# Checklista – Examination: Secure Cloud Solution (Medilync AB)

## ✅ Utfört

* • Skapat tre virtuella Linux-servrar (web01, db01, dev01) i rätt subnät och VNet
* • Tilldelat rätt Network Security Groups (NSG) till varje subnet
* • Skapat användare i Microsoft Entra ID: Nurse User, Finance User, Developer User, Admin User
* • Tilldelat roller (Reader, Contributor, Ägare) i Medilync-ProdRG och Medilync-DevRG
* • Dokumenterat varje steg med skärmbilder
* • Tilldelat dig själv rollen Ägare tillfälligt (för administration) och noterat detta

## 🔜 Att göra

* • Skapa och konfigurera Azure Bastion för dev01 (åtkomst utan Public IP)
* • Aktivera loggning och övervaka resurser via Log Analytics / Azure Monitor
* • Verifiera och dokumentera kryptering av data (disk, in-transit)
* • Skapa eller verifiera MFA och villkorlig åtkomst för användare (t.ex. Nurse User)
* • Begränsa behörigheter via RBAC-villkor för Admin-rollen (om tillämpligt)
* • Färdigställ projektdokumentation (text, skärmbilder, arkitektur)
* • Ladda upp dokumentation till GitHub (README.md + screenshots-mapp)
* • Eventuell hotbildsanalys om det krävs i kursen
* • Ta bort ägarrollen för Allen Muco efter projektets slutförande (säkerhetsåtgärd)

(IDAG 24 APRIL, DET SISTA JAG GÖR ATT TABORT BASTION FÖR ATT SPARA PENGAR. DET BLEV FEL MED CMK trots att web01 var frikopplad. Vi skulle fortsätta den 25 april 2025 med att felsöka detta, kanske skapa en ny disk från början om det skulle bli svårt att åtgärda. )

* **Dokumentation: Aktivering av Microsoft Defender for Cloud i Medilync-projektet**
* **Projekt:** Examination – Secure Cloud Solution **Datum:** 2025-04-24 **Student:** Allen Camille Muco **Syfte:** Aktivera Microsoft Defender for Cloud för att öka säkerheten och övervakningen i det molnbaserade projektet för Medilync AB.
* **Steg för aktivering:**

1. **Navigering till Microsoft Defender for Cloud**
   * Via Azure-portalen valde jag "Microsoft Defender för moln".
   * I översikten visades en överblick över säkerhetsstatus, regler, regelefterlevnad och resurser.
2. **Öppning av Miljöinställningar**
   * Från menyn valdes "Miljöinställningar".
   * Valde prenumerationen "Azure subscription 1".
3. **Defender-planer**
   * Valde fliken "Defender-planer" under inställningar.
   * Överst visades två delar:
     + **Grundläggande CSPM (kostnadsfri)**: Aktiverad.
     + **Defender CSPM (5 USD/resurs/månad)**: Visades som valfri. Jag valde att **inte** aktivera denna då den grundläggande planen är tillräcklig för projektets syfte.
4. **Aktivering av skydd för molnarbetsbelastningar (CWP)**
   * Jag aktiverade endast de som är relevanta för mina resurser:
     + **Servrar**: Aktiverad för samtliga 3 servrar (web01, db01, dev01).
     + Övriga som App Service, Databaser, Minne etc. har lämnats inaktiverade då inga instanser finns.
5. **Statuskontroll**
   * Bekräftelse i portalen visade "Övervakningstäckning: Fullständigt" för de aktiverade delarna.

* **Slutsats:**
* Microsoft Defender for Cloud har nu aktiverats på ett kostnadseffektivt sätt med fokus på säkerhetsövervakning av servrar inom projektets prenumeration. Den grundläggande planen (CSPM) är tillräcklig för övervakning och efterlevnad, utan att skapa onödiga kostnader.
* Denna konfiguration dokumenteras och kommer att inkluderas i slutlig projektrapport samt delas på GitHub tillsammans med övriga projektfiler.
* **Nästa steg:** Fortsätta med att konfigurera ytterligare säkerhetsfunktioner (t.ex. Azure Policy eller Security Center alerts) beroende på krav.
* **Aktivering av Microsoft Defender for Cloud i projektet 'Examination – Secure Cloud Solution'**
* **Syfte:** Aktivera säkerhetsövervakning för resurser inom projektet i Azure genom Microsoft Defender for Cloud, för att få ökad insyn i säkerhetsstatus, efterlevnad och hotidentifiering.
* **1. Översikt över aktiverade Defender-planer:**
* **Grundläggande CSPM** *(Cloud Security Posture Management)*
  + ✔ Aktiverad (gratisnivå)
  + Ger grundläggande säkerhetsrekommendationer, säkerhetsstatus och efterlevnadsöversikt.
  + Anses tillräcklig för examenssyftet.
* **Defender for Servers**
  + ✔ Aktiverad för 3 servrar: web01, db01, dev01
  + Pris: ca 15 USD/server/månad (kostnadsfritt i 30 dagar)
  + Ger hotidentifiering, sårbarhetsbedömning och logganalys
* **Defender for Resource Manager**
  + ✔ Aktiverad
  + Ger synlighet i kontrollplansaktiviteter och skyddar mot attacker via ARM API.
* **2. Ej aktiverade Defender-planer (bedömdes som ej nödvändiga):**
* Defender CSPM (utökad betaltjänst)
* Defender for App Service
* Defender for Databaser
* Defender for Containers
* Defender for Key Vaults
* **Motivering:**
* Fokus i examensuppgiften ligger på grundläggande säkerhetskontroller, övervakning och segmentering, inte avancerad molnworkload-säkerhet.
* **Slutsats:** Det aktuella säkerhetsbehovet är uppfyllt med Grundläggande CSPM, Defender for Servers och Defender for Resource Manager. Dessa aktiveringar ger såväl synlighet som skydd för projektets kritiska resurser utan onödiga kostnader.

**Dokumentation: Aktivering av Microsoft Defender for Cloud i Medilync-projektet**

**Projekt:** Examination – Secure Cloud Solution **Datum:** 2025-04-24 **Student:** Allen Camille Muco **Syfte:** Aktivera Microsoft Defender for Cloud för att öka säkerheten och övervakningen i det molnbaserade projektet för Medilync AB.

**Steg för aktivering:**

1. **Navigering till Microsoft Defender for Cloud**
   * Via Azure-portalen valde jag "Microsoft Defender för moln".
   * I översikten visades en överblick över säkerhetsstatus, regler, regelefterlevnad och resurser.
2. **Öppning av Miljöinställningar**
   * Från menyn valdes "Miljöinställningar".
   * Valde prenumerationen "Azure subscription 1".
3. **Defender-planer**
   * Valde fliken "Defender-planer" under inställningar.
   * Överst visades två delar:
     + **Grundläggande CSPM (kostnadsfri)**: Aktiverad.
     + **Defender CSPM (5 USD/resurs/månad)**: Visades som valfri. Jag valde att **inte** aktivera denna då den grundläggande planen är tillräcklig för projektets syfte.
4. **Aktivering av skydd för molnarbetsbelastningar (CWP)**
   * Jag aktiverade endast de som är relevanta för mina resurser:
     + **Servrar**: Aktiverad för samtliga 3 servrar (web01, db01, dev01).
     + Övriga som App Service, Databaser, Minne etc. har lämnats inaktiverade då inga instanser finns.
5. **Statuskontroll**
   * Bekräftelse i portalen visade "Övervakningstäckning: Fullständigt" för de aktiverade delarna.

**Slutsats:**

Microsoft Defender for Cloud har nu aktiverats på ett kostnadseffektivt sätt med fokus på säkerhetsövervakning av servrar inom projektets prenumeration. Den grundläggande planen (CSPM) är tillräcklig för övervakning och efterlevnad, utan att skapa onödiga kostnader.

Denna konfiguration dokumenteras och kommer att inkluderas i slutlig projektrapport samt delas på GitHub tillsammans med övriga projektfiler.

**Nästa steg:** Fortsätta med att konfigurera ytterligare säkerhetsfunktioner (t.ex. Azure Policy eller Security Center alerts) beroende på krav.

**🔐 Aktivering av multifaktorautentisering (MFA)**

För att öka säkerheten i det virtuella molnprojektet "Examination – Secure Cloud Solution" aktiverades multifaktorautentisering (MFA) för samtliga användare i Microsoft Entra ID, med undantag för kontots ägare för att förenkla fortsatt administration och testning.

**Steg för genomförande:**

1. Navigerade till: **Microsoft Entra ID > Användare > Multifaktorautentisering per användare**
2. Markerade användarna:
   * Admin User
   * Developer User
   * Finance User
   * Nurse User
3. Klickade på **Aktivera MFA**
4. Bekräftade aktiveringen via popup-rutan
5. Verifierade att status ändrats till enabled för ovanstående användare

Ägarkontot (allen.muco@hotmail.com) lämnades med status disabled för att underlätta vidare konfigurationer och administration.

**Skärmdumpar:**

* MFA-status per användare före och efter aktivering (inkluderat i separat bilaga/skärmdumpsmapp)

**Notering:**

MFA-aktivering via användarsidan är en direkt metod men lämpar sig bäst i labb- eller testmiljö. I produktionsmiljö rekommenderas policybaserad MFA genom **villkorlig åtkomst**.

**🛡️ Villkorlig åtkomst – dokumentation utan aktivering**

Eftersom funktionen kräver Microsoft Entra ID P1/P2-licens, som kan medföra extra kostnader, valdes det att inte aktivera policybaserad MFA i detta projekt. Däremot dokumenteras nedan hur detta skulle konfigureras:

**Steg för att konfigurera policybaserad MFA:**

1. Gå till **Microsoft Entra ID > Säkerhet > Villkorad åtkomst**
2. Klicka på **+ Ny princip**
3. Namnge policyn, t.ex. Require MFA for All Users
4. Välj **Användare eller arbetsbelastningar** > Välj användargrupp eller alla användare (exkludera ev. break-glass-konto)
5. Välj **Molnappar eller åtgärder** > Välj Alla molnappar
6. Under **Grant** (Tilldelning):
   * Välj Grant access
   * Markera Require multifactor authentication
7. Klicka på **Aktivera** och välj På
8. Klicka på **Skapa** för att spara policyn

Denna dokumentation visar förståelse för hur villkorsstyrd åtkomst med MFA kan implementeras, även om den inte aktiverades i praktiken.

**🔒 RBAC-villkor – dokumentation utan aktivering**

RBAC-baserade villkor tillåter att man begränsar en rolltilldelning till exempelvis en specifik plats, enhet eller tidsperiod. Funktionen kräver dock **Microsoft Entra ID P2** eller **Microsoft Entra ID Governance-licens**, och har därför inte aktiverats i detta projekt.

**Exempel: Tilldela Admin User tillfällig behörighet i Medilync-ProdRG**

**Steg för att skapa en rolltilldelning med villkor:**

1. Gå till **Resursgrupp > Åtkomstkontroll (IAM)**
2. Klicka på **+ Lägg till > Tillägg som kan användas**
3. Välj roll, t.ex. Ägare, och användare Admin User
4. Klicka på fliken **Villkor** (kräver P2/Governance-licens)
5. Lägg till t.ex.:
   * Begränsning till inloggning från specifik plats/IP
   * Tillfälligt tillträde (tidsbaserat)
6. Bekräfta och klicka på **Lägg till**

Eftersom licenskravet inte är uppfyllt i detta labb-projekt, dokumenteras endast förståelsen för funktionen.

✅ Dessa moment är dokumenterade och sparade till projektets slutliga dokumentation/README.