

7.2.2. Bitlocker - 3

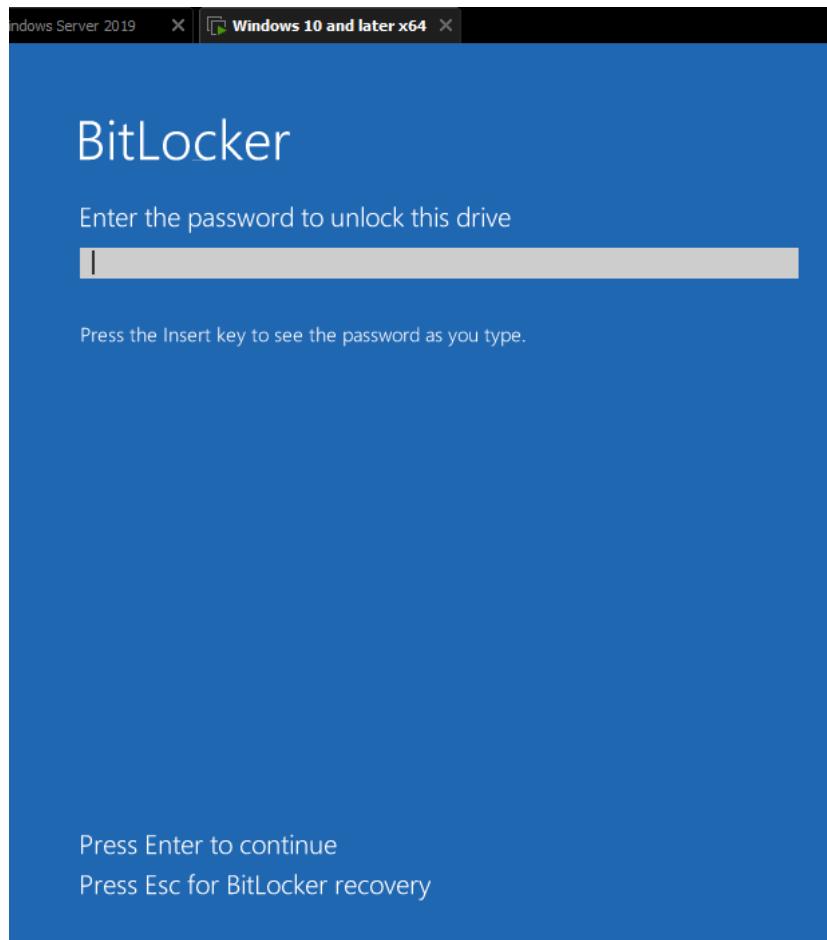
Thursday, December 11, 2025 12:19

Tämä sivu jatkuu koskien "7.2.2. Bitlocker - 2" mitä siinä oikein tapahtui

Harjoitus jatkuu - muu testausta - START HERE;

Muuta testausta ja tarkistusta koskien tästä Bitlocker

- Nyt jouduin VM2:sta uudelleen käynnistä normaalisti



Klikkasin esc ja nyt tuli tämä (alempi kuva)

BitLocker recovery

Enter the recovery key for this drive

Use the number keys or function keys F1-F10 (use F10 for 0).

Recovery key ID (to identify your key): 1FB34D98-1B56-4562-A7D3-6291585A4619

Here's how to find your key:

- Contact your organization's help desk
- For more information go to: aka.ms/recoverykeyfaq

Press Enter to continue

Press Esc for more recovery options

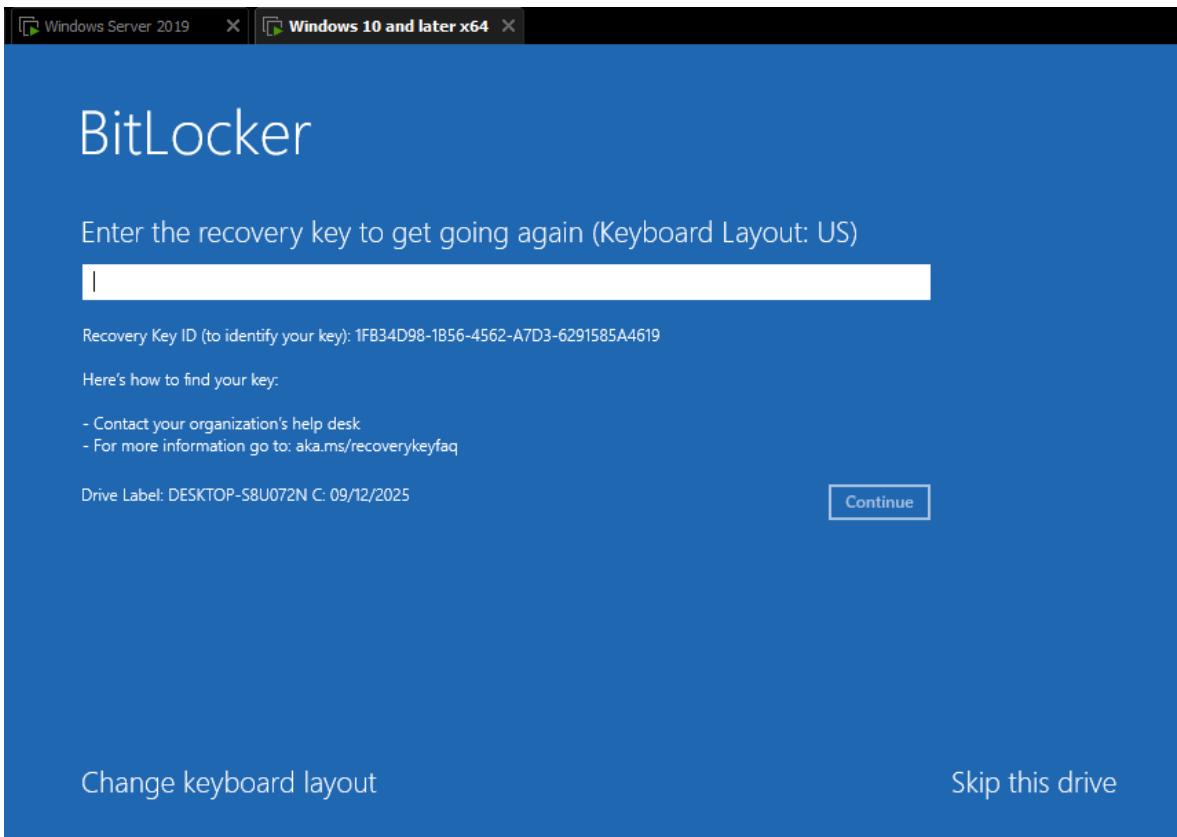
Ihan esc, nyt meni mustaan ruutuun

2019 | Windows 10 and later x64



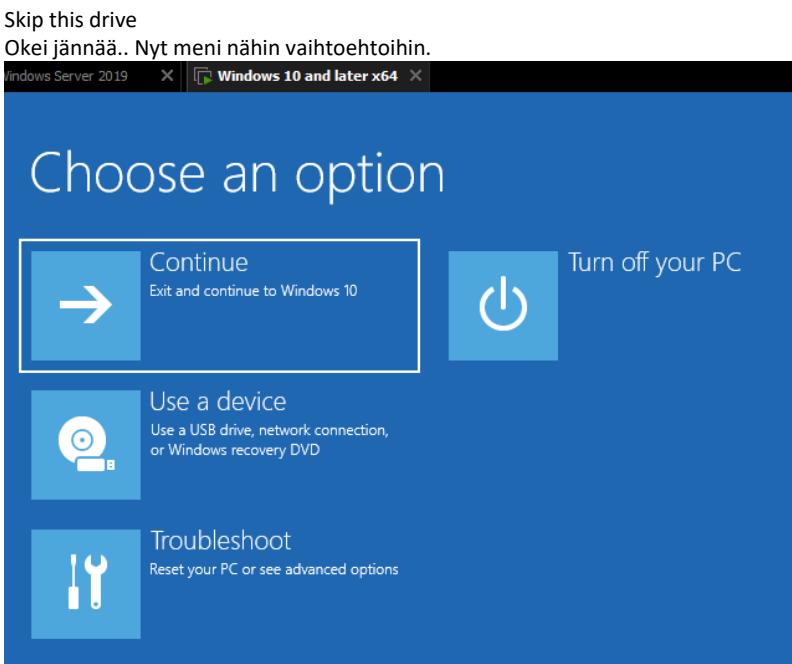
..

Preparing BitLocker recovery



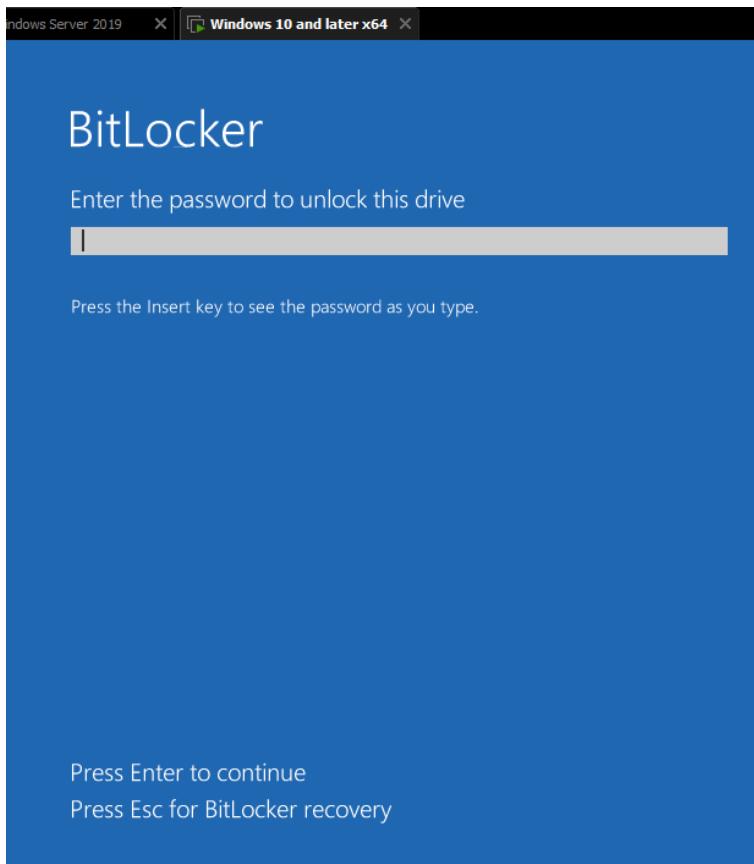
Change keyboard layout

Skip this drive



Continue .. Ainakin varmasti menee takaisin kirjautumisen hommaan

- Nyt syötettiin salasana (Salasana123)



Normaali kirjautuminen (user name & password) kenttä eli normi windows kirjautumisen kenttä tuli ja toimi, mutta **miksi?**

- Tarkistuksena näyttävän onkin toimiva ja eli bitlocker on päällä.



Pieni pohdinta ja mitä nyt tapahtui??

Nyt kun BitLocker kysyy **salasanaa jokaisessa käynnistyksessä** (sininen ruutu ennen Windowsin latausta), se johtuu siitä että otit BitLockerin käyttöön ilman TPM:ää.

Miksi BitLocker kysyy salasanaa joka kerta?

- **TPM (Trusted Platform Module)** on suunniteltu säilyttämään avaimet turvallisesti ja avaamaan levyn automaattisesti käynnistyksen yhteydessä.
- Koska VM2:ssa ei ole TPM:ää (tai et käytä sitä), BitLocker vaatii **salasanan tai USB-avaimen joka kerta** ennen kuin Windows voi käynnistää.
- Tämä on normaali ja odotettu käytös, kun BitLocker toimii ilman TPM:ää.

Vaihtoehdot jos et halua salasanaa joka kerta

1. **Lisää virtuaalinen TPM**
 - Hyper-V:ssä ja VMware Workstation Prosssa voit lisätä virtuaalisen TPM:n (vaatii UEFI + Secure Boot).
 - Tällöin BitLocker voi käyttää TPM:ää ja avata levyn automaattisesti ilman salasanaa.
2. **Network Unlock (vain domain-ypäristössä)**
 - Jos kone käynnistyy yrityksen sisäverkossa, BitLocker voi avata levyn automaattisesti verkon kautta.
 - Tämä vaatii WDS-palvelimen ja AD-integraation.

3. USB-startup key

- Voit määrittää BitLockerille USB-avaimen, joka pitää olla liitettyä käynnistykseen yhteydessä.
- Tämä korvaa salasanan, mutta vaatii fyysisen USB:n.

Käytännön suositus

- Testilabroissa (VM ilman TPM):** Salasanan kysyminen joka kerta on normaalista, et voi poistaa sitä ilman TPM:ää.
- Tuotanto-ympäristössä:** Suositeltavaa käyttää TPM:ää, jolloin käyttäjä ei näe sinistä ruutua joka kerta.

BitLocker toimii nyt oikein. Se kysyy salasanaa joka kerta, koska TPM puuttuu. Jos haluat päästää eroon tästä, sinun täytyy ottaa käyttöön TPM (fyysisen tai virtuaalisen) tai käyttää Network Unlockia.

Miksi se nyt kysyy joka kerta?

- VMWorkstationissa ei ole **TPM-sirua** oletuksena.
- Kun BitLocker toimii ilman TPM:ää, se **pakottaa salasanan tai USB-avaimen joka käynnistykseen**.
- Tämä on suunniteltu turvamekanismi, koska ilman TPM:ää BitLocker ei voi luottaa laitteen käynnistysympäristöön.

Miten sen saa toimimaan kuin oikea työasema?

1. Lisää virtuaalinen TPM (suositeltu tapa)

- VMware Workstation Pro (vain uudemmat versiot) tukkee **virtuaalista TPM:ää**, jos VM on asetettu UEFI + Secure Boot -tilaan.
- Kun TPM on käytössä, BitLocker voi tallentaa avaimen TPM:ään → levy avautuu automaattisesti käynnistykseen, eikä salasanaa kysytä joka kerta.
- Käyttäjä näkee vain Windowsin kirjautumisruudun, kuten oikeassa koneessa.

2. Network Unlock (vain domain-ympäristössä)

- Jos kone on AD-domainissa ja sisäverkossa, BitLocker voi avata levyn automaattisesti verkon kautta.
- Tämä vaatii WDS-palvelimen ja erityisen Network Unlock -palvelun. Ei yleensä labrassa käytössä.

3. USB-startup key

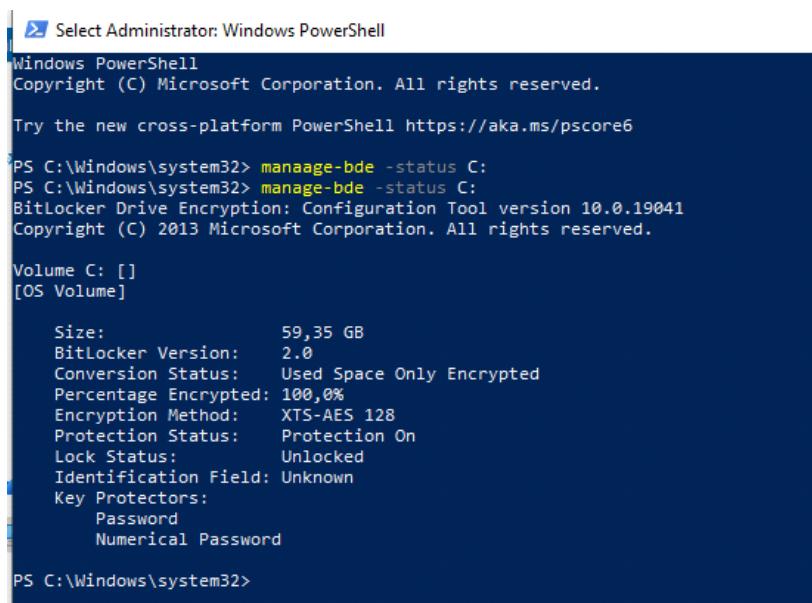
- Voit määrittää BitLockerille USB-avaimen, joka pitää olla liitettyä käynnistykseen yhteydessä.
- Tämä korvaa salasanan, mutta vaatii fyysisen USB:n joka bootissa → ei yhtä kätevää kuin TPM.

Käytännön ero

- Oikea työasema (Win10/11 + TPM):** Käynnistyy suoraan kirjautumisruutuun, BitLocker avautuu taustalla automaattisesti.
- VM ilman TPM:ää:** Näyttää sinisen BitLocker-ruudun joka kerta, koska avain pitää syöttää manuaalisesti.

Jos halutaan tarkistaa 100% varmastusta, että onko bitlocker päällä vai?

Tämä on VM2 tavallinen käyttäjä & mene powershell kautta ja aktivoi "run as administrator"
manage-bde -status -tulosteella BitLocker on **täysin päällä ja toiminnassa** VM2:ssa



```
PS C:\Windows\system32> manage-bde -status C:
PS C:\Windows\system32> manage-bde -status C:
BitLocker Drive Encryption: Configuration Tool version 10.0.19041
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Volume C: []
[OS Volume]

  Size:          59,35 GB
  BitLocker Version: 2.0
  Conversion Status: Used Space Only Encrypted
  Percentage Encrypted: 100,0%
  Encryption Method: XTS-AES 128
  Protection Status: Protection On
  Lock Status: Unlocked
  Identification Field: Unknown
  Key Protectors:
    Password
    Numerical Password

PS C:\Windows\system32>
```

Analyysi tulosteesta

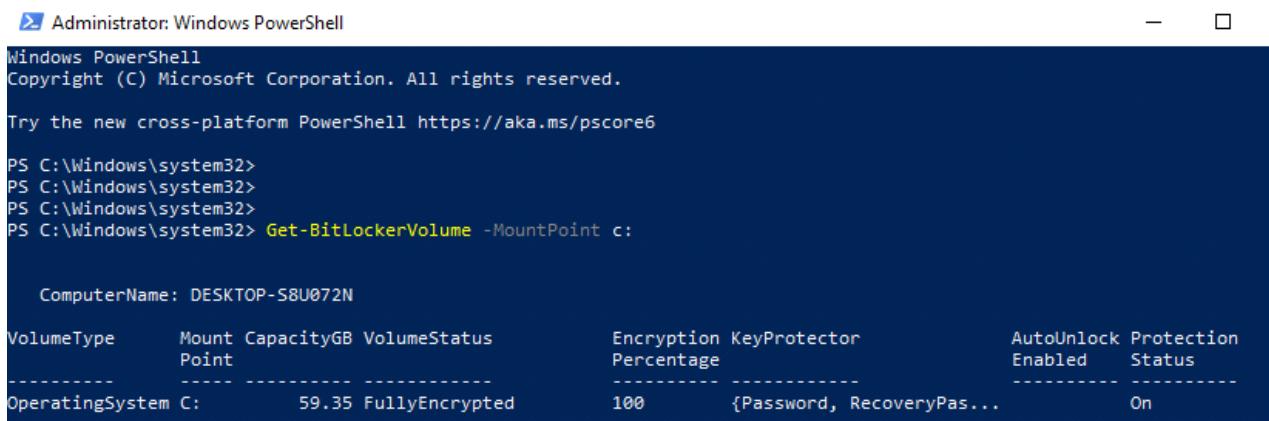
- Size: 59,35 GB** → C:-levyn koko.
- BitLocker Version: 2.0** → Käytössä uudempia BitLocker-versioita (Windows 10/Server 2016 ja uudemmat).
- Conversion Status: Used Space Only Encrypted** → Vain käytetty levytila on salattu (nopeampi asennusvaihtoehto).
- Percentage Encrypted: 100,0%** → Salaus on valmis, kaikki käytetty tila on salattu.
- Encryption Method: XTS-AES 128** → Salausalgoritmi on XTS-AES 128-bittinen (oletus Windows 10/11:ssä).
- Protection Status: Protection On** → BitLocker-suojaus on aktiivinen.
- Lock Status: Unlocked** → Levy on tällä hetkellä avattu (koska syötit salasanan käynnistykseen).

- **Key Protectors: Password, Numerical Password** → Käytössä on sekä salasana (joka syötetään bootissa) että palautusavain (48-numeroinen recovery key).

Mitä tämä tarkoittaa?

- Levy **on salattu ja suojuettu** → BitLocker toimii.
- Salas on **valmis (100 %)** → ei enää kesken.
- Levy on **avattu** → siksi voit käyttää Windowsia normaalista.
- Sinulla on käytössä **salasana + recovery key** → molemmat toimivat avaimina levyn avaamiseen.

BitLocker on nyt **toiminassa ja oikein konfiguroitu** VM2:ssa. Ainoa ero oikeaan työasemaan on se, että koska VM:ssä ei ole TPM:ää, se kysyy salasanaa joka bootissa. Mutta muuten tämä on täysin toimiva BitLocker-salaus.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32> PS C:\Windows\system32> Get-BitLockerVolume -MountPoint c:

ComputerName: DESKTOP-S8U072N

VolumeType      Mount CapacityGB VolumeStatus      Encryption KeyProtector          AutoUnlock Protection
Point          Point    Percentage           Percentage   Enabled     Status
-----
OperatingSystem C:       59.35 FullyEncrypted    100        {Password, RecoveryPas... On

#####
#
```

Mahdollinen jatkotoimenpide?

Harjoituksen kannalta

- **Pidä BitLocker päällä:** Koska olet jo saanut sen toimimaan, se on hyvä pohja jatkoharjoituksille. Voit testata mm. recovery keyn käyttöä, AD-tallennusta, GPO-asetuksia ja eri avausmenetelmiä.
- **Voit myös sulkea sen:** Jos seuraavat harjoitukset eivät liity BitLockeriin, voit purkaa salauksen (*Turn off BitLocker* → levy dekryptataan). Tämä nopeuttaa VM:n käyttöä, koska bootissa ei kysytä salasanaa.

Voiko salasanan poistaa?

- **Ilman TPM:ää:** Ei voi poistaa kokonaan. BitLocker vaatii jonkin avausmekanismin (salasana, PIN, USB-avain). Jos poistat salasanan, levy ei enää avaudu → Windows ei käynnisty.
- **TPM käytössä (fysinen tai virtuaalinen):** Silloin BitLocker voi avata levyn automaattisesti, eikä salasanaa kysytä joka bootissa. Tämä on se "normaali työasema" -kokemus.
- **Vaihtoehto USB-startup key:** Voit korvata salasanan USB-avaimella. Tällöin levy avautuu automaattisesti, kun USB on kiinni, mutta se ei ole yhtä kätevää kuin TPM.

Suositus sinulle

- **Jos haluat jatkaa BitLocker-harjoituksia** → pidä se päällä VM2:ssa, niin voit testata eri avausmenetelmiä.
- **Jos haluat, että VM toimii kuten normaali Win10/11 työasema ilman salasanaa bootissa** → lisää virtuaalinen TPM VMware Workstationiin ja ota BitLocker käyttöön sen kanssa.
- **Jos seuraavat harjoitukset eivät liity BitLockeriin** → voit purkaa salauksen, ettei salasana hidasta joka bootissa.

salasanaa ei voi poistaa kokonaan **ilman TPM:ää**. Harjoituksen kannalta kannattaa pitää BitLocker päällä, mutta jos haluat "normaalin" työaseman kokemuksen, tarvitset TPM:n.

Koskeeko tämä VM1 (Windows Server, administrator-kone)?

- **BitLocker on levykohtainen:** jos otit sen käyttöön VM2:ssa, se koskee vain VM2:n C:-asemaa.
- **VM1 (Windows Server)** ei automaattisesti saa BitLockeria päälle, ellei sitä erikseen asenneta ja oteta käyttöön.
- **Administrator-rooli VM1:ssä** ei vaikuta siihen, onko BitLocker päällä – se vain antaa sinulle oikeudet hallita BitLockeria (ottaa käyttöön, poistaa, hakea recovery keyt AD:stä).

Käytännön ero

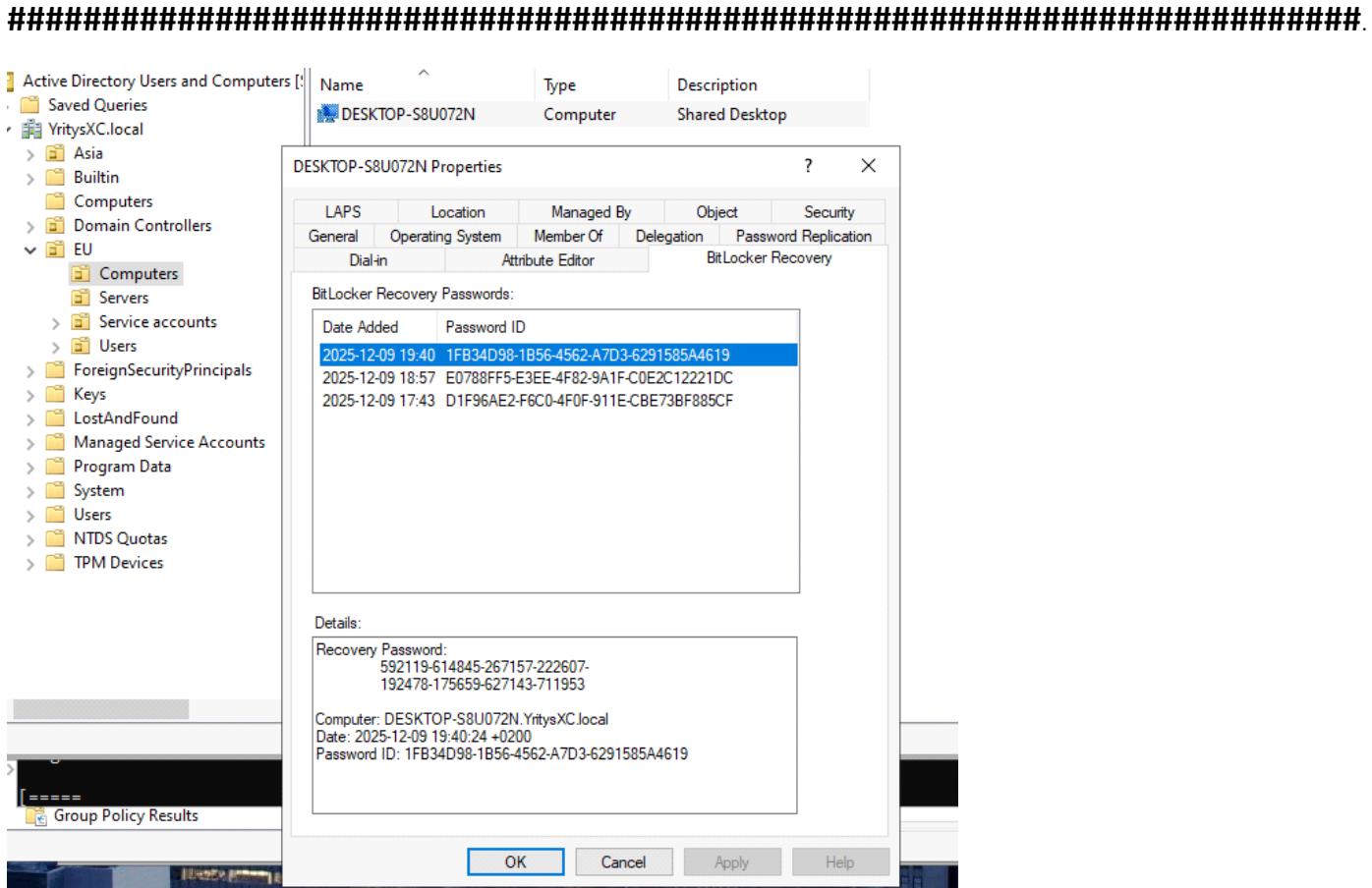
- **VM2 (työasema):** BitLocker on päällä → levy salattu, bootissa kysyy salasanaa.
- **VM1 (Windows Server, admin):** BitLocker ei ole päällä, ellei sinä tai GPO ota sitä käyttöön. VM1 toimii hallintakoneena, josta voit katsoa AD:stä recovery keyt, mutta se ei itse ole automaattisesti salattu.

Yhteenveto

- BitLocker ei koske VM1:stä itsestään, ellei sitä erikseen asenneta ja oteta käyttöön siellä.

- VM1:n rooli on nyt enemmän **hallinta/admin**: se näyttää ADUC:ssa recovery keyt ja hallitsee GPO-asetuksia.
- Jos haluat, voit toki ottaa BitLockerin käyttöön myös VM1:ssä, mutta se ei ole pakollista harjoituksen kannalta.

VM1 ei ole automaattisesti BitLocker-salattu, vaan vain VM2 on. VM1 toimii hallintakoneena, ja BitLocker koskee vain sitä levyä, johon se on otettu käyttöön



Koskien mitä tämä tarkoittaakaan??

samalla koneella (VM2) ja samalla käyttäjällä näkyy useita eri BitLocker Recovery Password ID -tietueita ja eri recovery passwordeja, tarkoittaa että BitLocker on luonut **useita eri palautusavaimia eri ajankohtina**. Tämä ei ole virhe – vaan normaali ja odotettu toiminta.

🔍 Mitä BitLocker Recovery tarkoittaa työasemassa?

- Recovery Password = 48-numeroinen varmuusavain, jolla salattu levy voidaan avata, jos normaali avaus (TPM, PIN, USB) ei toimi.
- Password ID = yksilöllinen tunniste, joka näkyy koneen ruudulla, kun BitLocker pyytää palautusavainta.
- Active Directory tallentaa jokaisen uuden recovery keyn, kun jokin seuraavista tapahtuu:

❖ Miksi sinulla näkyy useita eri recovery key -tietueita?

Tämä tapahtuu, kun:

Tilanne	Mitä tapahtuu	Miksi uusi avain syntyy
Otit BitLockerin käyttöön useamman kerran	Esim. salaus pois → takaisin päälle	BitLocker luo uuden avaimen joka kerta
Vaihdoin avausmenetelmää	Esim. salasana → USB → PIN	Jokainen muutos luo uuden avaimen
Tallensit recovery keyn eri tavalla	USB, tiedosto, tuloste	Jokainen tallennus voi synnyttää uuden avaimen
Testasit eri ajankohtina	Samalla koneella, samalla käyttäjällä	BitLocker ei korvaa vanhaa, vaan lisää uuden
Käytit manage-bde -protectors -add komentoa	Manuaalinen avaimen lisäys	Luo uuden recovery keyn

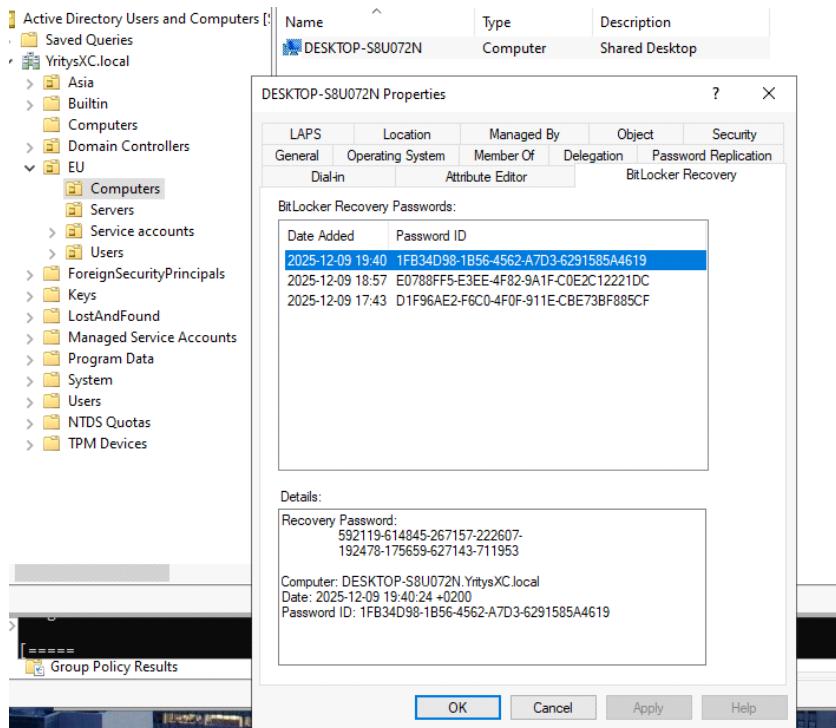
✓ Mitä tämä tarkoittaa käytännössä?

- Kaikki avaimet ovat voimassa, kunnes ne poistetaan.
- AD tallentaa ne aikaleimalla, joten voit jäljittää milloin mikäkin avain on luotu.
- Kun kone pyytää palautusavainta, se näyttää **Password ID:n**, ja admin voi hakea oikean avaimen AD:stä.
- Tämä on tärkeää auditointia ja hallintaa varten – ei virhe, vaan ominaisuus.

⌚ Suositus lab-harjoituksiin

- Voit testata, että AD tallentaa recovery keyt oikein.
- Voit simuloida ongelmatilanteen: lukitse levy → käytä AD:stä haettua avainta → avaa levy.
- Voit myös poistaa vanhoja avaimia, jos haluat siistiä AD:n tietueita (manage-bde -protectors -delete).

BitLocker Recovery -välilehdellä näkyvät eri ID:t ja avaimet kertovat, että BitLocker on konfiguroitu useita kertoja, ja jokaisella kerralla on syntynyt uusi palautusavain. Tämä on täysin normaalia ja osa BitLockerin suojauslogiikkaa.



Kuvassa näkyvät kolme eri **Password ID:tä ja eri Recovery Passwordit** BitLocker Recovery -välilehdellä tarkoittavat, että:

- **BitLocker on konfiguroitu tai muokattu useita kertoja saman koneen (DESKTOP-S8U072N) osalta.**
- Jokaisella kerralla BitLocker on luonut **uuden palautusavaimen (recovery key).**
- Active Directory **ei korvaa vanhoja avaimia**, vaan tallentaa ne kaikki aikaleiman kanssa.

Tämä on täysin normaalia ja osa BitLockerin suunnittelua: **Jokainen uusi avain = uusi suojaustilanne**, ja AD tallentaa ne kaikki, jotta admin voi jäljittää ja palauttaa levyn missä tahansa tilanteessa.

Miksi näin tapahtuu?

- Otit BitLockerin käyttöön useamman kerran (esim. testasit eri asetuksilla).
- Vaihdoit avausmenetelmää (salasana, USB, PIN).
- Tallensit recovery keyn eri tavalla (USB, tiedosto, tuloste).
- Käytit komentoa manage-bde -protectors -add tai muutit suojausasetuksia.

Kaikki nämä synnyttävät **uuden avaimen**, joka tallentuu AD:hen - eli tulee tähän "bitlocker recovery" polkuun ja siihen listan alle.

BitLocker Recovery -välilehdellä näkyvät eri ID:t ja avaimet kertovat, että BitLocker on konfiguroitu useita kertoja, ja jokaisella kerralla on syntynyt uusi palautusavain. Tämä on täysin normaalia ja osa BitLockerin suojauslogiikkaa.