Microsoft® Official Course

Module 4

Implementing Distributed Active Directory® Domain Services Deployments

Microsoft®

Module Overview

- Overview of Distributed AD DS Deployments
- Deploying a Distributed AD DS Environment
- Configuring AD DS Trusts

Lesson 1: Overview of Distributed AD DS Deployments

- Discussion: AD DS Components Overview
- Overview of Domain and Forest Boundaries in an AD DS Structure
- Why Implement Multiple Domains?
- Why Implement Multiple Forests?
- Integrating On-Premises AD DS with Cloud Services
- Implementing Windows Azure AD
- DNS Requirements for Complex AD DS Environments

Discussion: AD DS Components Overview

- What is an AD DS domain?
- What is an AD DS tree?
- What is an AD DS forest?
- What is a trust relationship?
- What is the global catalog?

Overview of Domain and Forest Boundaries in an AD DS Structure

AD DS object	Boundary type
Domain	Domain partition replication
	Administrative permissions
	Group Policy application
	Auditing
	Password and account policies
	Domain DNS zone replication
Forest	Security boundary
	Schema partition replication
	Configuration partition replication
	Global catalog replication
	Forest DNS zone replication

Why Implement Multiple Domains?

Organizations may choose to deploy multiple domains to meet:

- Domain replication requirements
- DNS namespace requirements
- Distributed administration requirements
- Forest administrative group security requirements
- Resource domain requirements

Why Implement Multiple Forests?

Organizations may choose to deploy multiple forests to meet:

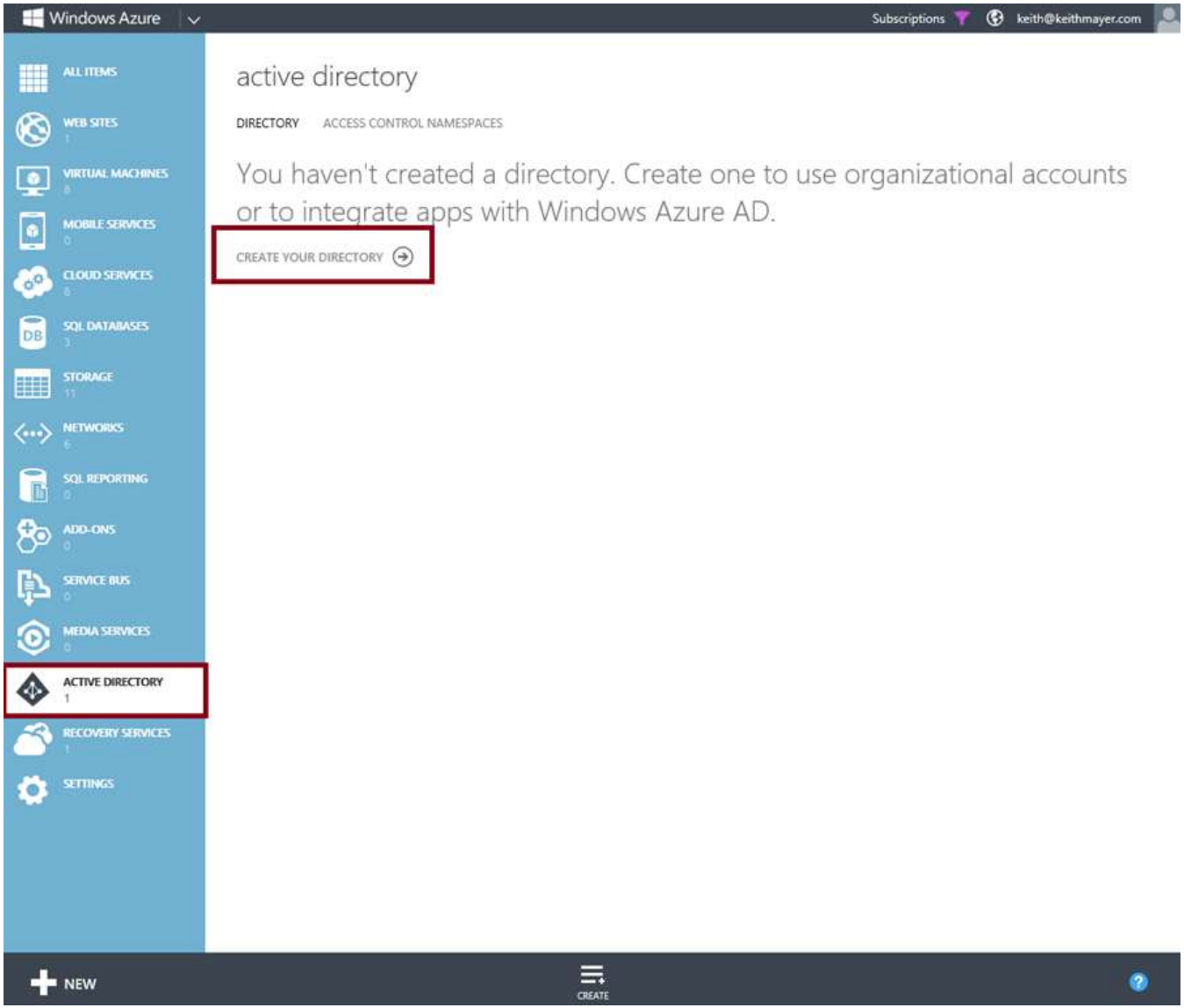
- Security isolation requirements
- Incompatible schema requirements
- Multinational requirements
- Extranet security requirements
- Business merger or divestiture requirements

Integrating On-Premises AD DS with Cloud Services

- Windows Azure AD:
  - Is a shared environment
  - Updating and upgrading is maintained by Microsoft
  - Can synchronize with on-premises AD DS
  - Does not support AD DS integrated applications

- AD in Windows Azure:
  - Is a private environment
  - Updating and upgrading is the responsibility of the customer
  - Can be part of on-premises AD DS
  - Supports AD DS-aware applications

Implementing Windows Azure AD



DNS Requirements for Complex AD DS Environments

When implementing DNS in a complex AD DS environment, you should:

- Verify the DNS client configuration
- Verify and monitor DNS name resolution
- Optimize DNS name resolution between multiple namespaces
- Use AD DS integrated DNS zones
- Consider deploying a GlobalNames zone
- Design interoperability for DNS in Windows Azure and on-premise

Lesson 2: Deploying a Distributed AD DS Environment

- Demonstration: Installing a Domain Controller in a New Domain in an Existing Forest
- AD DS Domain Functional Levels
- AD DS Forest Functional Levels
- Upgrading a Previous Version of AD DS to Windows Server 2012 R2
- Migrating to Windows Server 2012 R2 AD DS from a Previous Version

Demonstration: Installing a Domain Controller in a New Domain in an Existing Forest

In this demonstration, you will see how to:

- Configure an AD DS domain controller
- Access the AD DS domain controller

AD DS Domain Functional Levels

New functionality requires that domain controllers are running a particular version of Windows

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

- Cannot raise functional level while domain controllers are running previous Windows Server versions

- Cannot add domain controllers running previous Windows Server versions after raising functional level

AD DS Forest Functional Levels

Windows Server 2003:

- Forest trusts
- Domain rename
- Linked-value replication
- Support for RODCs
- Improved KCC
- Conversion of inetOrgPerson objects to user objects
- Deactivation and redefinition of attributes and object classes

Windows Server 2008:

- No new features; sets minimum level for all new domains

Windows Server 2008 R2:

- Active Directory Recycle Bin

Windows Server 2012:

- No new features; sets minimum level for all new domains

Windows Server 2012 R2:

- No new features; sets minimum level for all new domains

Upgrading a Previous Version of AD DS to Windows Server 2012 R2

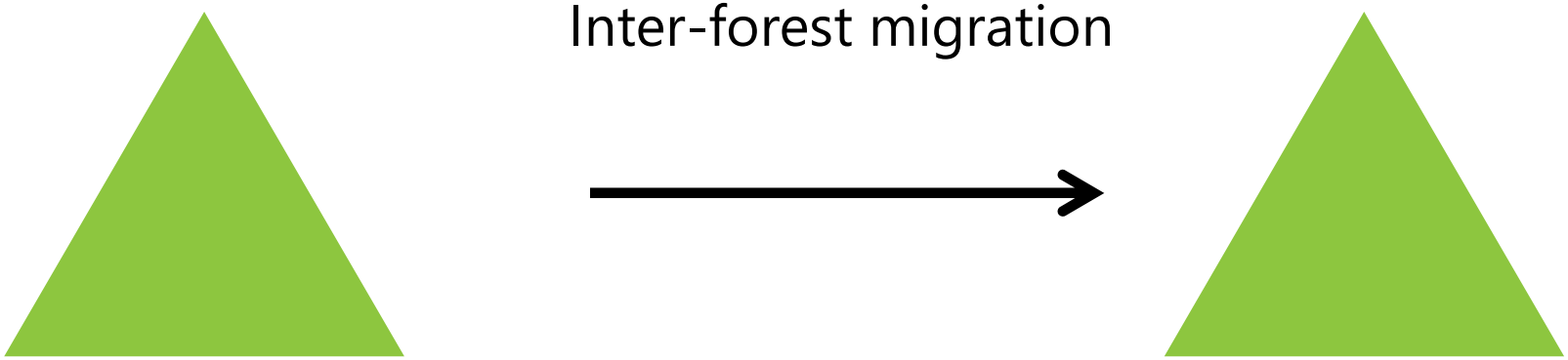
Options to upgrade AD DS to Windows Server 2012 R2:

- In-place upgrade (from Windows Server 2008, Windows Server 2008 R2 or Windows 2012)
  - Only domain controllers running Windows Server 2008 x64, Windows Server 2008 R2, or Windows 2012 can be upgraded
- Introduce a new Windows Server 2012 R2 server into the domain and promote it to be a domain controller
  - This option is recommended
- Both options require that the schema is at the Windows Server 2012 R2 level
  - The Active Directory Domain Services Installation Wizard will upgrade the schema automatically when run with appropriate permissions
  - ADPrep is available

Migrating to Windows Server 2012 R2 AD DS from a Previous Version

fabrikam.net

Adatum.com



Security Principals that are migrated:

- User accounts
- Managed service accounts
- Computer accounts
- Groups

Accounts get new SIDs, but resource access is maintained by using SID History

Migrating to Windows Server 2012 R2 AD DS from a Previous Version

fabrikam.net

Adatum.com

Department	IT
distinguishedName	CN=April Reagan,OU=IT,DC=fabrikam,DC=net
givenName	April
name	April Reagan
objectSID	S-1-5-21-322346712-1256085132-1900709958-1375

Department	IT
distinguishedName	CN=April Reagan,OU=IT,DC=Adatum,DC=com
givenName	April
name	April Reagan
objectSID **NEW**	S-1-5-21-433457823-2367196243-2011810069-2486
sIDHistory	S-1-5-21-322346712-1256085132-1900709958-1375

Security Principals that are migrated:

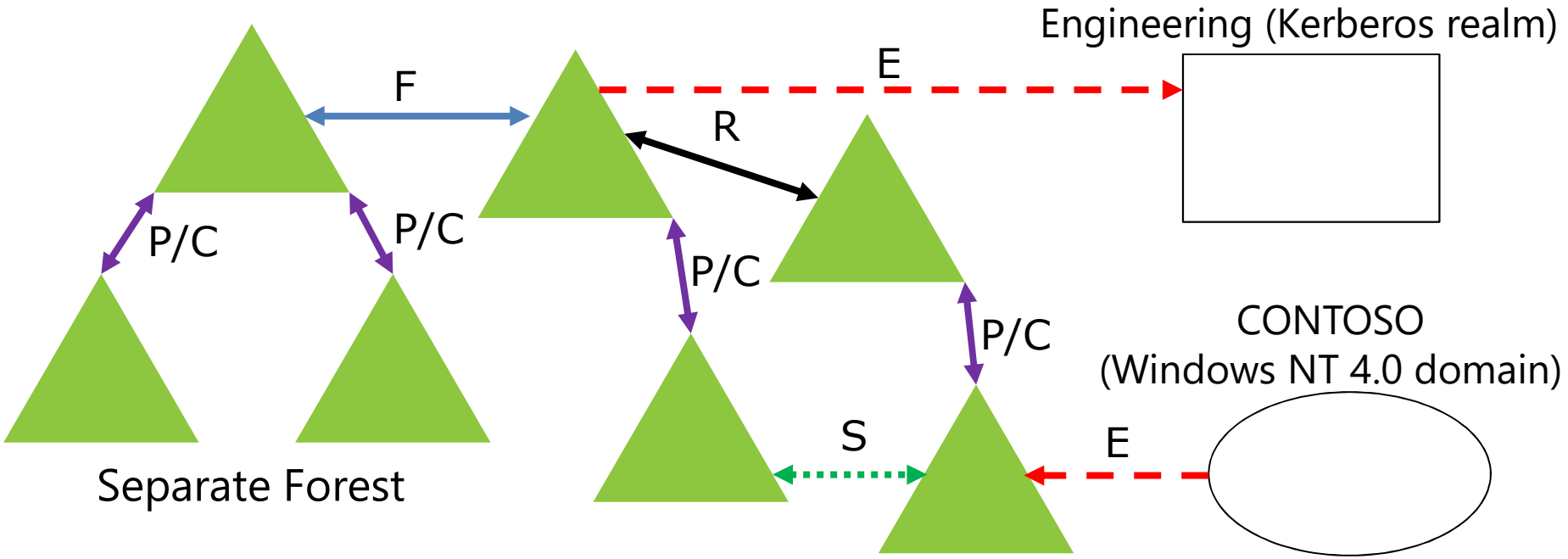
- User accounts
- Managed service accounts
- Computer accounts
- Groups

Accounts get new SIDs, but resource access is maintained by using SID History

Lesson 3: Configuring AD DS Trusts

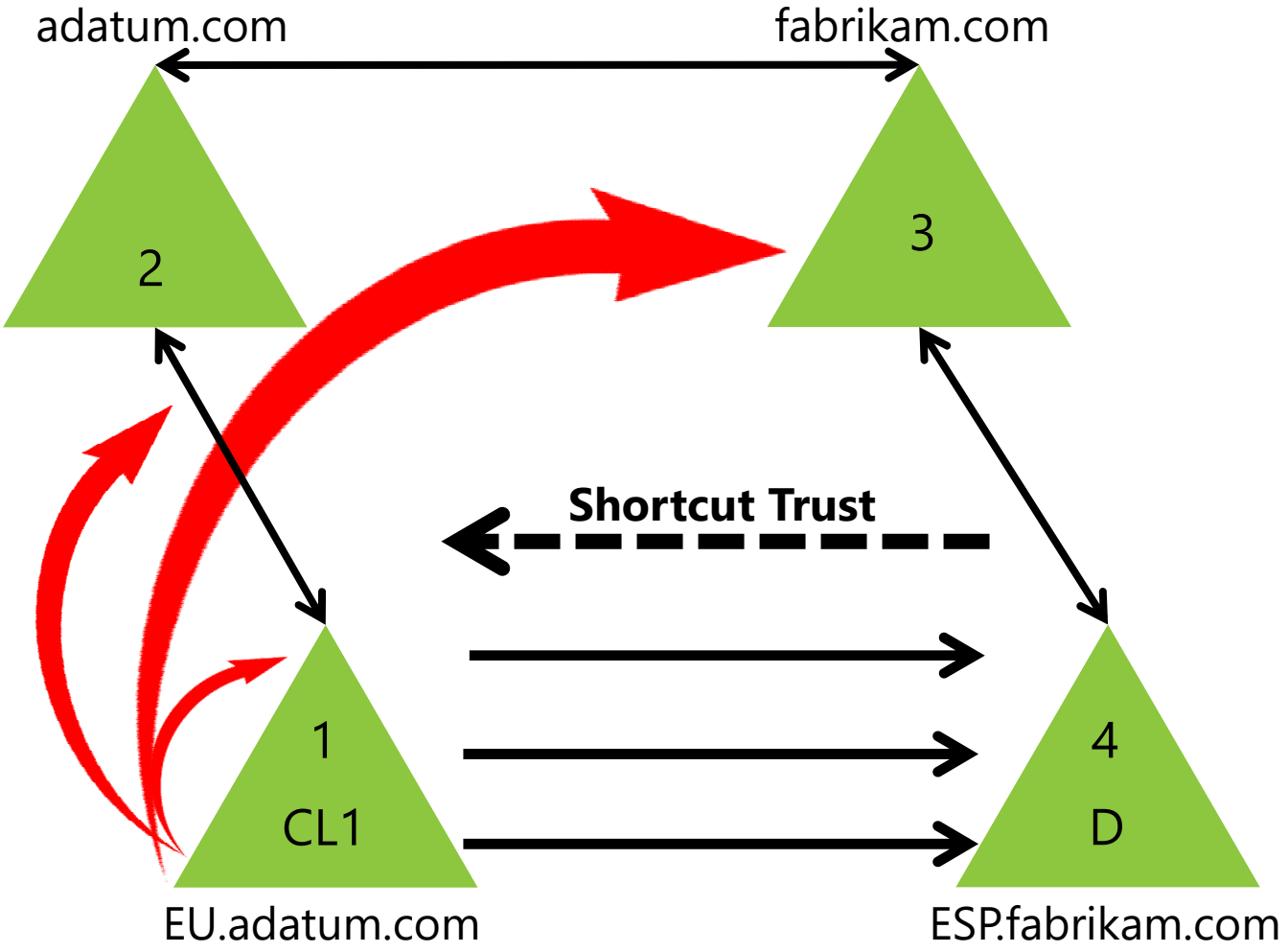
- Overview of Different AD DS Trust Types
- How Trusts Work Within a Forest
- How Trusts Work Between Forests
- Configuring Advanced AD DS Trust Settings
- Demonstration: Configuring a Forest Trust

Overview of Different AD DS Trust Types



Trust type	Transitive?	Color
P/C - Parent-child	Yes	Purple
R - Tree root	Yes	Black
E - External (domain or Kerberos realm)	No	Red/Dashed
S - Shortcut	Yes	Green/Dotted
F - Forest (complete or selective)	Yes	Blue

How Trusts Work Within a Forest

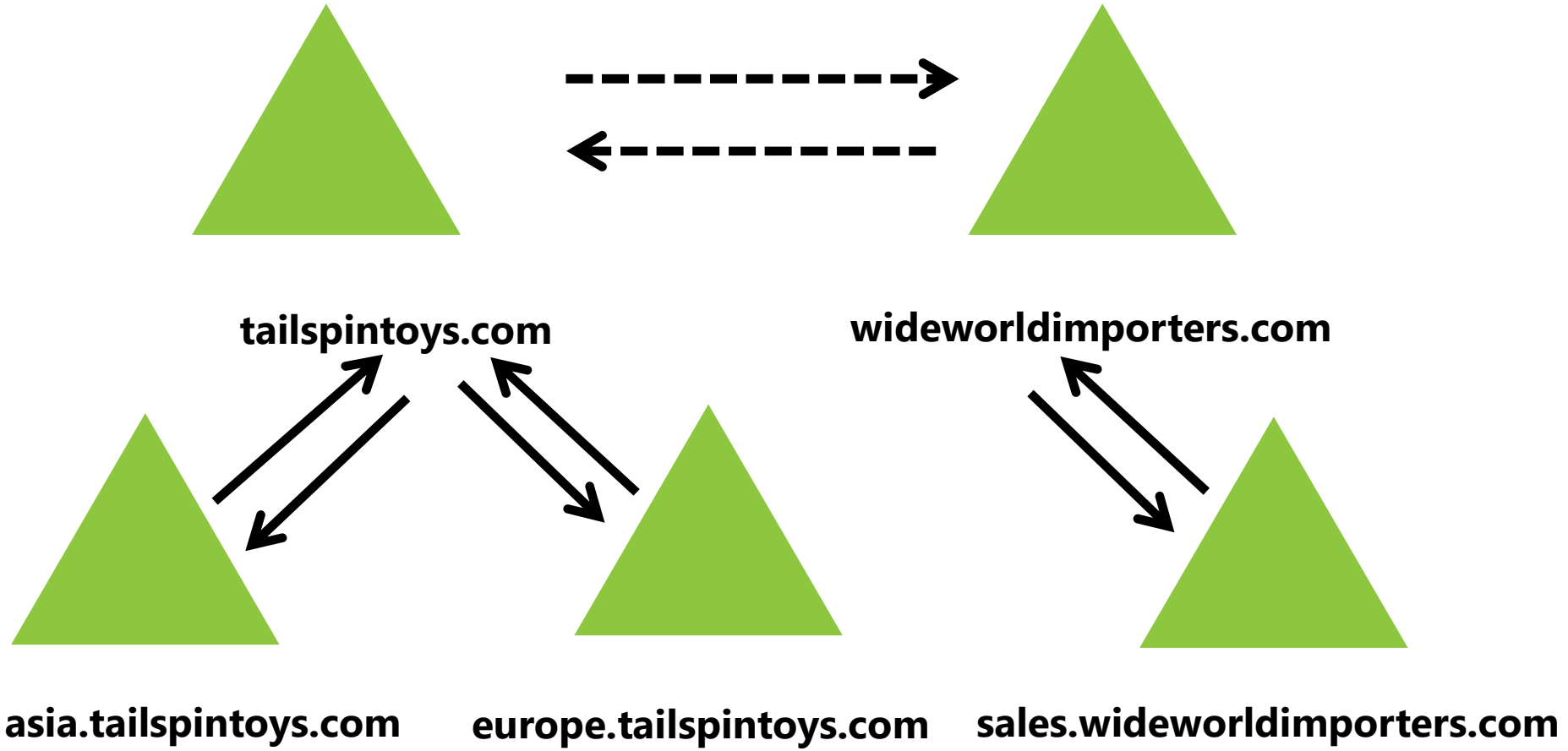


Client computer CL1 requests access to a file on File server D

How Trusts Work Between Forests

What Is a Forest Trust?

A forest trust is a one-way or two-way trust relationship between the forest root domains of two forests



Configuring Advanced AD DS Trust Settings

Security considerations in forest trusts:

- SID filtering
- Selective authentication
- Name suffix routing

An incorrectly configured trust can allow unauthorized access to resources

Demonstration: Configuring a Forest Trust

In this demonstration, you will see how to:

- Configure DNS Name Resolution by using a conditional forwarder
- Configure a two-way selective forest trust

Lab: Implementing Distributed AD DS Deployments

- Exercise 1: Implementing Child Domains in AD DS
- Exercise 2: Implementing Forest Trusts

Logon Information

Virtual Machines 20412D-LON-DC1,
20412D-TOR-DC1,
20412D-LON-SVR2,
20412D-TREY-DC1
User Name: Adatum\Administrator
Password: Pa$$w0rd

Estimated Time: 45 minutes

Lab Scenario

A. Datum Corporation has deployed a single AD DS domain with all the domain controllers located in its London datacenter. As the company has grown and added branch offices with large numbers of users, it is becoming increasingly apparent that the current AD DS environment does not meet company requirements. The network team is concerned about the amount of AD DS–related network traffic that is crossing WAN links, which are becoming highly utilized.

The company has also become increasingly integrated with partner organizations, some of which need access to shared resources and applications that are located on the A. Datum internal network. The security department at A. Datum wants to ensure that the access for these external users is as secure as possible.

Lab Scenario

As one of the senior network administrators at A. Datum, you are responsible for implementing an AD DS infrastructure that will meet the company requirements. You are responsible for planning an AD DS domain and forest deployment that will provide optimal services for both internal and external users, while addressing the security requirements at A. Datum.

Lab Review

- Why did you configure a delegated subdomain record in DNS on LON-DC1 before adding the child domain na.adatum.com?
- What are the alternatives to creating a delegated subdomain record in the previous question?
- When you create a forest trust, why would you create a selective trust instead of a complete trust?

Module Review and Takeaways

- Common Issues and Troubleshooting Tips