Welkom bij hét IT-Infra event van het jaar!

knvi | it-infra

Azure AD Domain Services;
De vervanging voor je lokale AD?

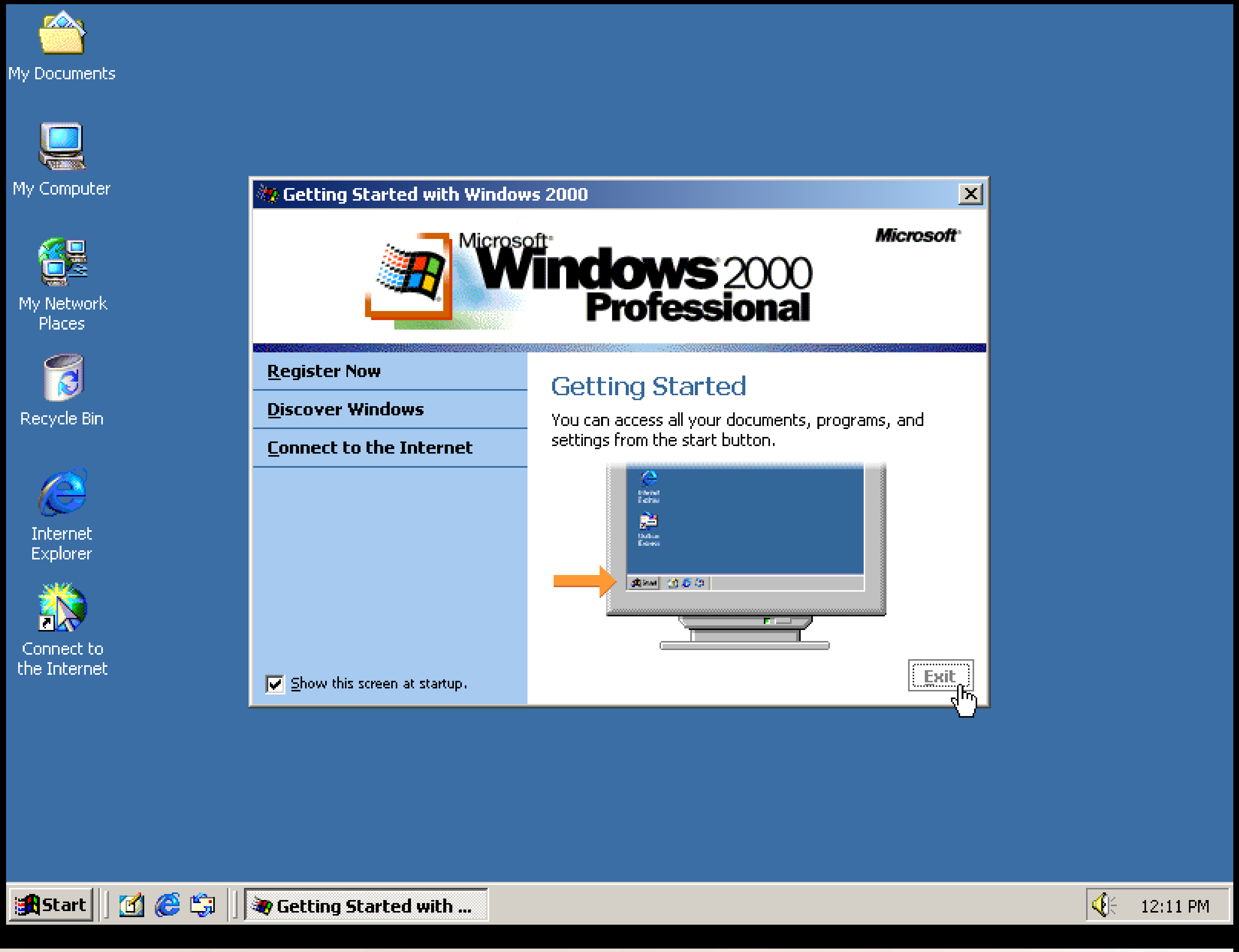
94% Bulletpoint FREE !

Erwin Derksen

@Erwin_derksen

DerkIT

ICT - Verandering - Communicatie



Getting Started with Windows 2000

Getting Started

You can access all your documents, programs, and settings from the start button.

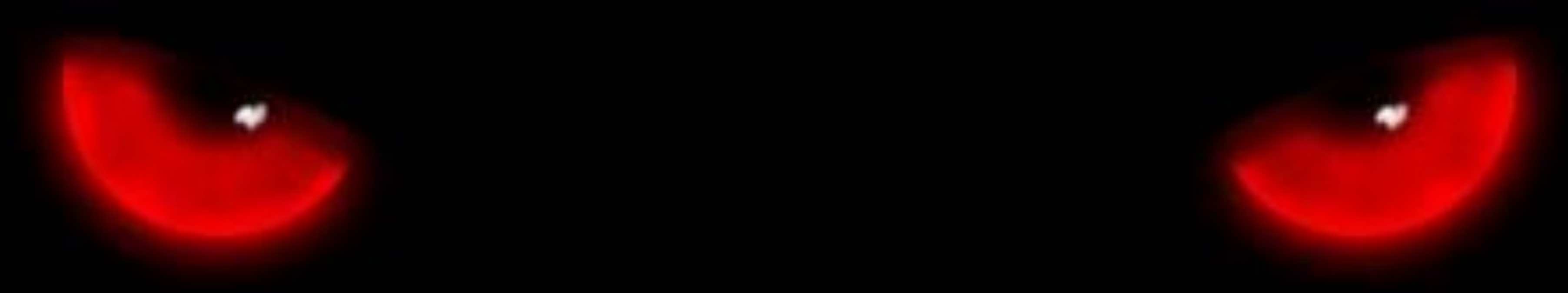
☑ Show this screen at startup.

Active Directory; OLD but still required…

Posterijen – P&T – PTT – KPN – TPG Post – TNT Post – PostNL
220 jaar postbedrijf 1799 – 2019
NEDERLAND
1
postnl
8 714341 083753

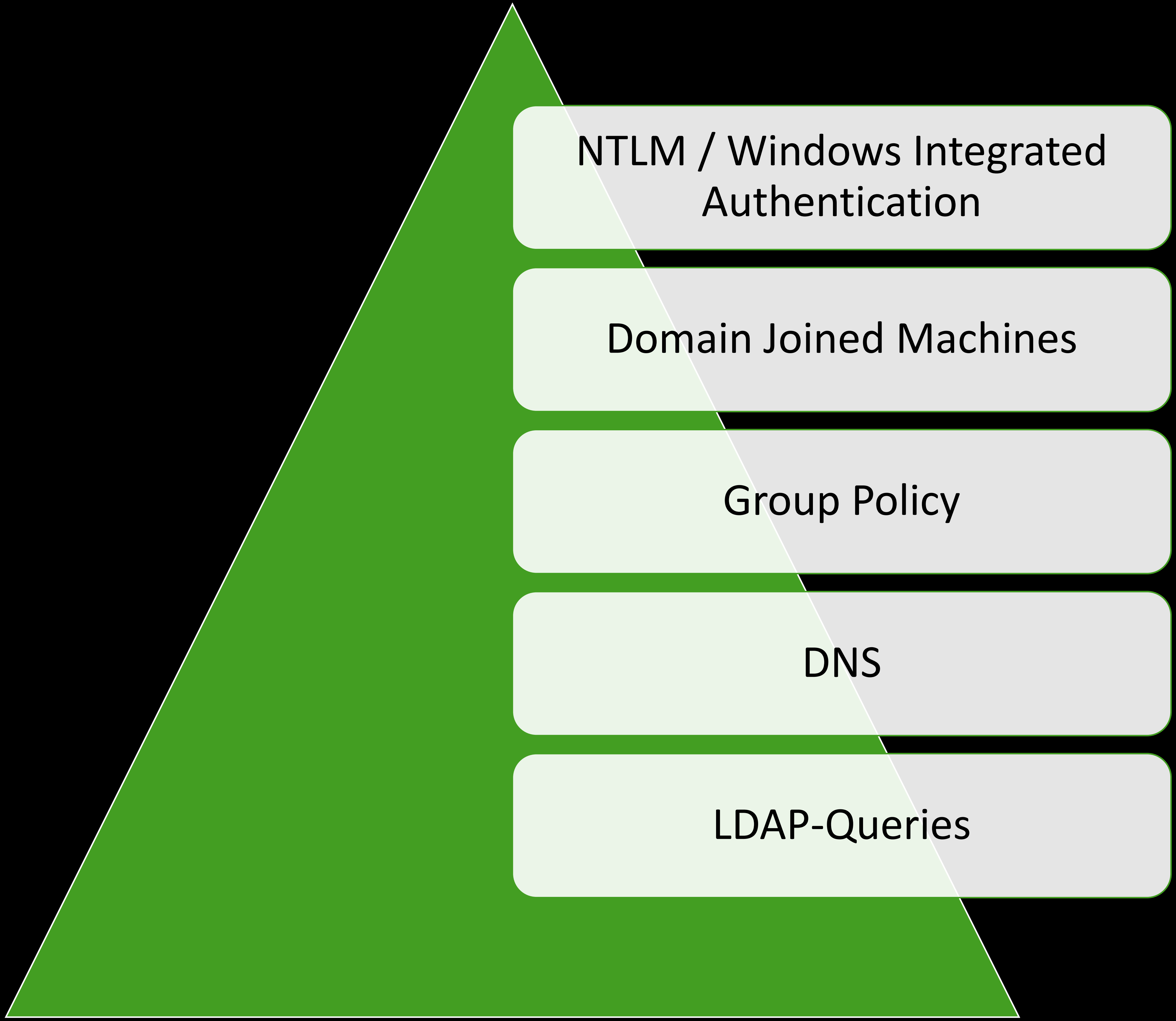
Companies are moving to the **cloud**

Legacy apps…..



…are Evil

AD Dependency....



NTLM / Windows Integrated Authentication

Domain Joined Machines

Group Policy

DNS

LDAP-Queries

What to do with AD-depending Apps?

1/4

‘Down the drain’

2/4 - ‘SaaS Alternative’

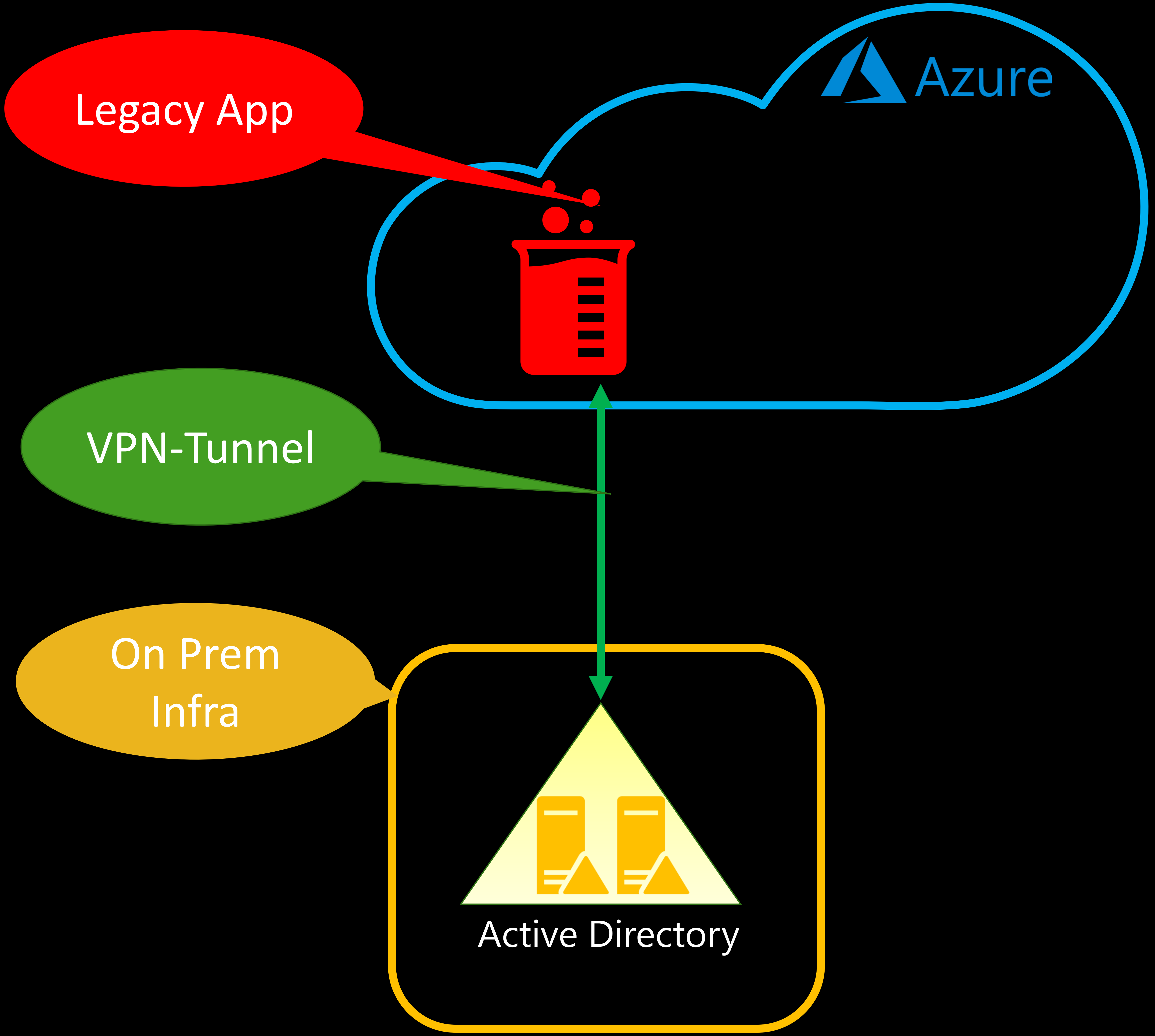
3/4 - ‘Rewrite’ –
“How hard can it be?”

4/4 Lift & Shift to the cloud

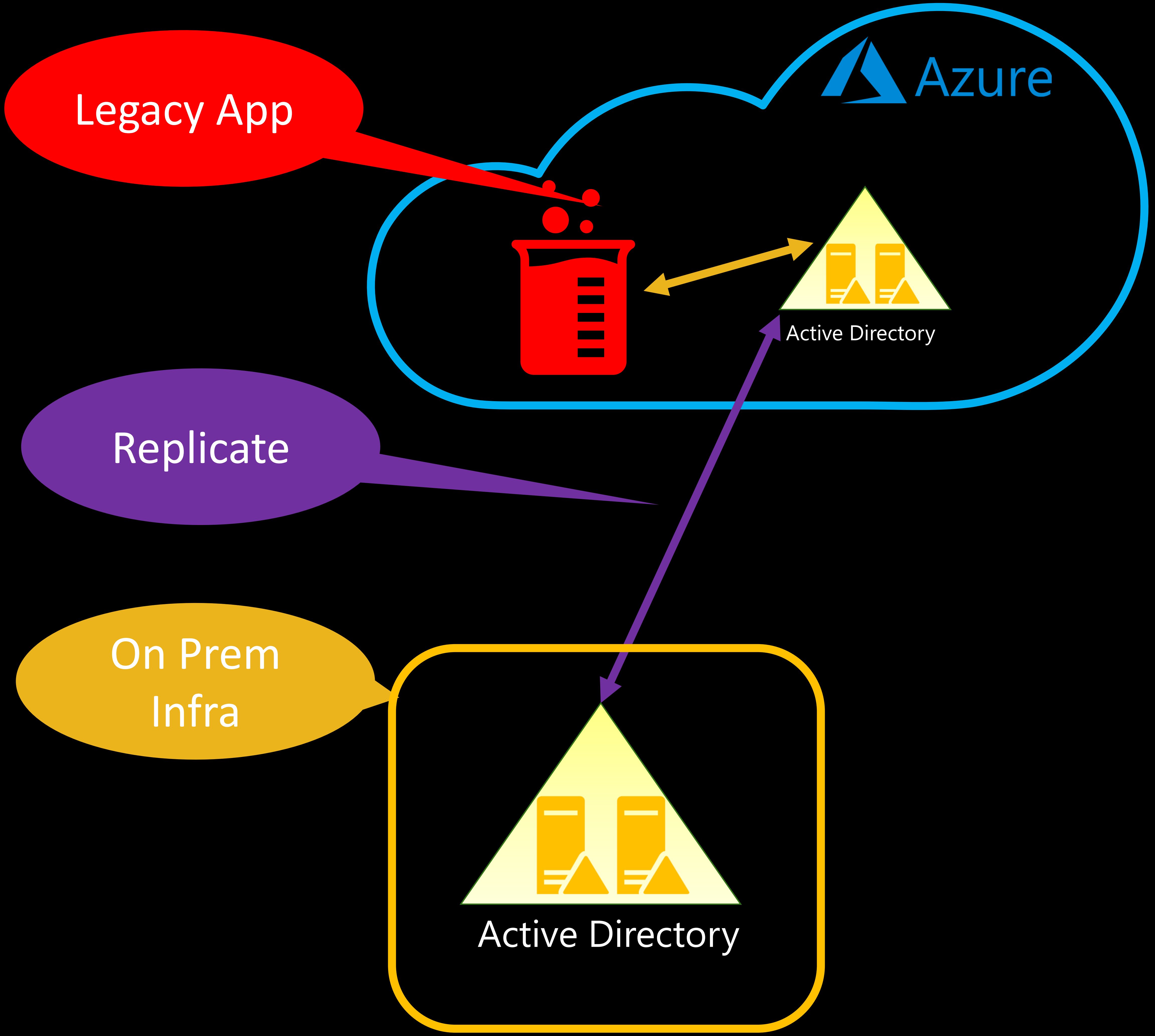
3 scenario’s

knvi | it-infra

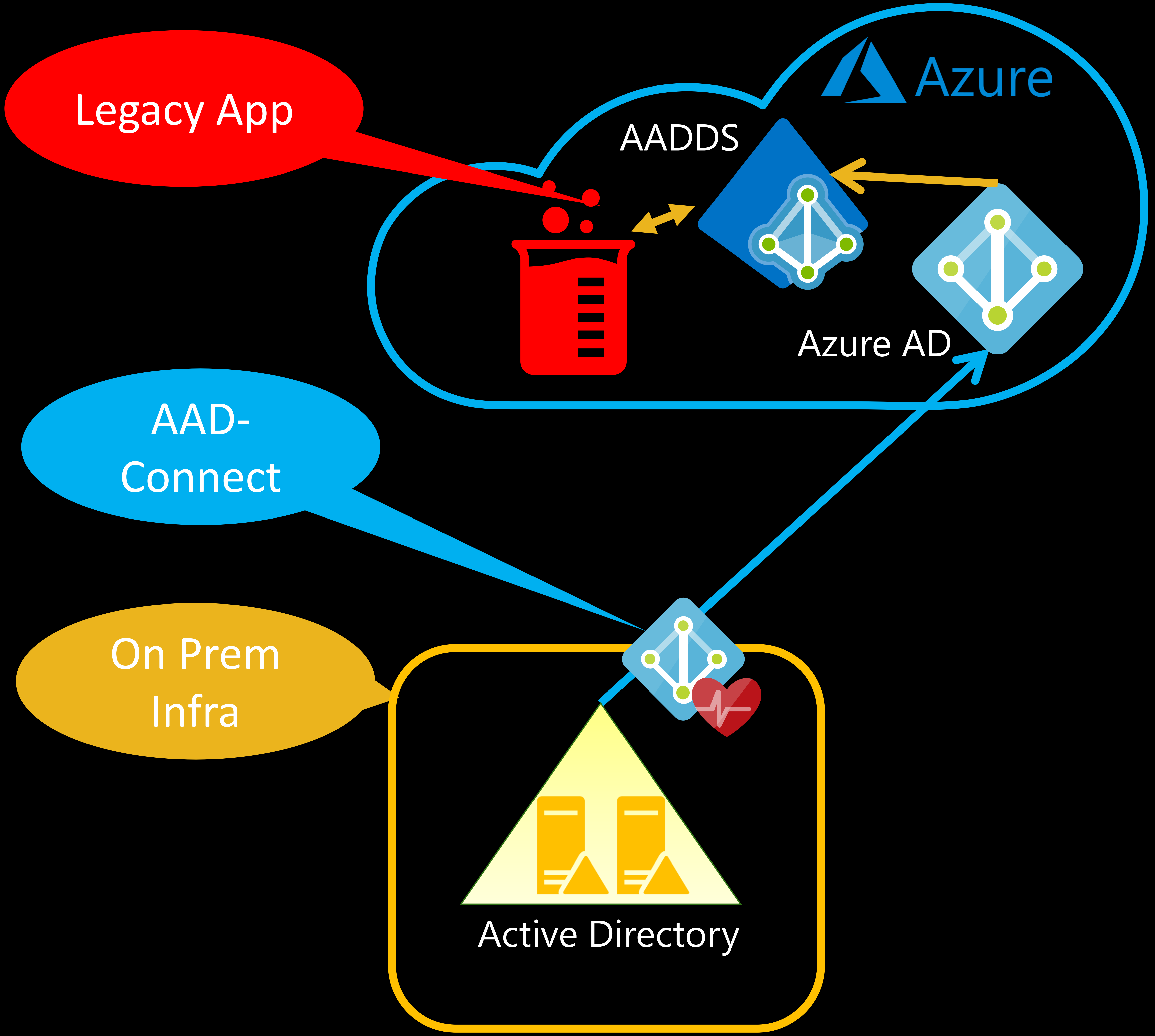
1/3 Connect to on prem AD



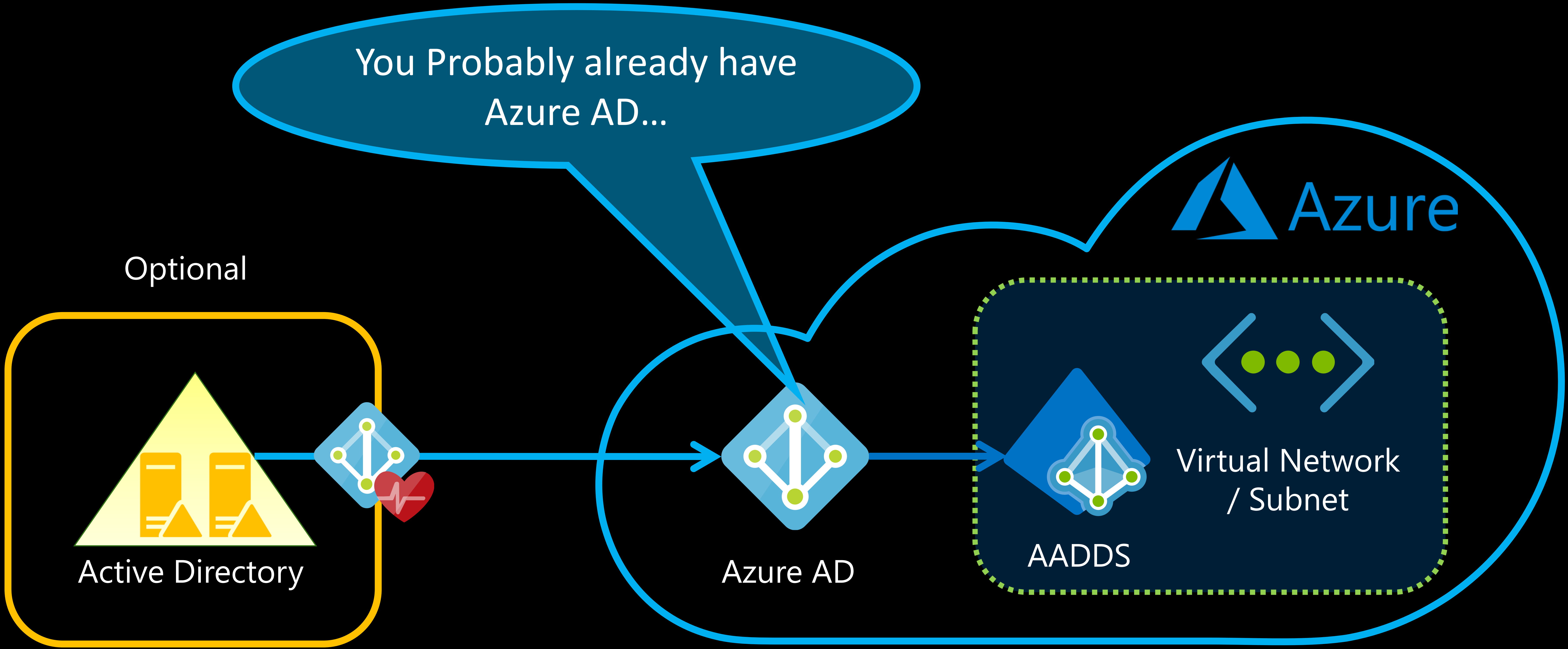
2/3
Run DC's as VM in Azure



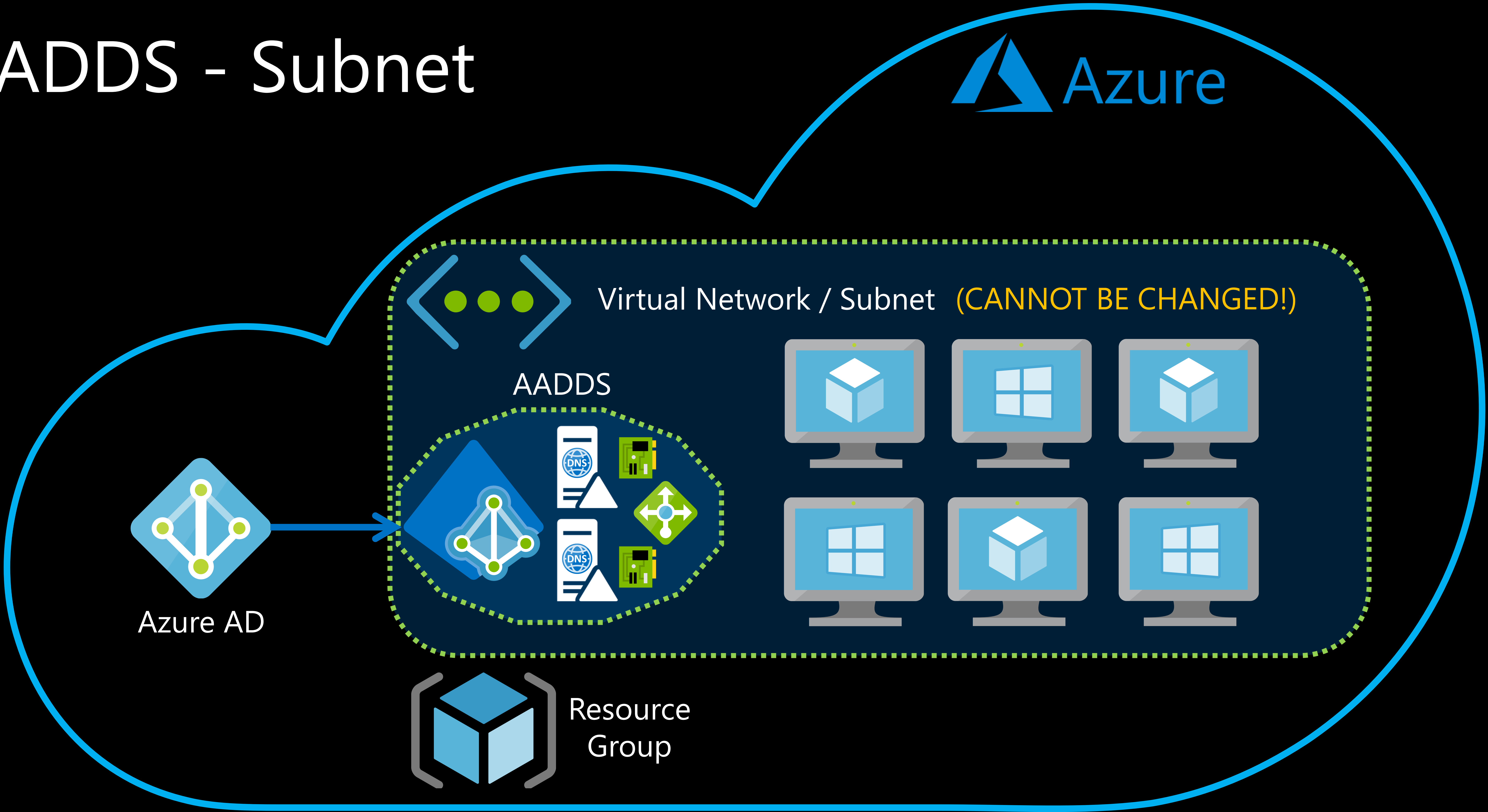
3/3 Azure AD Domain Services



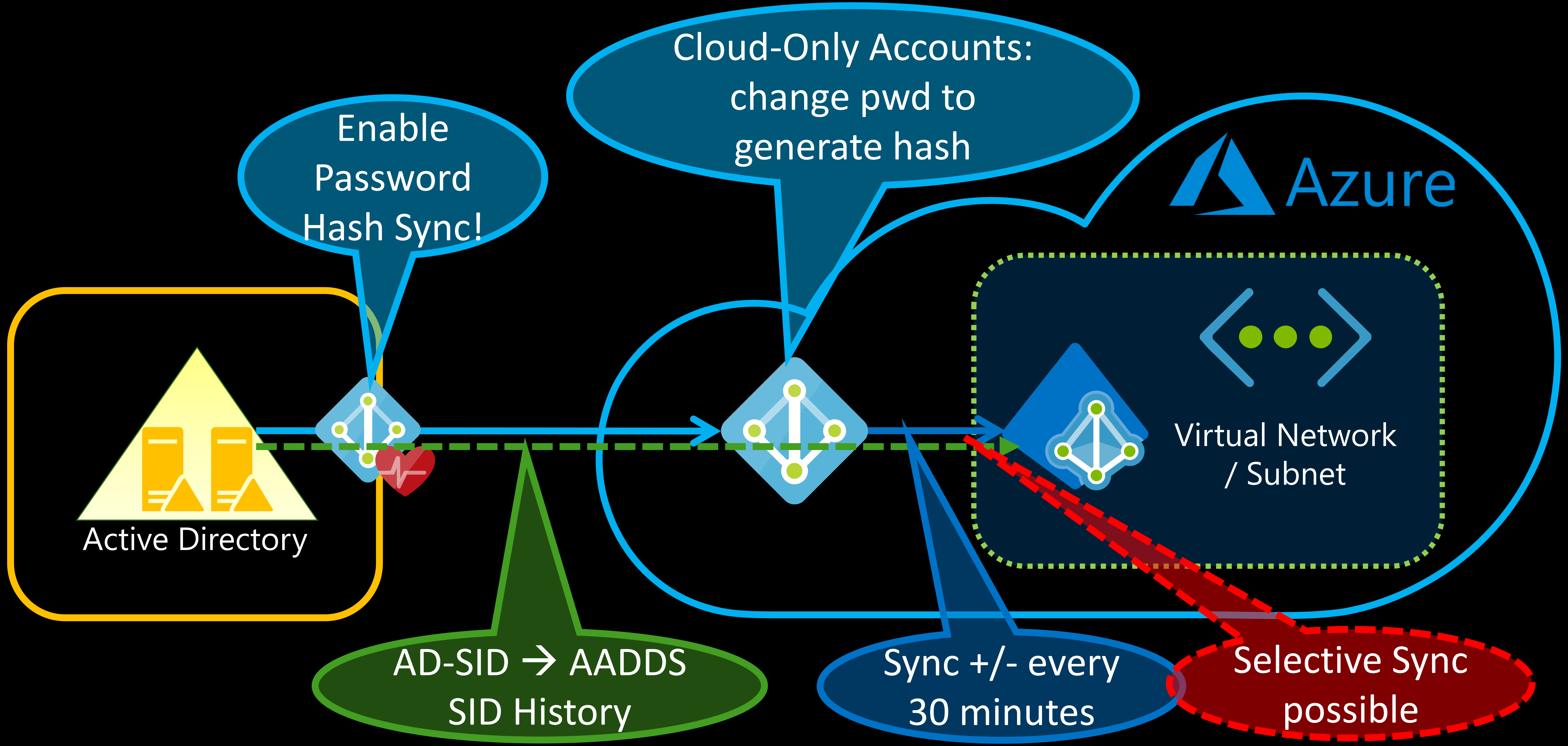
AADDS – Basics



AADDS - Subnet

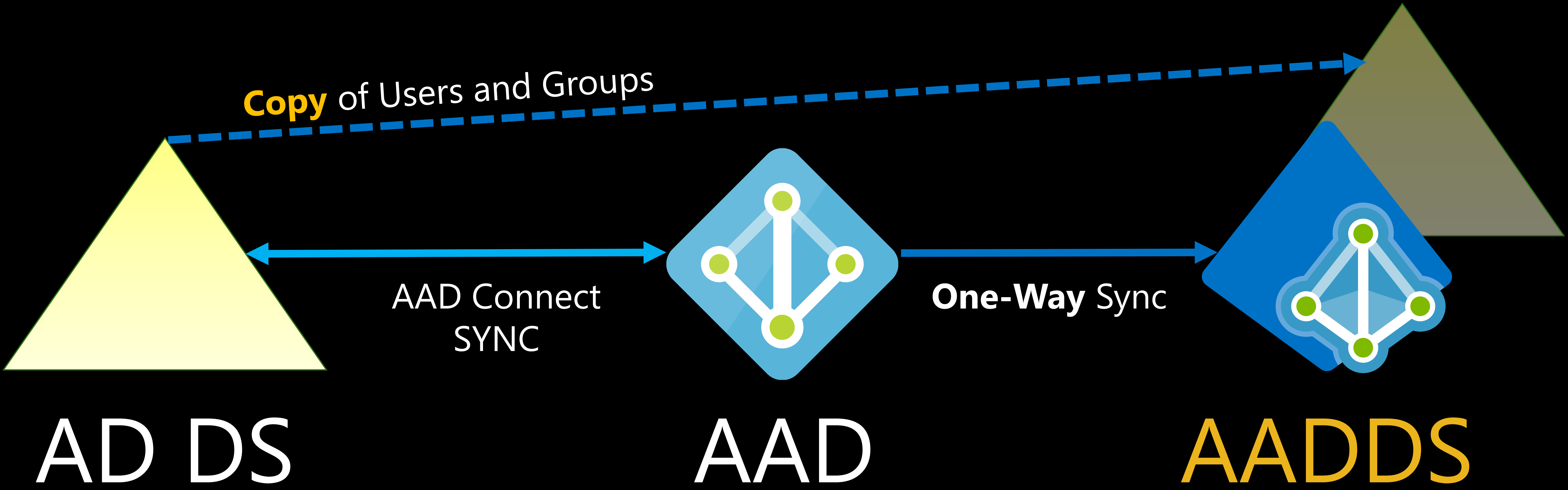


AADDS – In Operation

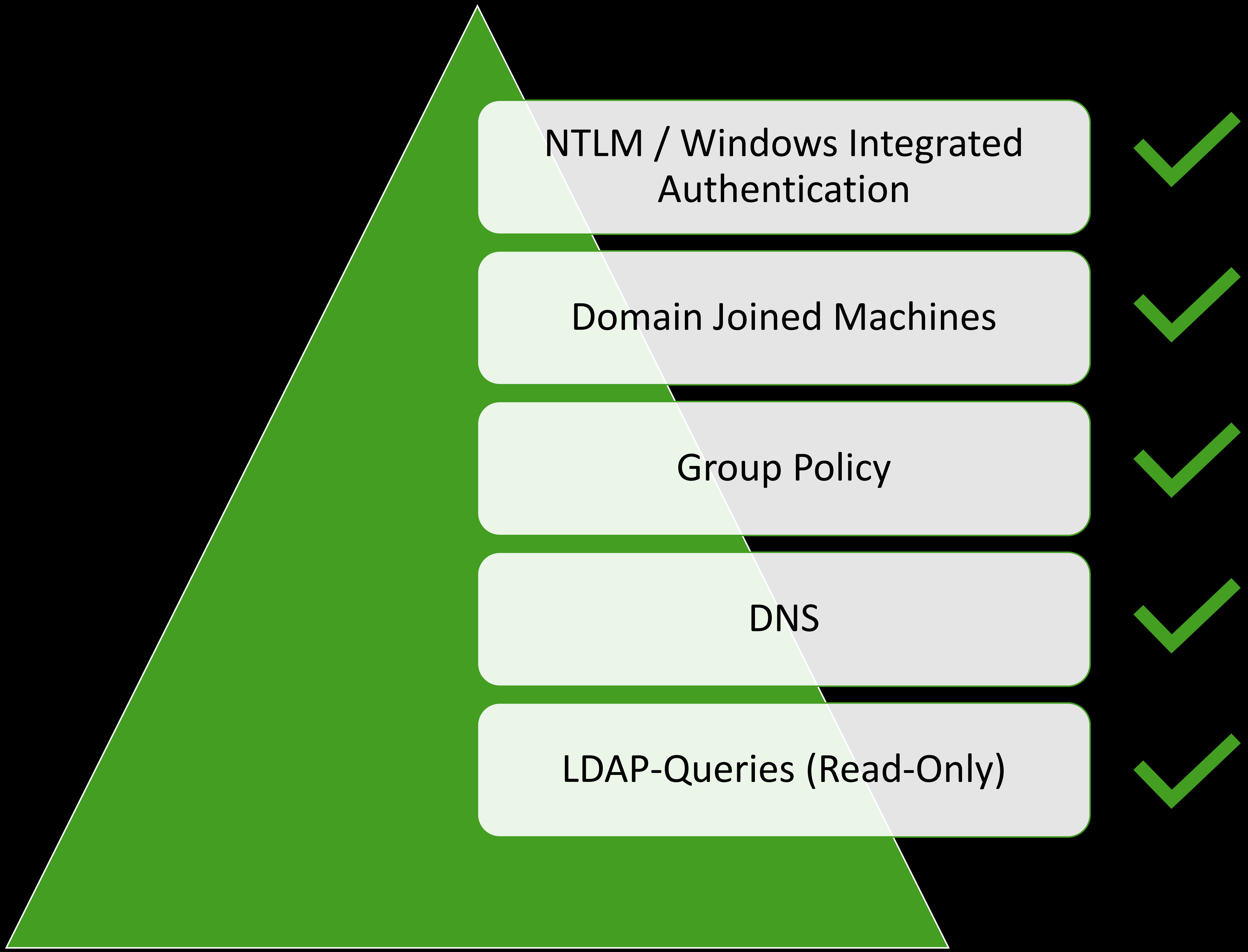

Enable Password Hash Sync!
Cloud-Only Accounts: change pwd to generate hash
Azure
Virtual Network / Subnet
Active Directory
AD-SID → AADDS SID History
Sync +/- every 30 minutes
Selective Sync possible

AADDS –ne AD

2 different AD's + Azure AD



But it is an AD Domain, so…



- NTLM / Windows Integrated Authentication ✓
- Domain Joined Machines ✓
- Group Policy ✓
- DNS ✓
- LDAP-Queries (Read-Only) ✓

AD ‘As a Service’

Implementing AADDS

knvi | it-infra

Erwin Derksen

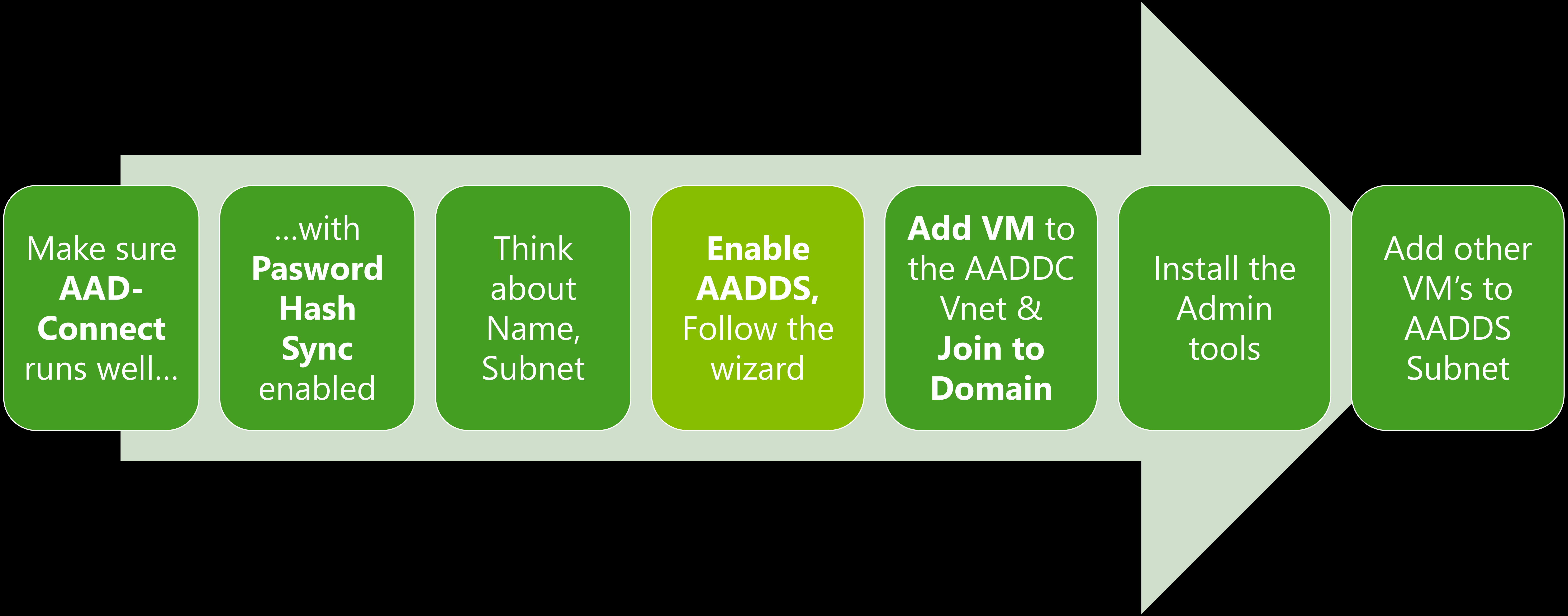
DerkIT

- HEAO-BI, Sinds 1999 in IT
- Uitsluitend pragmatische projecten
- Business <u>en</u> Techniek
- Presentatievaardigheden

CLOUDTRANSFORMERS
MASTERS IN CLOUDSOLUTIONS

Kwaliteit is geen toeval

AADDS Deployment Overview



Make sure **AAD-Connect** runs well…

…with **Pasword Hash Sync** enabled

Think about Name, Subnet

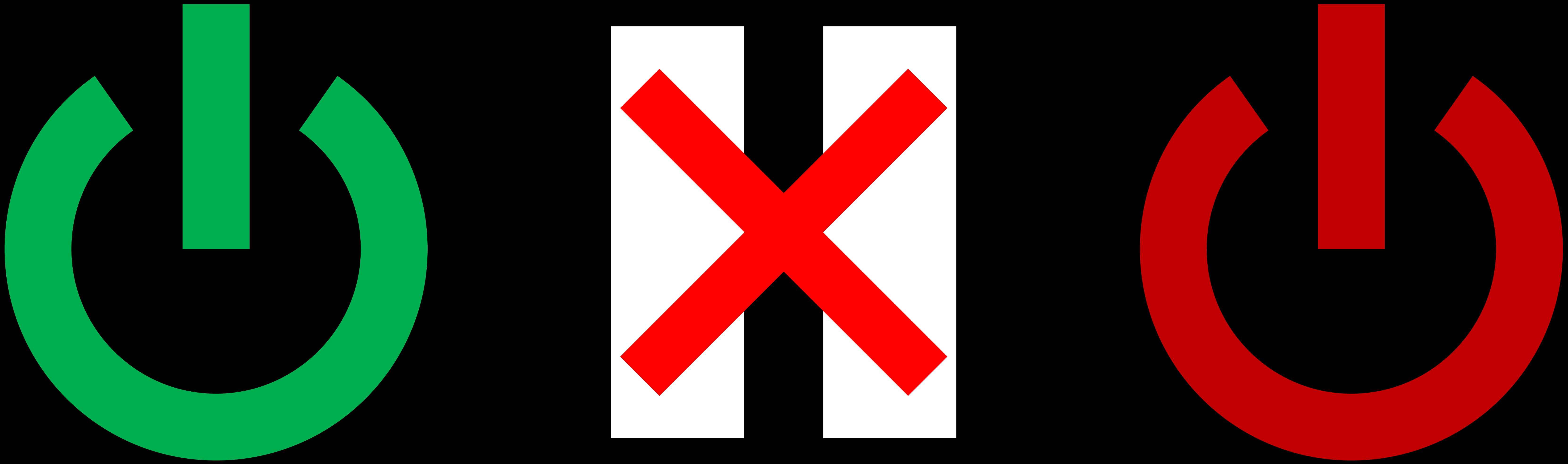
Enable AADDS, Follow the wizard

Add VM to the AADDC Vnet & **Join to Domain**

Install the Admin tools

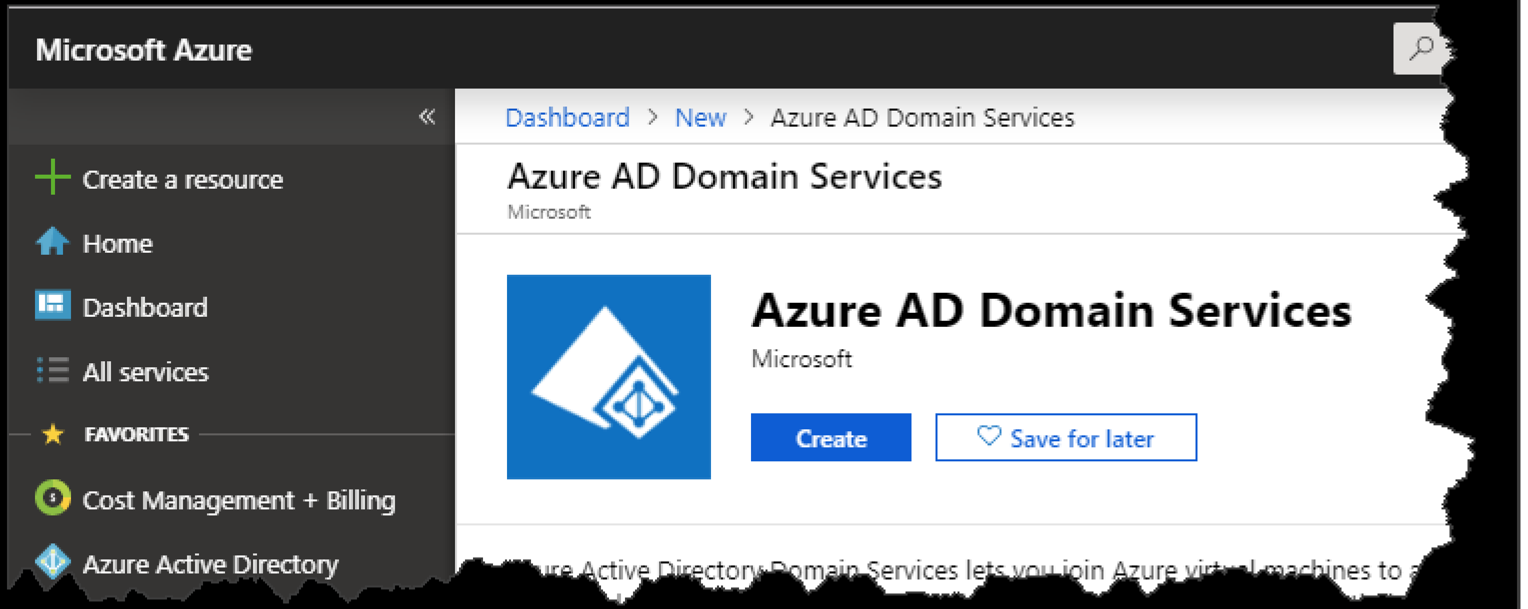
Add other VM’s to AADDS Subnet

No real cost saving option.



Even **geduld** A.U.B.

Create AADDS



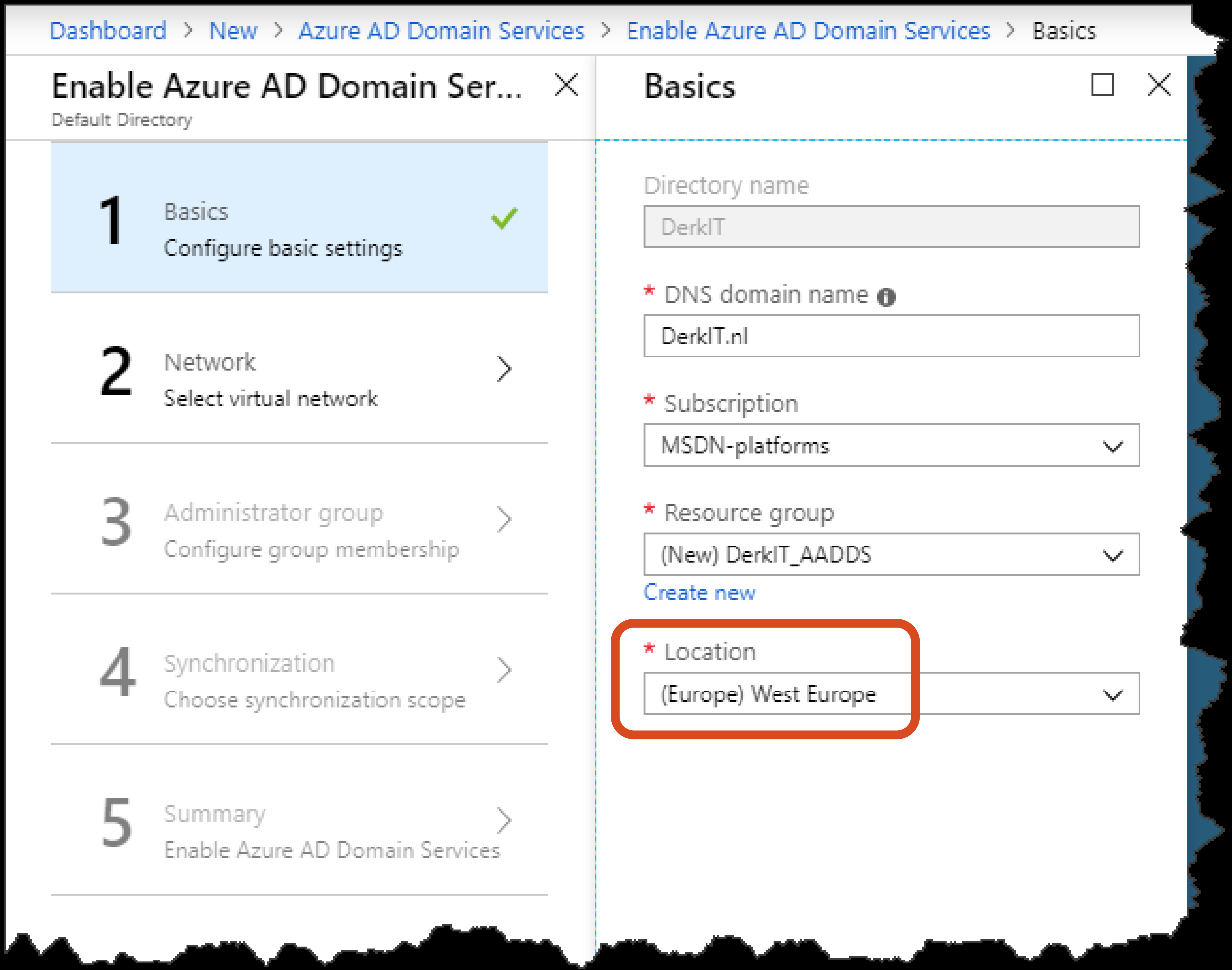
Microsoft Azure

Dashboard > New > Azure AD Domain Services

Azure AD Domain Services
Microsoft

Azure AD Domain Services
Microsoft

ure Active Directory Domain Services lets you join Azure virtual machines to



Dashboard > New > Azure AD Domain Services > Enable Azure AD Domain Services > Basics

Enable Azure AD Domain Ser...
Default Directory

1 Basics ✓
Configure basic settings

2 Network >
Select virtual network

3 Administrator group >
Configure group membership

4 Synchronization >
Choose synchronization scope

5 Summary >
Enable Azure AD Domain Services

Basics

Directory name: DerkIT

* DNS domain name: DerkIT.nl

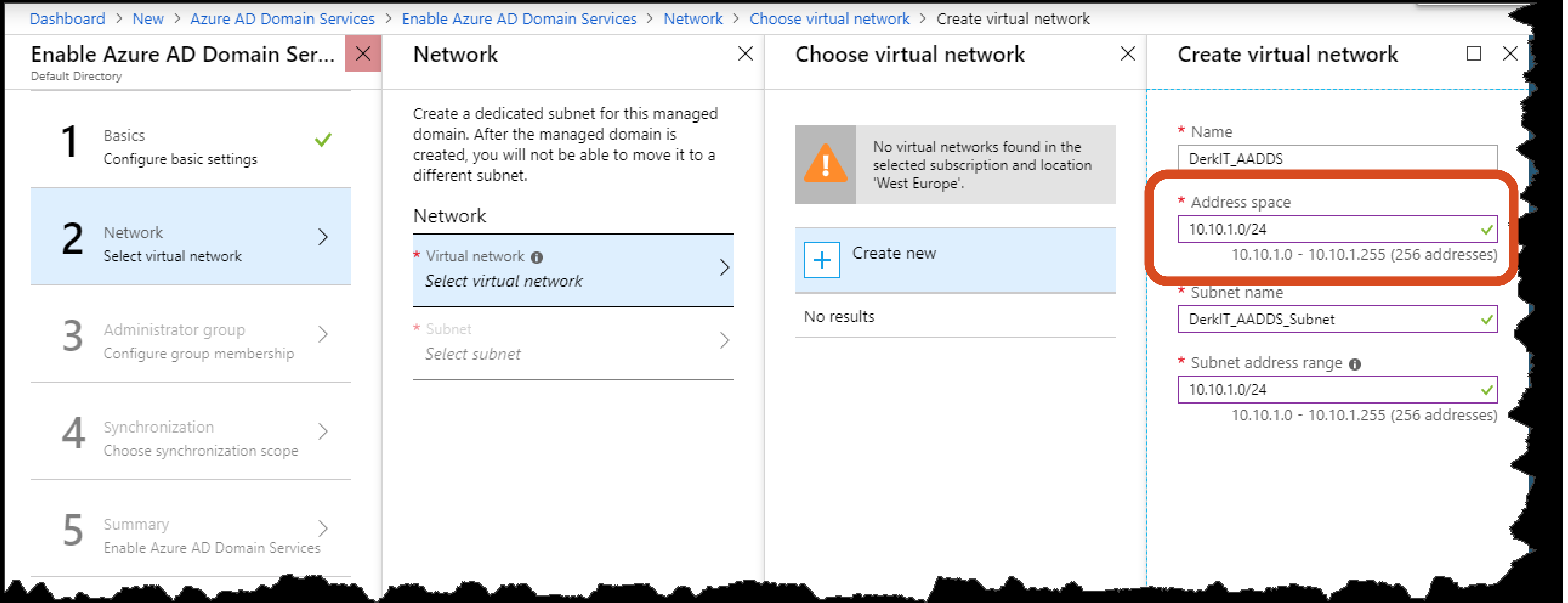
* Subscription: MSDN-platforms

* Resource group: (New) DerkIT_AADDS

* Location: (Europe) West Europe

Create AADDS

Think of Naming & IP-range



Dashboard > New > Azure AD Domain Services > Enable Azure AD Domain Services > Network > Choose virtual network > Create virtual network

Enable Azure AD Domain Ser...
Default Directory

1 Basics
Configure basic settings ✓

2 Network
Select virtual network

3 Administrator group
Configure group membership

4 Synchronization
Choose synchronization scope

5 Summary
Enable Azure AD Domain Services

Network

Create a dedicated subnet for this managed domain. After the managed domain is created, you will not be able to move it to a different subnet.

Network

* Virtual network
Select virtual network

* Subnet
Select subnet

Choose virtual network

No virtual networks found in the selected subscription and location 'West Europe'.

Create new

No results

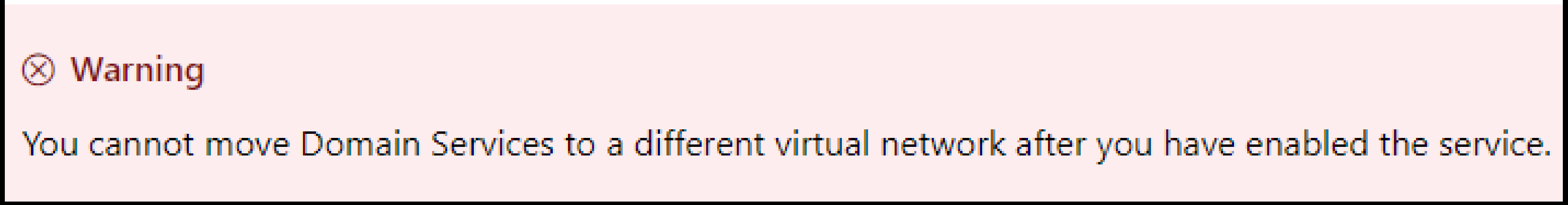
Create virtual network

* Name
DerkIT_AADDS

* Address space
10.10.1.0/24 ✓
10.10.1.0 - 10.10.1.255 (256 addresses)

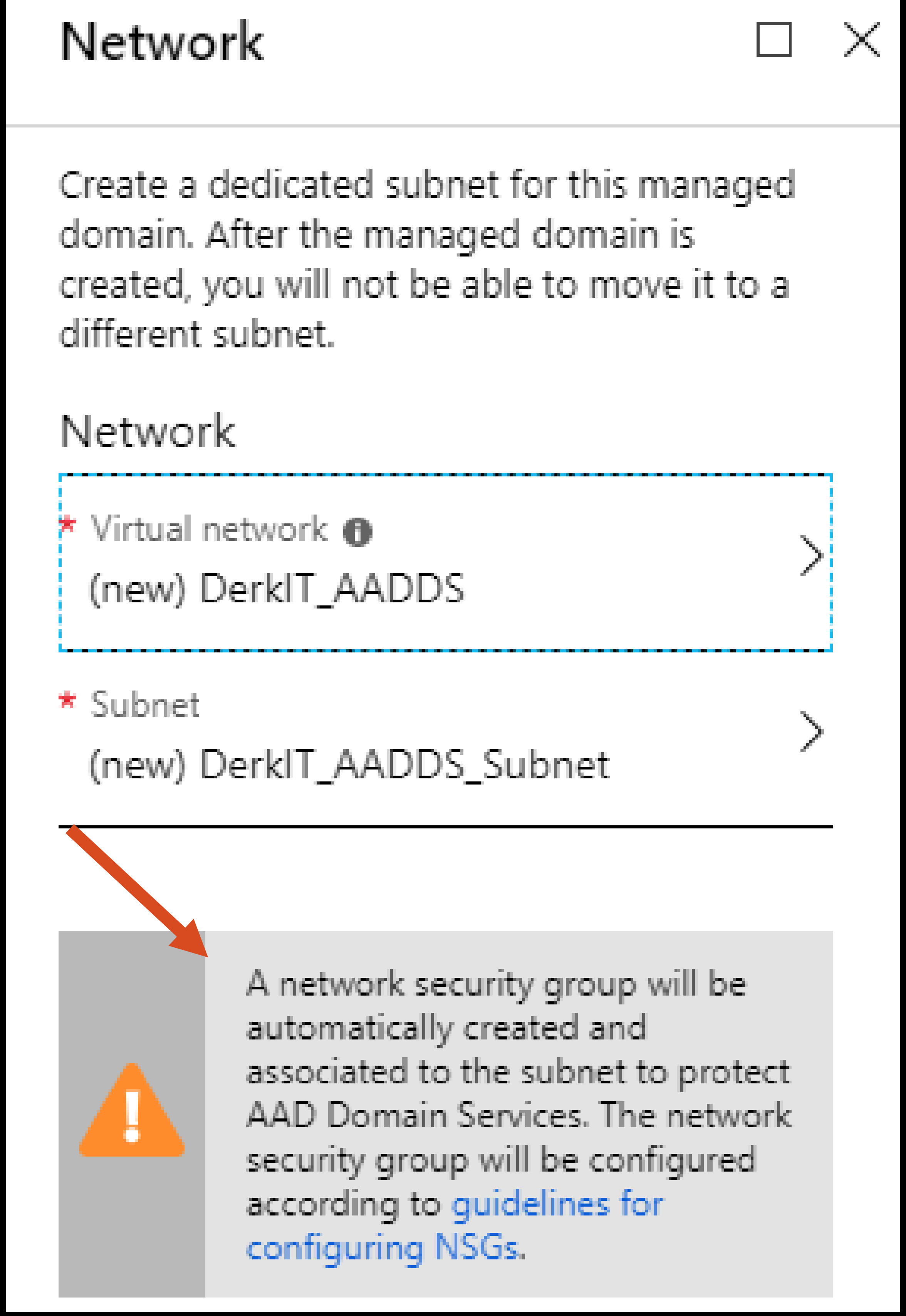
* Subnet name
DerkIT_AADDS_Subnet ✓

* Subnet address range
10.10.1.0/24 ✓
10.10.1.0 - 10.10.1.255 (256 addresses)



Warning

You cannot move Domain Services to a different virtual network after you have enabled the service.



Network

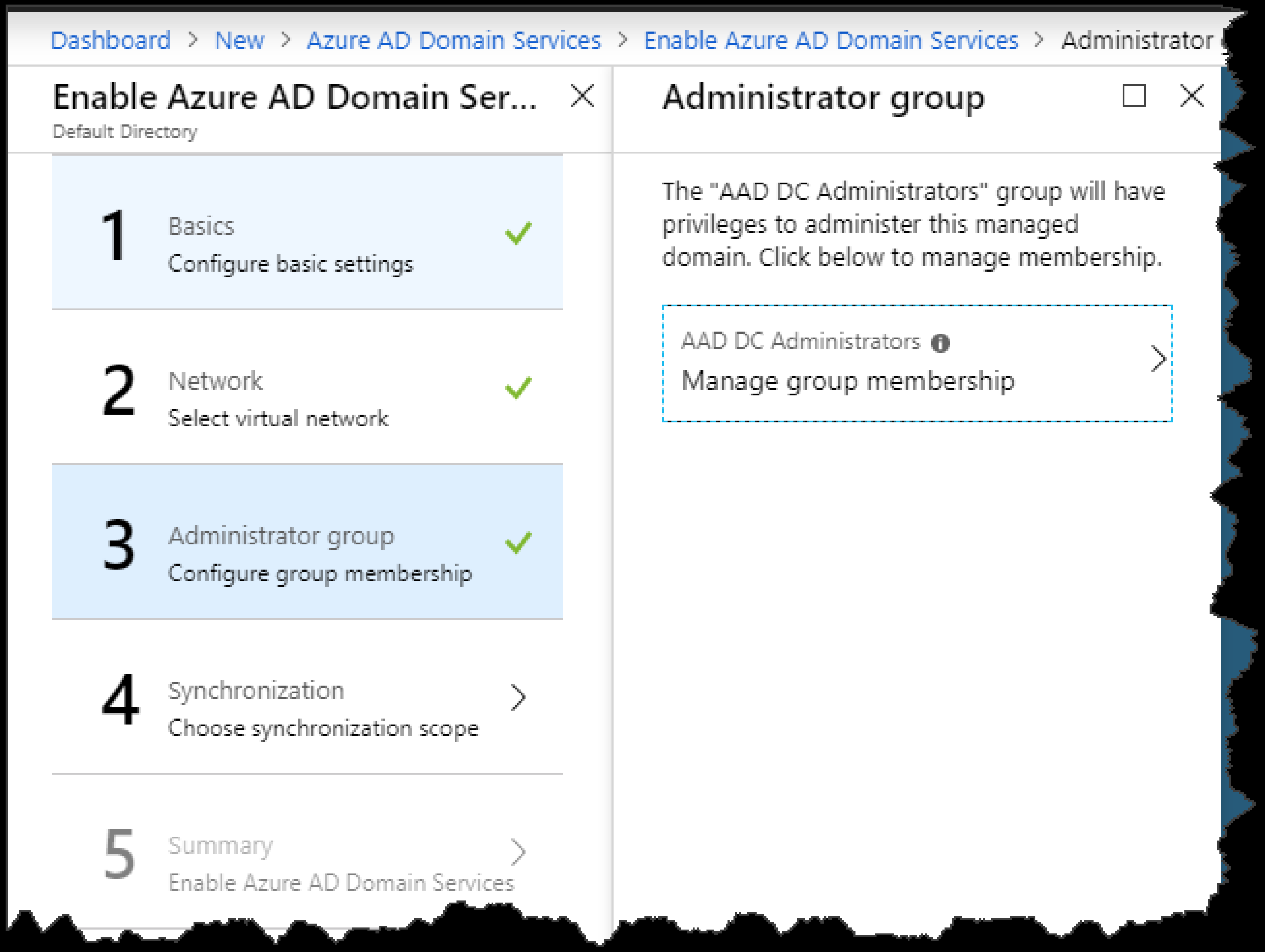
Create a dedicated subnet for this managed domain. After the managed domain is created, you will not be able to move it to a different subnet.

Network

* Virtual network
(new) DerkIT_AADDS

* Subnet
(new) DerkIT_AADDS_Subnet

A network security group will be automatically created and associated to the subnet to protect AAD Domain Services. The network security group will be configured according to guidelines for configuring NSGs.



Dashboard > New > Azure AD Domain Services > Enable Azure AD Domain Services > Administrator

Enable Azure AD Domain Ser...
Default Directory

1 Basics
Configure basic settings ✓

2 Network
Select virtual network ✓

3 Administrator group
Configure group membership ✓

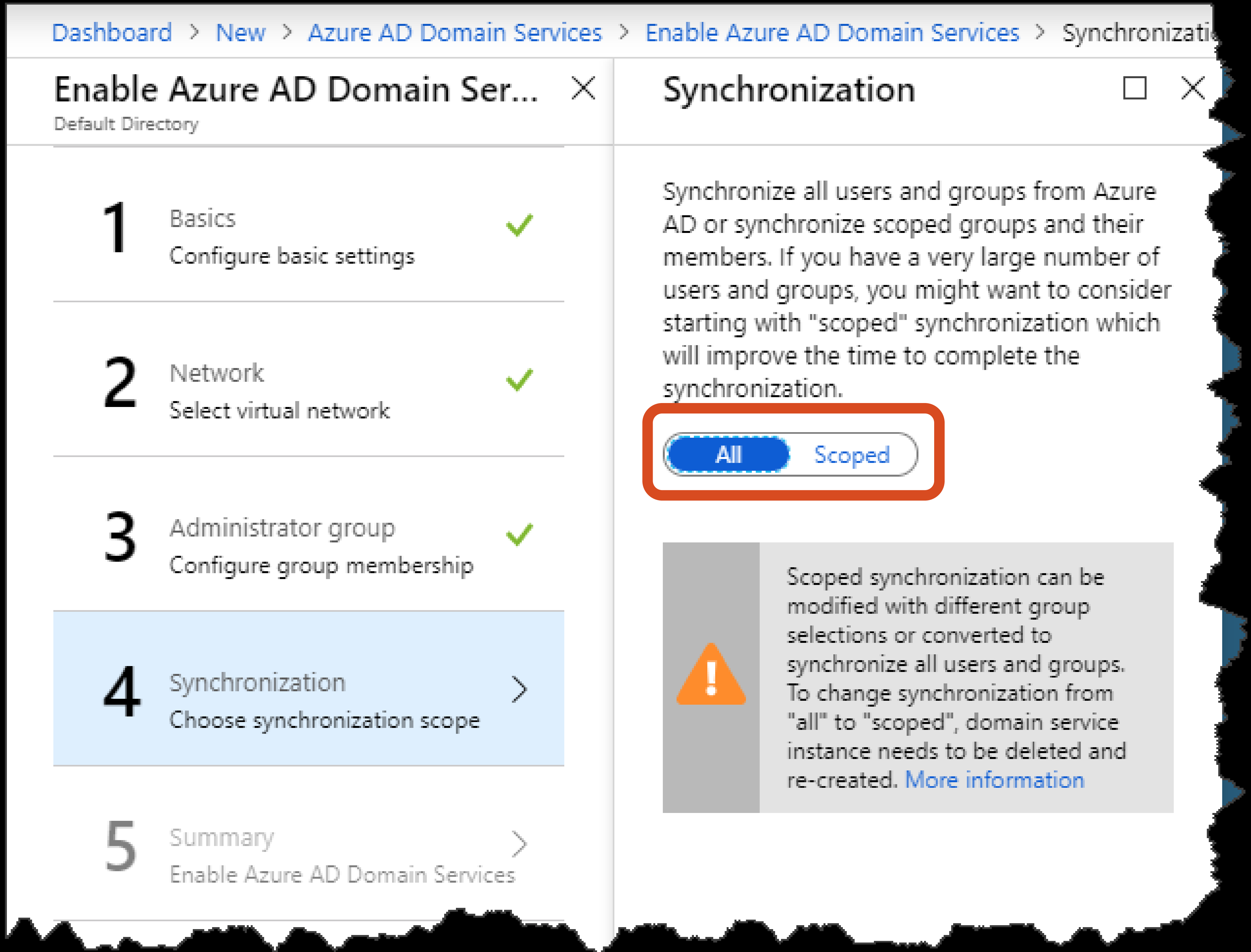
4 Synchronization
Choose synchronization scope >

5 Summary
Enable Azure AD Domain Services >

Administrator group

The "AAD DC Administrators" group will have privileges to administer this managed domain. Click below to manage membership.

AAD DC Administrators
Manage group membership >



Dashboard > New > Azure AD Domain Services > Enable Azure AD Domain Services > Synchronizati

Enable Azure AD Domain Ser...
Default Directory

1 Basics
Configure basic settings ✓

2 Network
Select virtual network ✓

3 Administrator group
Configure group membership ✓

4 Synchronization
Choose synchronization scope >

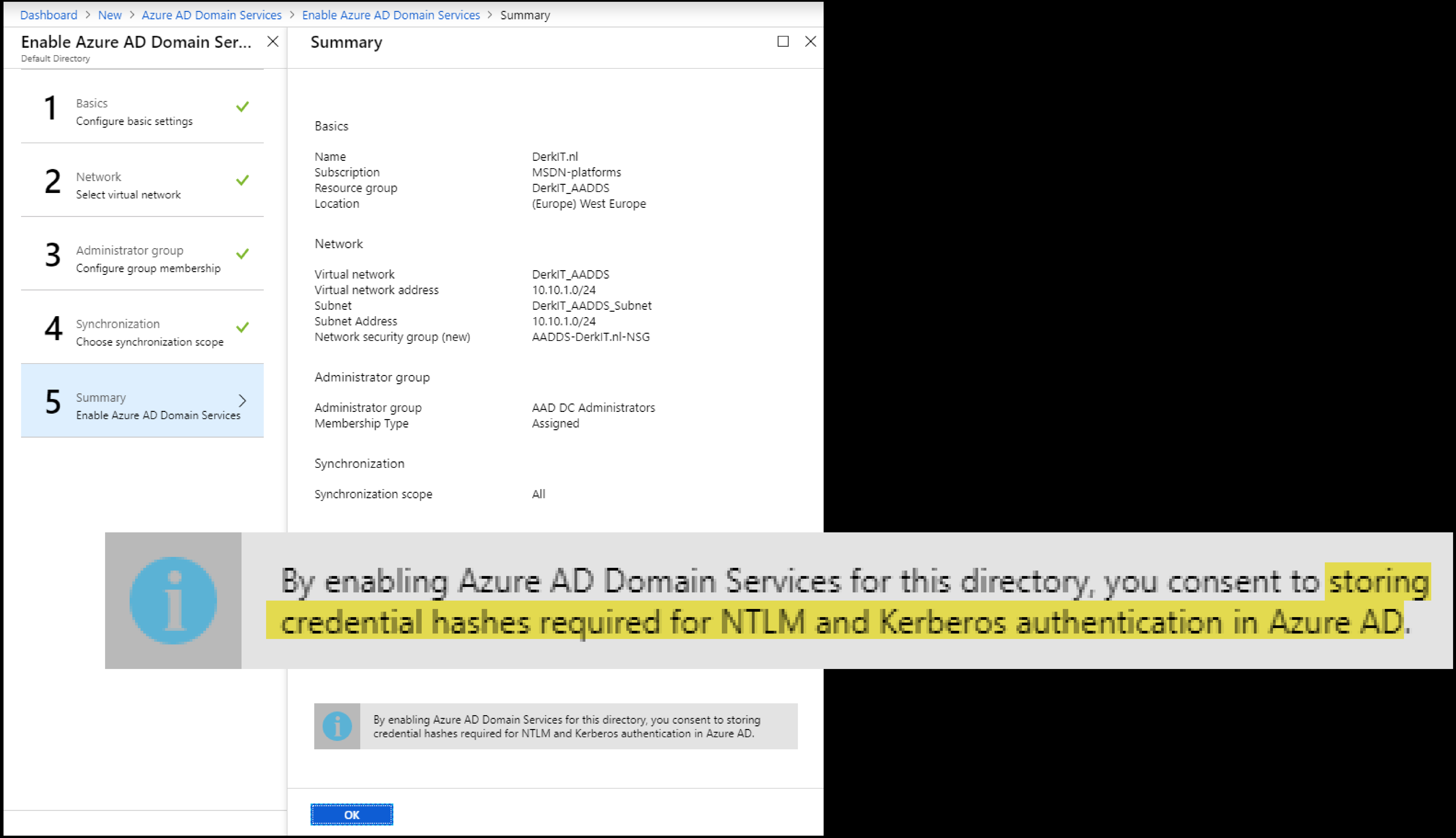
5 Summary
Enable Azure AD Domain Services >

Synchronization

Synchronize all users and groups from Azure AD or synchronize scoped groups and their members. If you have a very large number of users and groups, you might want to consider starting with "scoped" synchronization which will improve the time to complete the synchronization.

[✓ All] Scoped

Scoped synchronization can be modified with different group selections or converted to synchronize all users and groups. To change synchronization from "all" to "scoped", domain service instance needs to be deleted and re-created. More information



Dashboard > New > Azure AD Domain Services > Enable Azure AD Domain Services > Summary

Enable Azure AD Domain Ser...

Default Directory

1 Basics ✓
Configure basic settings

2 Network ✓
Select virtual network

3 Administrator group ✓
Configure group membership

4 Synchronization ✓
Choose synchronization scope

5 Summary >
Enable Azure AD Domain Services

Summary

Basics

Name	DerkIT.nl
Subscription	MSDN-platforms
Resource group	DerkIT_AADDS
Location	(Europe) West Europe

Network

Virtual network	DerkIT_AADDS
Virtual network address	10.10.1.0/24
Subnet	DerkIT_AADDS_Subnet
Subnet Address	10.10.1.0/24
Network security group (new)	AADDS-DerkIT.nl-NSG

Administrator group

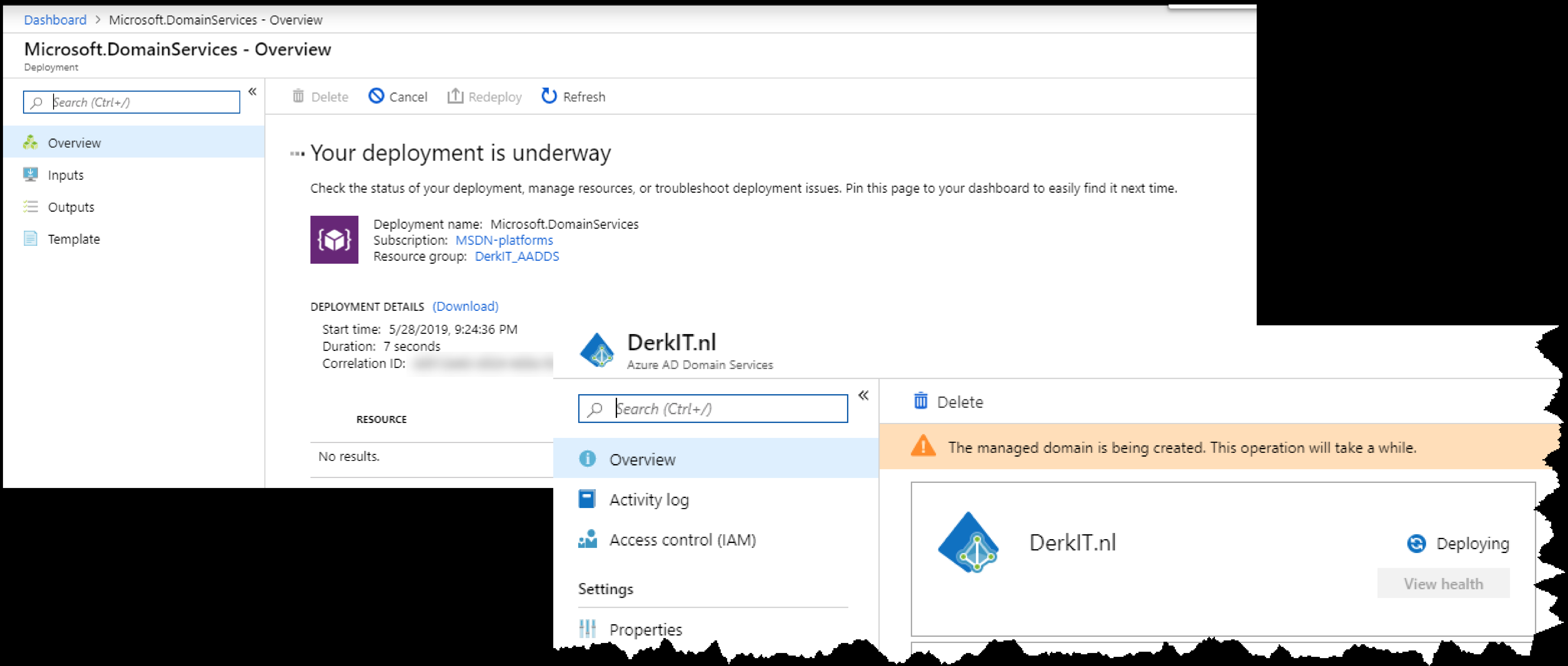
Administrator group	AAD DC Administrators
Membership Type	Assigned

Synchronization

Synchronization scope	All

By enabling Azure AD Domain Services for this directory, you consent to **storing credential hashes required for NTLM and Kerberos authentication in Azure AD**.

By enabling Azure AD Domain Services for this directory, you consent to storing credential hashes required for NTLM and Kerberos authentication in Azure AD.



Dashboard > Microsoft.DomainServices - Overview

Microsoft.DomainServices - Overview

Deployment

Your deployment is underway

Check the status of your deployment, manage resources, or troubleshoot deployment issues. Pin this page to your dashboard to easily find it next time.

Deployment name: Microsoft.DomainServices
Subscription: MSDN-platforms
Resource group: DerkIT_AADDS

DEPLOYMENT DETAILS (Download)

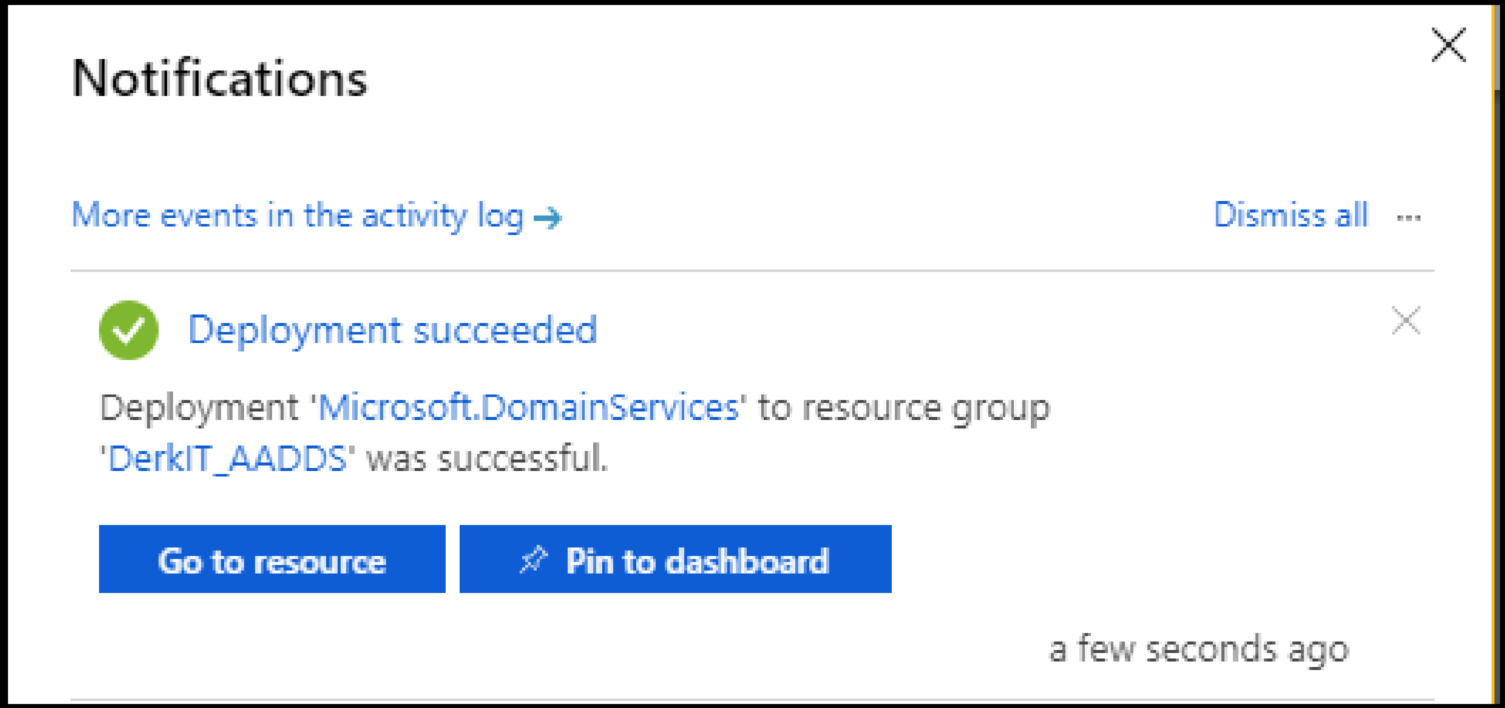
Start time: 5/28/2019, 9:24:36 PM
Duration: 7 seconds
Correlation ID: [redacted]

RESOURCE
No results.

DerkIT.nl
Azure AD Domain Services

The managed domain is being created. This operation will take a while.

DerkIT.nl — Deploying

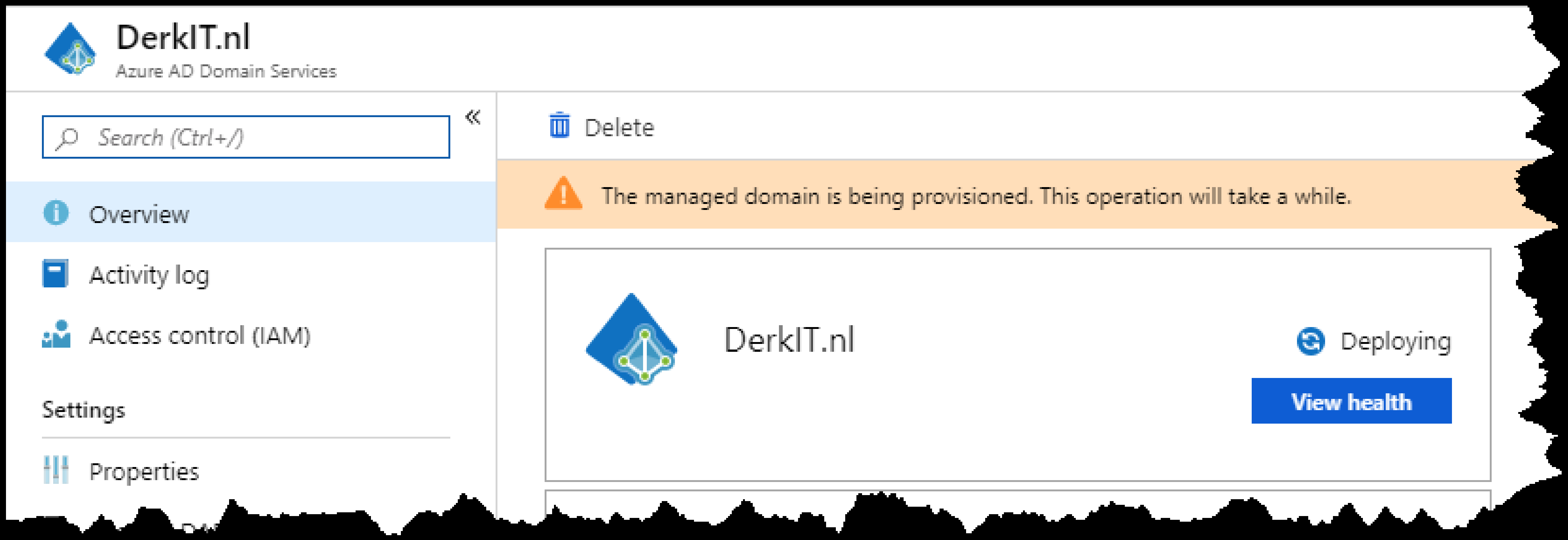


Notifications

Deployment succeeded

Deployment 'Microsoft.DomainServices' to resource group 'DerkIT_AADDS' was successful.

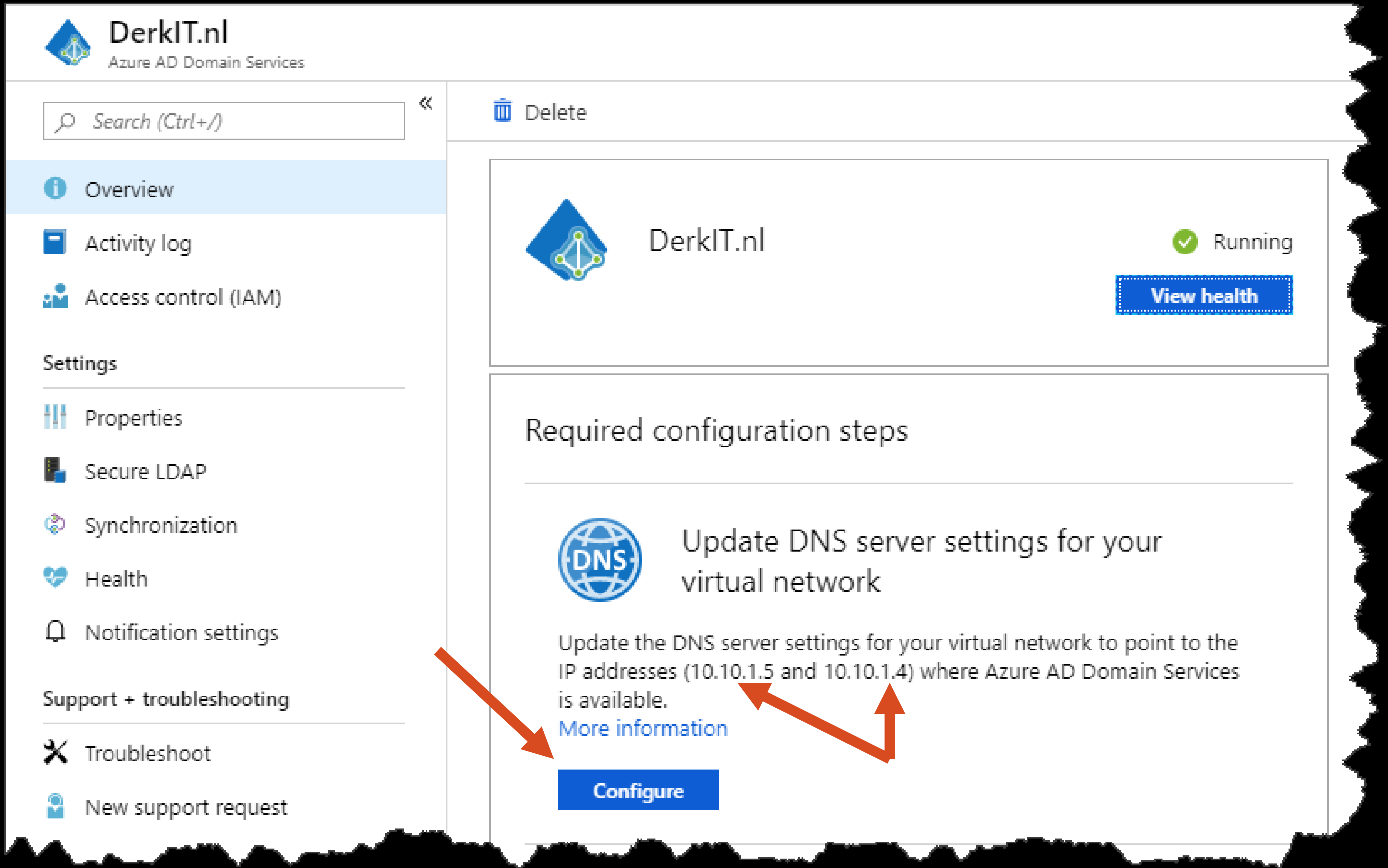
a few seconds ago



DerkIT.nl
Azure AD Domain Services

The managed domain is being provisioned. This operation will take a while.

DerkIT.nl — Deploying



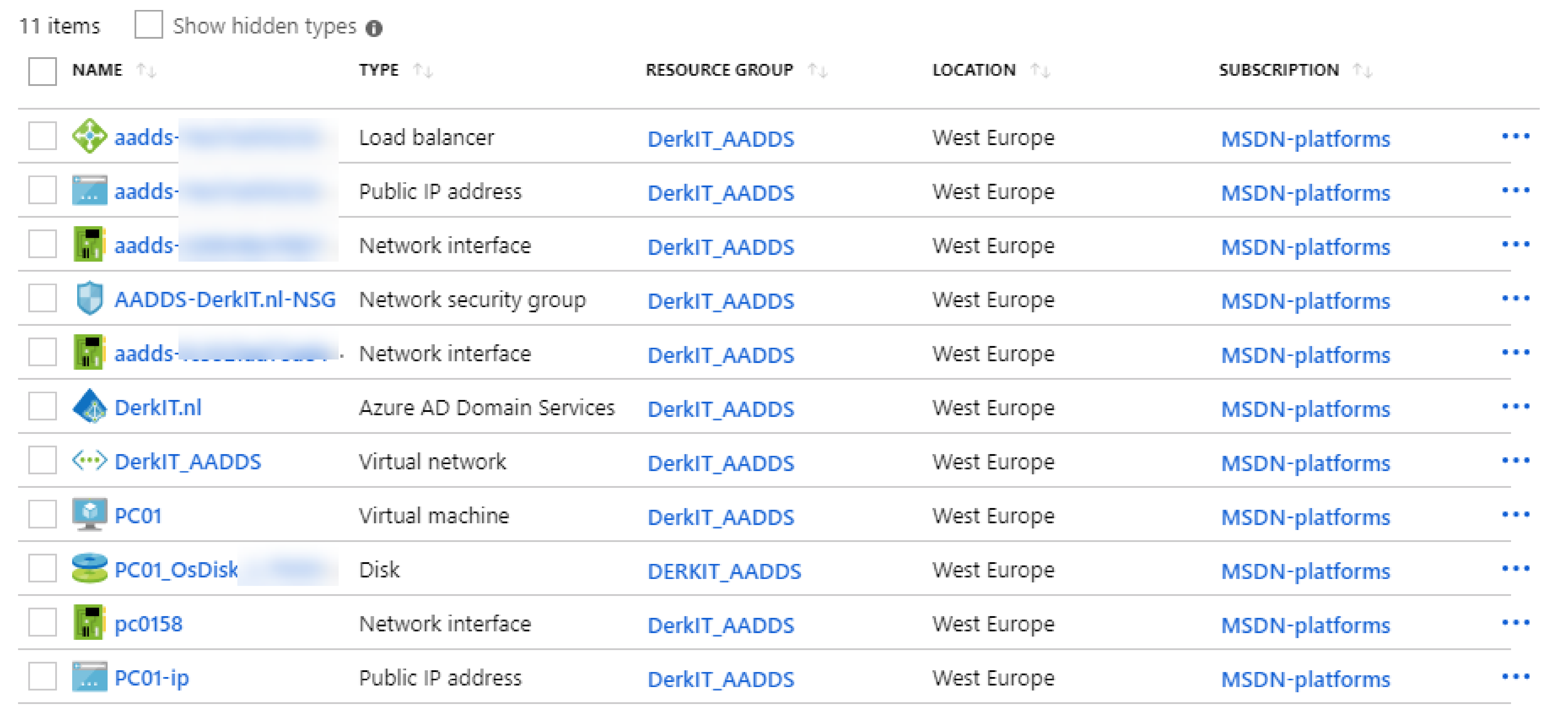
DerkIT.nl
Azure AD Domain Services

DerkIT.nl — Running

Required configuration steps

Update DNS server settings for your virtual network

Update the DNS server settings for your virtual network to point to the IP addresses (10.10.1.5 and 10.10.1.4) where Azure AD Domain Services is available.

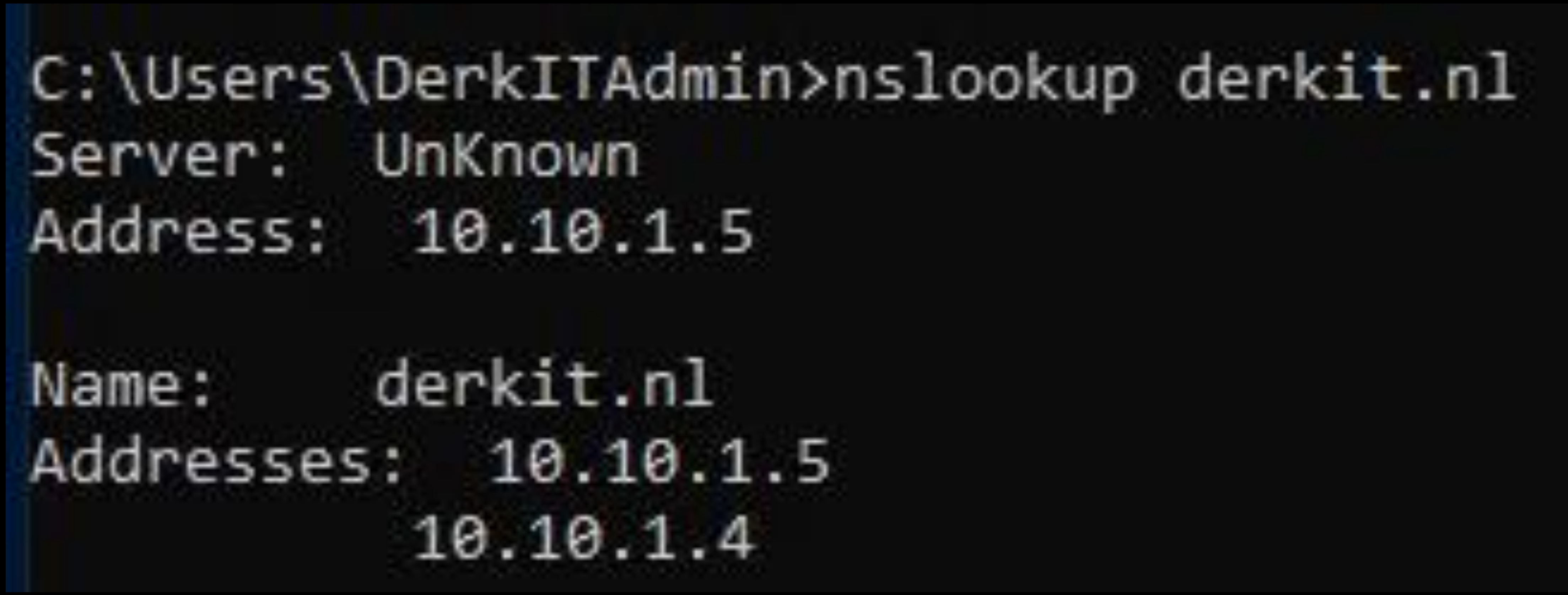


11 items □ Show hidden types

□	NAME	TYPE	RESOURCE GROUP	LOCATION	SUBSCRIPTION	
□	aadds-[redacted]	Load balancer	DerkIT_AADDS	West Europe	MSDN-platforms	•••
□	aadds-[redacted]	Public IP address	DerkIT_AADDS	West Europe	MSDN-platforms	•••
□	aadds-[redacted]	Network interface	DerkIT_AADDS	West Europe	MSDN-platforms	•••
□	AADDS-DerkIT.nl-NSG	Network security group	DerkIT_AADDS	West Europe	MSDN-platforms	•••
□	aadds-[redacted]	Network interface	DerkIT_AADDS	West Europe	MSDN-platforms	•••
□	DerkIT.nl	Azure AD Domain Services	DerkIT_AADDS	West Europe	MSDN-platforms	•••
□	DerkIT_AADDS	Virtual network	DerkIT_AADDS	West Europe	MSDN-platforms	•••
□	PC01	Virtual machine	DerkIT_AADDS	West Europe	MSDN-platforms	•••
□	PC01_OsDisk[redacted]	Disk	DERKIT_AADDS	West Europe	MSDN-platforms	•••
□	pc0158	Network interface	DerkIT_AADDS	West Europe	MSDN-platforms	•••
□	PC01-ip	Public IP address	DerkIT_AADDS	West Europe	MSDN-platforms	•••

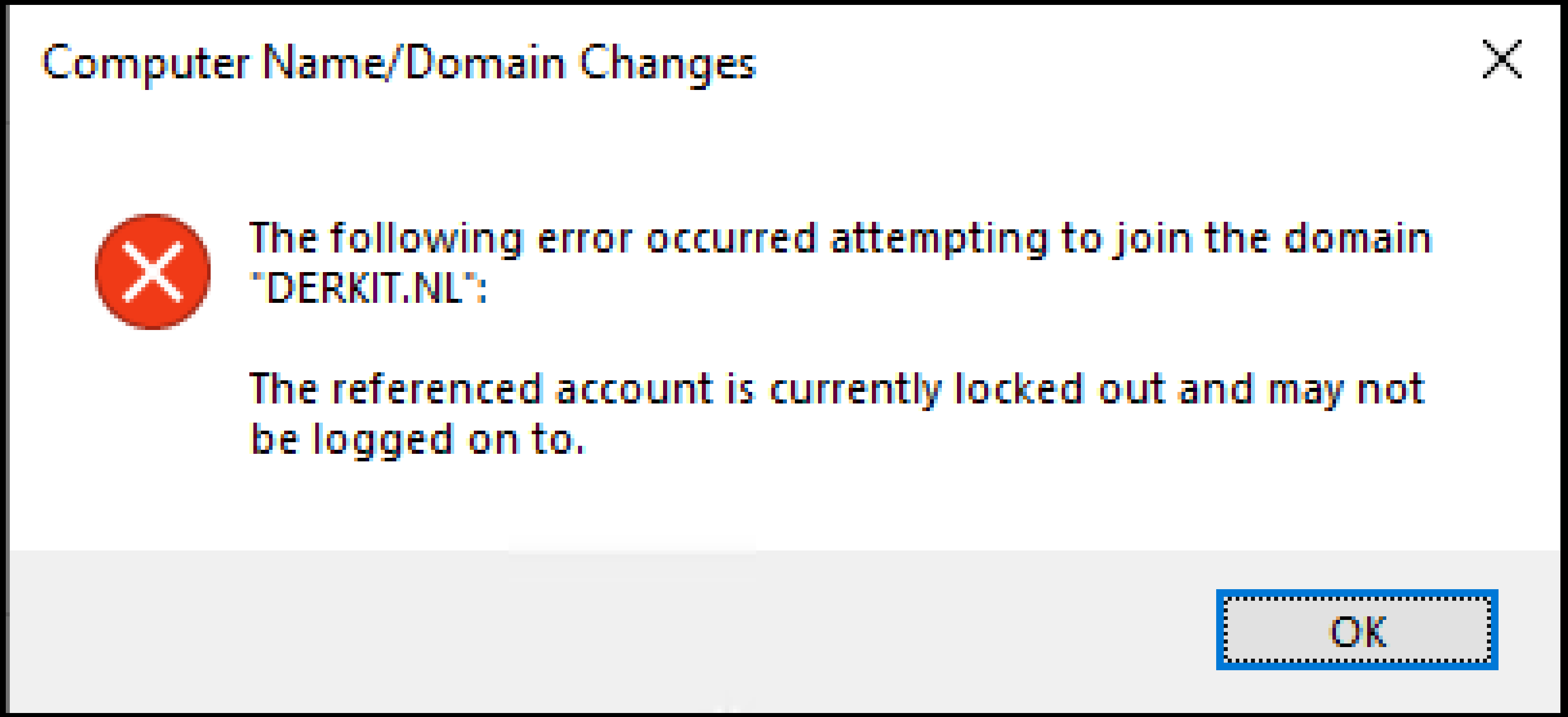
Create & Add VM to Virtual Network

- Logon with local admin
- Configure IP and DNS
- Join to Domain



```
C:\Users\DerkITAdmin>nslookup derkit.nl
Server:  UnKnown
Address:  10.10.1.5

Name:    derkit.nl
Addresses:  10.10.1.5
          10.10.1.4
```



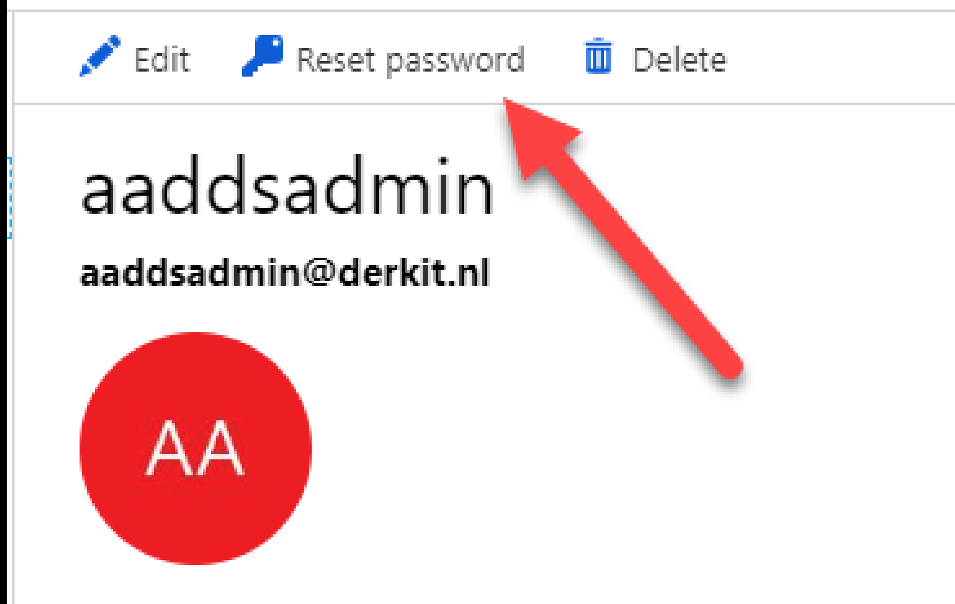
Computer Name/Domain Changes

The following error occurred attempting to join the domain "DERKIT.NL":

The referenced account is currently locked out and may not be logged on to.

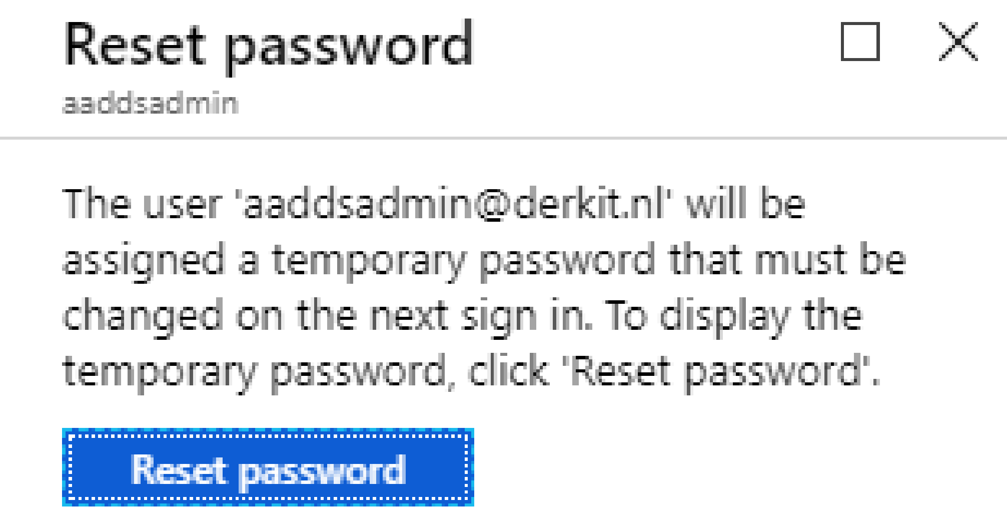
Change your password to generate the Hash!

Reset in AzureAD? Then do this...



aaddsadmin

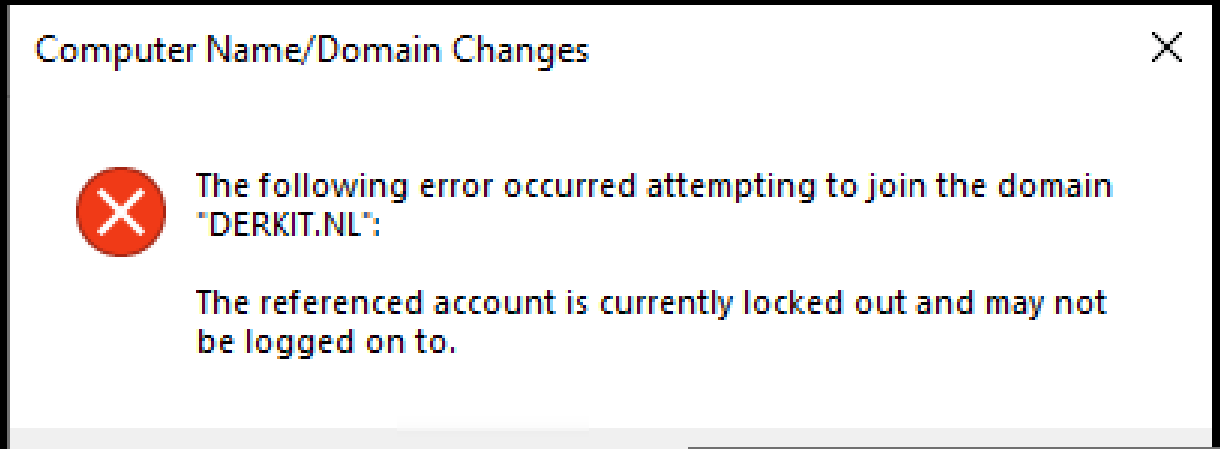
aaddsadmin@derkit.nl



Reset password

aaddsadmin

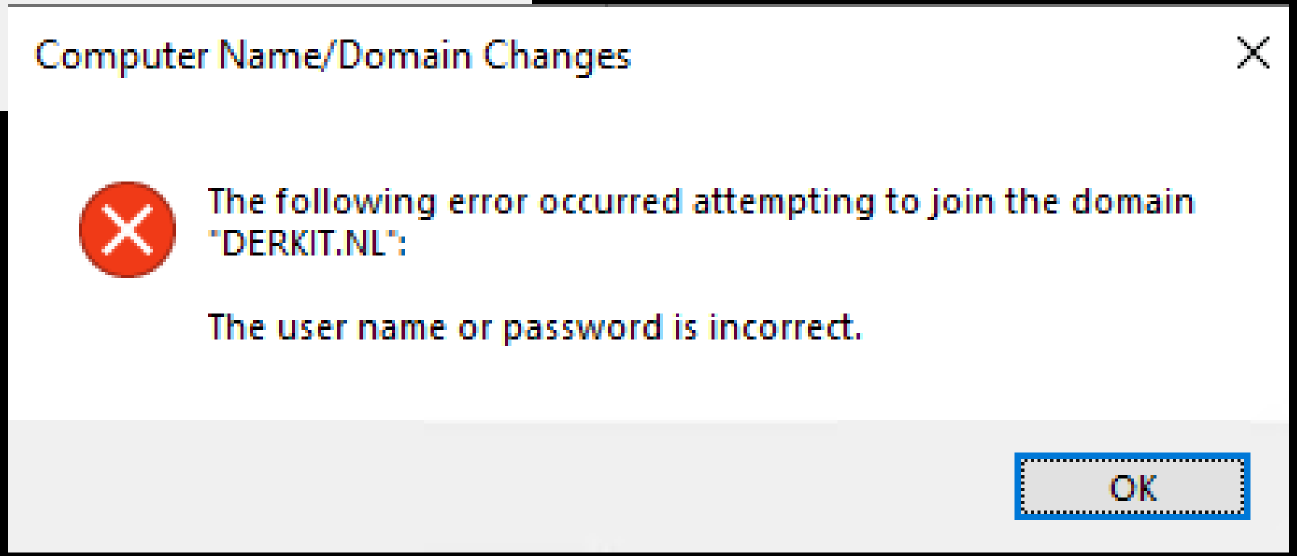
The user 'aaddsadmin@derkit.nl' will be assigned a temporary password that must be changed on the next sign in. To display the temporary password, click 'Reset password'.



Computer Name/Domain Changes

The following error occurred attempting to join the domain "DERKIT.NL":

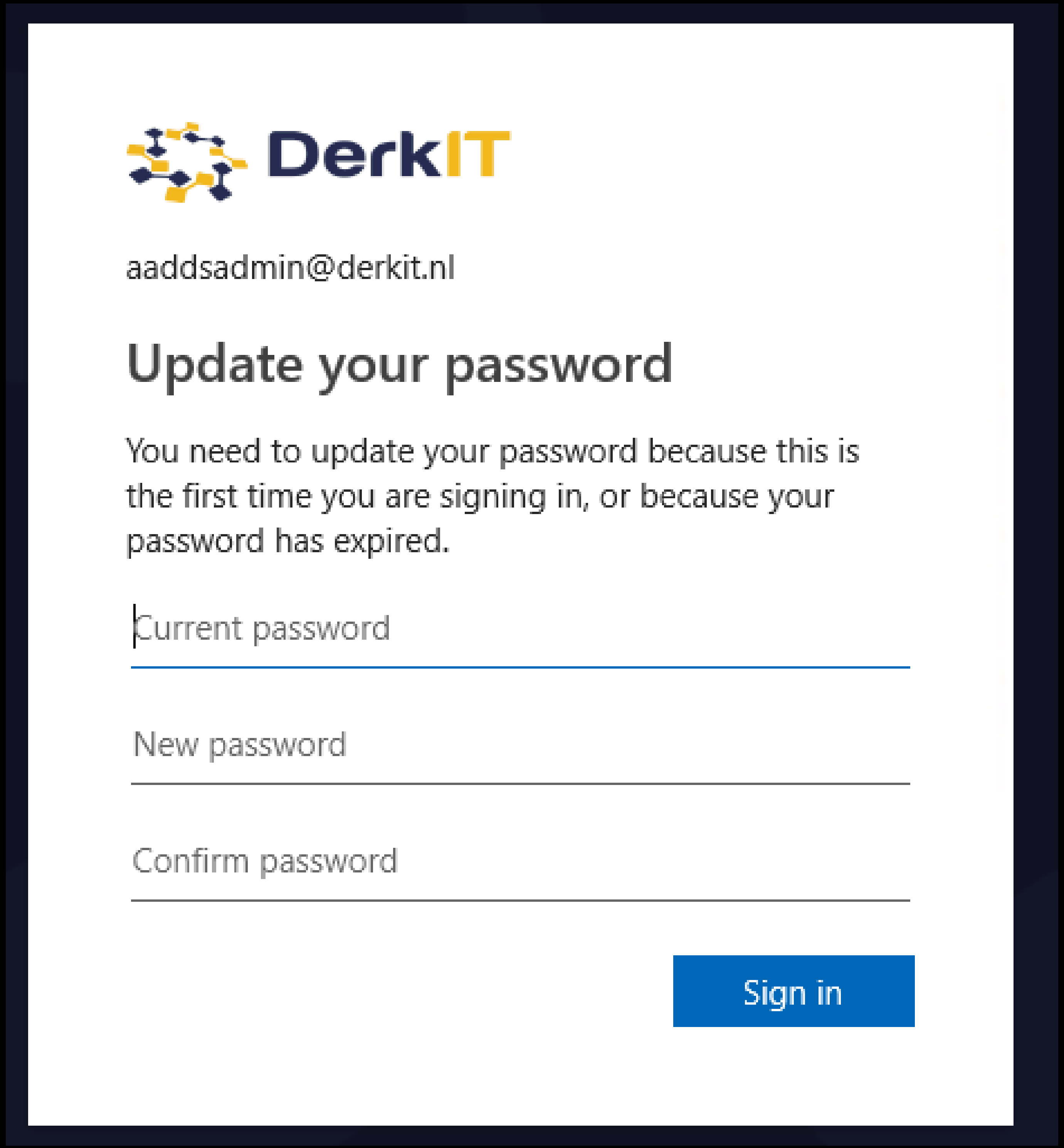
The referenced account is currently locked out and may not be logged on to.



Computer Name/Domain Changes

The following error occurred attempting to join the domain "DERKIT.NL":

The user name or password is incorrect.



aaddsadmin@derkit.nl

Update your password

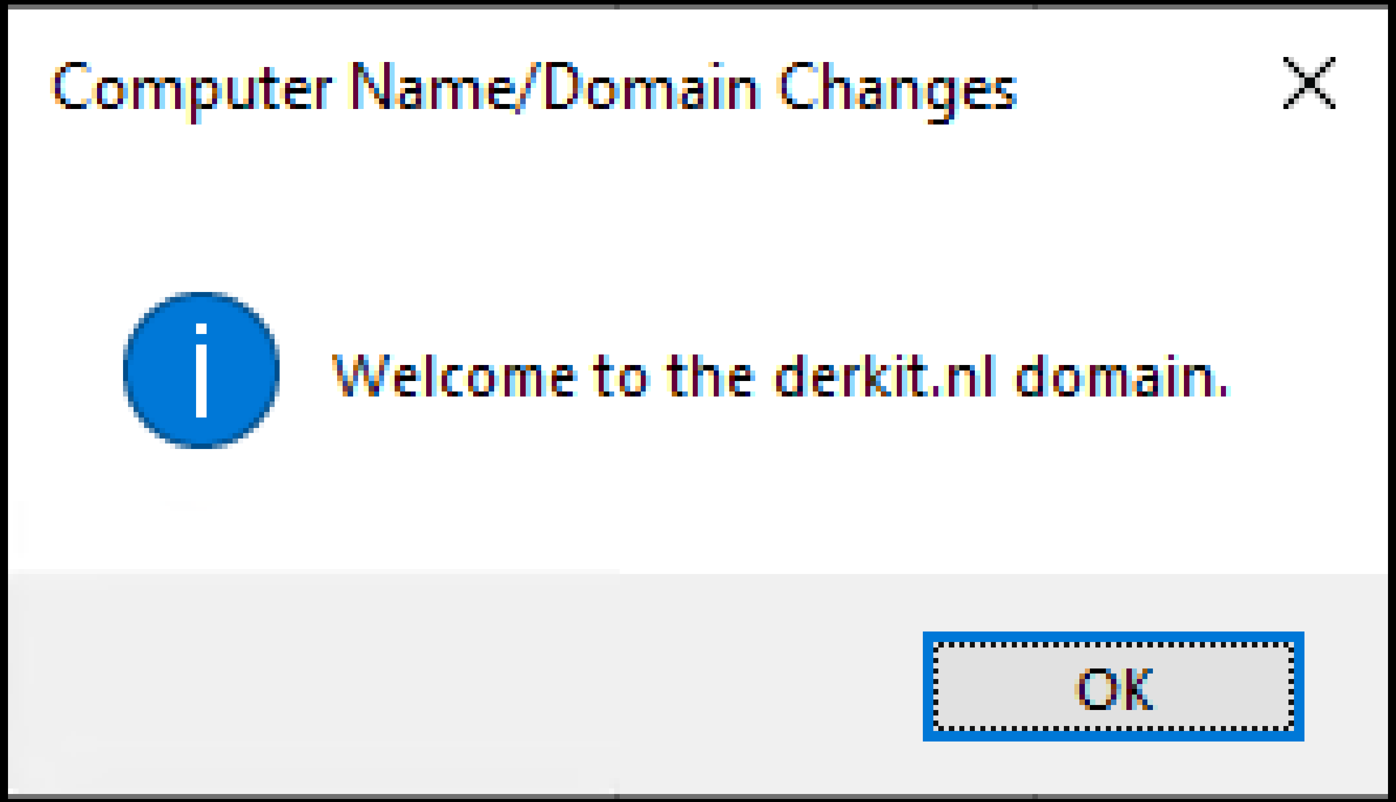
You need to update your password because this is the first time you are signing in, or because your password has expired.

Current password

New password

Confirm password

Be Patient…
Sync in Progress…

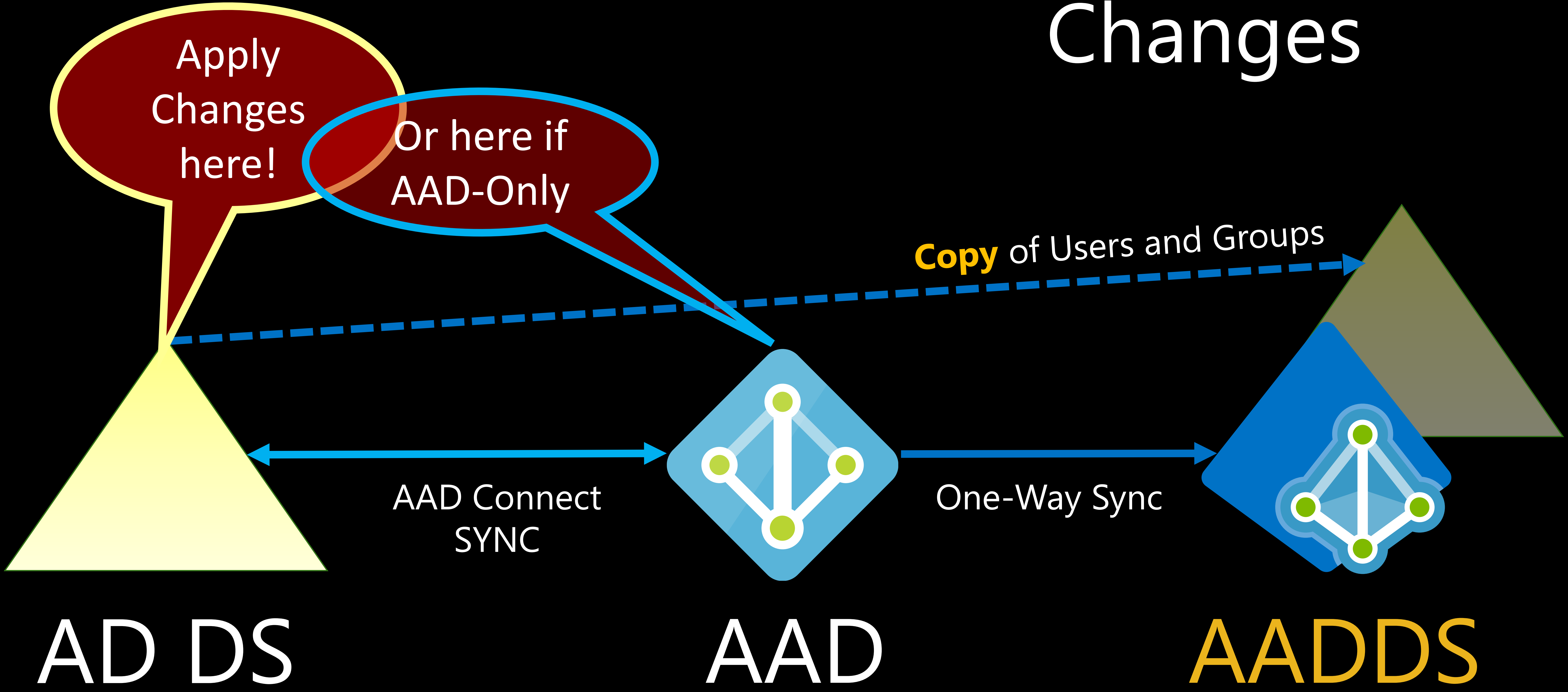


Computer Name/Domain Changes

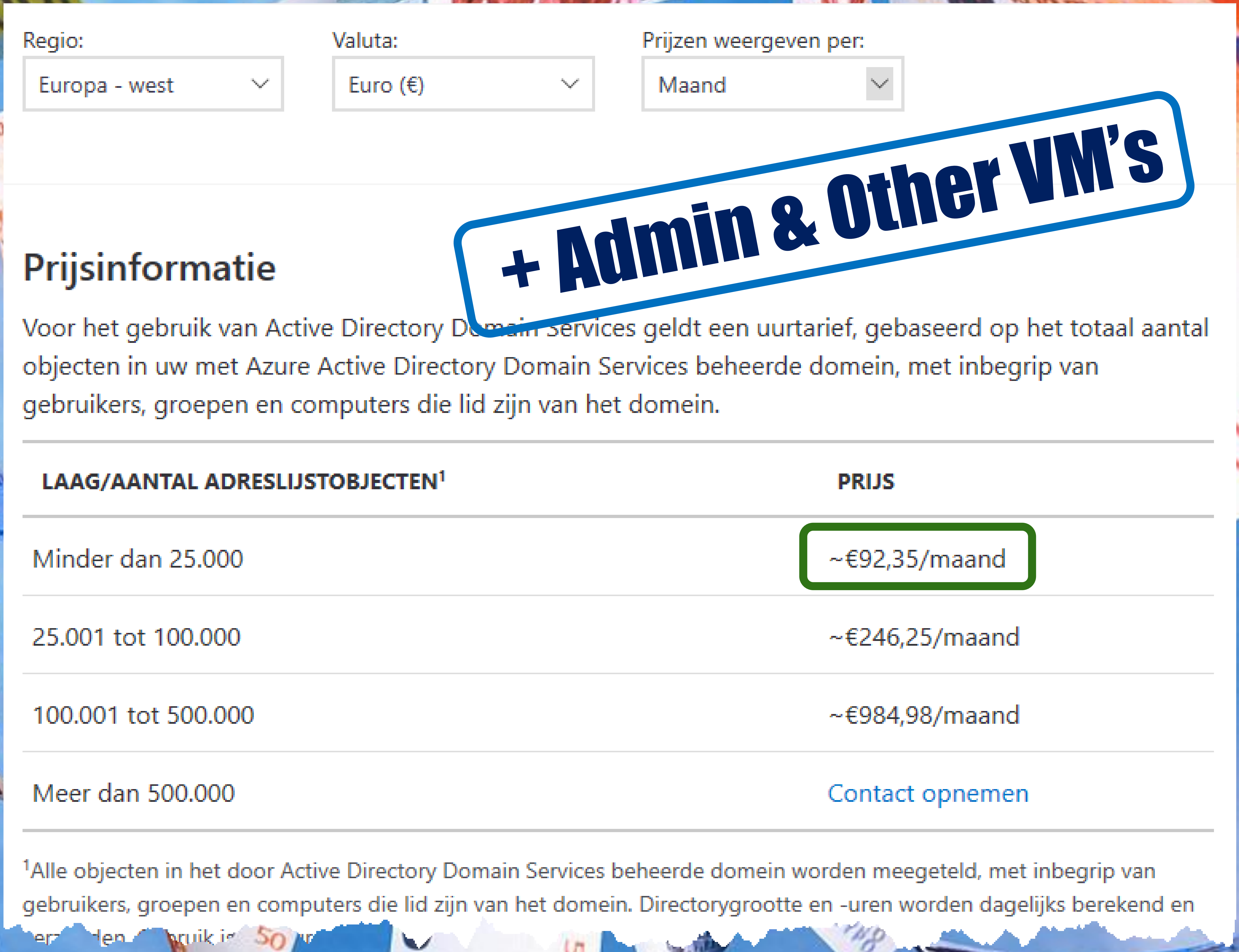
Welcome to the derkit.nl domain.

Administration?

Changes



- New accounts & Groups
- Group Membership
- Passwords!



Regio: Europa - west

Valuta: Euro (€)

Prijzen weergeven per: Maand

+ Admin & Other VM's

Prijsinformatie

Voor het gebruik van Active Directory Domain Services geldt een uurtarief, gebaseerd op het totaal aantal objecten in uw met Azure Active Directory Domain Services beheerde domein, met inbegrip van gebruikers, groepen en computers die lid zijn van het domein.

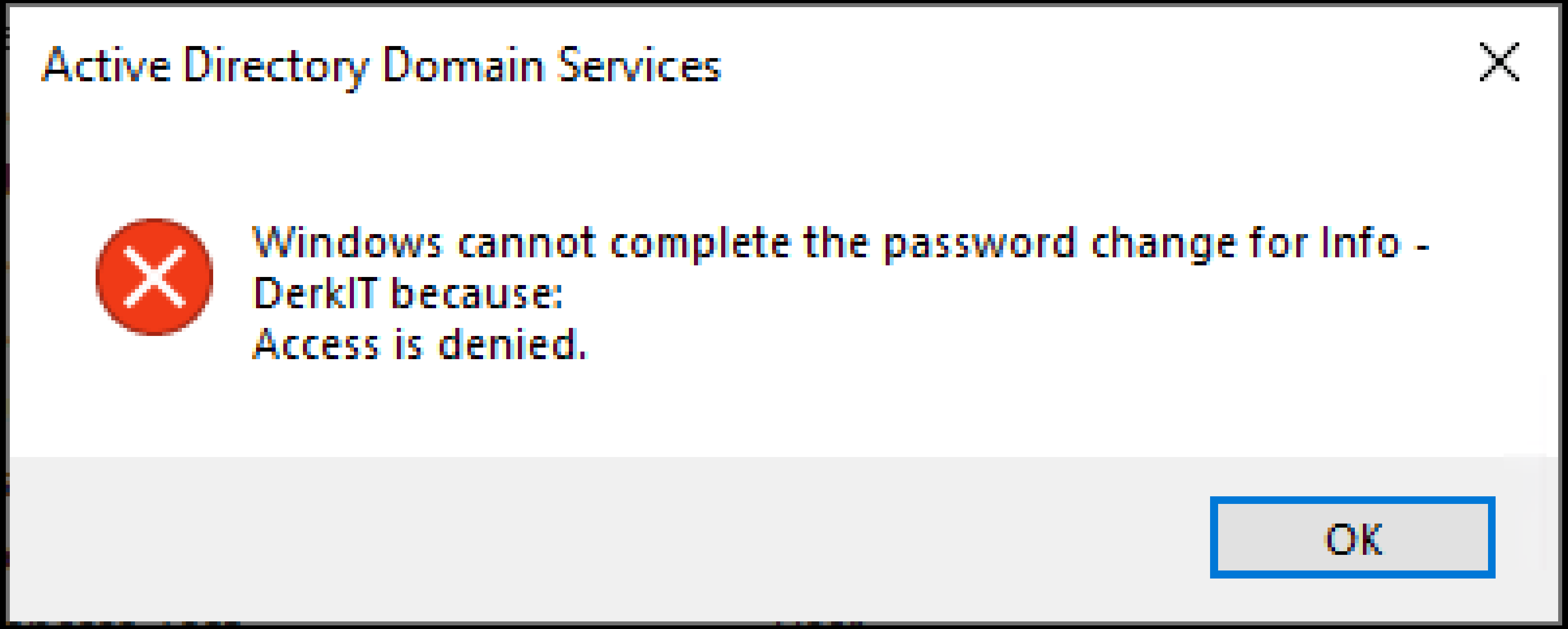
LAAG/AANTAL ADRESLIJSTOBJECTEN[1]	PRIJS
Minder dan 25.000	~€92,35/maand
25.001 tot 100.000	~€246,25/maand
100.001 tot 500.000	~€984,98/maand
Meer dan 500.000	Contact opnemen

[1] Alle objecten in het door Active Directory Domain Services beheerde domein worden meegeteld, met inbegrip van gebruikers, groepen en computers die lid zijn van het domein. Directorygrootte en -uren worden dagelijks berekend en

Beperkingen, Issues, Ontwikkelingen

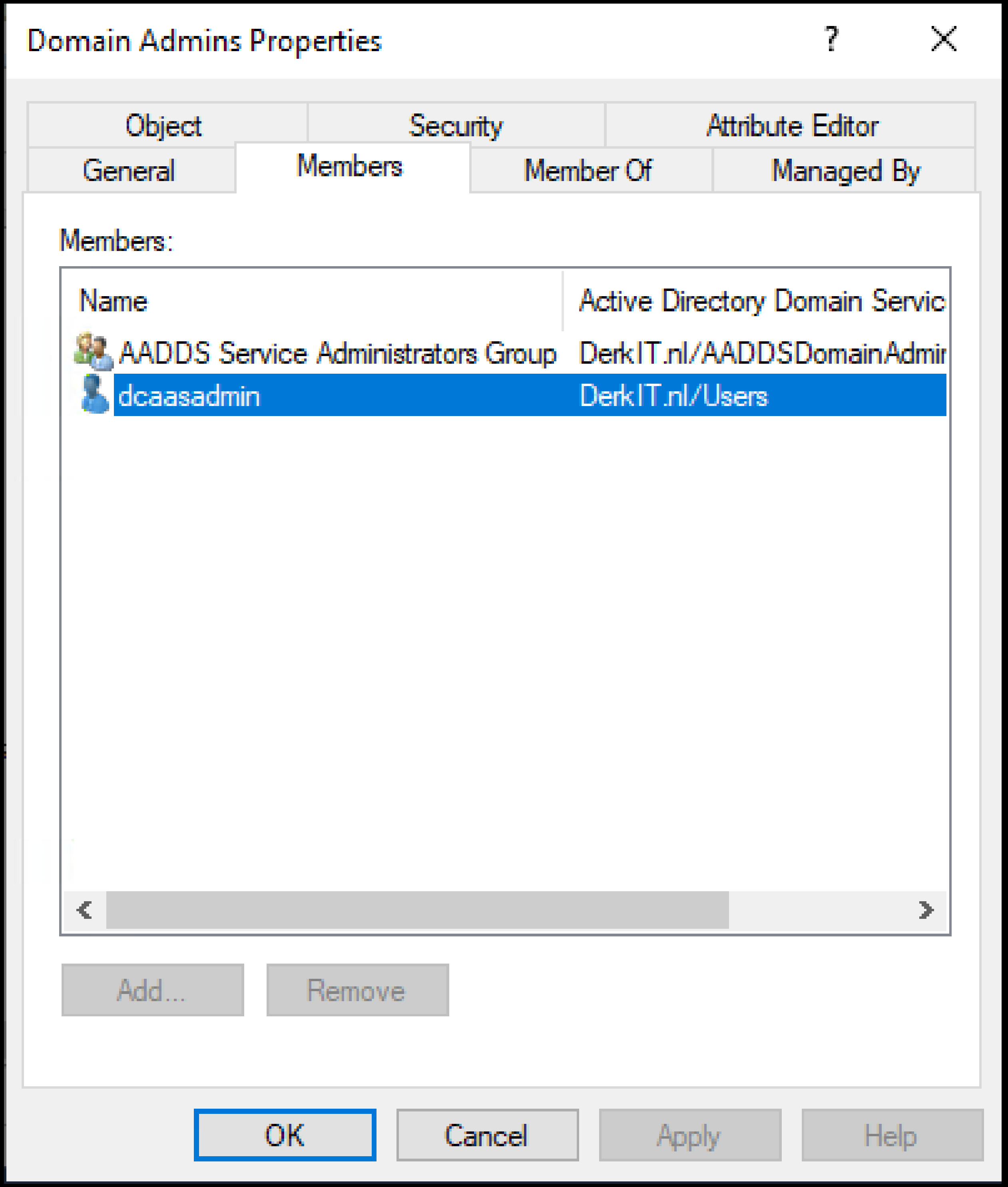
You are **not** a full Domain Admin

- Member of AADDC Admins
- No Enterprise or schema admin
  - No Schema Modifications!
  - No Trusts
  - No Forest or Tree structure, just single domain
  - No Sites and Services



Active Directory Domain Services

Windows cannot complete the password change for Info - DerkIT because:
Access is denied.



Domain Admins Properties

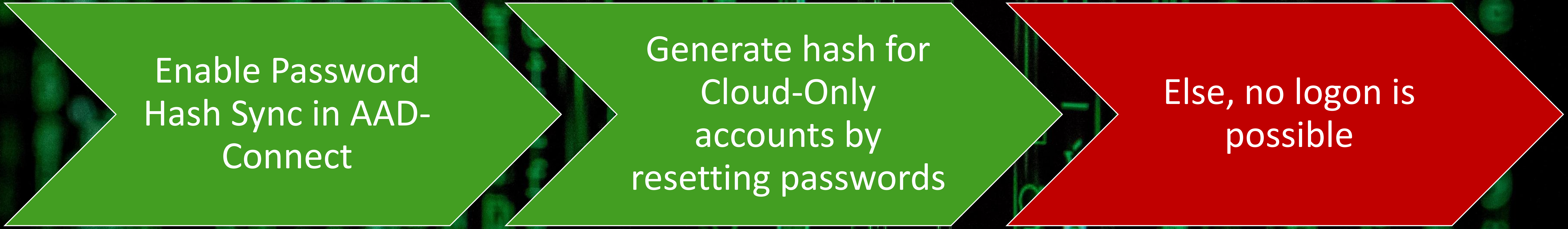
Members:

Name	Active Directory Domain Servic
AADDS Service Administrators Group	DerkIT.nl/AADDSDomainAdmir
dcaasadmin	DerkIT.nl/Users

30m Non-Adjustable One-Way sync interval

- From Azure AD to AADDS, Only Users & Groups
- Interval also applies to locks and password changes!
- **Manage your users & groups in on prem or Azure AD!!!!**
- NOT adjustable (yet), can you believe it!

Password Hashes are Required



Enable Password Hash Sync in AAD-Connect

Generate hash for Cloud-Only accounts by resetting passwords

Else, no logon is possible

You can have only ONE…

Not Multi-Region

- Single Virtual Network
- Region & Network CANNOT be changed after deployment
- Region Gone = AADDS Gone
- That’s on Microsoft’s list ;-)

- Are you multi-region by yourself?

Roadmap?

Waarvoor inzetten?

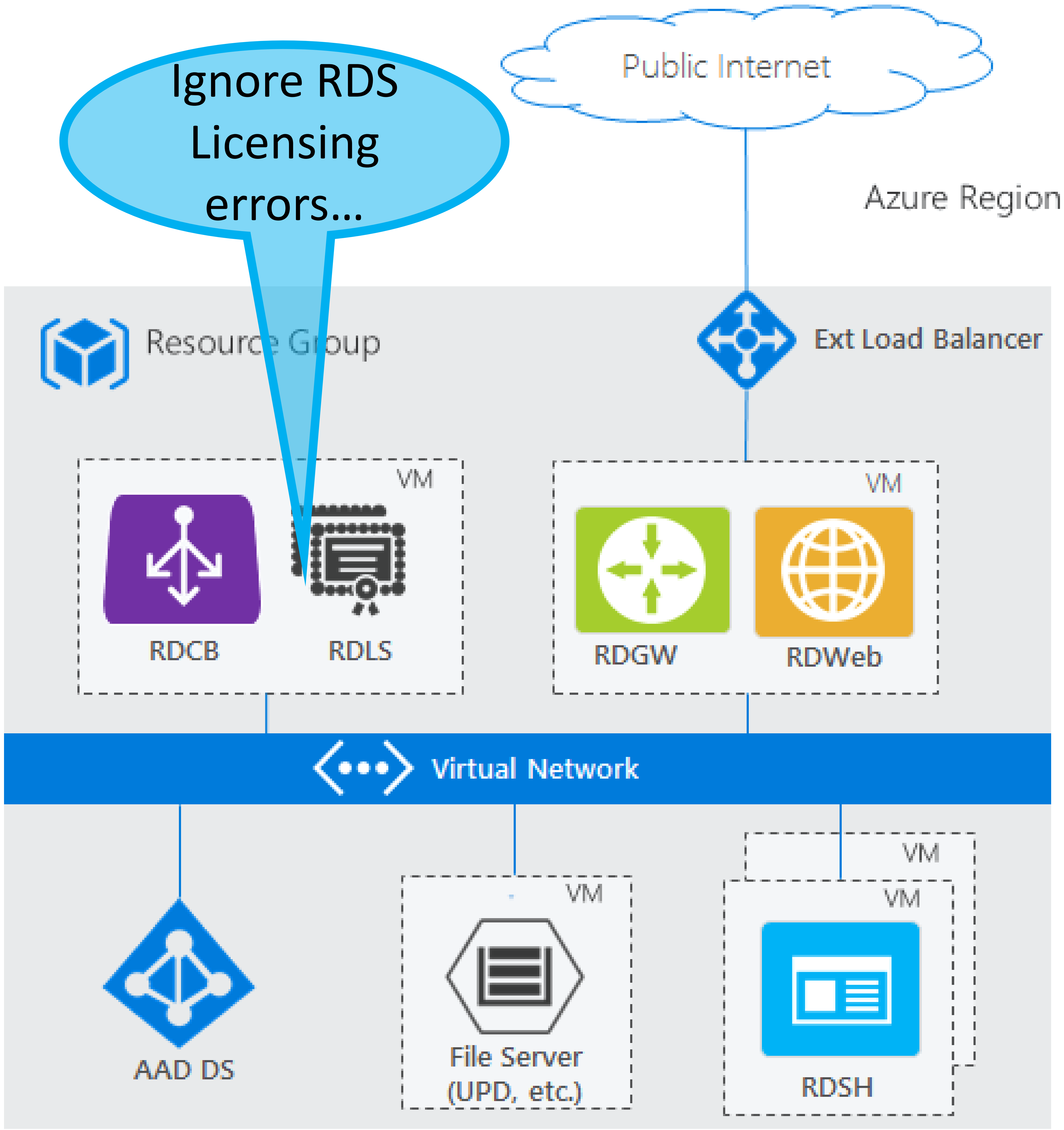
knvi | it-infra

Use Cases

Legacy Apps!!!

- RDS / Citrix is supported!

- Testing (?)
- Azure Files ACL's
  - Not Exposing your Storage Account



Ignore RDS Licensing errors…

AADDS:
Not the most disruptive,
but an **effective** solution.

Launch your legacy to the cloud ;-)

DerkIT

ICT - Verandering - Communicatie

That’s all folks!

DerkIT

ICT - Verandering - Communicatie

Kwaliteit is geen toeval