

Molndrift av tjänster och applikationer

DEVOPS22

Del 6; Azure AD, IAM, RBAC, ADDS, Storage

Kort summering av föregående lektion/ev. lektioner

Föregående lektion:

- Frågor kring förra lektionen?
 - Azure AD / tenant
 - AAD vs AD
 - Flytta subscriptions
 - Users, groups...

Lektionstillfällets mål och metod

Mål med lektionen:

- Azure AD
- Identity and Access Management (IAM) och RBAC
- Azure AD Connect
- Azure AD DS
- Storage Account

Lektionens arbetsmetod/er:

- Beskriv kortfattat hur vi kommer att arbeta under dagens lektion.

Global administrator

- Eftersom du skapat allt i din egen, nya tenant, så har du blivit tilldelad rollen "Global administrator"
- Se till att du har mer än en.
- Microsofts rekommendation är att ha max 5 st
- Andra admins:
- <https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles>

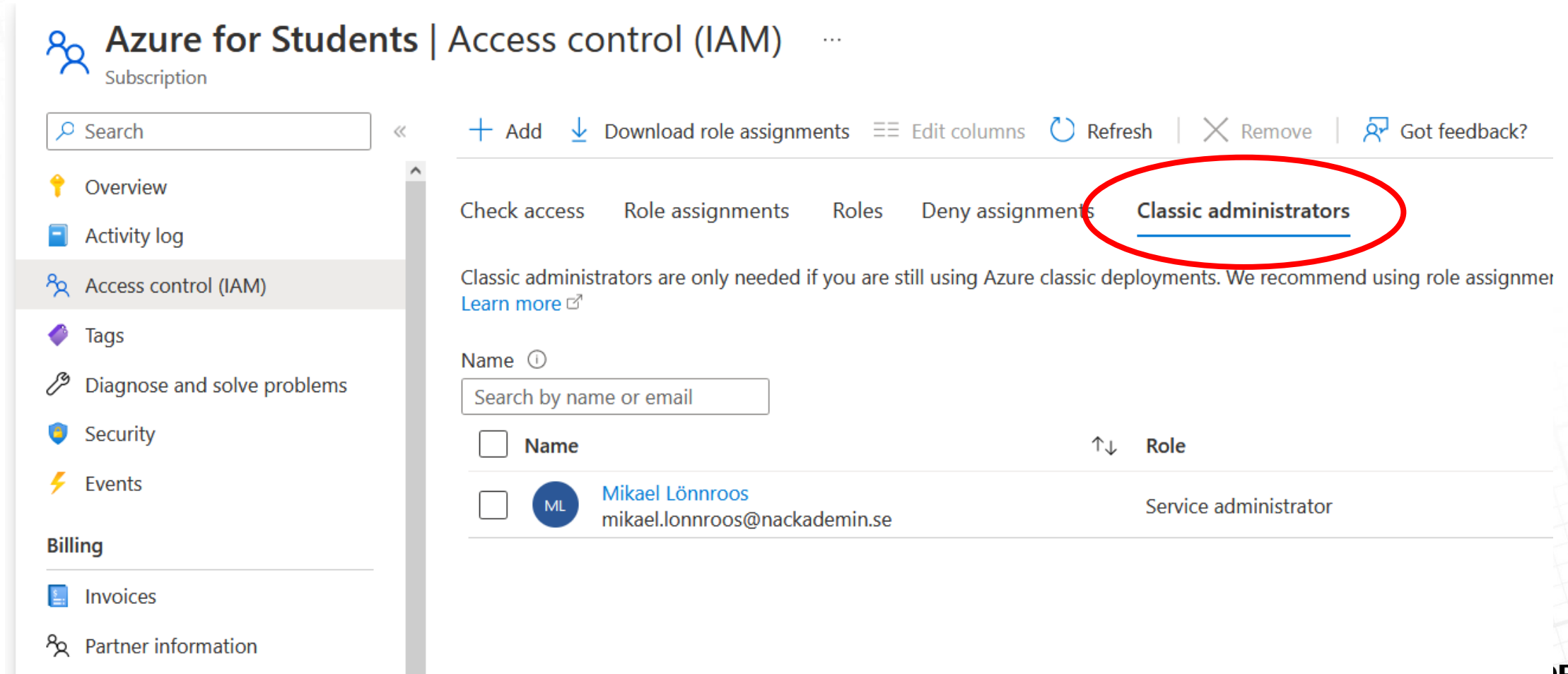
Administration

- Skapa användare i Azure-portalen, prova logga in med den användaren, byt lösen och/eller lås användaren för att simulera tjänstledighet, prova logga in med den användaren igen etc. Se vad som händer och se vilka felmeddelanden som kommer upp.
- Skapa grupper, lägg med användare etc
- Skapa Administrative units, lägg med användare etc

Azure classic subscription administrators

- Microsoft rekommenderar att man administrerar resurser på Azure via Azure role-based access control (Azure RBAC)
- Men om man använder den klassiska modellen, så behöver vi också använda ett par klassiska administrator-roller; Service Administrator och Co-Administrator
- Man behöver bara lägga till en Co-Administrator om användaren behöver hantera Azure klassiska resurser genom att använda Azure Service Management PowerShell moduler.
- Om användaren enbart använder Azure portalen för att hantera klassiska resurser, så behöver man inte addera användaren som en Co-Administrator.

Azure classic subscription administrators



The screenshot shows the 'Azure for Students | Access control (IAM)' page. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM) (selected), Tags, Diagnose and solve problems, Security, Events, Billing, Invoices, and Partner information. The main content area has a top bar with a search box and action buttons: Add, Download role assignments, Edit columns, Refresh, Remove, and Got feedback?. Below this is a sub-navigation bar with links: Check access, Role assignments, Roles, Deny assignments, and **Classic administrators** (circled in red). A message states: 'Classic administrators are only needed if you are still using Azure classic deployments. We recommend using role assignments. [Learn more](#)'. Below the message is a search box labeled 'Name' with the placeholder 'Search by name or email'. A table lists classic administrators with columns for Name and Role. One administrator is listed: Mikael Lönnroos (mikael.lonnroos@nackademin.se) with the role of Service administrator.

Azure for Students | Access control (IAM) ...

Subscription

Search


« + Add ↓ Download role assignments ≡ Edit columns ↺ Refresh | ✕ Remove | 👤 Got feedback?

Check access Role assignments Roles Deny assignments **Classic administrators**

Classic administrators are only needed if you are still using Azure classic deployments. We recommend using role assignments. [Learn more](#)

Name ⓘ

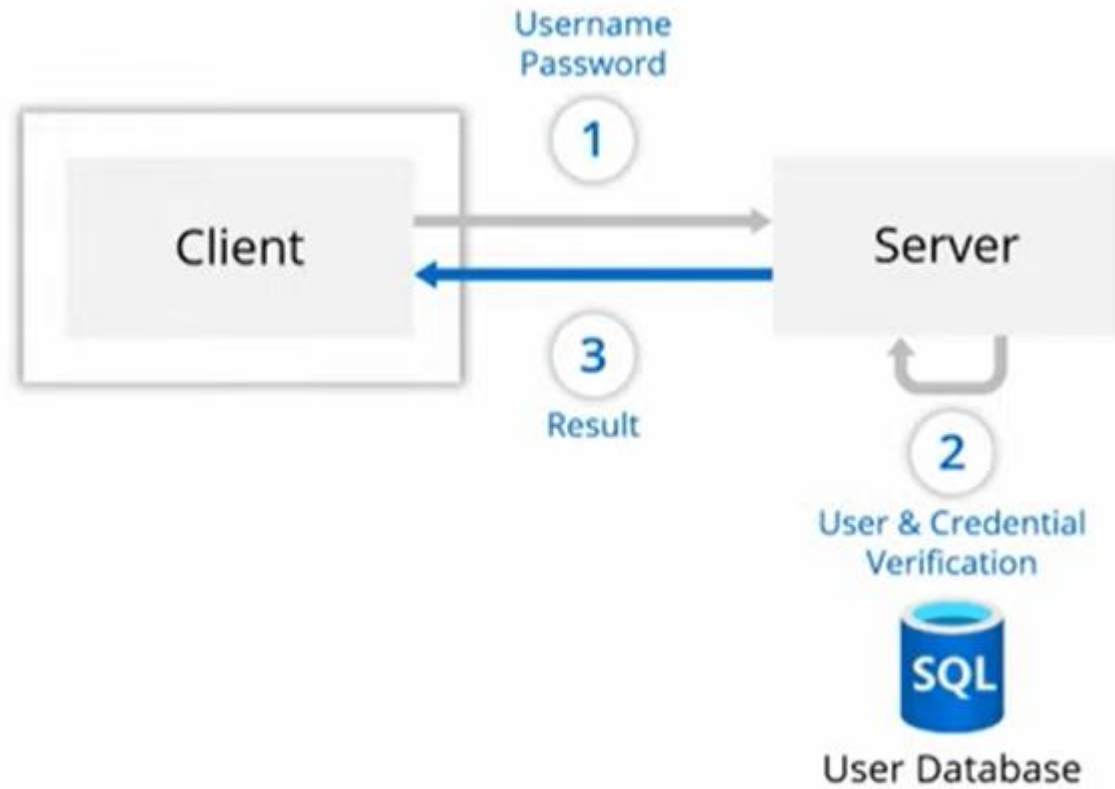
Search by name or email

<input type="checkbox"/> Name	↑↓ Role
<input type="checkbox"/>  Mikael Lönnroos mikael.lonnroos@nackademin.se	Service administrator

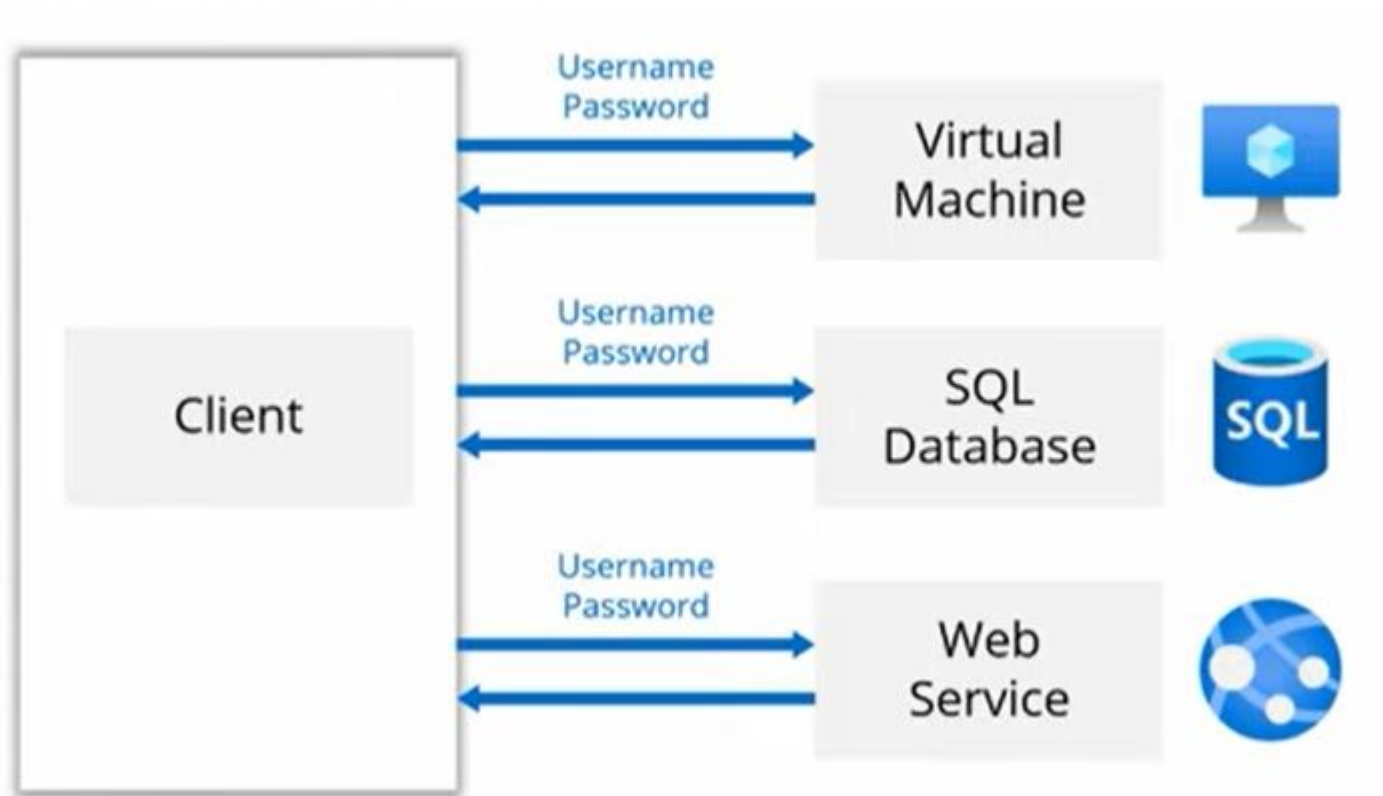
Identity

- Something that can be *authenticated*
- It can be a user with a *username* and *password*
- Or it can be an *application* or *other servers* with *secrets keys* or *certificates*

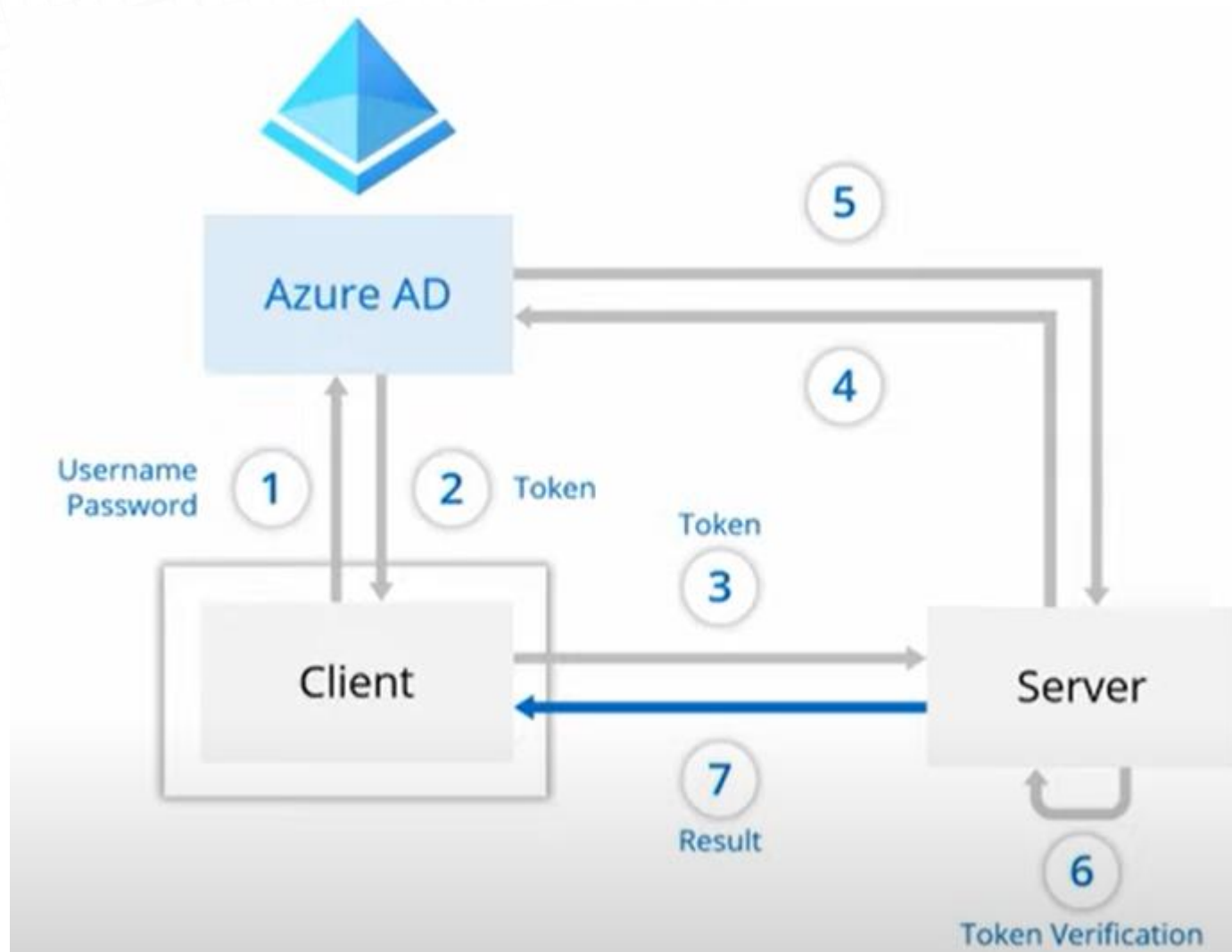
Classic approach



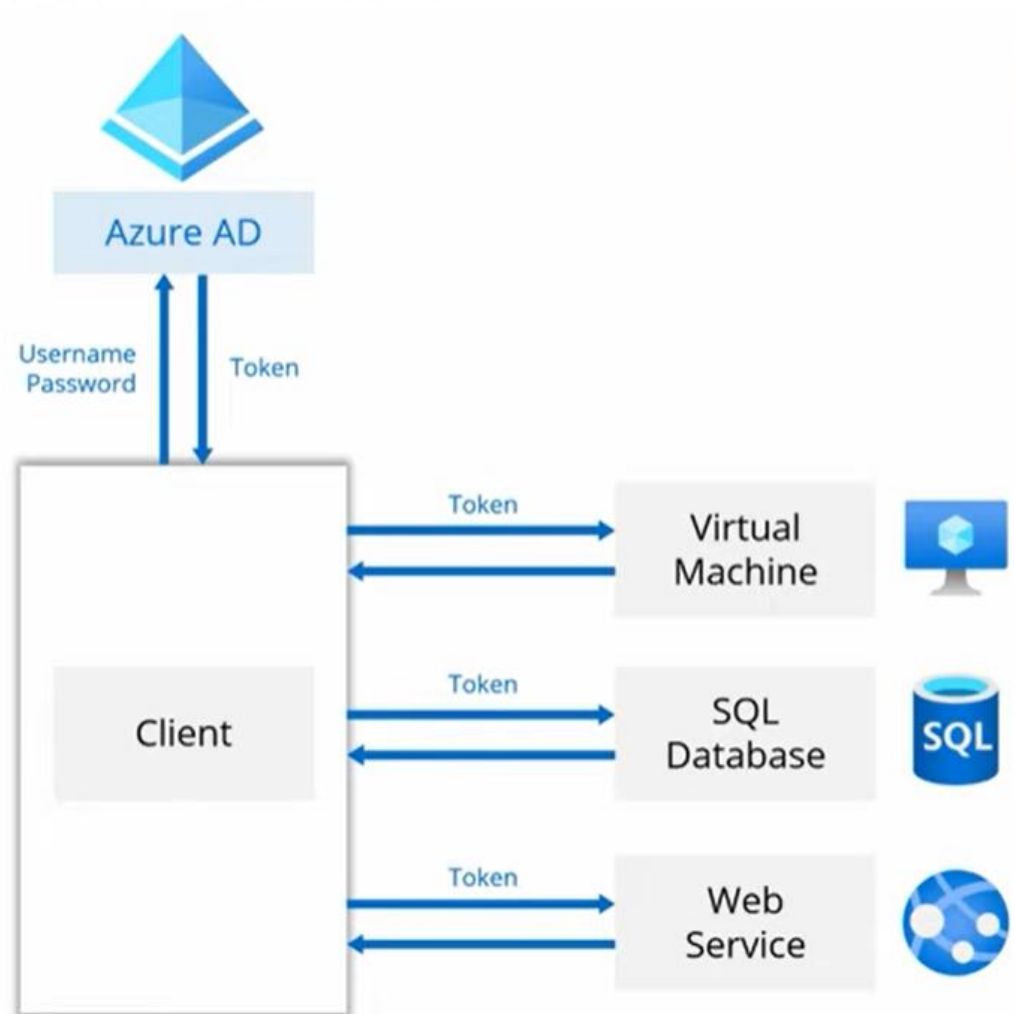
Classic approach



Identity provider

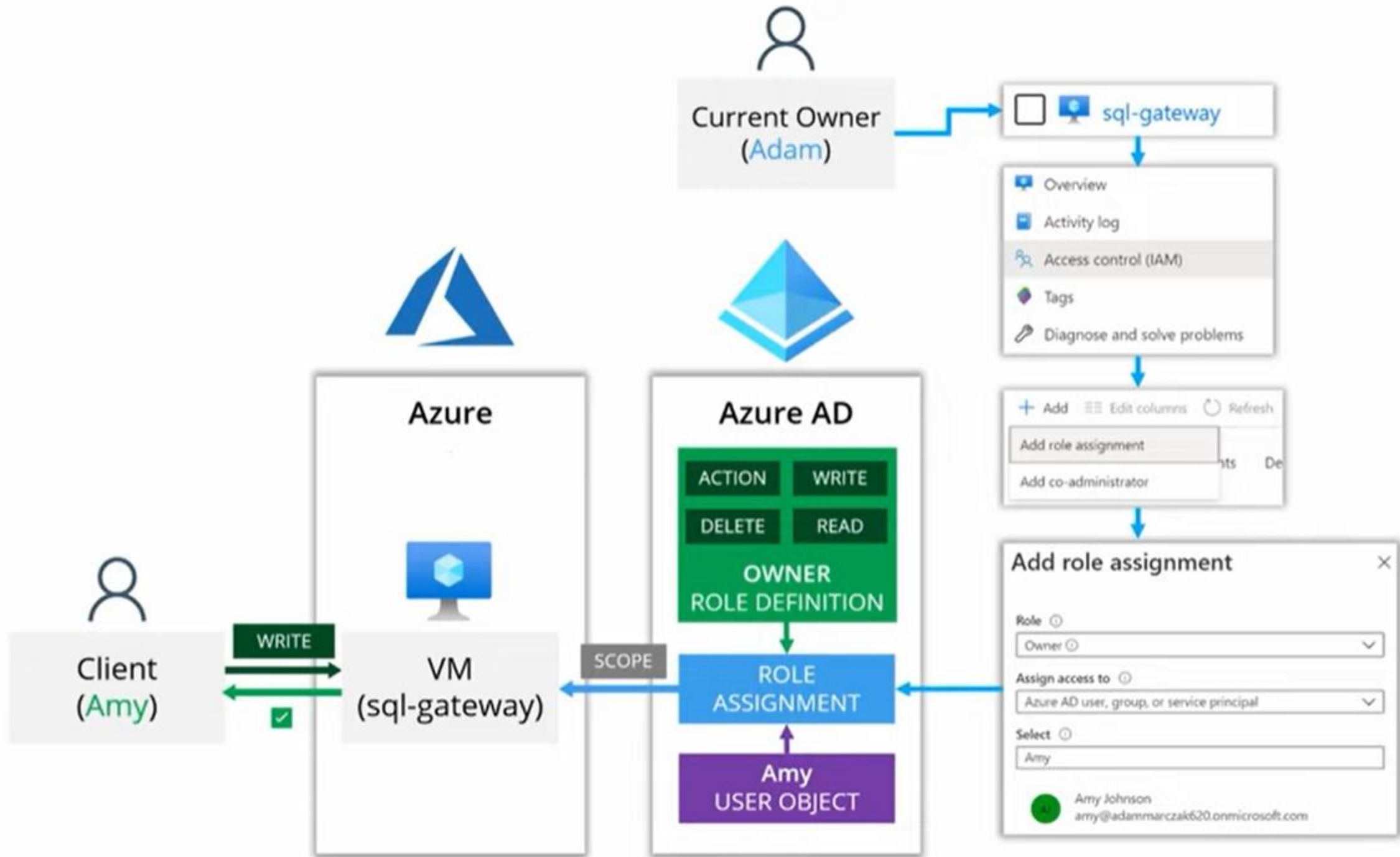


Identity provider



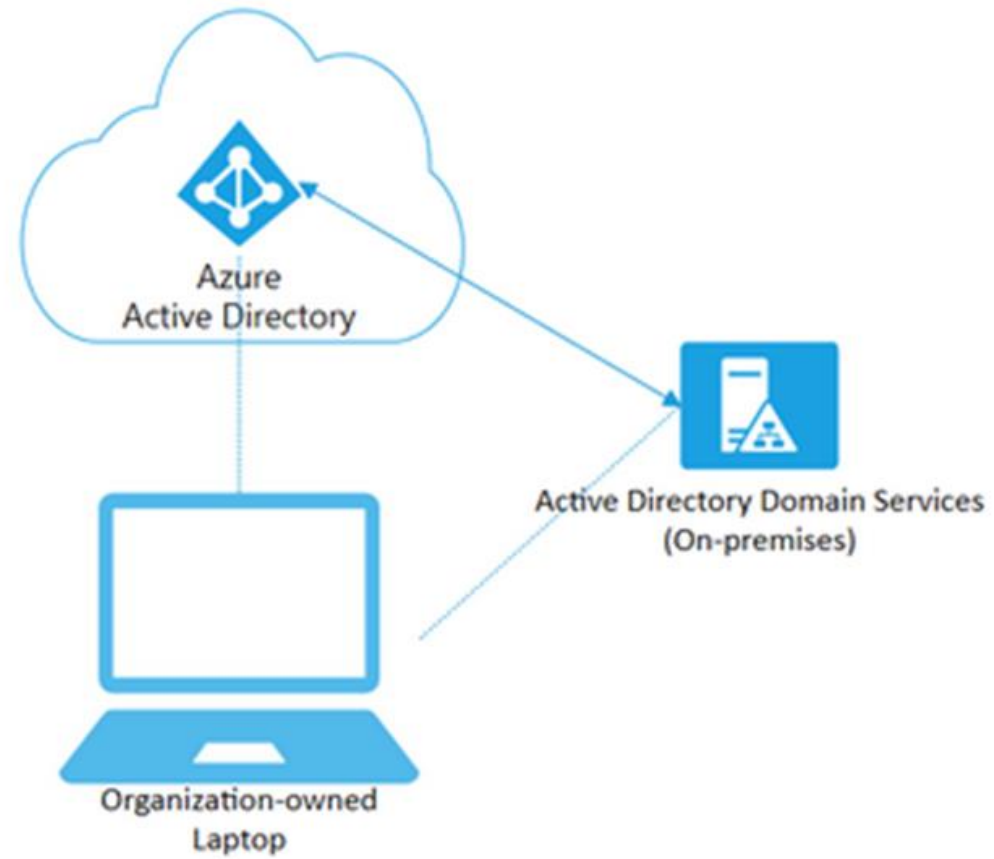
Access Management

- Process of *controlling, verifying, tracking* and *managing access* to *authorized users* and *applications*.
- Azure role-based access control (Azure RBAC)
- Azure AD P1 eller högre krävs om man vill skapa egna roller. Använder man Free, så har man enbart tillgång till de fördefinierade rollerna.



Valfri övning

- Skapa minst en användare + en role, sätt in användaren i rollen.
- Gå in i valfri del av er Azure-installation och ge ovanstående role rättigheter (exempelvis läsrättighet på resource group)
- Logga in som användaren du skapat, och verifiera att denne har de rättigheter som du angav ovan.
- Kontrollera om rättigheter ärvs, alltså om man ger läsrättigheter på exempelvis en resource-group, ärvs då rättigheterna nedåt så användaren även har läsrätt på underliggande object?



Azure AD Connect

- Koppla ihop lokalt AD med Azure AD
- Hämta programmet till din on-premise server, pgm finns i Azure AD > Azure AD Connect
- <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity>
- <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-roadmap#install-azure-ad-connect>
- <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/cloud-sync/what-is-cloud-sync>

Azure AD Connect

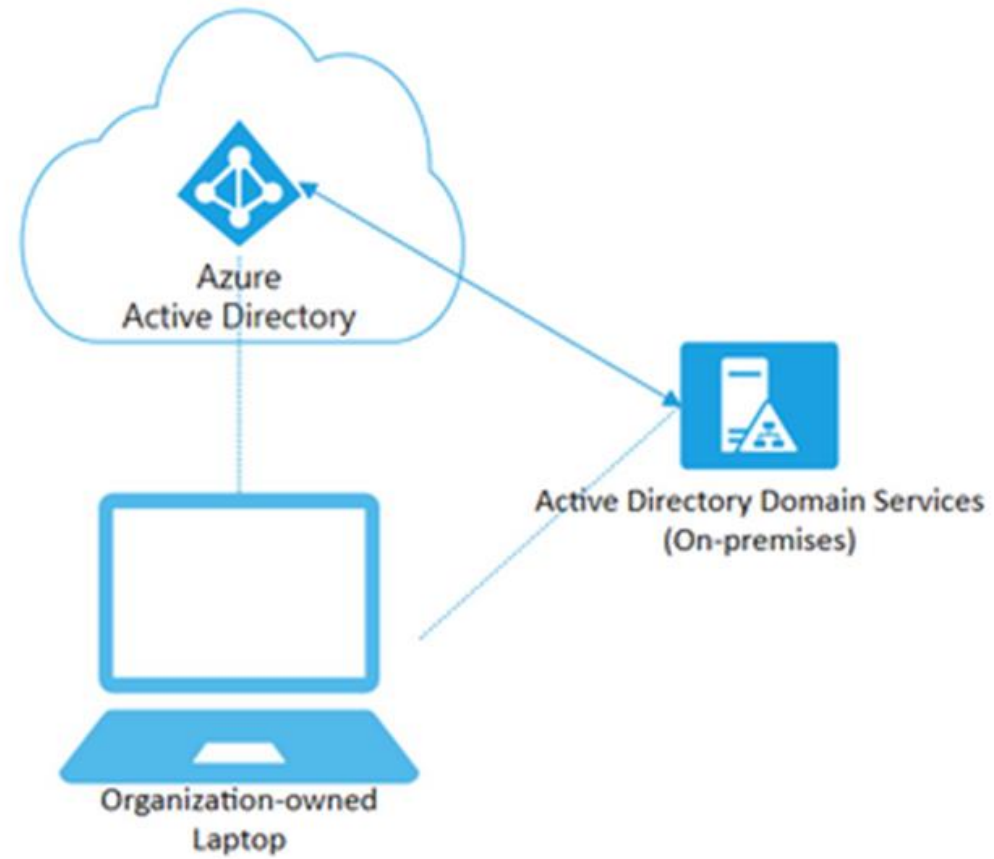
- Skapa ett OU på AD-servern i skolan, lägg in minst 5 st användare där
- Ladda ner och installera på en av servrarna i skolan
 - Password Hash Synchronization som minst
 - Enable single sign-on
 - Ange en global administrator på Azure AD
 - Ange en enterprise admin på lokalt AD
 - Synka bara det OU som du skapade nyss, annars får man med alla default-användare och default-grupper också (och vad ska du med dem till i Azure?)
- Kolla gärna i Azure AD Sync Services för att se vad som händer

Azure AD Connect

- Det går att tvinga sync med PowerShell
 - Import-Module ADSync
 - Start-ADSyncSyncCycle -PolicyType Initial
 - Start-ADSyncSyncCycle -PolicyType Delta

Nr 1 – AD Connect

- Installera AD Connect och synka mot din egen tenant.
- Ta en skärmbild på det OU du skapat på din lokala server, innehållande användarna i det OU't. Jag vill se OU, namn på kontot och type.
- Ta en skärmbild på dina Users från ditt Azure AD. Utöver de vanliga kolumnerna (Display Name, UPN, User type, On-premises sync enabled, Identities, Company name, Creation type) så vill jag även se kolumnen *On-premises last sync date time* i skärmbilden.
- Ladda upp dessa två bilder till Studentportalen
- Skriv en kort förklaring av varje steg du tog för att slutföra uppgiften, inklusive eventuella utmaningar du stötte på och hur du överkom dem



Azure AD Domain Services

- Man borde ha minst två global administrators
- MS rekommenderar max 5 st
- Lägg till en admin

Azure AD Domain Services

- Azure Active Directory Domain Services lets you join Azure virtual machines to a domain without the need to deploy or manage domain controllers. Users sign in to these virtual machines using their corporate Active Directory credentials and can access resources seamlessly. Azure Active Directory Domain Services features domain join, LDAP, NTLM and Kerberos authentication are widely used in enterprises. Migrate legacy directory-aware applications running on premises to Azure without having to worry about identity requirements.

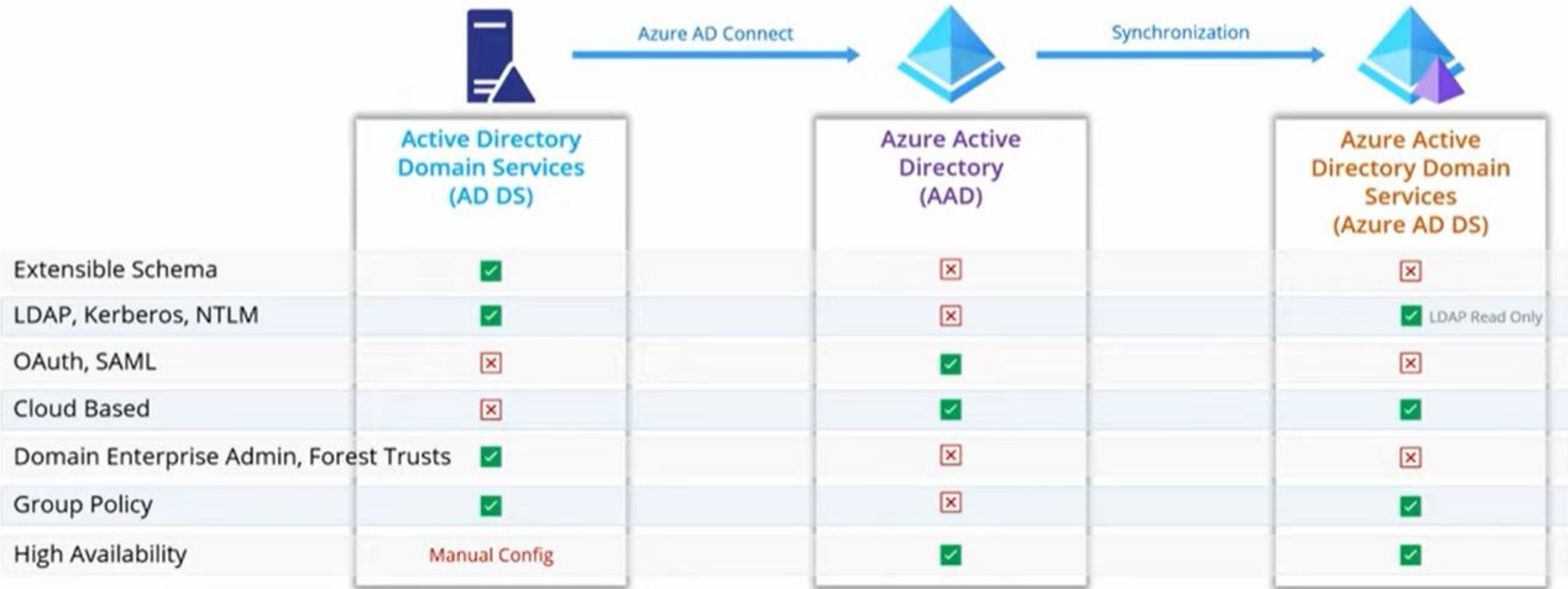
Azure AD Domain Services

- SKU
 - Standard
 - Enterprise
 - Premium
 - <https://azure.microsoft.com/en-us/pricing/details/active-directory-ds/>
- Network
 - Rekommenderbart är att lägga domainkontrollanter i ett separat subnet.
- Lägg till admin

Azure AD Domain Services

- Det tar ca en timme att skapa dessa två AD+DNS-servrar, alla beroenden i form av nic, adresser etc.
- När allt är klart, så behöver vi byta från Azure-DNS till de två nya servrarnas DNS.
- Att göra på VM's som ska gå med i domainen:
 - Starta om så de får rätt DNSer av DHCP
 - Gå med i AADDS-domainen via kontrollpanelen > system (eller liknande)
- *Gör labb i slutet på dagen eller under lunchen, den tar för mycket tid annars*

AD DS, Azure AD, Azure AD DS



Azure Storage Accounts

- Azure file shares are deployed into *storage accounts*, which are top-level objects that represent a shared pool of storage. This pool of storage can be used to deploy multiple file shares, as well as other storage resources such as blob containers, queues, or tables. All storage resources that are deployed into a storage account share the limits that apply to that storage account.
- <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-planning>

Azure Storage

- Durable and highly available.
 - Redundancy ensures that your data is safe in the event of transient hardware failures. You can also opt to replicate data across datacenters or geographical regions for additional protection from local catastrophe or natural disaster. Data replicated in this way remains highly available in the event of an unexpected outage.
- Secure.
 - All data written to an Azure storage account is encrypted by the service. Azure Storage provides you with fine-grained control over who has access to your data.

Azure Storage

- Scalable.
 - Azure Storage is designed to be massively scalable to meet the data storage and performance needs of today's applications.
- Managed.
 - Azure handles hardware maintenance, updates, and critical issues for you.
- Accessible.
 - Data in Azure Storage is accessible from anywhere in the world over HTTP or HTTPS. Microsoft provides client libraries for Azure Storage in a variety of languages, including .NET, Java, Node.js, Python, PHP, Ruby, Go, and others, as well as a mature REST API. Azure Storage supports scripting in Azure PowerShell or Azure CLI. And the Azure portal and Azure Storage Explorer offer easy visual solutions for working with your data.

Azure Storage services

- To access an Azure file share, the user of the file share must be authenticated and have authorization to access the share. This is done based on the identity of the user accessing the file share. Azure Files integrates with three main identity providers
- *Nästa sida*

Azure Storage services

- On-premises Active Directory Domain Services (AD DS, or on-premises AD DS)
 - Azure storage accounts can be domain joined to a customer-owned, Active Directory Domain Services, just like a Windows Server file server or NAS device. You can deploy a domain controller on-premises, in an Azure VM, or even as a VM in another cloud provider; Azure Files is agnostic to where your domain controller is hosted. Once a storage account is domain-joined, the end user can mount a file share with the user account they signed into their PC with. AD-based authentication uses the Kerberos authentication protocol.

Azure Storage services

- Azure Active Directory Domain Services (Azure AD DS)
 - Azure AD DS provides a Microsoft-managed domain controller that can be used for Azure resources. Domain joining your storage account to Azure AD DS provides similar benefits to domain joining it to a customer-owned Active Directory. This deployment option is most useful for application lift-and-shift scenarios that require AD-based permissions. Since Azure AD DS provides AD-based authentication, this option also uses the Kerberos authentication protocol.

Azure Storage services

- Azure storage account key
 - Azure file shares may also be mounted with an Azure storage account key. To mount a file share this way, the storage account name is used as the username and the storage account key is used as a password. Using the storage account key to mount the Azure file share is effectively an administrator operation, since the mounted file share will have full permissions to all of the files and folders on the share, even if they have ACLs. When using the storage account key to mount over SMB, the NTLMv2 authentication protocol is used.

Azure Storage services

- Each service is accessed through a storage account.
- Azure Blobs
 - A massively scalable object store for text and binary data. Also includes support for big data analytics through Data Lake Storage Gen2.Managed.
- Azure Files
 - Managed file shares for cloud or on-premises deployments.

Azure Storage services

- Azure Queues
 - A messaging store for reliable messaging between application components.
- Azure Tables
 - A NoSQL store for schemaless storage of structured data.
- Azure Disks
 - Block-level storage volumes for Azure VMs.
- <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview#how-it-works>

Azure Storage

- Rita och berätta skillnaderna mellan dessa

Locally-redundant storage (LRS)

Zone-redundant storage (ZRS)

Geo-redundant storage (GRS)

Read-access geo-redundant storage (RA-GRS)

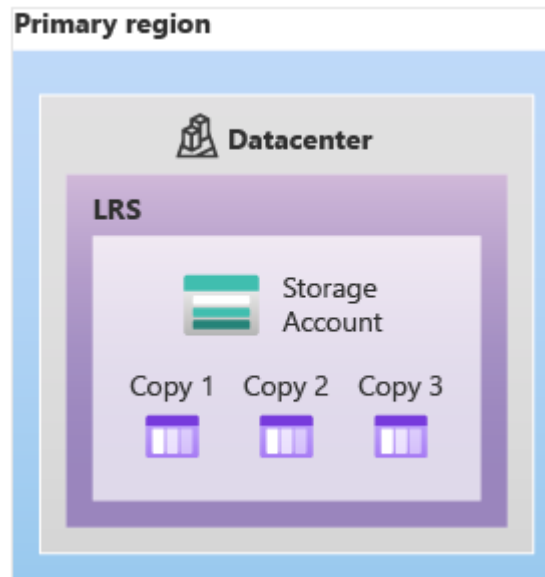
Geo-zone-redundant storage (GZRS)

Read-access geo-zone-redundant storage (RA-GZRS)

Read-access geo-redundant storage (RA-GRS) ^

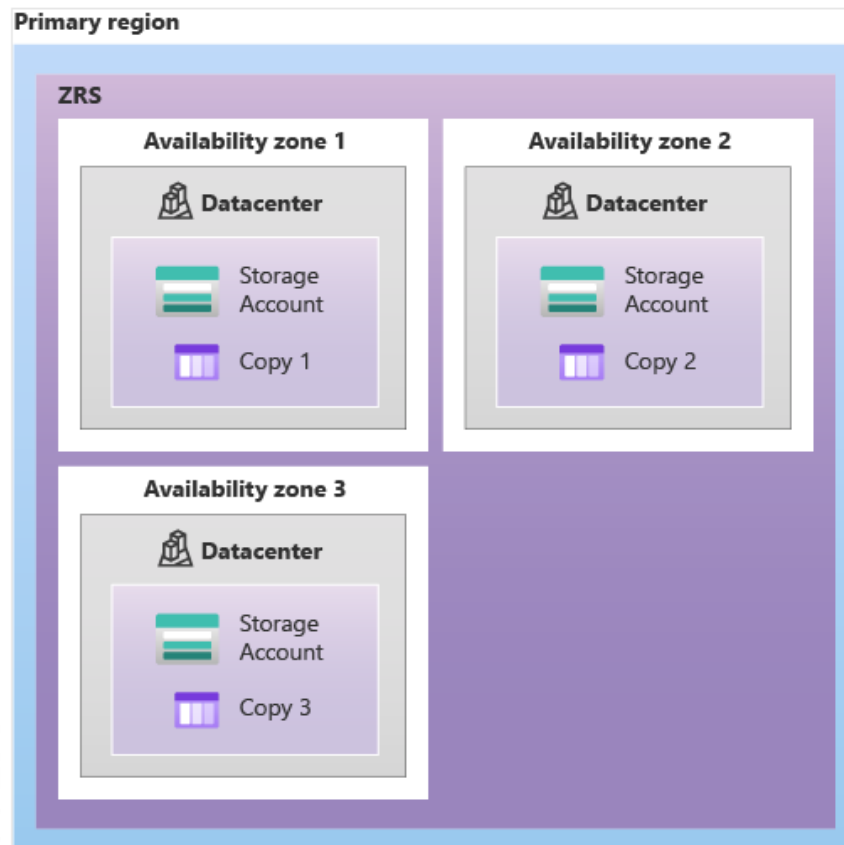
Locally redundant storage (LRS)

- Locally redundant storage (LRS) replicates your storage account three times within a single data center in the primary region



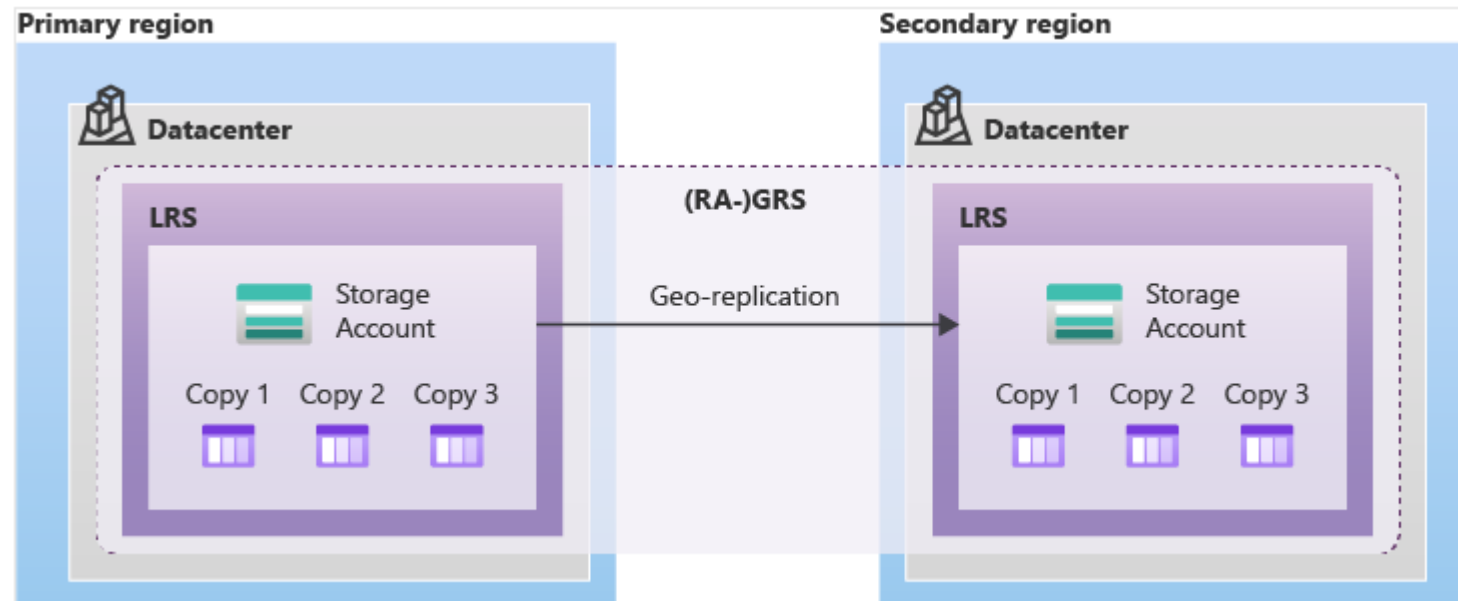
Zone-redundant storage (ZRS)

- Zone-redundant storage (ZRS) replicates your storage account synchronously across three Azure availability zones in the primary region



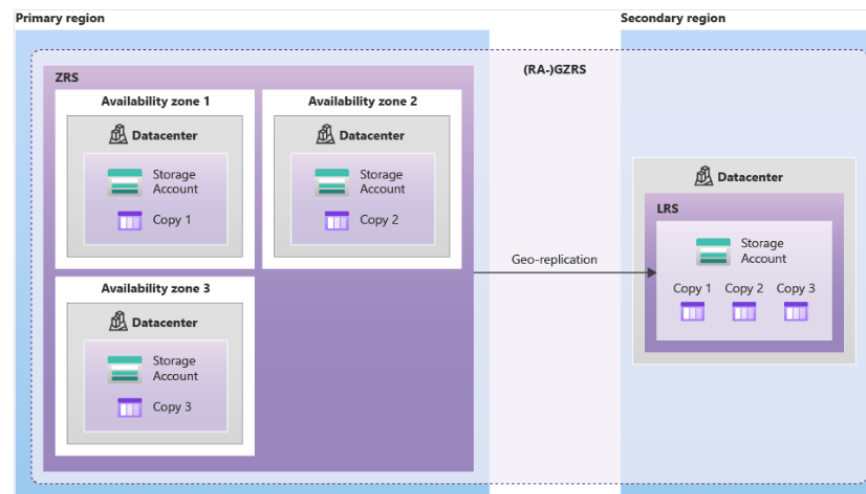
Geo-redundant storage (GRS)

- Geo-redundant storage (GRS) copies your data synchronously three times within a single physical location in the primary region using LRS.

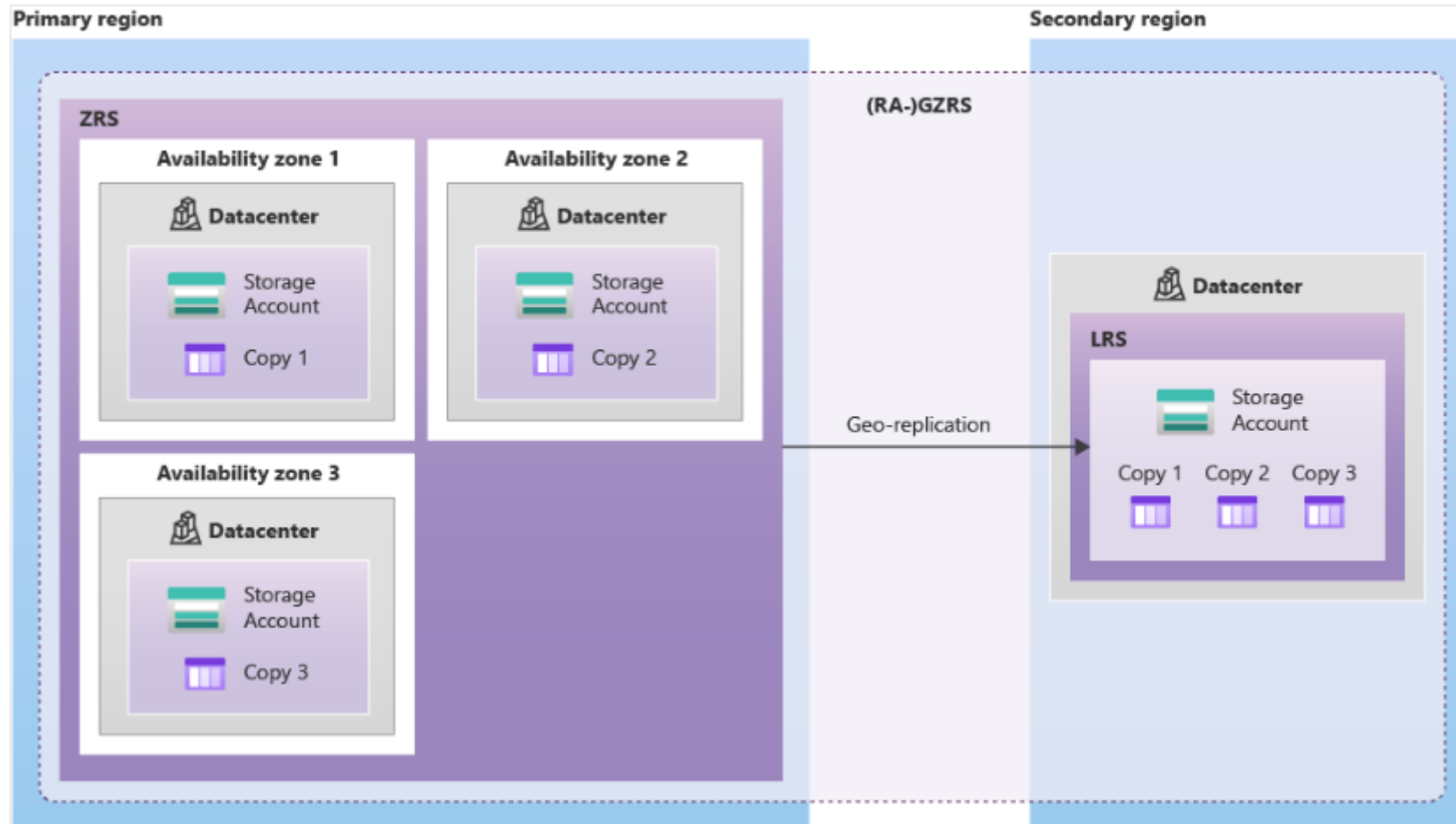


Geo-zone-redundant storage (GZRS)

- Geo-zone-redundant storage (GZRS) combines the high availability provided by redundancy across availability zones with protection from regional outages provided by geo-replication.
- Data in a GZRS storage account is copied across three Azure availability zones in the primary region and is also replicated to a secondary geographic region for protection from regional disasters..



Geo-zone-redundant storage (GZRS)



Read access to data in the secondary region

- Geo-redundant storage (with GRS or GZRS) replicates your data to another physical location in the secondary region to protect against regional outages.
- With an account configured for GRS or GZRS, data in the secondary region is not directly accessible to users or applications, unless a failover occurs.
- The failover process updates the DNS entry provided by Azure Storage so that the secondary endpoint becomes the new primary endpoint for your storage account.
- During the failover process, your data is inaccessible. After the failover is complete, you can read and write data to the new primary region.

Azure Storage Services

- Visa och förklara
 - Blob
 - Share
 - Queue
 - Table
- Azure Storage Explorer både lokalt nerladdad och i portalen
- Se till att huvudnycklarna inte sprids!
- Azure Storage Explorer är enkelt sätt att ladda upp filer

Övning

- Öva på de delar vi gått igenom idag, främst Shares på Storage Accounts
 - Skapa share, anslut till det hemifrån eller från skolan etc som ett vanligt share
- Ladda ner Azure Storage Explorer
 - Anslut till share, prova att använda det med att kopiera några filer

Övning (framskjuten då den tar lång tid)

- Installera Azure AD Directory Service i er tenant
- Vänta till det är klart. Det tar ganska lång tid
- Ändra DNS-pekare på er VM så den pekar på AADDS DNS-servrar

Nr 2 – Azure Storage Services, File Share

- Skapa ett Azure Storage Account + Azure File Share
- Se till att detta share är nåbart från internet, och kopiera in några valfria filer till detta share, så det ligger några filer där.
- Ta kopia på PowerShell-skriptet och lägg det i inlämningsmappen på Studentportalen, se till att Azure storage account key finns med, så att jag kan verifiera att det fungerar.
- Skriv en kort förklaring av varje steg du tog för att slutföra uppgiften, inklusive eventuella utmaningar du stötte på och hur du överkom dem, ange om detta är en IaaS-, PaaS- eller SaaS-tjänst, tillsammans med en personlig reflektion kring säkerhet om att sprida *Azure storage account key* på detta sätt

Summering av dagens lektion

- Kort summering kring vad vi har gått igenom under dagens lektionstillfälle.
 - Azure AD,
 - IAM, RBAC
 - Azure AD Connect
 - Azure AD Domain Services
 - Storage Account
- Lyft gärna de studerande reflektioner kring dagens lektion.
(Vad tar de med sig från dagens lektion? Finns det något som var extra svårt att förstå? Finns det något som vi behöver repetera? Hur upplevde de dagens arbetsmetoder?)

Framåtblick inför nästa lektion

- Berätta kort vad ni kommer att behandla vid nästa lektionstillfälle.
 - Nästa lektion kommer vi fortsätta med Azure.
- Finns det något som de studerande kan/måste förbereda sig inför nästa lektionstillfälle.