

**Molndrift av tjänster och applikationer**

**DEVOPS22**

**Del 5; Azure AD (Microsoft Entra ID)**

# Kort summering av föregående lektion/ev. lektioner

## **Föregående lektion:**

- Frågor kring förra lektionen?
  - VM
  - Diskar
  - Virtual Gateway
  - VPN

# Lektionstillfällets mål och metod

## **Mål med lektionen:**

- Göra klart P2S VPN
- Mittkursutvärdering
- Intro till Azure AD

## **Lektionens arbetsmetod/er:**

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

# Mittkursutvärdering

- Prata ihop er om ni vill, men varje student fyller i eget svar.
- BÖRJA
  - Finns det något du vill att vi ska BÖRJA med för att göra denna kurs mer givande?
- SLUTA
  - Finns det något du vill att vi ska SLUTA med som du inte anser är bra eller relevant för kursen?
- FORTSÄTTA
  - Vad vill du att vi ska FORTSÄTTA göra som vi redan gör idag?



# Kursens syfte och mål

- Syftet med kursen är att ge de studerande de kunskaper och färdigheter som krävs för att drifta egenutvecklade applikationer och IT- tjänster i publika moln.
- Målet för kursen är att de studerande ska kunna uppvisa självständiga färdigheter och kunskap i tillämpningsområden, kravställning av system, kunskap om moderna verktyg samt förmåga till implementering av molnssystem.

# Kursen går igenom följande moment

- Utveckla och driftsätta applikationer med hjälp av Platform as a Service (PaaS)
- Tjänster inom molnbaserade infrastruktur.
- Uppsättning av säker åtkomstkontroll av molnbaserade tjänster.
- Virtual Infrastructure Management.
- Infrastructure as a Service (IaaS) med t.ex. Microsoft Windows Azure, Googles Cloud-plattform, Amazon AWS eller en annan publik molntjänst.
- Användningsfall Molnimplementationer, t.ex. containers, serverless, auto-scaling.
- Monitorering och metrics.



# De studerande ska ha kunskaper i/om

- Drift av tjänster i publika moln samt där tillhörande ekonomiska och säkerhetsmässiga aspekter
- Skillnader mellan lokala och publika moln samt skillnad och fördel mellan infrastructure as a service (IaaS), platform as a service (PaaS) och software as a service (SaaS)
- Containerhantering



# De studerande ska ha färdigheter i att

- Installera servertjänster i publika moln.
- Drifta och flytta virtuella maskiner mellan privata och publika moln.
- Utföra monitorering av miljöerna och insamling av metrics

# De studerande ska ha kompetens för att

- Hantera drift av applikationer och tjänster i privata så väl som publika moln.
- Hantera användarsäkerhet vid drift av tjänster i publika moln.

# För Godkänd (G) krävs

- Ha kännedom om skillnader mellan lokala och publika moln samt skillnad och fördel mellan Infrastructure as a Service (IaaS), Platform as a service (PaaS) och Software as a Service (SaaS)
- Ha kunskaper om containerhantering i molnet
- Utföra monitorering av miljöerna och insamling av metrics
- Kan hantera drift av applikationer och tjänster i privata så väl som publika moln samt där tillhörande ekonomiska och säkerhetsmässiga aspekter och kontohantering
- Kunna drifta och flytta virtuella maskiner mellan privata och publika moln
- Kunna installera tjänster till publika moln och hantera tillhörande användarsäkerhetsaspekter

# För Väl Godkänd (VG) krävs

- Studenten kan med säkerhet hantera drift av applikationer i tjänster i privata så väl som publika moln
- Studenten kan kommunicera kring val och tillvägagångssätt för molnimplementationer

# Examinationsform

4 individuella inlämningsuppgifter.

# 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

## 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



# Nr 3 – Nginx via Azure Container Instance

- Skapa en egen Azure Container Instance, använd nginx som image/avbild
- Se att du kan skapa den, starta om och liknande
- När den är igång, surfa till den med http
- Om den inte fungerar – kontrollera att porten för http (tcp port 80) är öppen i NSG
- Ta en skärmdump av Welcome to nginx-webbsidan, se till att webbläsarens adress syns i bilden, ladda upp 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

# Nr 4 – Plan för att migrera till Azure

- Analysera först Antons Motoroljas system
- Dokumentera därefter vilka steg som behövs för en migrering, och i vilken ordning du avser att göra resp steg.
- I dokumentet vill jag även veta hur lång arbetstid du avser att lägga på respektive steg och hur lång tid resp steg tar.
- I anslutning till stegen vill även veta vilka resurser i Azure du avser att använda (och varför). Detta ska innehålla en ekonomisk och säkerhetsmässig förklaring.
- Lägg upp dokumentet på Studentportalen.



# Gör klart VPN

- PPT från förra lektionen (dag 4)
- Gör klart P2S VPN

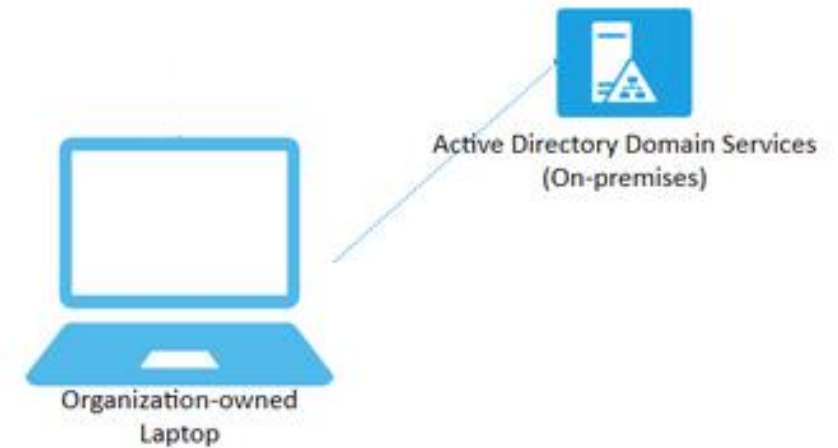


# Traditionellt AD

- Rita och berätta
  - AD
  - GPO, olika OS
  - LDAP

# Active Directory, AD

- Active Directory Domain service is basically a database, where you can have all your computers, users and others organized.
- It provides authentication and authorization to applications, file services, printers, and more on-premises resources.
- AD uses protocols such as NTLM and Kerberos for authentication and LDAP for resource discovery.



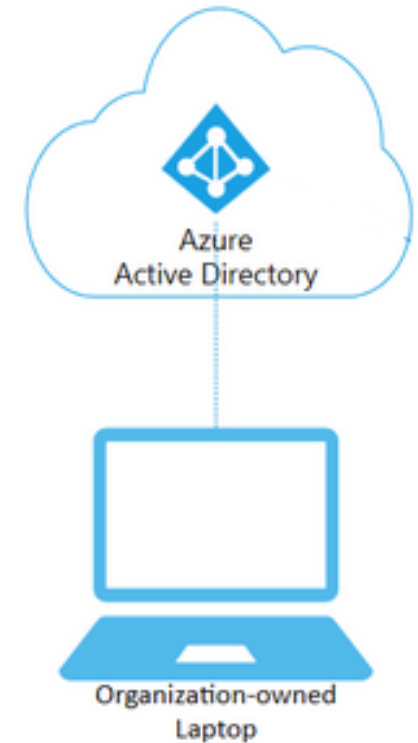


# Active Directory, AD

- With a great feature Group policy, you can distribute settings throughout a whole network.
- There are many security groups, user and admin accounts, passwords, identity and access rights, and that's why securing AD is the key.
- Nevertheless, the important point of view is that AD was not designed to cope with the world of web-based Internet services.

# Azure Active Directory, AAD

- First, Azure Active Directory is not Active Directory, unfortunately, its name leads to many confusions.
- However, AAD has a similar function with authentication and authorization to applications.
- Nyligen bytt namn till Microsoft Entra ID
  - <https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/new-name>



# Azure Active Directory, AAD

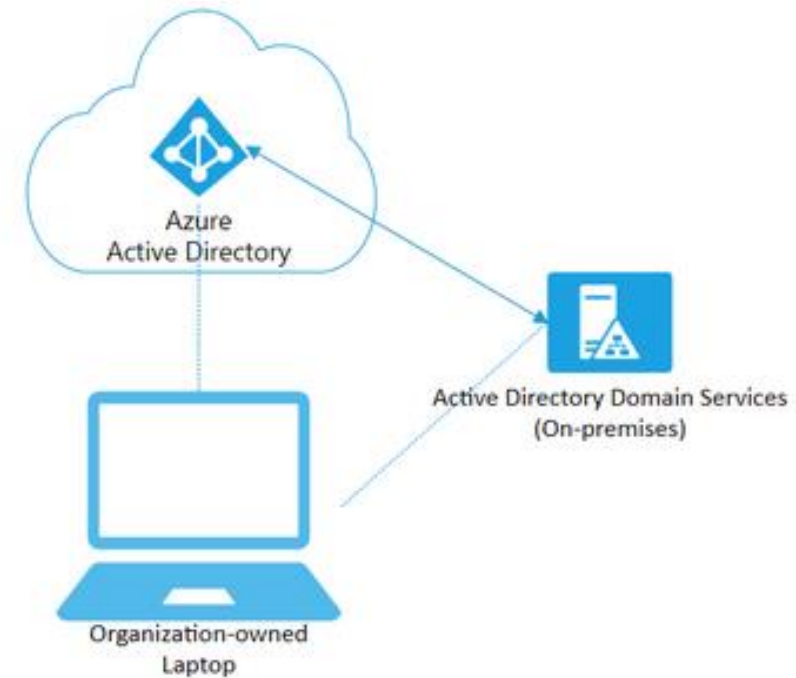
- Compared with AD, Azure Active Directory was designed to support web-based services that use RESTful interfaces for Office 365, Google Apps, etc.
- It also uses different protocols for working with these services (SAML, OAuth 2.0.). You could say that AAD is "AD service in the cloud".
- Another difference is that there is no such thing in AAD as forests and domains.
- Instead, you are a tenant representing your whole organization and you can manage all users with their passwords, permissions, etc.

# Azure Active Directory, AAD

- A user with one identity can sign on to thousands of SaaS applications and not just into Microsoft's Office 365, Sharepoint or Exchange online. And he can do it without a repeated requirement for logging in

# Active Directory vs Azure Active Directory

- In AAD there is no such thing as Group Policy or support of LDAP, but you can find many other brand new features.
- Nowadays, there are various models of using Active Directory services and every company has different needs and possibilities.
- In case your organization doesn't need missing features of AD, you can move to Azure Active Directory and decommission classic Active Directory.



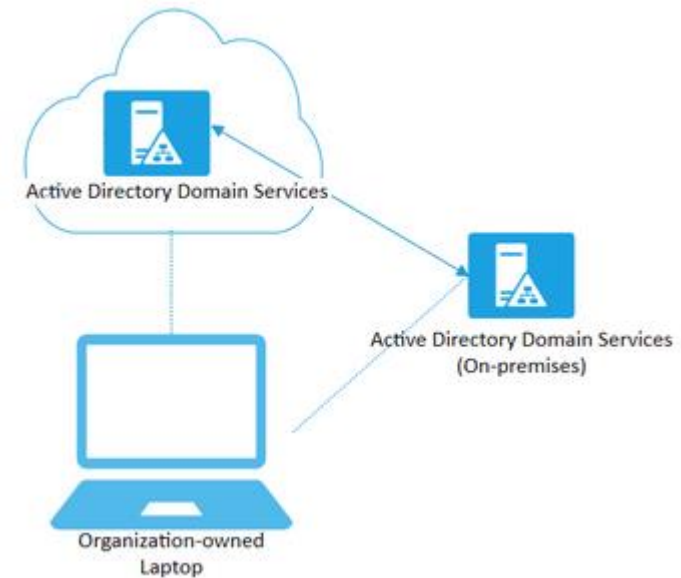
# Hybrid Azure AD

- There are various scenarios containing Hybrid Azure AD, which means combinations of AD and AAD.
- This type of architecture offers a combination of both and thanks to Azure AD Connect your user/passwords data are synchronized.
- In the end, you can use just classic AD, however, you can hear every day more and more about the advantages of moving to the cloud.



# Fortsätta med enbart AD?

- Teoretiskt går det att enbart fortsätta med traditionellt AD
- Vi etablerar VPN-tunnlar/ExpressRoute mellan miljöerna, så alla system når varandra
- Plus att det går att installera ADDS på en IaaS-server som finns i molnet.





# Breakout-room

- Diskutera i grupp fördelar och nackdelar med lite olika AD-scenarion.
- Ska vi fortsätta med enbart traditionellt AD?
  - Vad vinner resp förlorar man på det?
- Gå över helt och hållet på Azure AD?
  - Vad vinner resp förlorar man på det?
- Köra Hybrid
  - Vad vinner resp förlorar man på det?

# Resultat från Breakout-room

- Funktion ska styra!!
- Krav från kunder, ex lagring lokalt. Finns dock fördelar att ha MS365 med sharepoint etc
- Legala krav

# Azure AD

- Azure Active Directory Free
  - Provides user and group management, on-premises directory synchronization, basic reports, self-service password change for cloud users, and single sign-on across Azure, Microsoft 365, and many popular SaaS apps.
- Azure Active Directory Premium P1
  - In addition to the Free features, P1 also lets your hybrid users access both on-premises and cloud resources. It also supports advanced administration, such as dynamic groups, self-service group management, Microsoft Identity Manager (an on-premises identity and access management suite) and cloud write-back capabilities, which allow self-service password reset for your on-premises users.

# Azure AD

- Azure Active Directory Premium P2
  - In addition to the Free and P1 features, P2 also offers Azure Active Directory Identity Protection to help provide risk-based Conditional Access to your apps and critical company data and Privileged Identity Management to help discover, restrict, and monitor administrators and their access to resources and to provide just-in-time access when needed.

# Azure AD

- "Pay as you go" feature licenses
  - You can also get additional feature licenses, such as Azure Active Directory Business-to-Customer (B2C). B2C can help you provide identity and access management solutions for your customer-facing apps. For more information, see [Azure Active Directory B2C documentation](#).

[Home](#) > [New](#) >

# Azure Active Directory

Microsoft



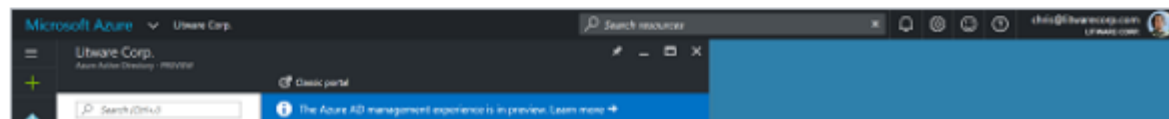
## Azure Active Directory

Microsoft

[Create](#)[Save for later](#)[Overview](#)[Plans](#)[Usage Information + Support](#)

Azure Active Directory is an Identity and Access Management as a service (IDaaS) solution that extends your on-premises directories into the cloud and provides single sign-on to Azure, Office 365 and thousands of cloud (SaaS) apps and access to web apps you run on-premises.

Built for ease of use, Azure Active Directory enables enterprise mobility and collaboration and delivers advanced identity protection through multi-factor authentication (MFA), security reports, audits, alerts and adaptive conditional access policies based on device health, user location and risk level.



[Home](#) > [New](#) > [Azure Active Directory](#) >

## Create tenant



Organization name \* ⓘ

Gullefjun ✓

Initial domain name \* ⓘ

gullefjun ✓

gullefjun.onmicrosoft.com

Country or region ⓘ

Sweden ✓



Tenant creation will take about one minute.

[Create](#)




# Eget domainnamn

- De flesta företag vill inte ha xxx.onmicrosoft.com...
- Custom domain names
- Lägg till custom domain
- Fyll i domainnamnet
- Därefter lägger du upp txt-pekaren i den externa DNS'en
- Efter godkänd validering är det klart.
- Då kan användare logga in med det riktiga företagsnamnet

[Home](#) > [Gullefjun](#)

- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties

[+ Add custom domain](#) [↻ Refresh](#) [🔧 Troubleshoot](#) | [☰ Columns](#) | [💙 Got feedback?](#)

 Looking to move an on-premises application to the cloud and use Azure Active Directory Domain Services?

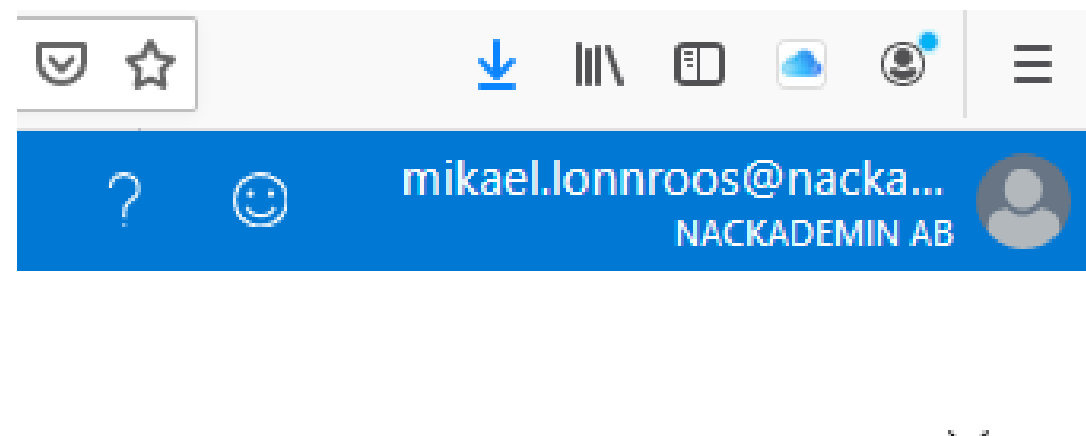
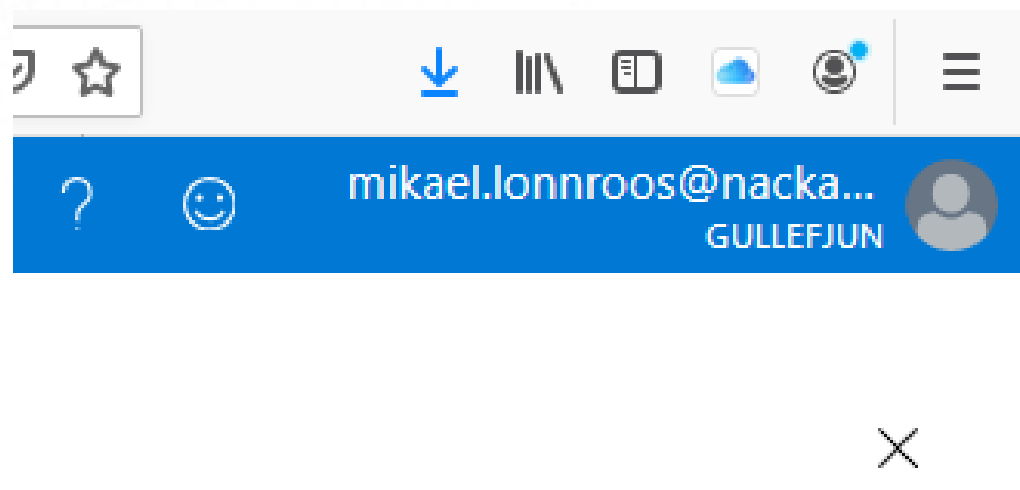
Search domains

+ Add filters

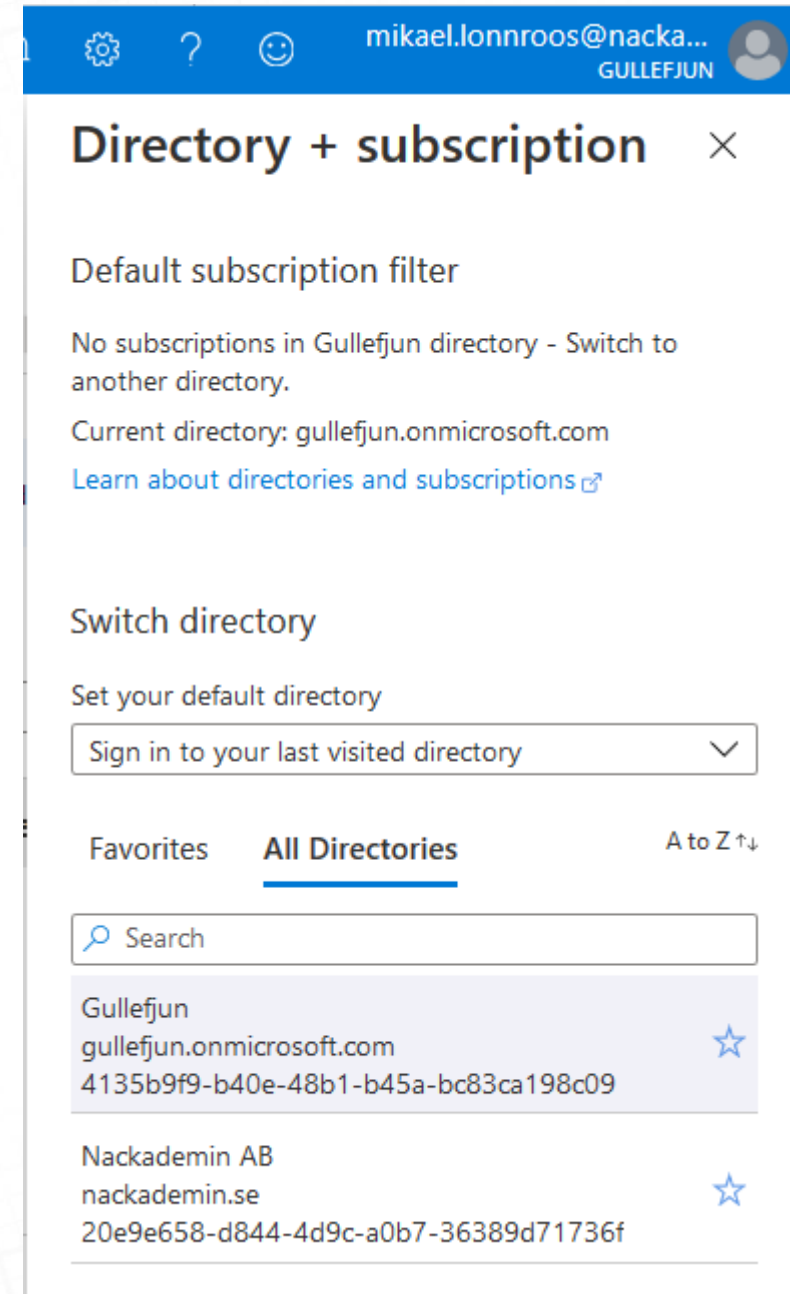
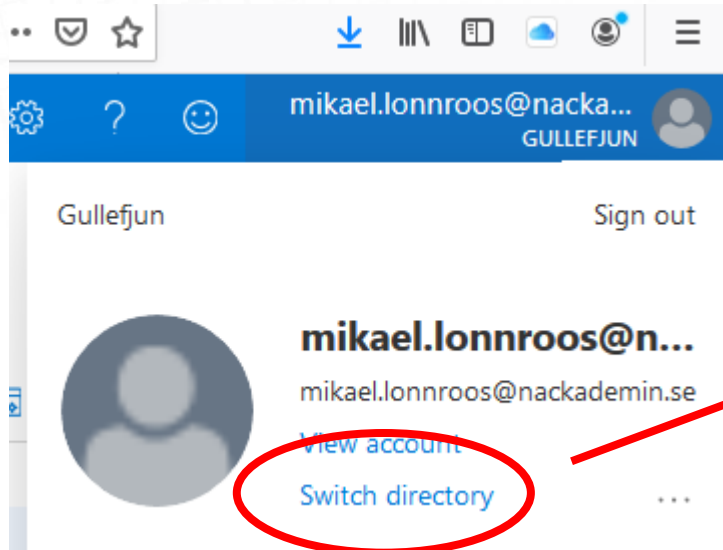
Name	Status	Federated	Primary
gullefjun.onmicrosoft.com	✔ Available		✔

# Eget domainnamn

# Men var har alla resurser tagit vägen?



# Var är resurserna?



Nackademin AB - Microsoft Az

https://portal.azure.com/#blade/Microsoft\_AAD\_IAM/ActiveDirectoryMenuBlade/C110%

Microsoft Azure

Search resources, services, and docs (G+)

mikael.lonnroos@nacka...  
NACKADEMIN AB

Home >

i

Nackademin AB | Overview

Azure Active Directory

Overview

Getting started

Preview hub

Diagnose and solve problems

Manage

Users

Groups

External Identities

Roles and administrators

Administrative units

Enterprise applications

Devices

App registrations

Identity Governance

Application proxy

Switch tenant

Delete tenant

Create a tenant

What's new

Preview features

Got feedback?

i

Azure Active Directory can help you enable remote work for your employees and partners. [Learn more](#)

Nackademin AB

Search your tenant

Tenant information

Your role

User [More info](#)

License

Azure AD for Office 365

Tenant ID

20e9e658-d844-4d9c-a0b7-363...

Primary domain

nackademin.se

Azure AD Connect

Status

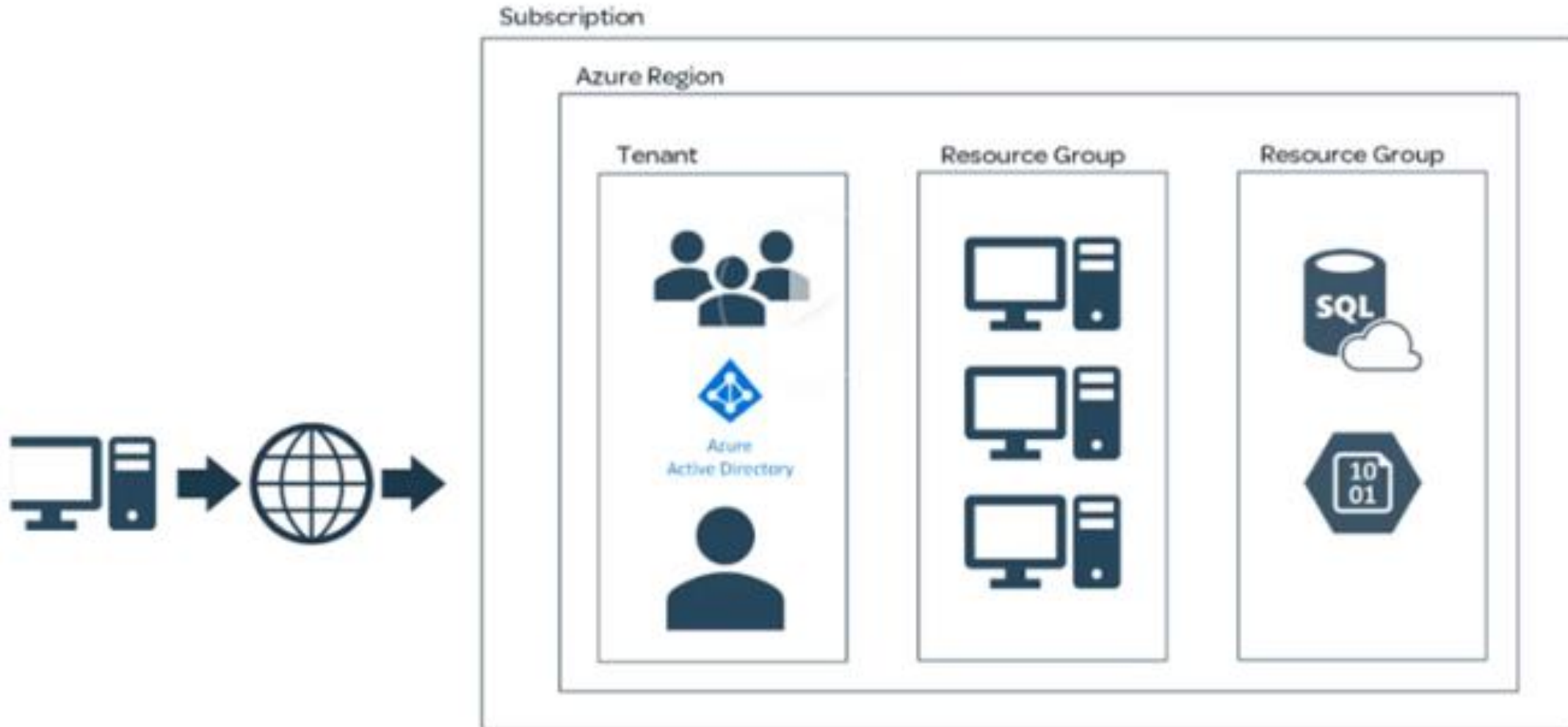
Enabled

Last sync

Less than 1 hour ago

DEMIN

# Azure Concepts





Change the directory - Microsoft X

Azure for Students - Microsoft X

+

← → ↺ 🏠

🔒 <https://portal.azure.com/#@nackademin.se/resource/subscriptions/a5bf7118-6fc2> 110%

⋮ 🛡️ ☆

📄 📁 📅 🌤️ 📷

☰

Microsoft Azure



🔍 Search resources, services, and docs (G+)

📄 📁 📅 🌤️ 📷 ? 😊

mikael.lonnroos@nacka...  
NACKADEMIN AB

👤

Home > Azure for Students


 **Azure for Students** 


Subscription


🔍 Search (Ctrl+)


⏪


[🔗 Manage](#) [🗑️ Cancel subscription](#) [✎ Rename](#) [➡ Change directory](#) [➡ Transfer billing ownership](#) [💙 Feedback](#)


 Overview

 Activity log


 Access control (IAM)


 Tags

 Diagnose and solve problems


 Security


Billing


 Invoices


 Partner information


Settings


 Programmatic deployment

 Resource groups

 Resources

 Usage + quotas

 Policies

 To check your remaining credit, visit <https://www.microsoftazuresponsorships.com> ➡

⤴ Essentials

Subscription ID  
a5bf7118-6fc2-4729-b1cd-08fbb2a9edc9

Subscription name  
[Azure for Students](#)

Directory  
Nackademin AB (nackademin.se)

Current billing period  
9/23/2020-10/22/2020

My role  
Account admin

Currency  
SEK

Offer  
Azure for Students

Status  
Active

Offer ID  
MS-AZR-0170P

[See more](#)



# Egen övning

- Skapa en egen Tenant / Azure AD
- Flytta din befintliga subscription till den nya tenanten (observera att detta steg kan ta ett bra tag).

# Global administrator

- Eftersom du skapat allt i tenanten, 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>

# Summering av dagens lektion

- Kort summering kring vad vi har gått igenom under dagens lektionstillfälle.
  - Kort om AD vs Azure AD
  - Domainnamn
  - Flytta en subscription
- 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.