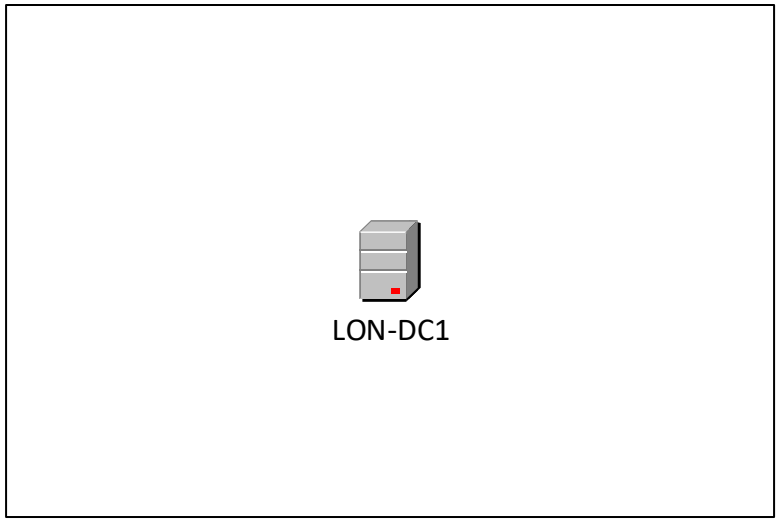
Windows Active Directory Trusts

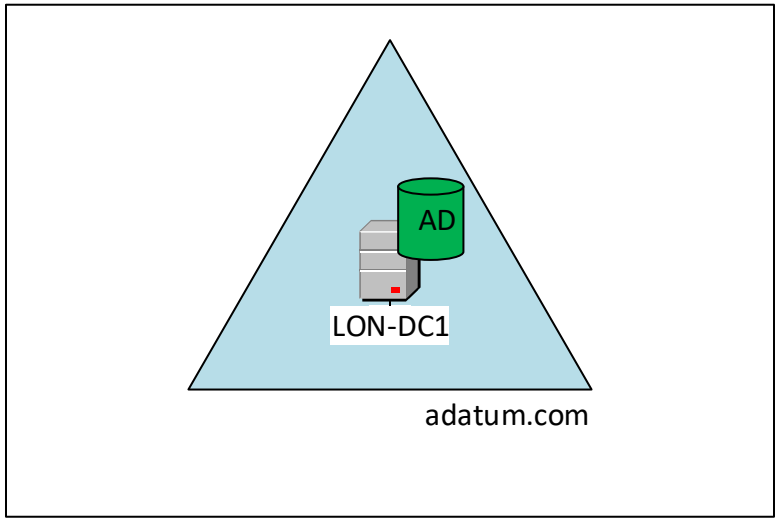
COOS295

Active Directory Domain



1st domain in 1st tree in forest:

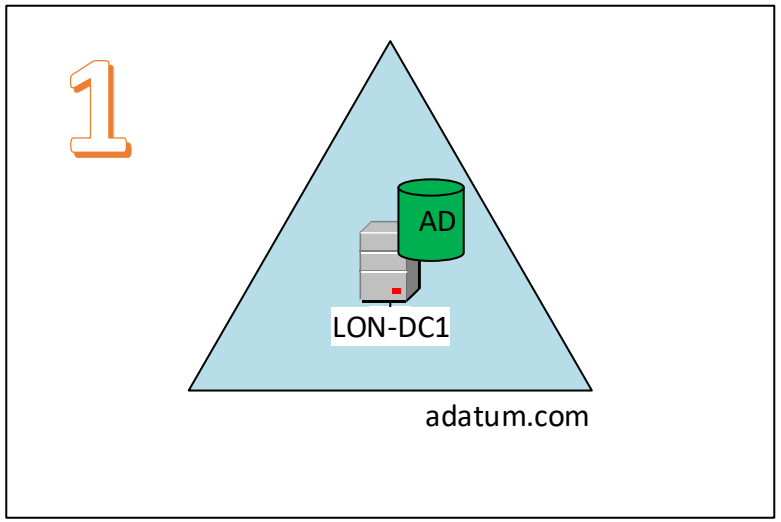
- Tree root domain
- Forest root domain

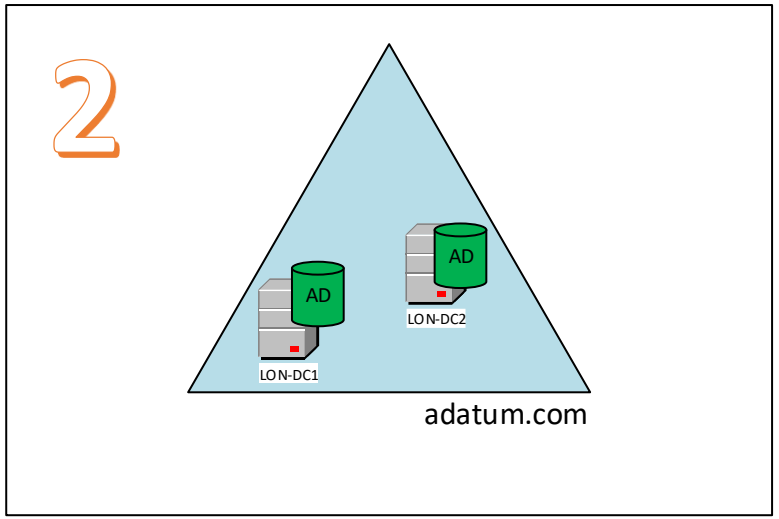


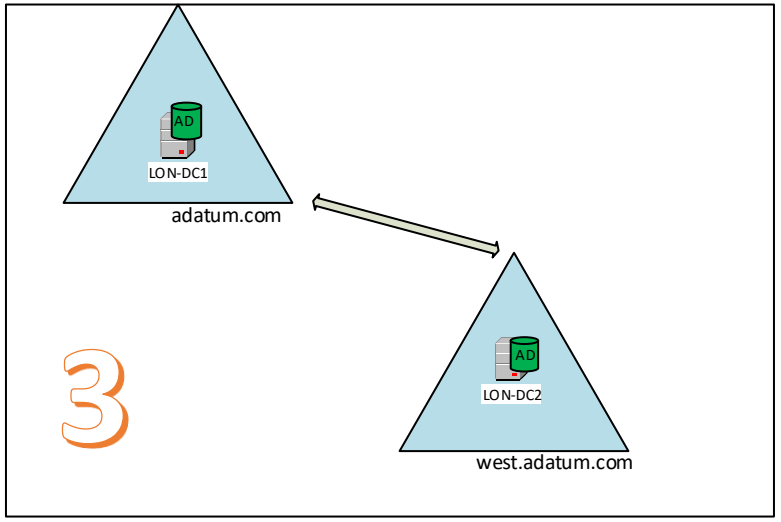
Creating a Domain Controller

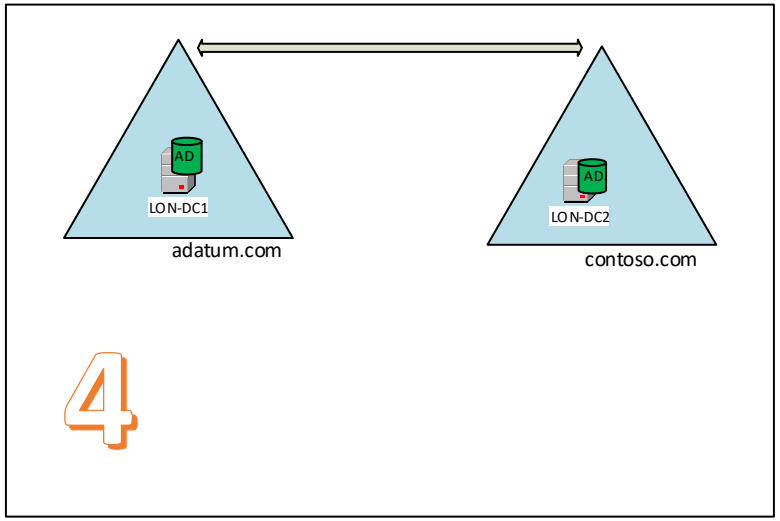
- Two steps:
  - Add Active Directory Domain Services role
  - Promote to a domain controller (dcpromo)
- During domain controller promotion can:
  1. Create first domain controller in new domain and forest
  2. Create an additional domain controller for an existing domain
  3. Create first domain controller for a child domain in an existing tree
  4. Create first domain controller for a new domain tree in an existing forest

Dcpromo Options

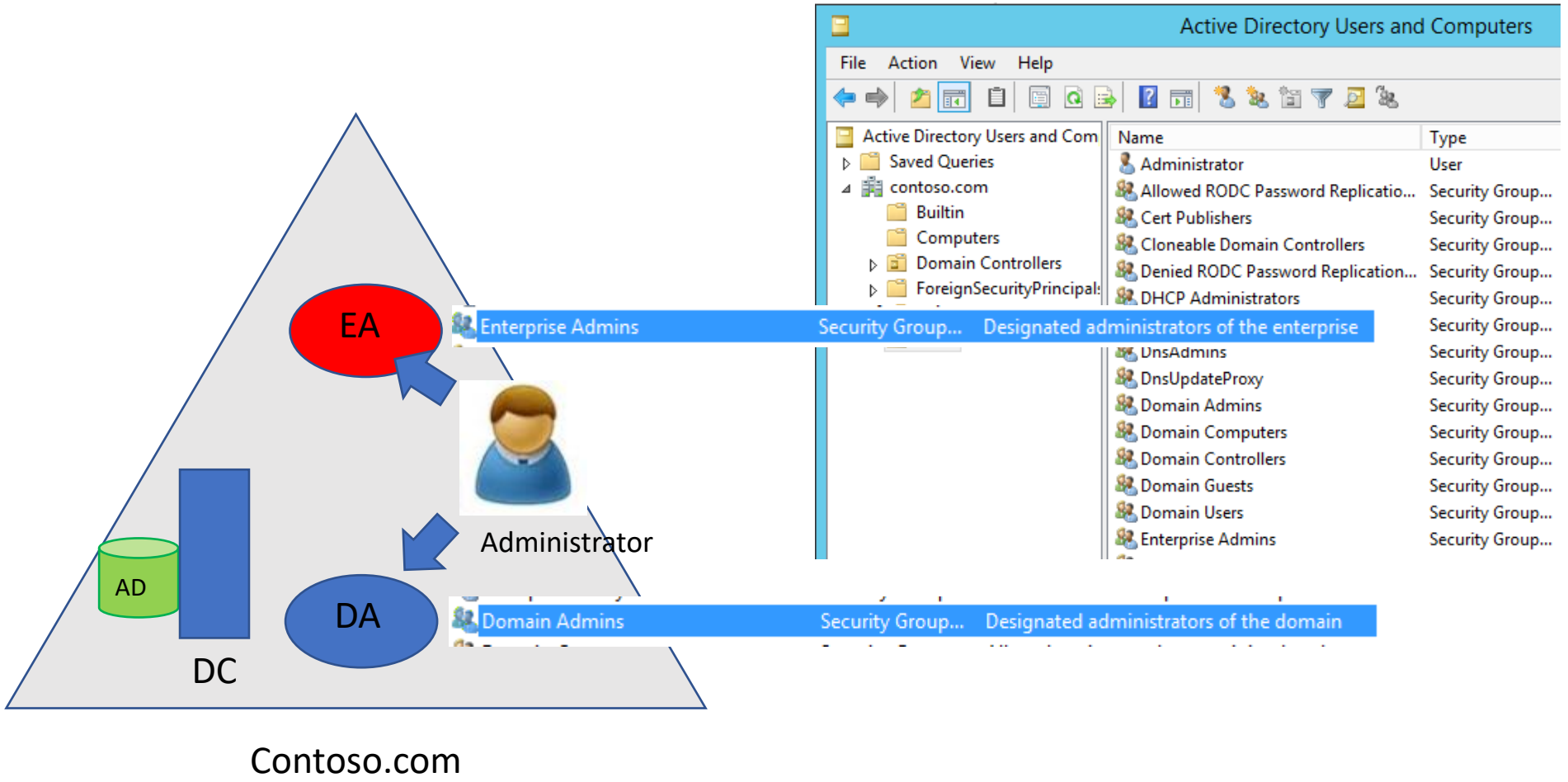








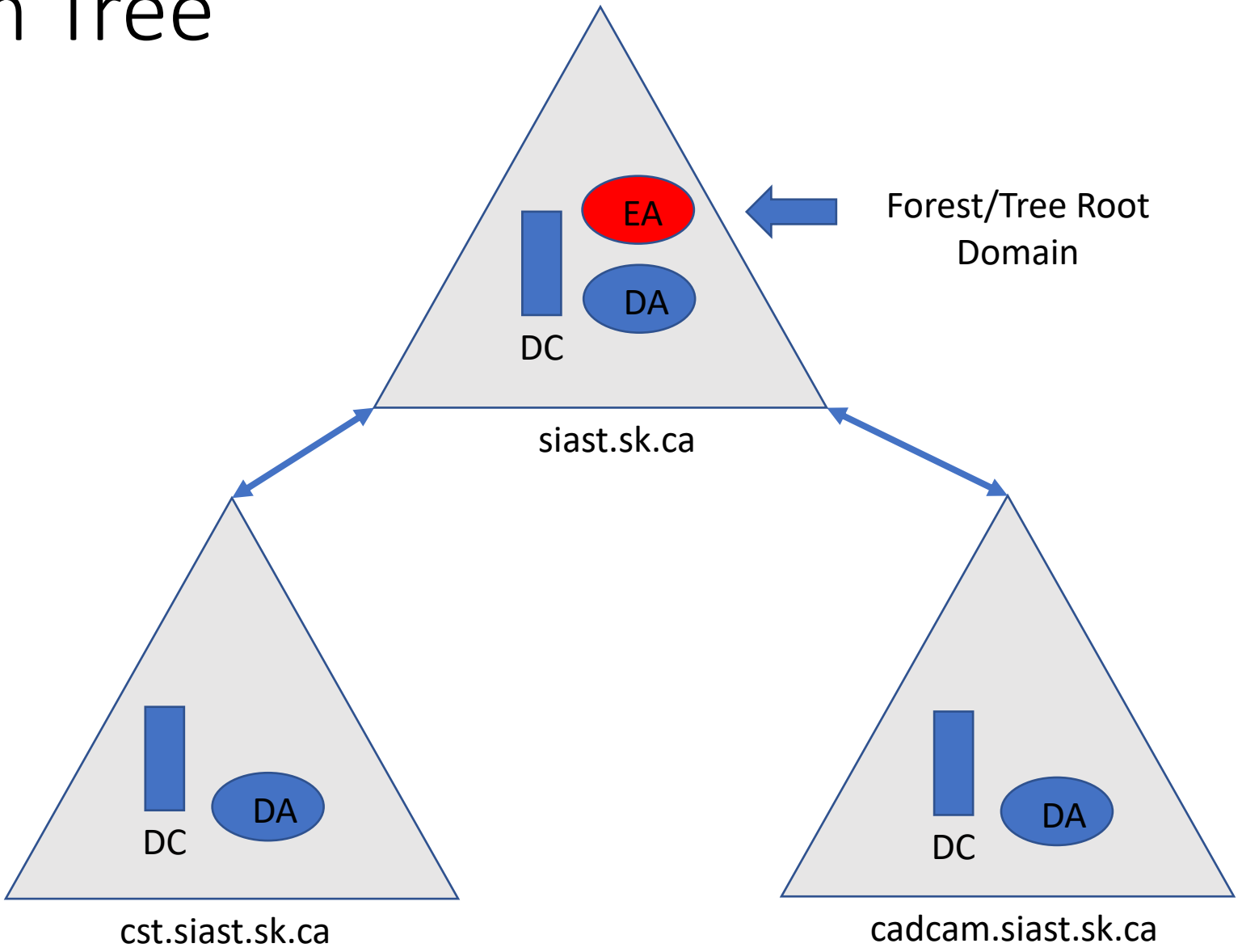
Forest root domain



Domain Tree

- Domain tree collection of domains that are grouped together in **hierarchical structure** share a **common root domain**.
- Can be a single domain or multiple domains.
- In a domain tree subsequent or child domain(s) are combined with the parent domain name to form its own unique DNS name, the domains with a tree have a contiguous namespace:
  - Parent: Adatum.com
  - Child: West DNS name: West.Adatum.com
  - Chile: Vancouver DNS name: Vancouver.West.Adatum.com

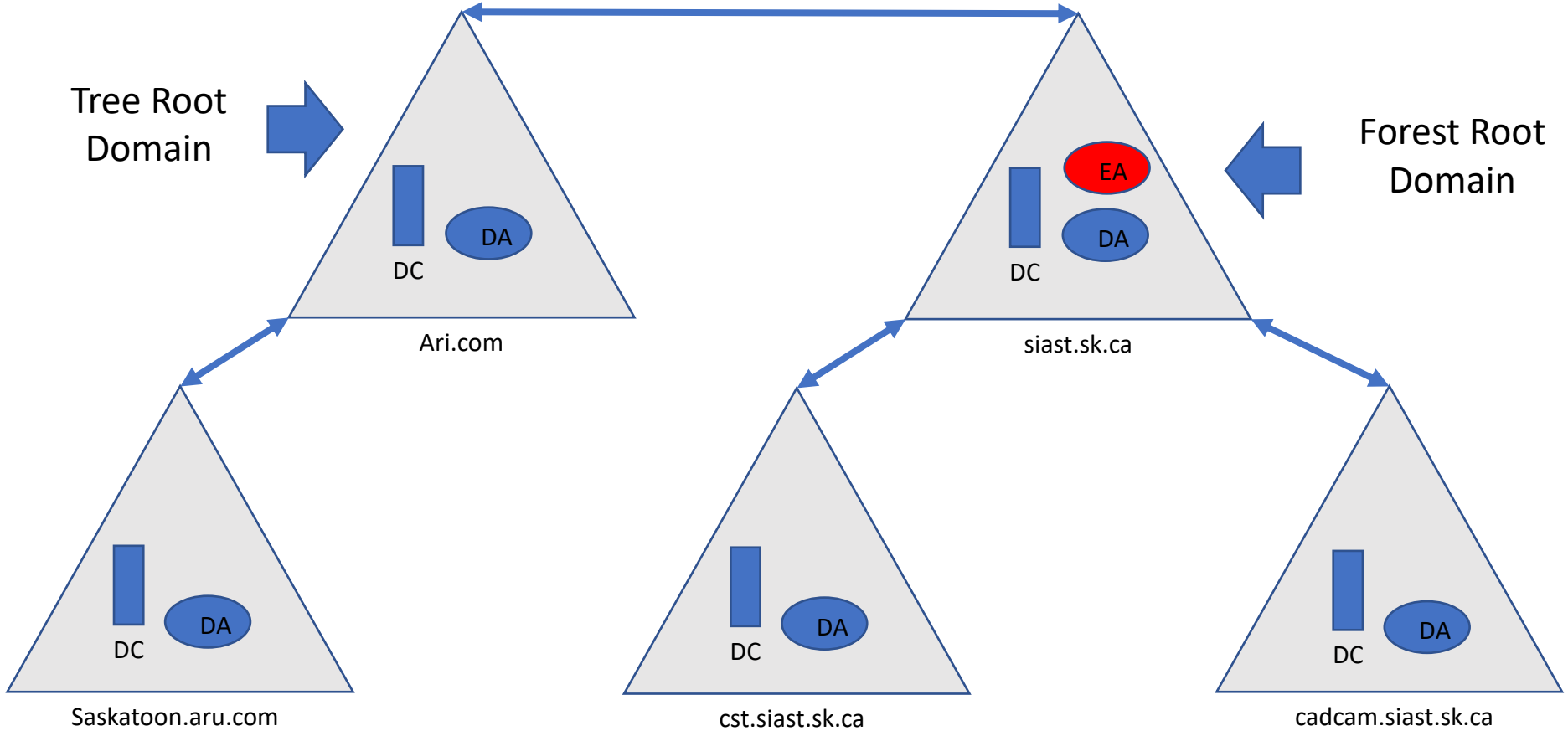
Domain Tree


EA
DA
DC
Forest/Tree Root
Domain
siast.sk.ca
DA
DC
cst.siast.sk.ca
DA
DC
cadcam.siast.sk.ca

Forest

- Contains one or more domain trees or domains, all of which share a common **logical structure**, **global catalog**, **directory schema**, configured with automatic two-way transitive trust relationships.
- A forest differs from a tree because it can use disjointed namespaces if it contains multiple trees.
  - 1st tree: Adatum.com
  - 2nd tree: Contoso.com

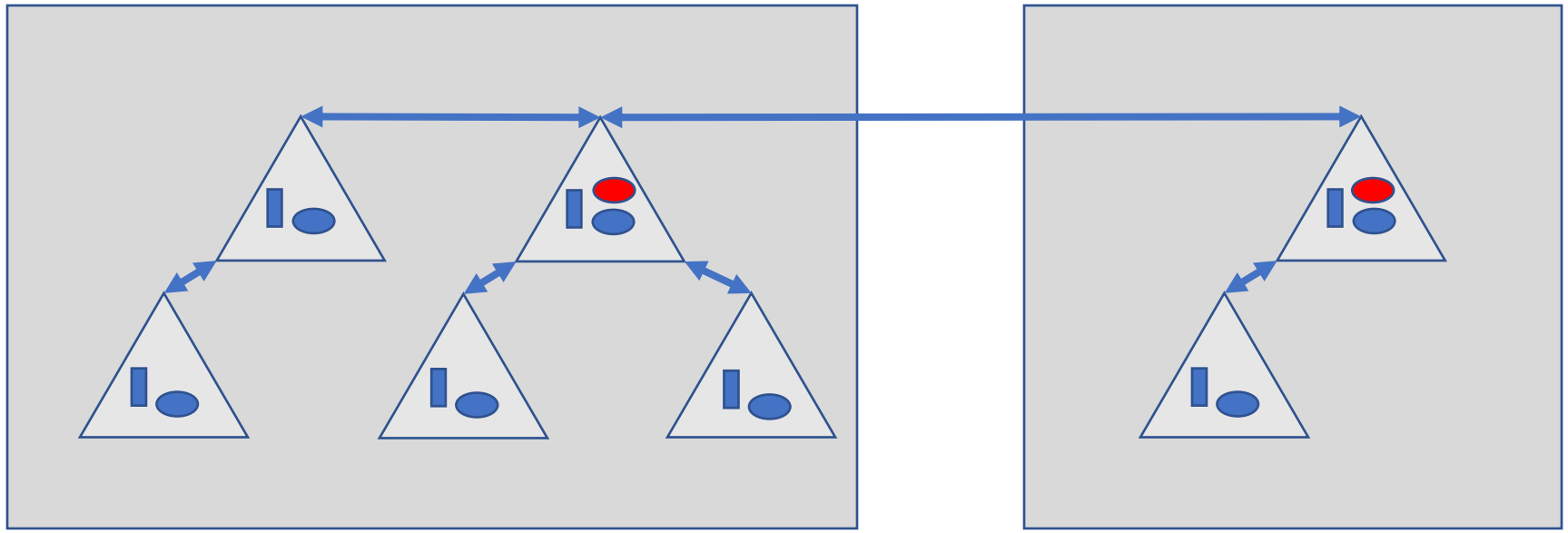
Forest


Tree Root Domain
Forest Root Domain
DC
DA
EA
Ari.com
siast.sk.ca
Saskatoon.aru.com
cst.siast.sk.ca
cadcam.siast.sk.ca

Active Directory Database

- Active Directory database is logically separated into the following directory partitions:
  - **Schema partition (one per forest)**: Contains definitions of all objects and attributes that can be created in the directory and the rules for creating and manipulating the objects.
  - **Configuration partition (one per forest)**: Contains information about the forest-wide Active Directory structure, including mapping existing domains and sites, and which domain controllers and services exist within the forest.
  - **Domain partition (one per domain)**: Contains information about users, groups, computers, and organizational units.
  - **Application partition**: Stores information about applications in Active Directory. Each application determines how it stores, categorizes, and uses application-specific information

Multiple Forests



Windows Trusts

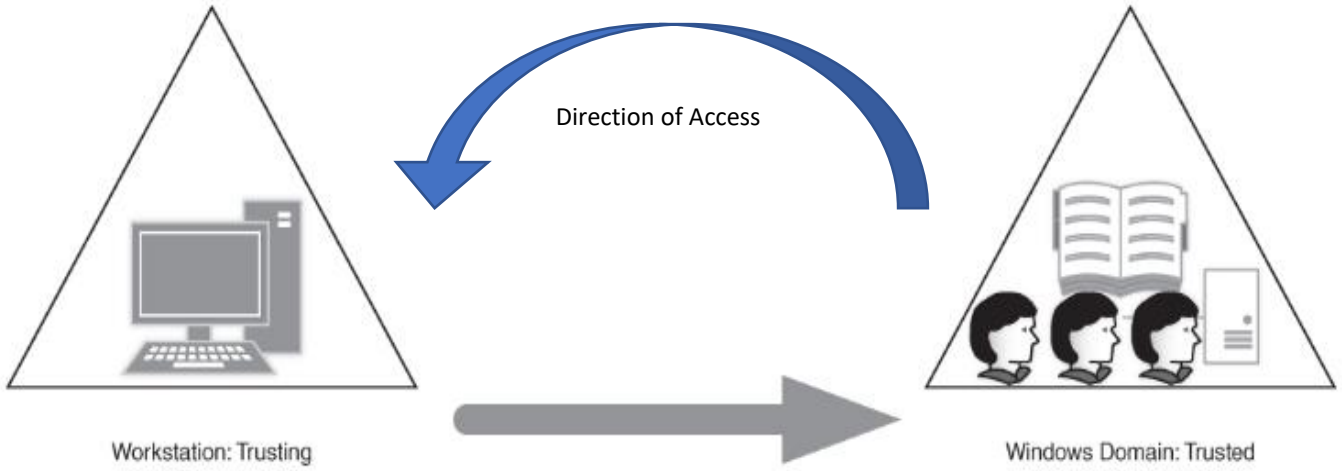
- ***Trusts*** are relationships between one Windows domain and another Windows domain or non-Microsoft Kerberos v5 realm.
- Trusts are created to allow users in one domain the ability to authenticate and then access resources on another domain, forest, or realm.
- If only a single domain, domain trusts don’t exist
  - Trusts DO still exist between domain controller and domain joined computers
  - When a computer is joined to a domain it is modified so that it allow or “trusts” another logon authority
  - Instead of using a local account stored in the SAM, it trusts the DC authentication with an account stored in AD
- Microsoft recommends single domain, single forest until you have specific requirements

Configuring Workstation Trusts

- When a workstation is not a part of the domain, only users who are local to the workstation's Security Account Manager (SAM) database have the ability to log on and access the workstation resources.
- Users or machines not known to the individual workstation are unable to authenticate against the workstation.
- To add (joining the domain) the workstation to the domain:
  - The local user of the workstation must be an administrator or member of the Administrators group on the workstation.
  - To complete the second half of the trust relationship, domain account credentials with the appropriate permissions must be provided to complete the trust.
  - Once authenticated and the request has been made from the workstation to the domain, a trust relationship is created between the workstation and the domain.
- When the workstation is added to the domain, domain users have the ability to authenticate and access the workstation's resources.

Workstation Trusts

- In this scenario, the workstation is the **trusting (resources)**, and the Windows domain is **trusted (users).**
- From the workstation's perspective it is a one-way outgoing trust, and from the Windows domain's standpoint, it is a one-way incoming trust.

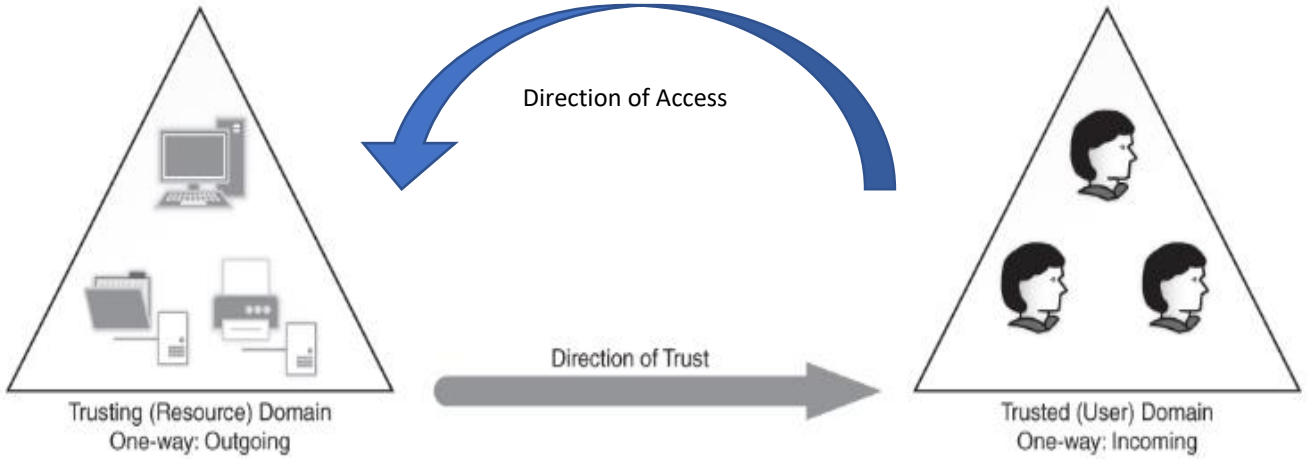


Domain Trusts

- The administration of multiple domains within or across forest relies on trusts for resource access
- If there are two companies with separate domains in separate forest:
  - graphics.contoso.local
  - graphics.adatum.local
- As each domain is in a separate forest, users in the graphics.contoso.local domain cannot access resources in the graphics.adatum.local domain.
- Each domain allows only security principles within its AD DS forest the ability to log on and/or access resources within that forest.
- There is no ability to grant users from external AD DS domains the rights to authenticate or access its resources.
- In order for users to authenticate and access resources across different domains a trust needs to be created.

Configuring Domain Trusts

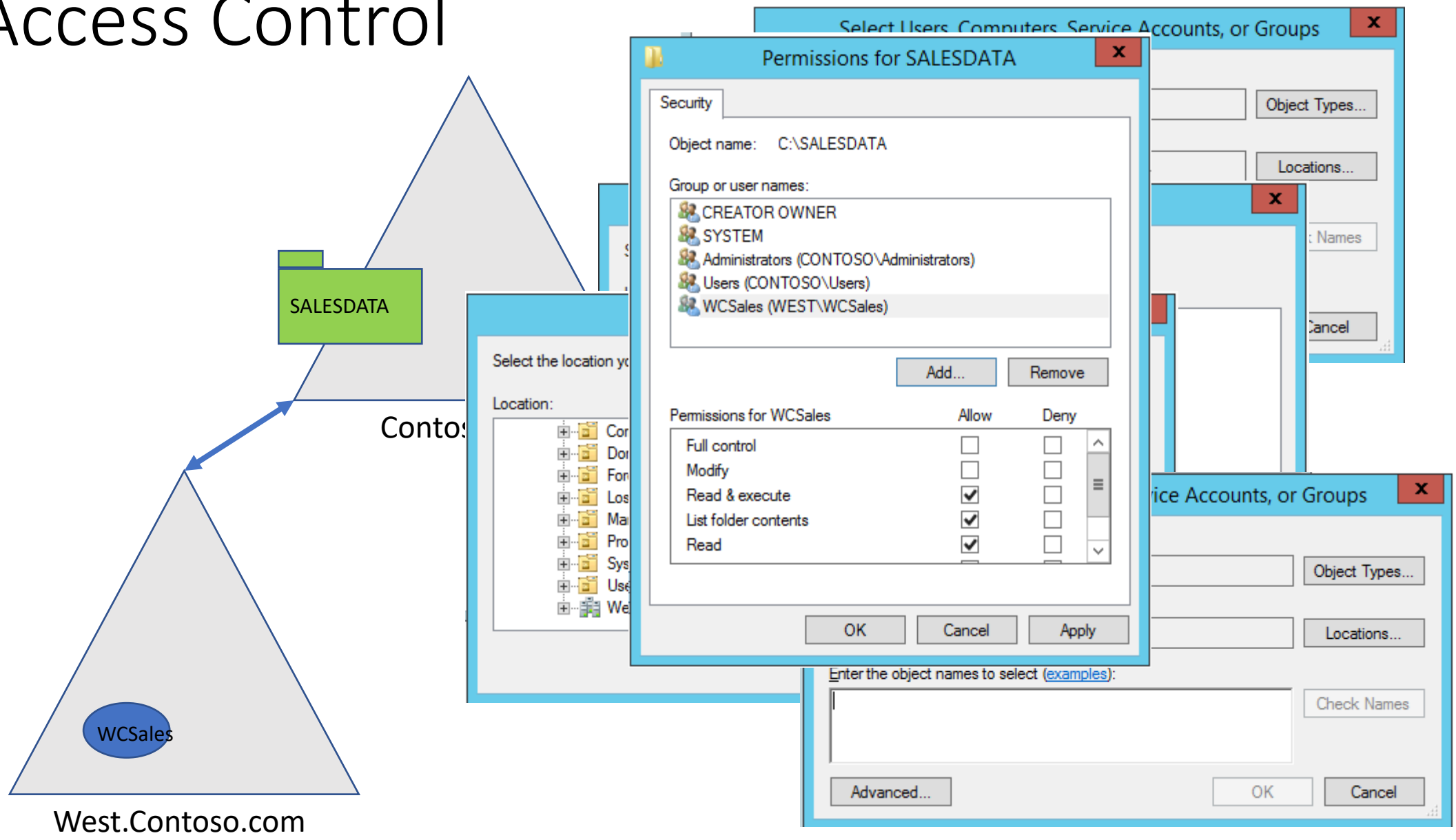
- Similar to the previous workstation scenario:
  - An administrator of the trusting domain, who is a member of the Domain Admins or Enterprise Admins group of the domain or forest initiates the outgoing trust request.
  - An administrator of the trusted domain, who is a member of the Domain Admins or Enterprise Admins groups, must initiate an incoming trust request.
  - Once the trust is complete, users in the trusted domain will be able to authenticate and access resources in the trusting domain.



Trusts and Access

- Normally, a **TRUST ≠ ACCESS**
- A Trust only establishes the relationship where the Trusting domain's administrator can "see" the users and groups in the Trusted domain
- The Trusted domain's users and groups have no access to resources in the trusting domain until the trusting domain's Administrator:
    - Adds Trusted domain users /groups to an ACL
    - Adds Trusted domain users/groups to a Domain Local Group in the Trusting domain that has resource access

Trust Access Control



Characteristics of Trusts

- There are 6 types of trusts used in different situations, they can be defined by three characteristics:
  - Method of Creation
    - Automatic or Manual
  - Direction
    - One-way or Two-way
  - Transitivity
    - Non-transitive or transitive

Method of Creation

- 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 a new 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.
- Two types of trusts are created automatically:
  - Parent-child
  - Tree root.

Manually Created Trusts

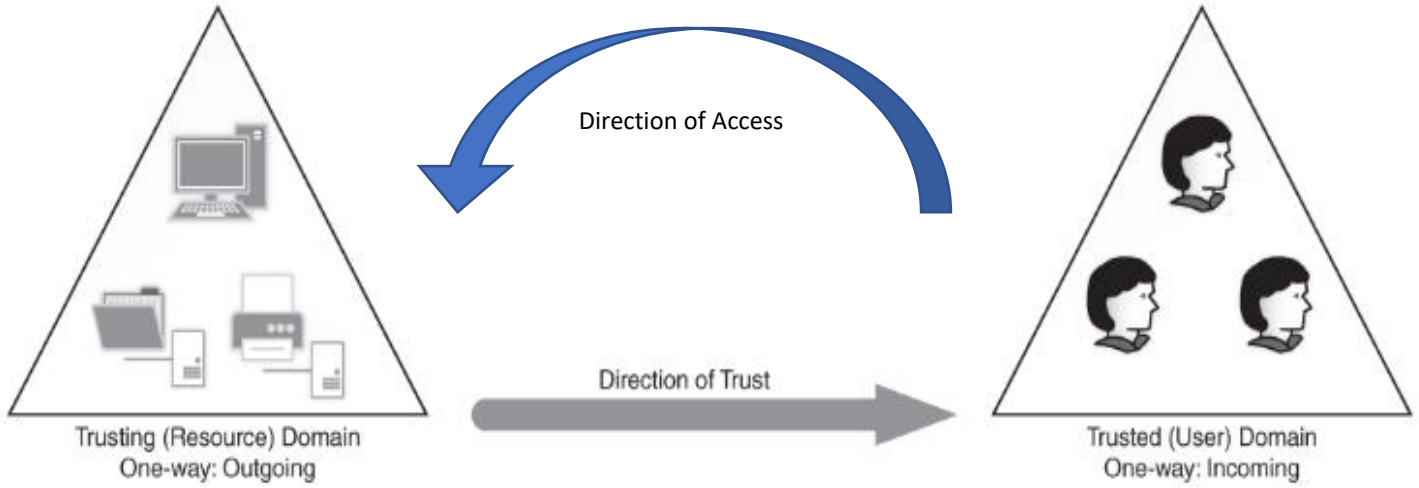
- Manually created trusts:
  - Can be created to connect two domains within the same forest to one other or to a forest or domain in a completely separate enterprise.
  - Can be one-way or two-way trusts.
  - Can be transitive or nontransitive in nature.
  - Four trusts can be created and configured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

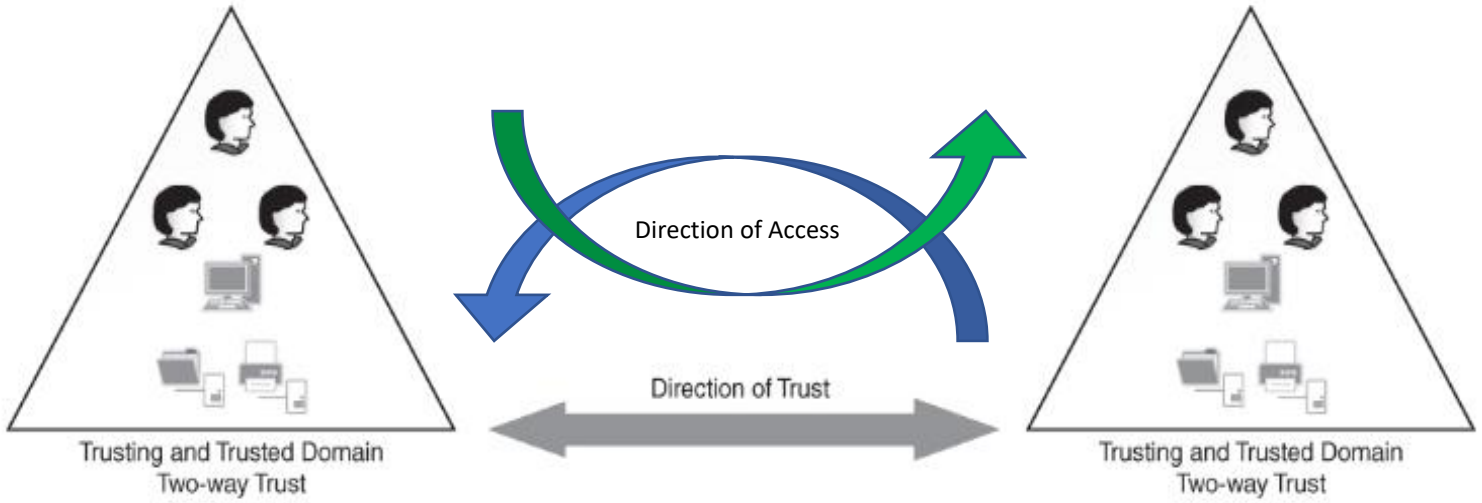
One Way Trust

- Direction is from the trusting domain to the trusted domain.
- Users in the trusted user domain can access resources in the trusting resource domain.
- However, any users in the resource domain cannot access resources in the trusted domain.



Two Way Trust

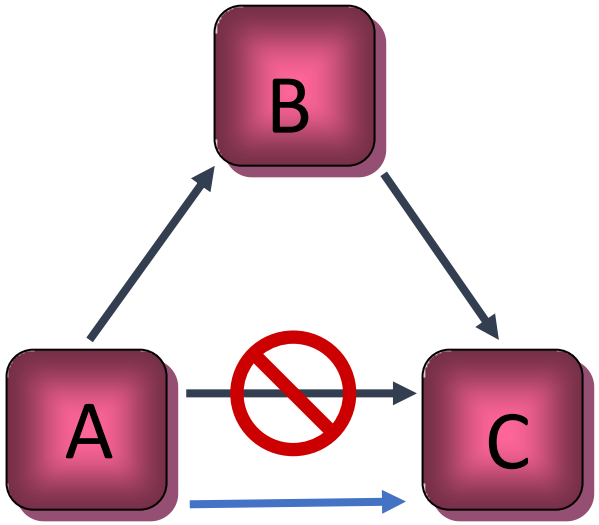
- Users in either domain can access resources in the internal domain or forest.
- Two-way trusts consist of two, one-way trusts.
- Each domain is trusting the other domain and each domain is trusted by the other domain.



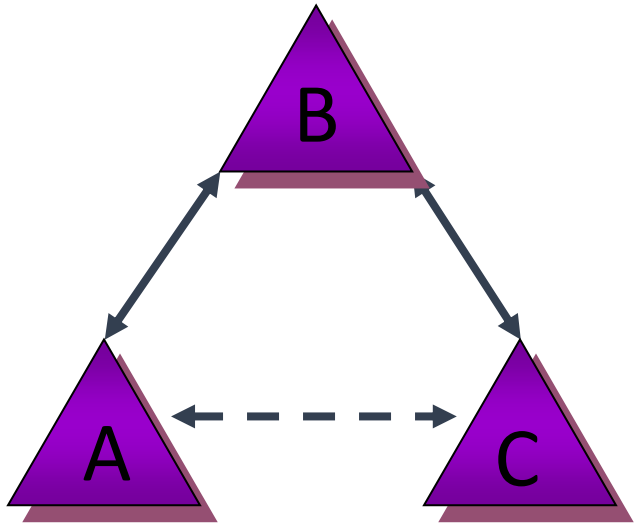
Transitivity

- 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.

Transitivity



Non-Transitive



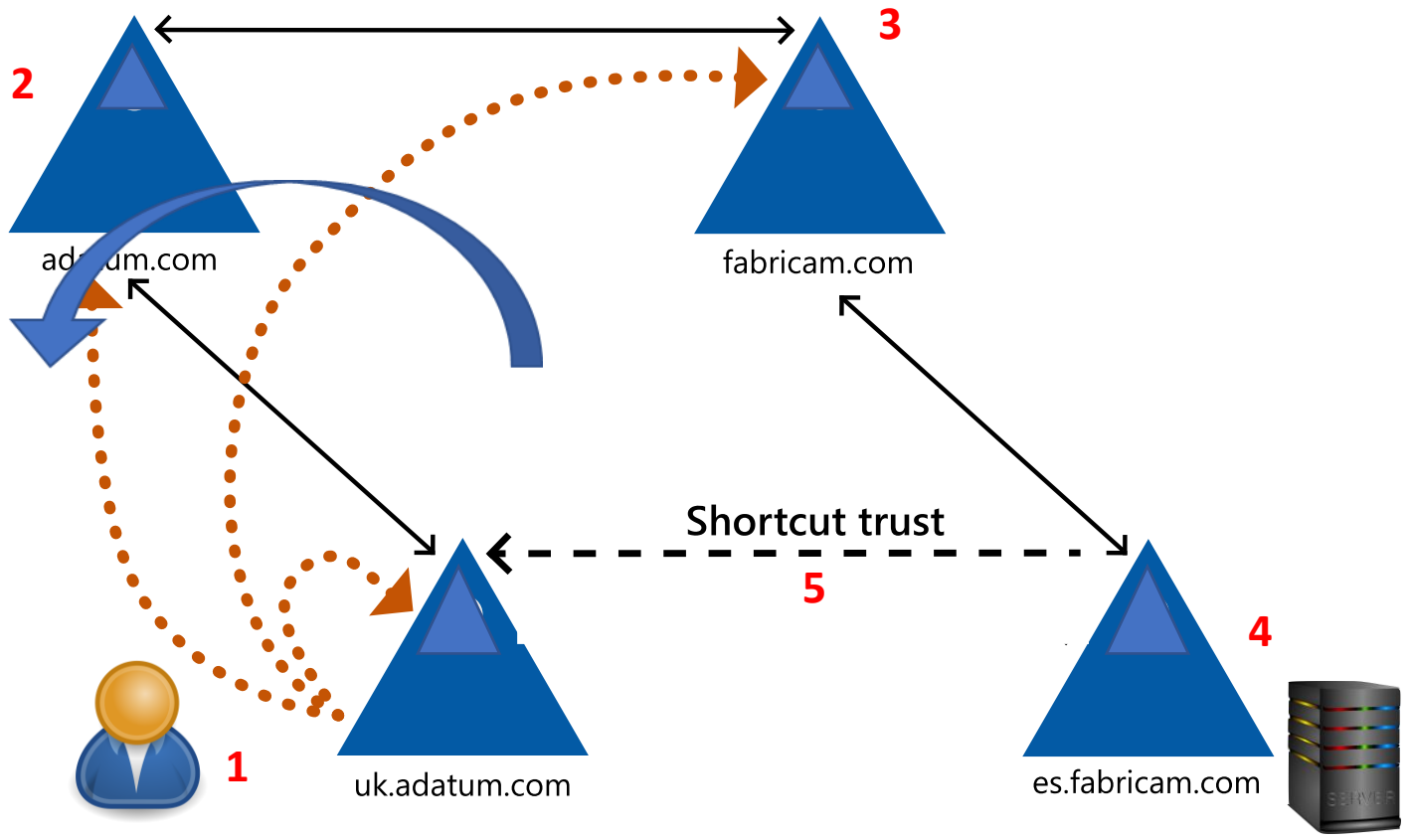
Transitive

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:
  - Secondary DNS zone, security issues
  - Conditional forwarders, update issue
  - Stub Zones, lesser security issues

How do trusts work in a forest?

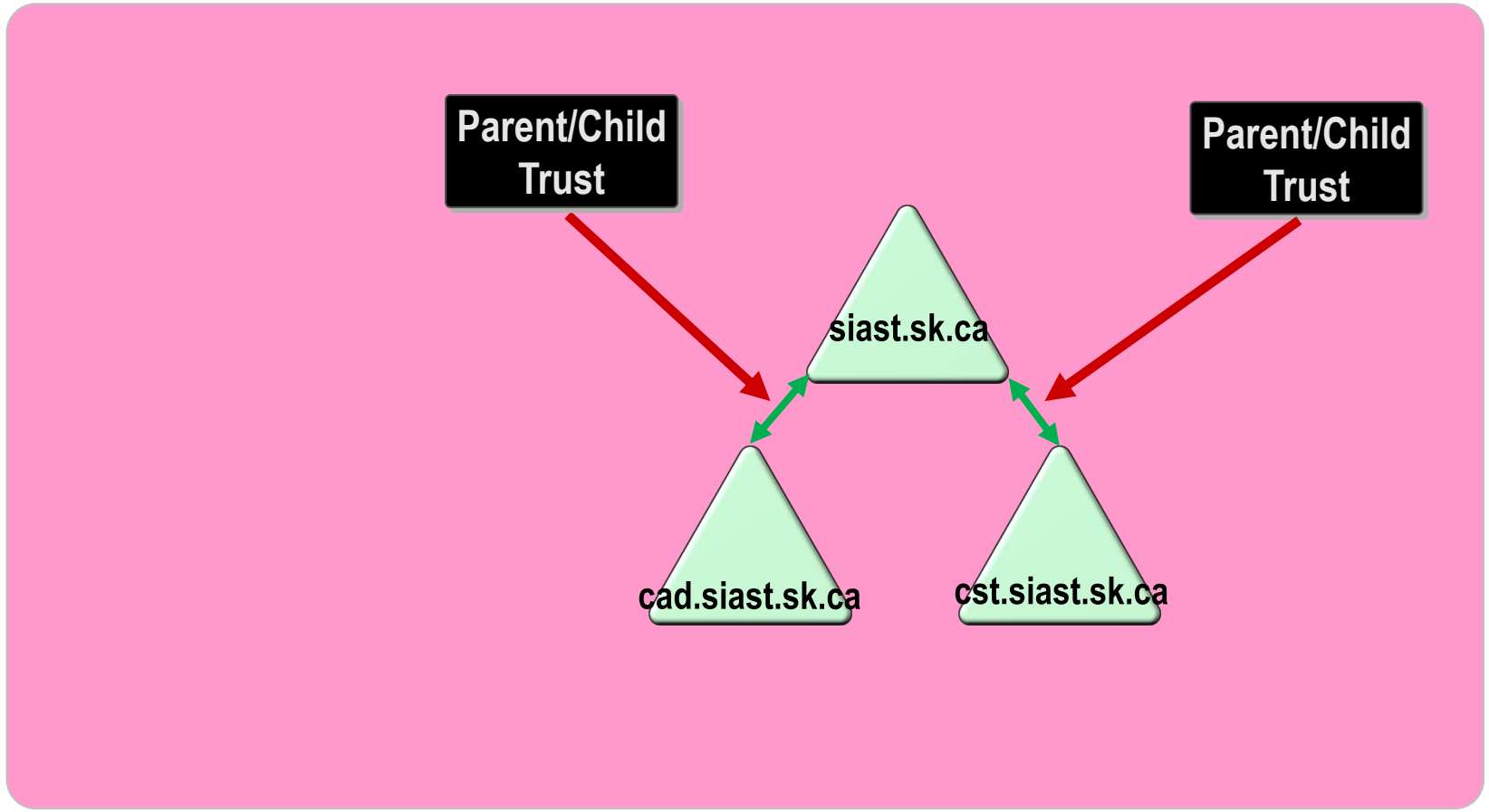
Uk.adatum.com
user on computer
CL1.uk.adatum.com
requests access to a file share on a domain-joined computer in es.fabrikam.com.



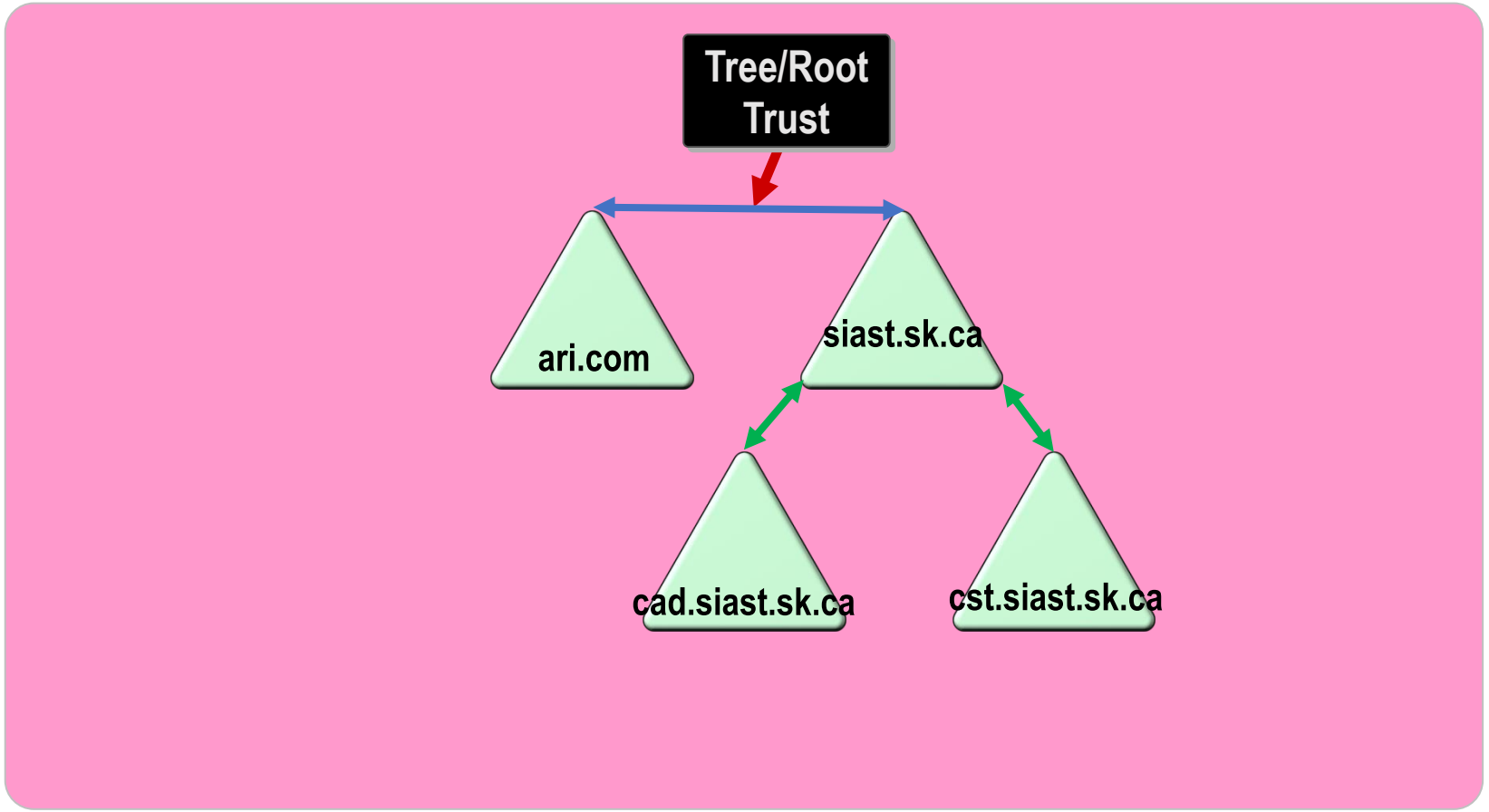
Automatic Trusts

- Created automatically when added domains to forest
  - Parent Child
  - Tree Root

Automatic Trusts



Automatic Trusts



Manual Trusts

- Must be manually created by Domain Administers in each domain, or an Enterprise Administrator:
  - External
  - Forest
  - Shortcut
  - Realm

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 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.

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.

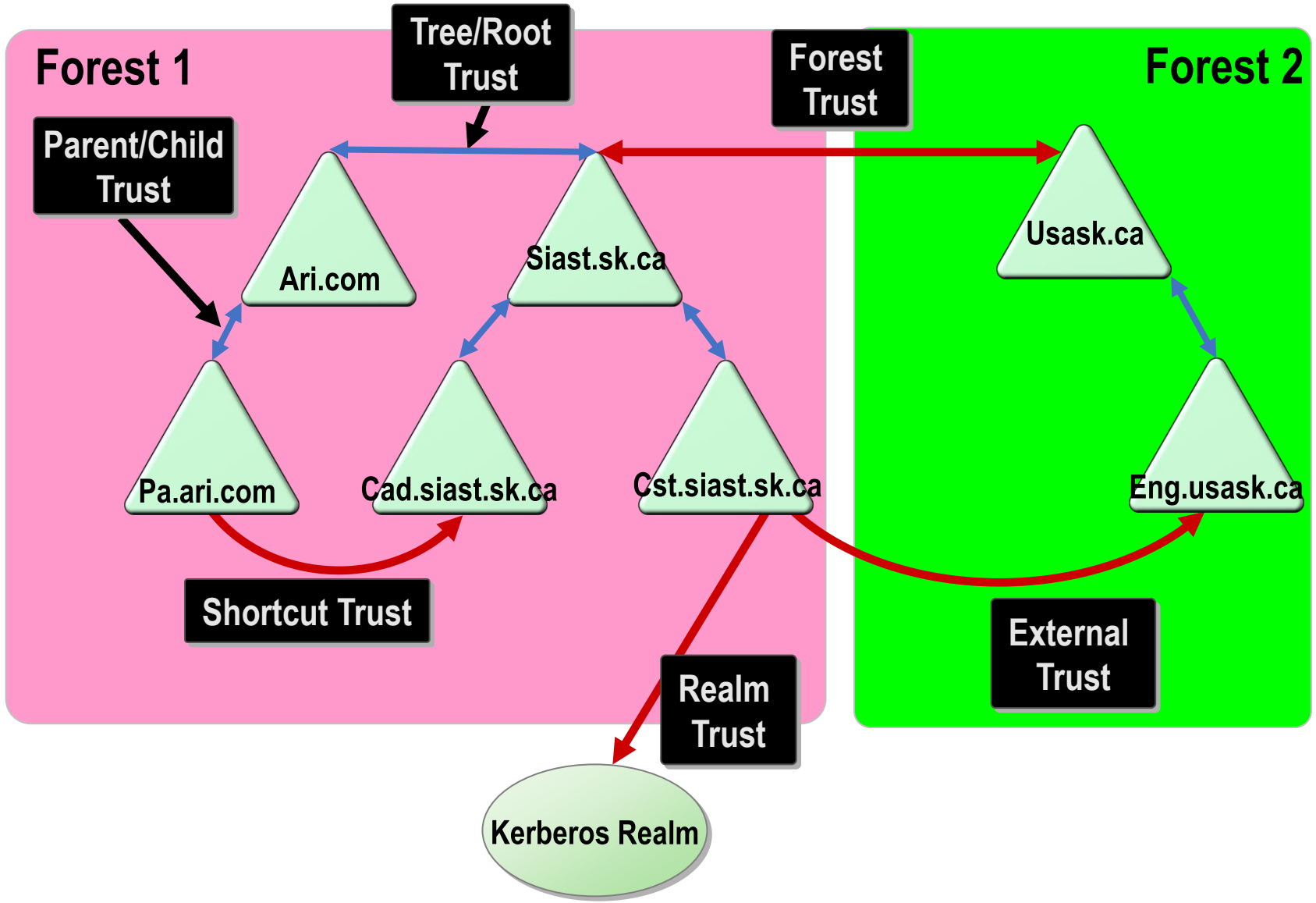
Creating Realm Trusts

- 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.

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.

Types of Trust



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.

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
  - 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.

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.