



AZ-802: Domain Controllers, FSMO, Sites and Trusts

AZ-802 domain 1 (Deploy and manage AD DS, 20-25 %), part 1 | DCs on-premises and in Azure, RODCs and their account security, FSMO roles, trusts, sites and replication; PowerShell, ntdsutil, repadmin

AZ-802 Domain 1 AD DS

Deploy domain controllers locally and in Azure

Recall (AZ-800 chapter): a forest holds domains, each DC replicates the schema, configuration and domain partitions, and Windows Server 2025 adds the **Windows Server 2025 functional level** (all DCs on 2025) and an optional 32 KB database page size. AZ-802 asks you to **deploy and manage DCs locally and in Azure, deploy RODCs and manage their account security, and manage and troubleshoot FSMO roles.**

PowerShell (ADDSDeployment module)	Effect
Install-WindowsFeature AD-Domain-Services - IncludeManagementTools	binaries only; nothing promoted yet
Install-ADDSForest -DomainName corp.contoso.com -InstallDns	new forest; asks for the DSRM password
Install-ADSDomainController -DomainName corp.contoso.com -SiteName Paris -InstallDns	extra writable DC in an existing domain
Install-ADSDomainController -ReadOnlyReplica -SiteName Lyon ...	RODC in one step (needs a writable 2008+ DC)
Add-ADDSReadOnlyDomainControllerAccount -DomainControllerAccountName LYON-RODC1 -SiteName Lyon -DelegatedAdministrator AccountName CORP\lyon-it	staged RODC, step 1: Domain Admin pre-creates the account
Install-ADSDomainController -UseExistingAccount ...	staged RODC, step 2: the delegated branch admin promotes
ntdsutil "ifm" "create sysvol full C:\IFM" q q	install from media: ship the database instead of replicating over a slow WAN

DC in an Azure VM

- ✓ baseline / mandatory ☐ recommended – verify in your context
- ✓ Static private IP set on the Azure NIC, never inside the guest
- ✓ NTDS database, logs and SYSVOL on a data disk with host caching None write caching could lose AD writes
- ✓ VNet DNS servers point to the DCs (Azure DNS cannot resolve the AD zone)
- ✓ Create an AD site and subnet for the Azure VNet address space clients in Azure then use the Azure DCs
- ☐ SHOULD Two DCs in different availability zones
- ☐ MUST Never restore a DC from a snapshot without VM-GenerationID support; Azure and Hyper-V supply it prevents USN rollback

☐ SHOULD NSG allows AD ports only from your subnets (88, 135, 389, 445, 464, 636, 3268-3269, 49152-65535)

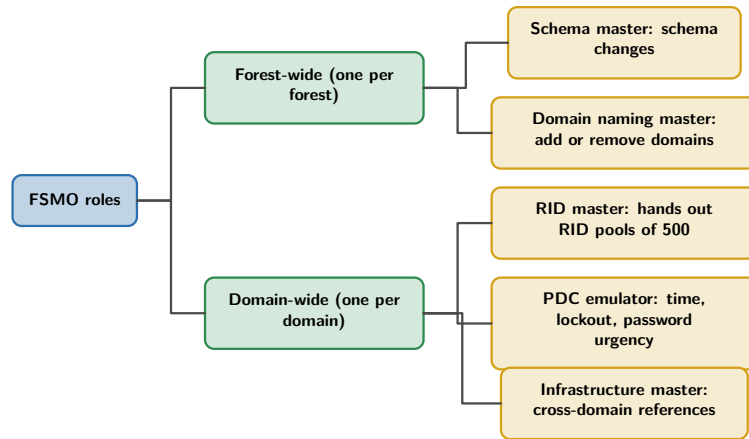
RODC account security and FSMO roles

Which RODC password control?

Conditions	Cache	Cache now	Default	Incident
Branch users must log on during a WAN outage	Y	Y	N	--
Account is privileged (Domain Admins, krbtgt...)	N	N	--	Y
RODC stolen or compromised	N	N	N	Y
Actions				
Add branch users to Allowed RODC Password Replication Group	X	X		
Prepopulate with repadmin /rodcpwdrepl		X		
Leave in Denied RODC Password Replication Group			X	X
Delete RODC account and reset cached passwords				X
Notes	cached at first logon	no first WAN logon needed	deny wins over allow	the delete wizard offers the reset

- Administrator role separation dsmgmt "local roles" "add CORP\lyon-it administrators" gives local admin on the RODC without any domain right
- Which accounts are cached? Get-AddDomainControllerPasswordReplicationPolicy Usage -Identity LYON-RODC1 -RevealedAccounts
- Each RODC has its own krbtgt_NNNNN tickets it issues are useless on writable DCs, which limits a stolen RODC

Five FSMO roles



```

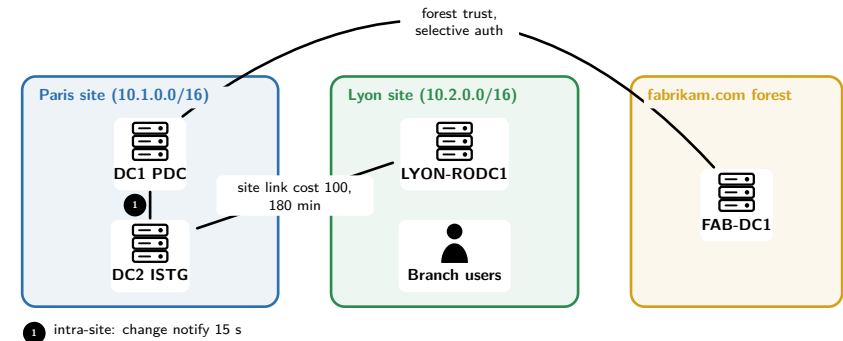
Find, transfer, seize
netdom query fsmo
Get-ADForest | Select SchemaMaster,DomainNamingMaster
Get-ADDomain | Select PDCEmulator,RIDMaster,InfrastructureMaster
# transfer: old holder online
Move-ADDirectoryServerOperationMasterRole -Identity DC2 `
  -OperationMasterRole PDCEmulator,RIDMaster
# seize: old holder dead, never bring it back
Move-ADDirectoryServerOperationMasterRole -Identity DC2 `
  -OperationMasterRole SchemaMaster -Force
  
```

⚠ Seizing is one-way

After seizing the **RID master** or **schema master**, the old holder must never return to the network: metadata-clean it (ntdsutil metadata cleanup or delete the DC in Active Directory Sites and Services), otherwise duplicate RIDs or schema conflicts follow. Infrastructure master: keep it off a global catalog unless every DC is a GC.

🔗 Multi-site, multi-domain and multi-forest

Two sites, a forest trust



Sites, subnets and links

```

New-ADReplicationSite -Name Lyon
New-ADReplicationSubnet -Name 10.2.0.0/16 -Site Lyon
New-ADReplicationSiteLink -Name Paris-Lyon `
  -SitesIncluded Paris,Lyon -Cost 100 `
  -ReplicationFrequencyInMinutes 15
repadmin /replsummary # failures per DC
repadmin /showrepl DC2 # inbound partners
repadmin /syncall /AdeP # push all, enterprise
  
```

Trust	Transitive	Use it when
Parent-child, tree-root	yes, two-way	automatic inside a forest
Shortcut	yes	speed up authentication between two deep domains of one forest
Forest	yes, between the two forests	merger: all domains of both forests, Kerberos; needs DNS resolution both ways (conditional forwarders)
External	no	one domain of another forest, or an NT4-style domain; NTLM
Realm	configurable	MIT Kerberos (Linux, UNIX) realm

- **Selective authentication** users of the trusted forest get nothing until you grant **Allowed to Authenticate** on each target computer object
- **Direction** trusting domain holds resources, trusted domain holds accounts; access flows opposite to the trust arrow
- **Create** Active Directory Domains and Trusts or `netdom trust corp.contoso.com /d:fabrikam.com /add /twoway /realm` (no `New-ADTrust` cmdlet exists)
- **Multi-domain admin** universal groups for cross-domain membership; group scope rules in sheet 02

Size the inter-site replication delay

PROBLEM

A password reset on DC1 (Paris) must reach LYON-RODC1. Intra-site change notification fires after 15 s, the Paris-Lyon site link replicates every 1 minutes. What is the worst-case delay, and what changes if the link interval drops to 15 min?

1. Default link

⇒ $D = 15 \text{ s} + 180 \text{ min} \approx 180.3 \text{ min} \approx 3 \text{ h}$

why: inter-site replication is scheduled, not notified

2. Tuned link

⇒ $D = 15 \text{ s} + 15 \text{ min} \approx 15.3 \text{ min}$

why: minimum interval

3. Password special case

⇒ RODC without the hash → forwards to a writable DC; a DC that rejects a password re-checks it on the PDC emulator

why: new passwords work before replication

GIVEN

- $n = 15 \text{ s}$ first-partner notification delay inside Paris
- $I = 180 \text{ min}$ default site-link interval (minimum 15)
- worst case $D = n + I$ (change misses the last inter-site cycle)

ANSWER

≈ 3 h by default, ≈ 15 min with a 15-min interval; enable change notification on the link (options attribute) for near-real-time

Check: Urgent replication (lockouts, RID changes) bypasses the interval; ordinary attribute changes do not

YOU MAY HEAR

"An RODC caches every password by default"

BUSTED

✓ ACTUALLY

It caches none until the PRP allows them

Only accounts in the Allowed group (or added explicitly) are cached; privileged groups sit in the Denied group.

YOU MAY HEAR

"Transfer and seize are the same"

BUSTED

✓ ACTUALLY

Seizing is forced and final

Transfer when the holder is online; seize only when it is permanently gone, then clean its metadata.

YOU MAY HEAR

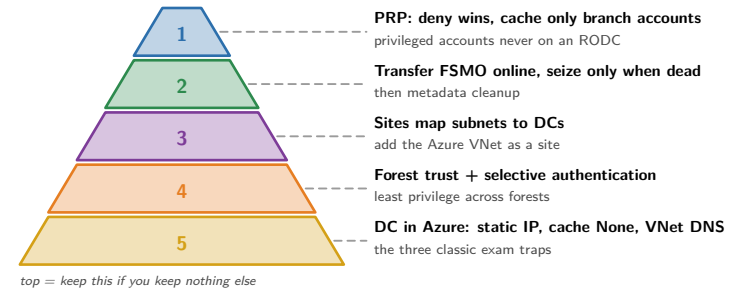
"A forest trust lets every user in"

BUSTED

✓ ACTUALLY

Selective authentication blocks by default

Grant Allowed to Authenticate per server; SID filtering stays on.



Q1 Which two FSMO roles are forest-wide?

A Schema master and domain naming master.

Q2 Which FSMO role is the time source of the forest?

A The PDC emulator of the forest root domain (sync it to an external NTP source).

Q3 Two steps of a staged RODC install?

A Domain Admin runs Add-ADDSDomainControllerAccount (delegating an admin), then the branch admin runs Install-ADDSDomainController -UseExistingAccount.

Q4 How do you cache branch passwords on an RODC before a WAN outage?

A Allow them in the PRP and prepopulate with repadmin /rodcpwdrepl.

Q5 Disk caching for NTDS on an Azure DC?

A None, on a data disk; the OS disk's ReadWrite cache could lose AD writes.

Q6 Default inter-site replication interval and cost?

A 180 minutes and cost 100; minimum interval 15 minutes.

Q7 Which trust type is non-transitive and uses NTLM?

A External trust.

Q8 What does selective authentication require on the target server?

A The Allowed to Authenticate permission for the trusted users or groups on its computer object.

Q9 What happens to a DC offline longer than the tombstone lifetime (180 days)?

A It may reintroduce lingering objects; demote it forcibly and clean its metadata rather than reconnect it.