

Configure Active Directory Forest Environments



Tim Warner

Principal Author Evangelist, Pluralsight

@TechTrainerTim TechTrainerTim.com



Overview



Configure and manage forest and domain trusts

Configure and manage AD DS sites

Configure and manage AD DS replication



Deploy and Manage Active Directory Domain Services

Deploy and Manage Domain Controllers

Configure Active Directory Forest Environments

Create and Manage AD DS Security Principals

Implement and Manage Hybrid Identities

Manage Windows Server with Group Policy



Configure and Manage Forest and Domain Trusts



AD DS Trust Types

Parent/child (transitive; two-way)

Tree root (transitive; two-way)

External (non-transitive; one- or two-way)

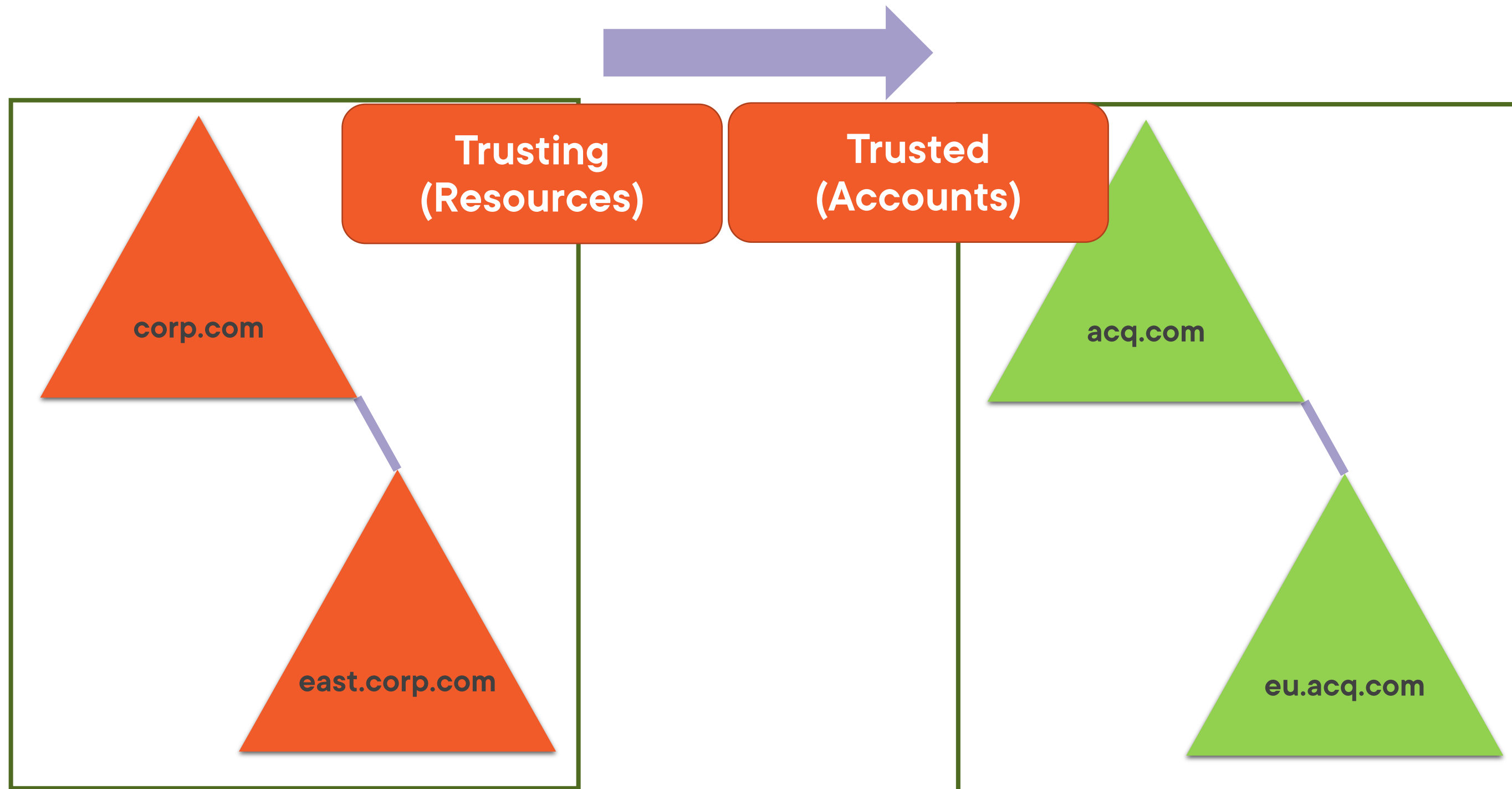
Realm (transitive or non-transitive; one- or two-way)

Forest (transitive; one- or two-way)

Shortcut (non-transitive; one- or two-way)



Forest and Domain Trust Relationships



SID Filtering

Domain quarantine

Occurs during migrations

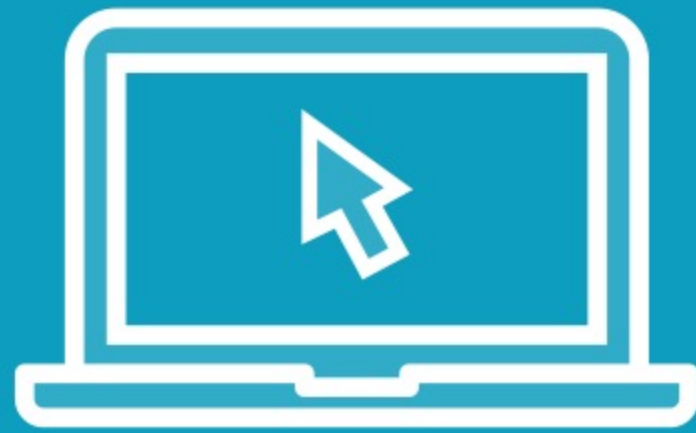
User account's SID-History attribute

Blocks the use of SIDs present in SID-History that don't originate from the trusted domain

Prevents SID spoofing exploits



Demo



1

View trusts

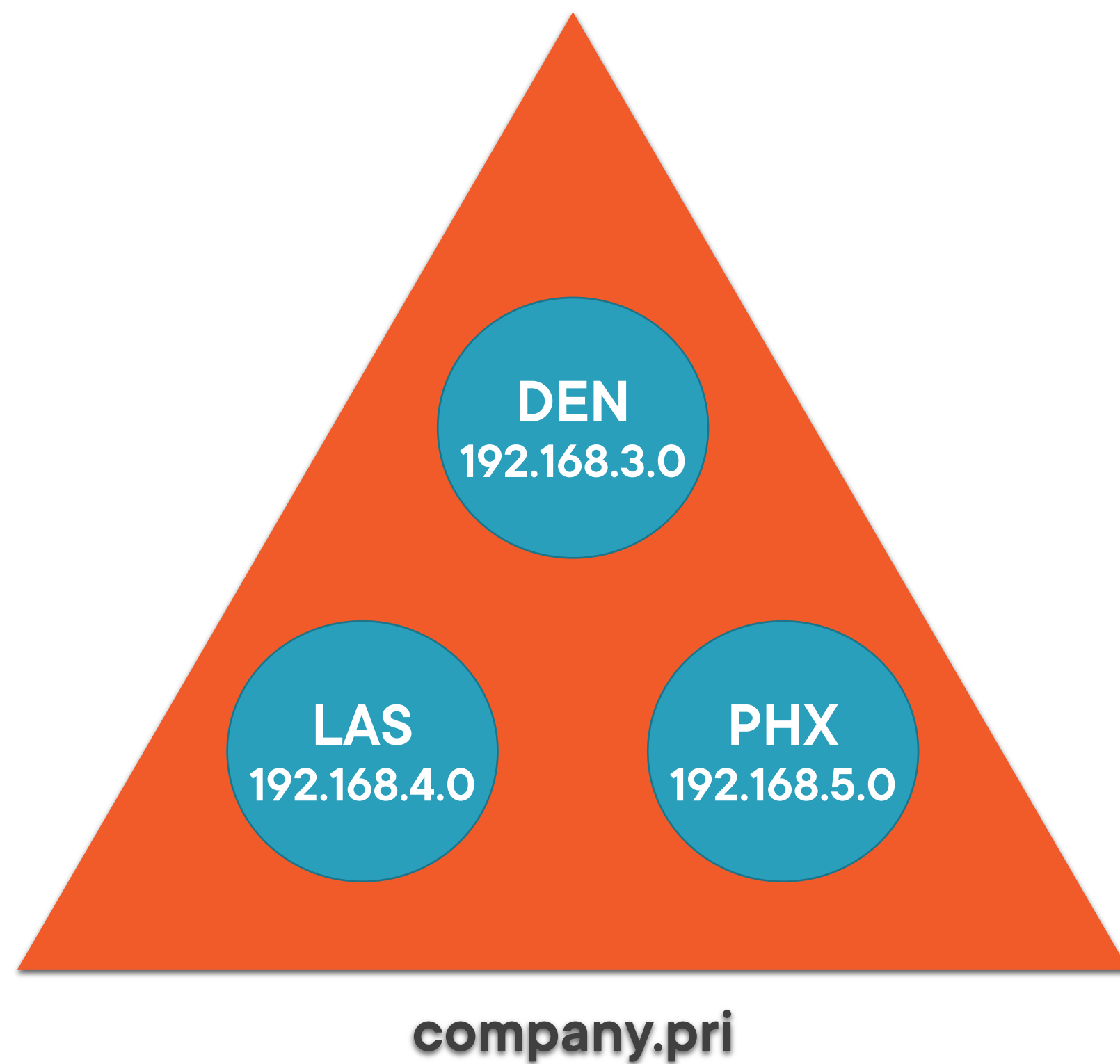
Configure selective authentication



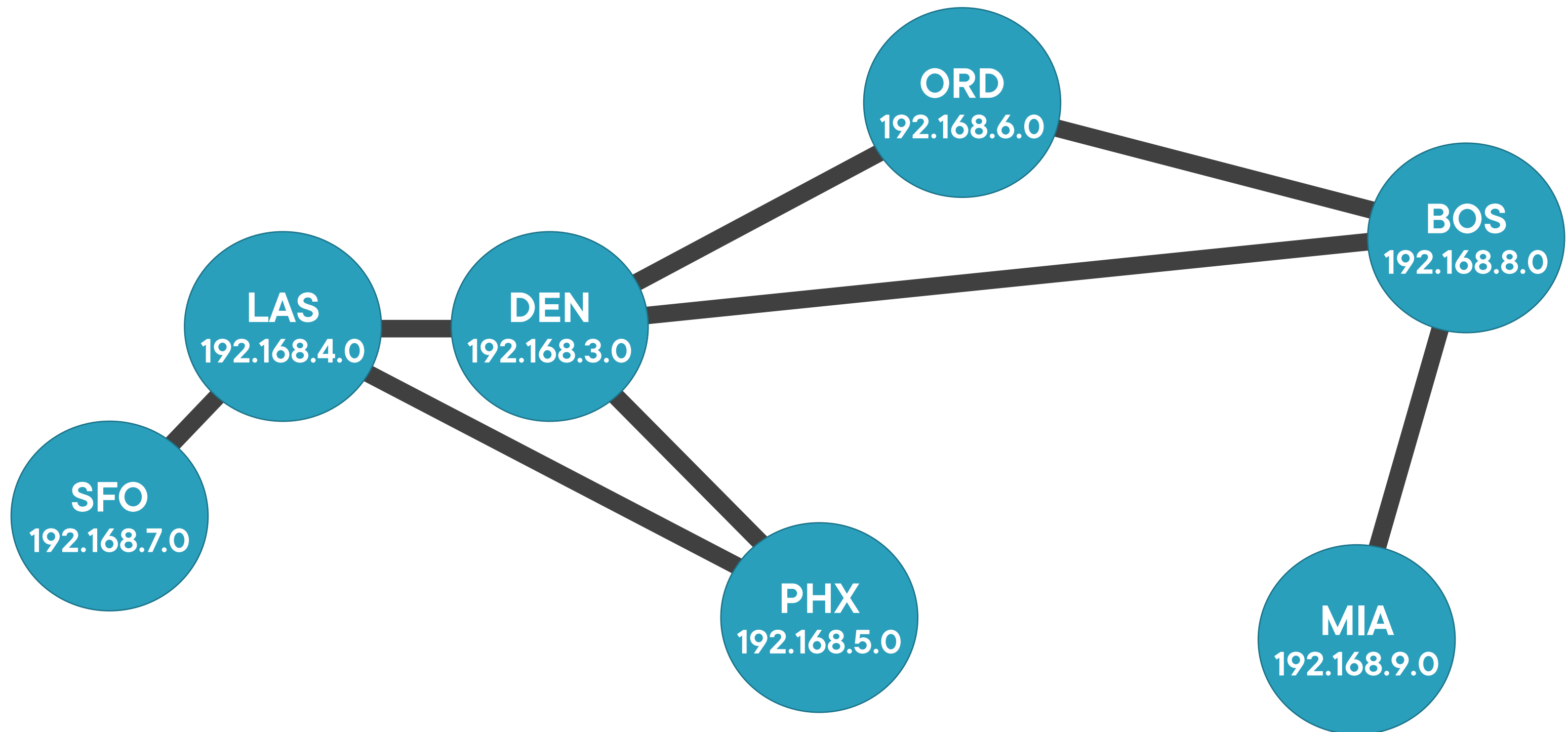
Configure and Manage Active Directory Domain Services Sites



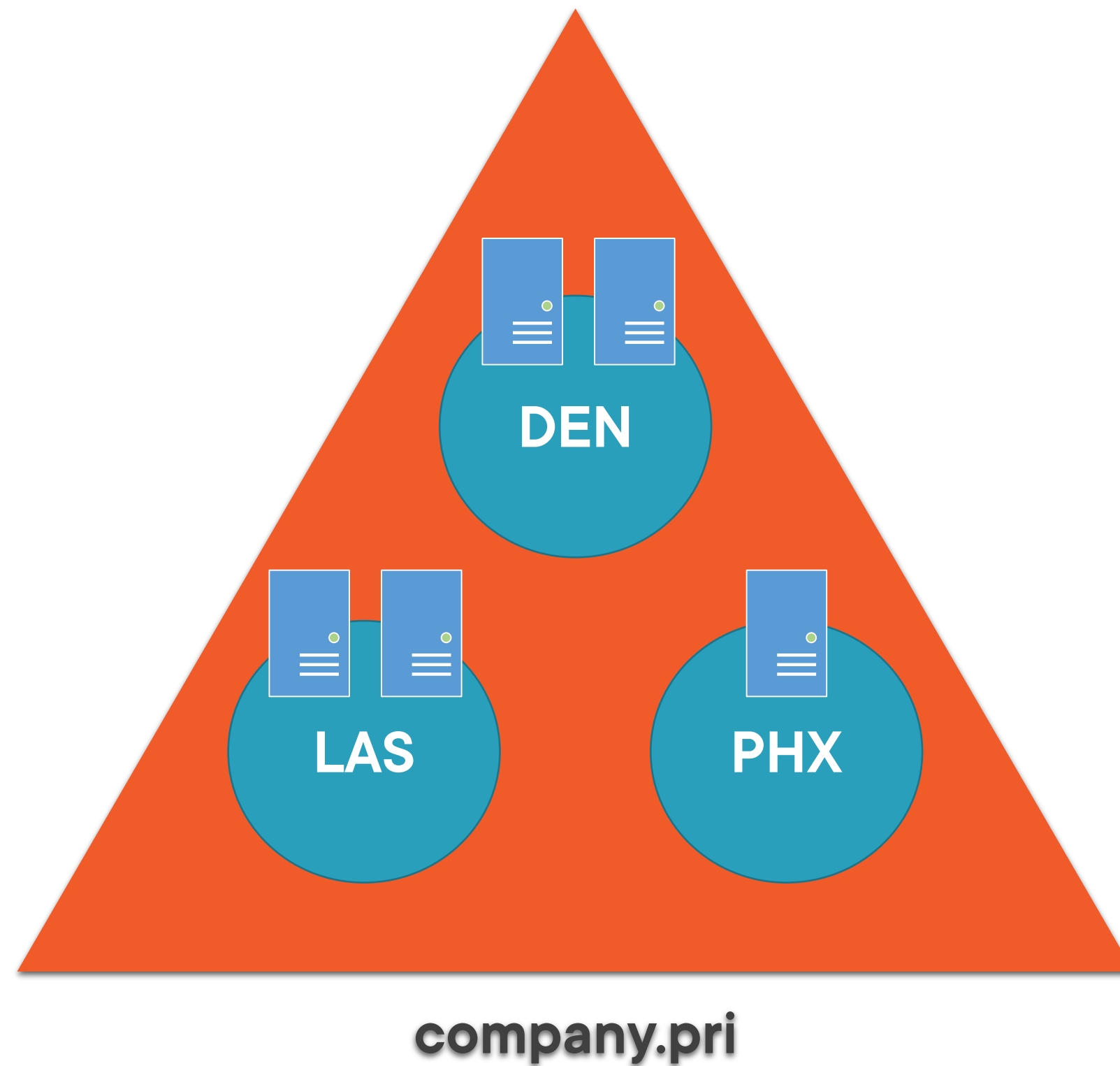
Active Directory Sites



Active Directory Sites



AD Domain Controllers and Sites



Configure and Manage AD DS Replication



AD DS Partitions

Configuration: Forest-wide AD DS structure (replicates to all DCs in forest)

Schema: All objects and attributes (replicates to all DCs in forest)

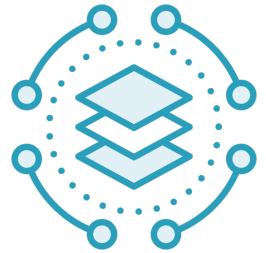
Domain: Users, groups, OUs (replicates to all DCs in domain)

Application: Custom data (replication specified by administrator)

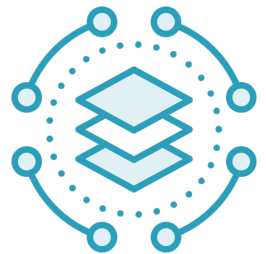
- forestDnsZones
- domainDnsZones



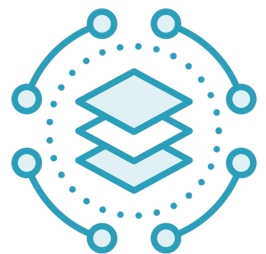
Active Directory Replication



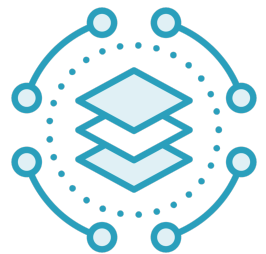
KCC: Process that dynamically builds connection objects between sites



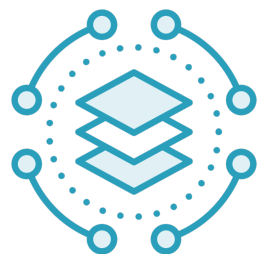
Intra-site replication interval: 15 seconds



Inter-site replication interval: 180 minutes (3 hours)



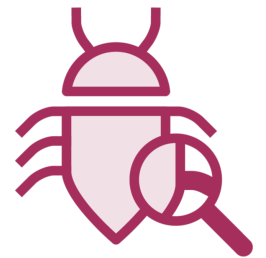
Site link: Transitive logical connection between sites & bridgehead servers (full inter-site connectivity is assumed)



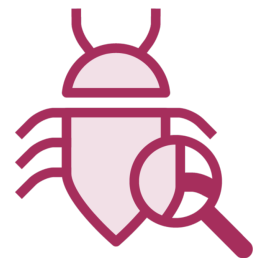
Site link bridge: Administrator-defined connection between DCs that don't have direct connectivity



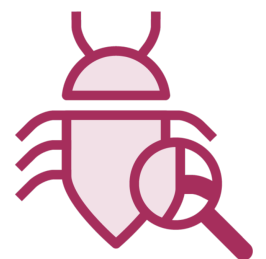
Active Directory Replication Troubleshooting



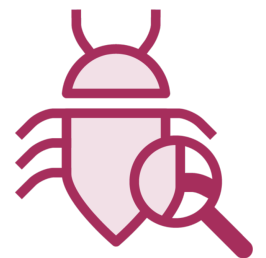
Repadmin.exe: Diagnose replication issues



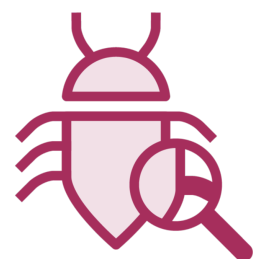
Dcdiag.exe: Tests DNS, FSMO, and site connectivity



Get-ADReplicationConnection



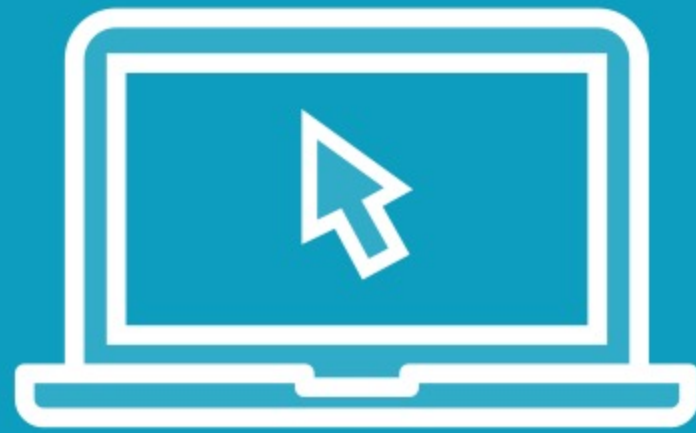
Get-ADReplicationFailure



Get-ADReplicationPartnerMetadata



Demo



2

Define subnets

Control replication

Repadmin



Summary



Microsoft proven practice is to standardize on one forest, one domain

- v1: Enhanced Security Admin Environment (ESAE)
- v2: Privileged access strategy for workstations and users

Regarding replication: "You are not smarter than the KCC"

- **timw.info/ykw**



Up Next:

Create and Manage AD DS Security
Principals

