

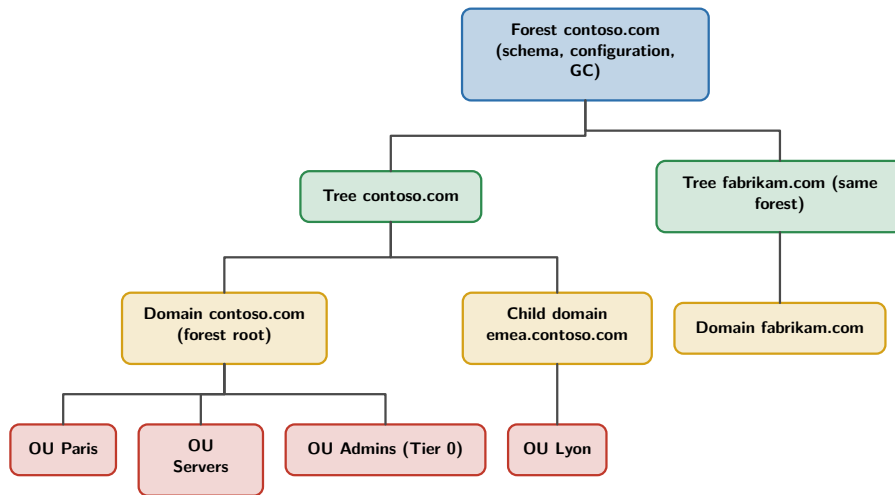


AZ-800: AD DS Forests, Domains, Sites and GPOs

AZ-800 domain 1 (AD DS on-premises and in the cloud), part 1 | Forests, domains, partitions, FSMO roles, functional levels, deploying DCs and RODCs, sites and replication, trusts, Group Policy, fine-grained password policies, recycle bin, gMSA; PowerShell and repadmin

AZ-800 Domain 1 Active Directory

Logical structure and operations masters



Trees in one forest trust each other automatically (two-way, transitive)

Schema Master <i>forest-wide, one per forest</i> only DC that can write schema changes (adprep /forestprep, Exchange extensions) NOT Domain Naming Master	Domain Naming Master <i>forest-wide</i> adds or removes domains and application partitions NOT RID Master
RID Master <i>per domain</i> hands out pools of 500 relative IDs for new SIDs; outage blocks object creation once pools run out NOT PDC Emulator	PDC Emulator <i>per domain</i> time source of the domain, receives urgent password changes, lockout processing, default GPO editing target NOT Infrastructure Master
Infrastructure Master <i>per domain</i> updates references to objects of other domains; irrelevant if every DC is a GC NOT Global catalog	

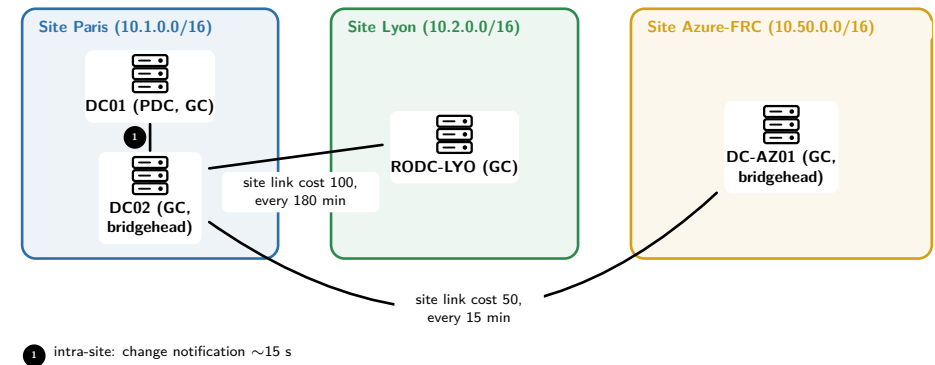
Command	What it does
<code>netdom query fsmo</code>	list the five role holders
<code>Move-ADDirectoryServerOperationMasterRole -Identity DC02 -OperationMasterRole PDCEmulator,RIDMaster</code>	transfer roles (graceful, both DCs online)
<code>Move-ADDirectoryServerOperationMasterRole -Identity DC02 -OperationMasterRole SchemaMaster -Force</code>	seize a role when the holder is gone forever (never bring it back)
<code>Get-ADForest Select ForestMode, SchemaMaster; Get-ADDomain Select DomainMode</code>	functional levels and roles
<code>Set-ADForestMode -Identity contoso.com -ForestMode Windows2016Forest</code>	raise the forest functional level (one way)

Deploy domain controllers

```
New forest, extra DC, RODC and install from media
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
# first DC of a new forest
Install-ADDSForest -DomainName contoso.com `
  -DomainNetbiosName CONTOSO -InstallDns `
  -SafeModeAdministratorPassword (Read-Host -AsSecureString)
# additional writable DC
Install-ADSDomainController -DomainName contoso.com `
  -SiteName Paris -InstallDns -Credential (Get-Credential)
# RODC for a branch, delegated local admin
Install-ADSDomainController -DomainName contoso.com `
  -ReadOnlyReplica -SiteName Lyon `
  -DelegatedAdministratorAccountName CONTOSO\lyon-admins
# install from media (slow WAN): on an existing DC
ntdsutil "activate instance ntds" ifm `
  "create sysvol full C:\IFM" quit quit
# then on the new DC: -InstallationMediaPath C:\IFM
```

Topic	Facts the exam uses
Functional levels	raise forest/domain levels after all DCs run the matching OS; Windows Server 2016 level was the latest for years; Windows Server 2025 adds a new level (32k database pages): check prerequisites
Server Core DCs	smaller attack surface; manage with PowerShell, RSAT, Windows Admin Center
Virtualised DCs	VM-GenerationID protects against USN rollback when restoring snapshots; still prefer backups over checkpoints
RODC Password Replication Policy	Allowed RODC Password Replication Group (empty by default) and Denied group (admins, krbtgt); prepopulate passwords for branch users
Admin role separation	a branch admin can manage the RODC server without any domain rights
Azure VM DCs	static private IP, data disk with host caching None for NTDS/SYSVOL, VNet DNS points to the DCs, separate site for the VNet
Removing a dead DC	metadata cleanup: delete the computer object in ADUC/ADAC or ntdsutil metadata cleanup, then seize its FSMO roles

Sites, replication and trusts



Inter-site replication runs between bridgeheads on the site link schedule; RODCs replicate inbound only

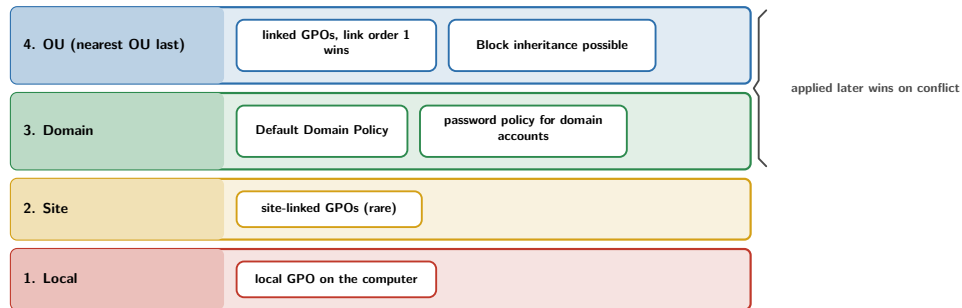
Command	What it does
repadmin /replsummary	largest replication delta and failures per DC
repadmin /showrepl DC02	inbound partners, last success, errors
repadmin /syncall DC01 /AdeP	push replication of all partitions across sites now
dcdiag /v /c /e	full DC health tests across the enterprise
New-ADReplicationSite Lyon; New-ADReplicationSubnet -Name 10.2.0.0/16 -Site Lyon	create a site and map its subnet
New-ADReplicationSiteLink Paris-Lyon -SitesIncluded Paris,Lyon -Cost 100 -ReplicationFrequencyInMinutes 60	site link (minimum interval 15 minutes)

Trust type	Direction and transitivity	Use
Parent-child, tree-root	two-way, transitive, automatic	inside a forest
Shortcut	one- or two-way, transitive	speed up Kerberos between deep domains of one forest
Forest	one- or two-way, transitive between the two forests only	merger: users in forest A use apps in forest B
External	one- or two-way, non-transitive (NTLM)	one domain of another forest, legacy NT4-style
Realm	Kerberos v5 realm (MIT, Linux)	non-Windows Kerberos

💡 Selective authentication and SID filtering

On a forest or external trust, selective authentication makes users of the trusted forest authenticate only to computers where they hold **Allowed to Authenticate**. SID filtering (quarantine) is on by default for external and forest trusts: it drops SIDs from other domains in SID history, blocking privilege escalation; relax it only temporarily during migrations (sheet 10).

☀ Group Policy and account policies



LSDOU: Local, Site, Domain, OU; Enforced links win over later links and ignore Block inheritance

- **Filtering** security filtering (Apply group policy permission, Authenticated Users need Read), WMI filters (OS version), item-level targeting in Preferences
- **Loopback processing** computer setting that applies user settings based on the computer's OU: Merge or Replace (kiosks, RDS hosts)
- **Refresh** every 90 minutes with a random 0-30 min offset (DCs every 5 minutes); gpupdate /force, Invoke-GPUdate -Computer; gpresult /h report.html to see what applied
- **Central store** copy ADMX/ADML to \\contoso.com\SYSTEM\contoso.com\Policies\PolicyDefinitions so every admin edits with the same templates
- **Password policy** domain-wide policy comes only from a GPO linked at the domain; exceptions use fine-grained password policies (PSO) on users or global groups, lowest precedence number wins
- **AD Recycle Bin** Enable-ADOptionalFeature 'Recycle Bin Feature' -Scope ForestOrConfigurationSet -Target contoso.com (irreversible); restore with Get-ADObject -IncludeDeletedObjects | Restore-ADObject within the deleted object lifetime (180 days default)
- **gMSA** Add-KdsRootKey -EffectiveImmediately (effective after 10 hours of replication), New-ADServiceAccount svc-web -DNSHostName svc-web.contoso.com -PrincipalsAllowedToRetrieveManagedPassword WebServers, Install-ADServiceAccount on each host

PROBLEM A password change on DC01 (Paris) must reach the RODC in Lyon. Worst-case delay for a normal (non-urgent) change?

- GIVEN**
- Intra-site: change notification to the bridgehead DC02 after about 15 seconds
 - Site link Paris-Lyon: replication every 60 minutes
 - Password changes also go to the PDC Emulator immediately (urgent forwarding)

1 DC01 → DC02 (same site)

≈ 15 s

Why: change notification with initial delay

2 DC02 → Lyon (inter-site)

≤ 60 min

Why: waits for the next scheduled replication

3 Total

≈ 60 min 15 s

Why: a user in Lyon with an old cached password authenticates through a writable DC meanwhile

ANSWER About one hour; lower the site link interval (minimum 15 min) or enable change notification on the site link for faster convergence

CHECK ✓ With a 15-minute interval: 15 s + 15 min ≈ 15 min 15 s

🚩 Recap and self-test

YOU MAY HEAR
"A domain is a security boundary"

BUSTED

✓ **ACTUALLY**
The forest is the security boundary
Any Domain Admin of any domain can compromise the whole forest.

YOU MAY HEAR
"Seized FSMO holders can come back online"

BUSTED

✓ **ACTUALLY**
Never reconnect a DC whose role was seized
Rebuild it; two Schema or RID masters corrupt AD.

YOU MAY HEAR
"Two password policies GPOs on two OUs give two domain password rules"

BUSTED

✓ **ACTUALLY**
Domain accounts take the password policy only from a domain-linked GPO
Use fine-grained password policies (PSO).

YOU MAY HEAR
"Forest trusts are transitive to every connected forest"

BUSTED

✓ **ACTUALLY**
Transitive only between the two forests
A trusts B and B trusts C does not give A → C.

Tick a box only when you could explain the point to someone else

☐ **Five FSMO roles: 2 forest, 3 domain**
transfer gracefully, seize only for dead DCs

☐ **Sites follow subnets**
site links set cost and interval

☐ **RODC for weak branches**
Password Replication Policy decides cached passwords

☐ **LSDOU, Enforced, Block inheritance**
gpresult proves what applied

☐ **PSO for exceptions, gMSA for services, Recycle Bin on**

Q1 Which FSMO role is the domain's authoritative time source?

A PDC Emulator (it should sync with an external NTP source).

Q2 Which two FSMO roles are forest-wide?

A Schema Master and Domain Naming Master.

Q3 Deploy a DC over a slow WAN link without replicating the whole database?

A Install from media (IFM) created with `ntdsutil ifm`.

Q4 Which group lists passwords an RODC may cache?

A Allowed RODC Password Replication Group (plus per-RODC policy); Denied group wins.

Q5 Default site link cost and replication interval?

A Cost 100, every 180 minutes (minimum 15).

Q6 Force replication of all partitions to all partners across sites?

A `repadmin /syncall /AdeP`.

Q7 A child OU blocks inheritance; a domain GPO must still apply. What do you set?

A Enforced on the domain GPO link.

Q8 Restore a deleted user with its group memberships without an authoritative restore?

A AD Recycle Bin (if enabled before the deletion): `Restore-ADObject`.

Q9 Run a scheduled task on three servers with an automatically rotated password?

A Group managed service account (gMSA), KDS root key created first.

Q10 Users of a partner forest may log on only to two file servers. Which trust option?

A Selective authentication with Allowed to Authenticate on those servers.