interactive logon information for each user object.• Support for fine-grained password policy.• Support for AES 128 and 256 with Kerberos authentication.• Introduction of RODCs.

AD DS domain functional levels (2 of 3)

OS version	Functionality
Windows Server 2012	<ul style="list-style-type: none">• Support KDC for claims, compound authentication, and Kerberos armoring.
Windows Server 2012 R2	<ul style="list-style-type: none">• Introduction of Protected Users prevented from:<ul style="list-style-type: none">• Authenticating by using NTLM authentication, Digest authentication, or CredSSP.• Using DES and RC4 cipher suites in Kerberos preauthentication.• Being delegated with unconstrained or constrained delegation.• Renewing user TGTs beyond the initial four-hour lifetime.• Introduction of authentication policies and authentication policy silos.
Windows Server 2016	<ul style="list-style-type: none">• PAM support for time-bound membership in privileged security groups.• Support for hybrid Azure AD join.

AD DS forest functional levels (3 of 3)

OS version	Functionality
Windows Server 2003	<ul style="list-style-type: none">• Forest trusts• Linked-value replication• Support for RODCs• Support for conversion between inetOrgPerson objects and user objects• Support for deactivating and redefining attributes and object classes
Windows Server 2008 R2	<ul style="list-style-type: none">• Introduction of optional features (starting with AD DS Recycle Bin)
Windows Server 2016	<ul style="list-style-type: none">• Privileged access management using Microsoft Identity Manager

Deploy new AD DS domains

- Creating a domain in a new forest forms a forest root domain.
- Additional domains in the same forest can be of one of two types:
 - Child domain:
 - The same namespace as the root
 - Tree domain:
 - A new, different namespace

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window, specifically the 'Deployment Configuration' step. The window title is 'Active Directory Domain Services Configuration Wizard'. The main heading is 'Deployment Configuration'. On the right, it says 'TARGET SERVER vm0'. A left-hand navigation pane lists the steps: 'Deployment Configuration' (selected), 'Domain Controller Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main content area is titled 'Select the deployment operation' and contains three radio buttons: 'Add a domain controller to an existing domain', 'Add a new domain to an existing forest' (which is selected), and 'Add a new forest'. Below this, the section 'Specify the domain information for this operation' contains three fields: 'Select domain type:' with a dropdown menu showing 'Child Domain', 'Parent domain name:' with a text box containing 'contoso.com' and a 'Select...' button, and 'New domain name:' with a text box containing 'us.contoso.com'. Below these fields, the section 'Supply the credentials to perform this operation' shows '<No credentials provided>' and a 'Change...' button. At the bottom right, there is a link 'More about deployment configurations'. The bottom of the window has four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.



**Demonstration: Install
a DC in a new domain in
an existing forest**

Upgrade and migrate AD DS domains

- Upgrade:
 1. Apply adprep AD DS schema updates:
 - Can be combined with the next step.
 2. Introduce a DC running a newer OS version:
 - Upgrade in place the Windows Server OS on existing DCs.
 - Deploy another server running the newer Windows OS as a DC.
- Migrate by using ADMT and leveraging **SID-History**:
 1. Create a restructuring plan.
 2. Prepare source and target domains.
 3. Migrate accounts.
 4. Migrate resources.
 5. Finalize migration.

Factors to consider when implementing complex AD DS environments

- DNS considerations:
 - Use AD DS–integrated DNS zones.
 - Choose between the centralized and decentralized model.
 - Verify DNS client settings.
 - Optimize cross-namespace name resolution.
- UPN considerations:
 - The choice of UPN suffixes.
 - The availability of Global Catalogs.



Lesson 3: Configure AD DS trusts

AD DS trusts

- Additional content in [Windows AD Trusts - Additional content](#) document

Lesson 3 overview

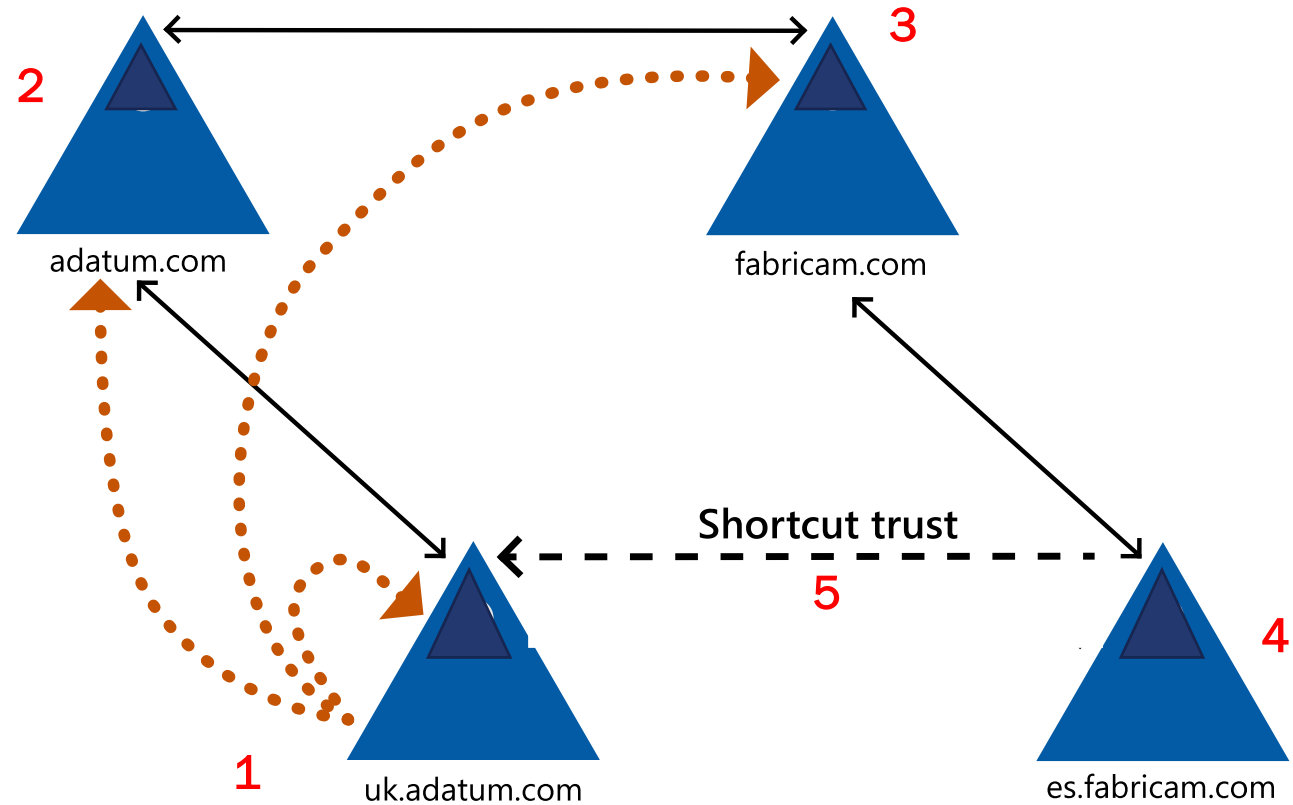
- Overview of AD DS trust types
- How do trusts work in a forest?
- How do trusts work between forests?
- Configure advanced AD DS trust settings
- Demonstration: Configure a forest trust

Overview of AD DS trust types

Trust type	Transitivity	Direction	Description
Parent and child	Transitive	Two-way	Created automatically when adding a domain to an AD DS tree.
Tree-root	Transitive	Two-way	Created automatically when you add an AD DS domain tree to an existing AD DS forest.
External	Nontransitive	One-way or two-way	Created explicitly between the local domain and an AD DS domain in another forest.
Realm	Transitive or nontransitive	One-way or two-way	Created explicitly between the local domain and a Kerberos v5 realm implemented by using a directory service other than AD DS.
Forest	Transitive	One-way or two-way	Trusts between two AD DS forests.
Shortcut	Transitive	One-way or two-way	Created explicitly between the local domain and another domain in the same forest.

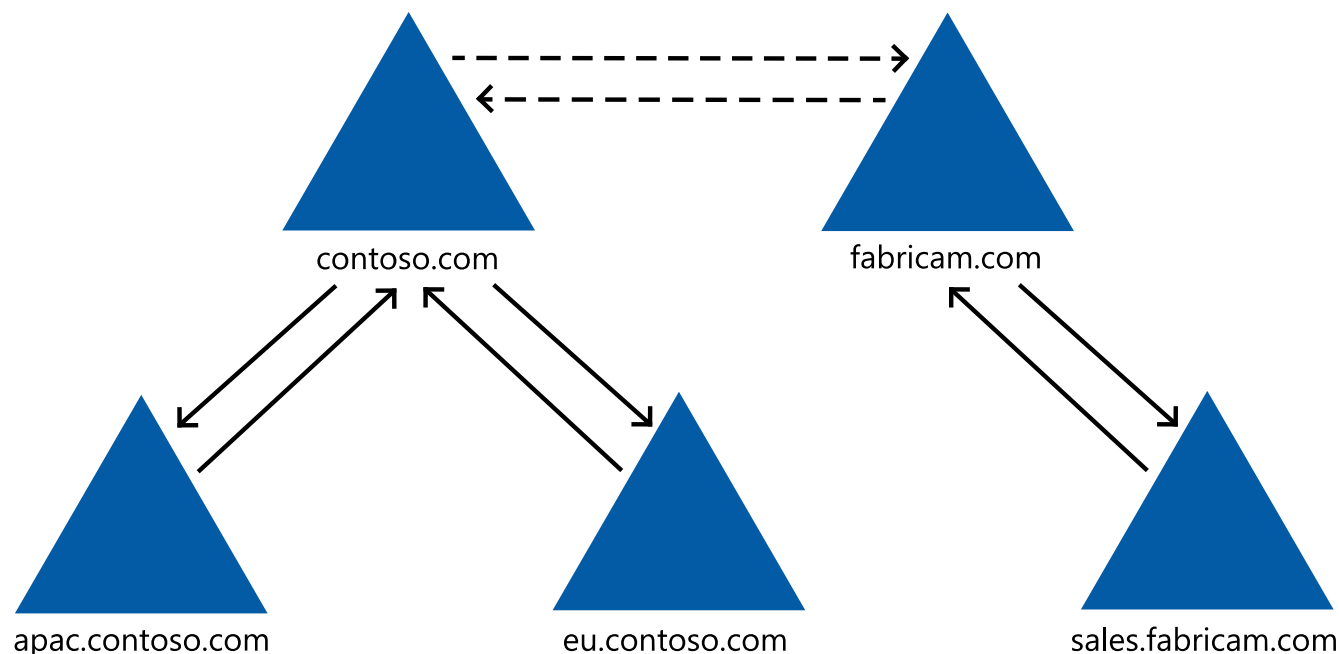
How do trusts work in a forest?

Uk.adatum.com
user on computer
CL1.uk.adatum.com
requests access to a file
share on a domain-joined
computer in
es.fabrikam.com.



How do trusts work between forests?

- Transitivity:
 - Extends to all domains on the other side of the trust.
 - Does not extend to forests trusted by the trusted forest.
- Kerberos-based authentication.
- UPN-based sign-in that leverages UPN suffix routing.



Configure advanced AD DS trust settings

- SID filtering:
 - Prevents potential exploit by blocking SIDs from domains/forests other than the directly trusted one.
- Authentication options:
 - Domain-wide (for domain trusts) or forest-wide (for forest trusts).
 - Users from the trusted domain/forest, constitute Authenticated Users.
 - Selective authentication.
 - Users from the trusted domain/forest require two levels of authorization:
 - On the computer object hosting a target resource (based on the Allowed to Authenticate permission).
 - On the shared resource (based on the resource ACL).





Lab 4: Domain and trust management in AD DS




Knowledge check

Knowledge check


1. What is the replication scope of the domainDnsZones partition?
 - a. All DCs in the domain
 - b. All DCs in the forest
 -  c. All DCs in the domain that host the DNS server role
 - d. All DCs in the forest that host the DNS server role
2. What is the replication boundary for DCs designated as Global Catalog servers?
 - a. All DCs in the domain
 -  b. All DCs in the forest
 - c. All DCs in the domain that host the DNS server role
 - d. All DCs in the forest that host the DNS server role

Knowledge check



3. What should the **Host Cache Preference** be set to for disks when the AD DS database resides on an Azure VM hosting a DC?

-  a. None
- b. Read only
- c. Write only
- d. Read and write

4. What is the most recent version of the Windows Server operating system associated with distinct functional levels?

- a. Windows Server 2012 R2
-  b. Windows Server 2016
- c. Windows Server 2019
- d. Windows Server 2022

Knowledge check

5. Which type of trust relationship can you create explicitly between two domains in the same forest?
- a. Forest
 - b. Parent and child
 -  c. Shortcut
 - d. Tree root
6. When using selective authentication between two domains, where should the Allowed to Authenticate permission be assigned to allow a user from the trusted domain to access resources hosted on a computer in the trusting domain?
- a. Trusting forest
 - b. Trusted forest
 - c. User account in the trusting forest
 -  d. Computer account in the trusted forest

Learn more

For more information, refer to:

- [Active Directory Domain Services Overview](#)

Thank you

©2022 Waypoint Ventures, LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.