Workplace Ninja

User Group Finland

# Entra Domain Services käytännössä – vinkit on-prem AD:n alasajoon ja siirtymävaiheisiin

# THANKS FOR THE SPONSORS!

PATCH MY PC

Microsoft

PLENTICS

Metropolia

twoday

NETOX

DELL

Workplace Ninja User Group Finland

intel

# Jami Susijärvi

- Työnantaja: Tietokeskus / Aurilo
- Teknologiakonsultti
- +20v kokemus
- Tykkään modernisoida ympäristöjä sekä ajaa palvelimia alas sekä säästää asiakkaan rahoja
- Uskon, että IT-ympäristöjä voi aidosti yksinkertaistaa – askel kerrallaan

# Entra Domain Services – mitä se on ja mitä ei?

- Azure PaaS palvelu
- Active Directory Domain Services palvelut pilvestä
  - Windows-toimialueen (domain) jäsenyys
  - Kirjautumiset AD-tunnuksilla
  - LDAP-hakemisto
  - Kerberos- ja NTLM-autentikointi
  - Group Policy –ryhmäkäytännöt
- Käytännössä Microsoftin hallitsemat kaksi Domain Controlleria
- Integroituu Entra ID (Azure AD) kanssa, tiedot replikoituu (AD DS -> ) Entra ID -> Entra DS
- Rajoitukset
  - Ei Domain Admin / Enterprise Admin oikeuksia
  - AD Schemaa et voi päivittää
  - Ei kirjoituksia Entra DS -> Entra ID
  - Rajoitetut Trust mahdollisuudet
  - Ei oheispalveluita kuten Certificate Services

# Lisenssointi

- Azure palvelu josta laskutetaan käytön perusteella
- SKU vaihtoehdot (Standard ~110$/kk, Enterprise ~290$/kk, Premium ~1200$/kk)
- Trustit vain Enterprise ja Premium

**Standard**

- 0 through 3,000 auth load (peak per hour)
- 0 through 25,000 object count
- Backup every 5 days

**Enterprise**

- 3,001 through 10,000 auth load (peak per hour)
- 25,001 through 100,000 object count
- Backup every 3 days

**Premium**

- 10,001 through 70,000 auth load (peak per hour)
- 100,001 through 500,000 object count
- Daily backup

| SKU | Meter type | Price |
|---|---|---|
| Standard | Directory Objects/Hour | $0.15 USD |
| Enterprise | Directory Objects/Hour | $0.4 USD |
| Premium | Directory Objects/Hour | $1.6 USD |

# Käyttöönotto

- Tarvitaan Entra ID tenantti ja Azure Subscription
- Azure Virtual Network
- Toimialueen nimi (ei voi myöhemmin vaihtaa), suosittelen käyttää internetissä reititettävää nimeä
- Valitaan SKU taso (tätä voi vaihtaa myöhemminkin)
- Valitaan mitä synkroinoidaan
- Asennus kestää noin tunnin
- SSL sertifikaatti jos käytetään LDAPS
- DNS asetukset, sisäverkkoon uudet palvelimet ja jos LDAPS julkiverkosta niin julki IP
- Mahdollinen VPN / Express Route
- Salasana synkrointi
  - Jos Active Directory Domain Services niin pitää olla Password Hash Synchronization (PSH)
    - PowerShell-komento, jolla pakotetaan täysi hash-synkronointi (NTLM / Kerberos)
  - Pilvi käyttäjien pitää vaihtaa salasana jotta generoidaan tarvittavat hashit.
  - Synkroinointi viiveet!

# DEMO

# Käyttötapauksia

Tapaus 1

- Puhdas pilviympäristö
- Sekalaisia palvelimia Azuressa kehittäjille
- Haluttiin hallita palvelimien käyttöoikeudet ja niiden elinkaari
- Ratkaisu
  - Otettiin Entra DS käyttöön
  - Määritettiin synkattavat tunnukset
  - Liitettiin palvelimet uuteen domainiin
  - Annettiin käyttäjille käyttöoikeudet palvelimiin, esim RDP
  - Käyttäjät vaihtoi salasasanat.

# Käyttötapauksia

Tapaus 2

- Käytössä Active Directory Domain Services
- Työasemat jo puhtaasti pilvessä ja halu ajaa AD alas
- Kuitenkin jotain palvelimia vielä jotka riippuvaisia AD:sta ja niistä ei päästä eroon vielä
- Ratkaisu
  - Otettiin Entra DS käyttöön
  - Määritettiin mitä synkataan Entra DS:ään ja synkattiin salasanan onpremisesta
  - VPN Azuren ja Onpremisen välille
  - Vaihdettiin palvelimet uuteen domainiin
  - Testaus että kaikki toimii
  - Onpremise AD:n alasajo

# Käyttötapauksia

Tapaus 3

- Puhdas pilviympäristö
- Päätetty ottaa käyttöön ohjelmisto joka vaati LDAPS
- Ratkaisu
  - Otettiin Entra DS käyttöön
  - Otettiin LDAPS käyttöön
  - Luvitettiin tarvittava IP internetistä Entra DS:ään

# Käyttötapauksia

Tapaus 4

- Puhdas pilviympäristö
- Päätetty ottaa käyttöön NAS onpremisessa joka vaatiin Active Directory liitoksen
- Ratkaisu
  - Otettiin Entra DS käyttöön
  - VPN Onpremisen ja Azuren välille
  - Liitettiin NAS Entra DS:ään
  - Käyttäjät vaihtoi salasanat

# Käyttötapauksia

Tapaus 5

- Laaja ympäristö jossa paljon historiaa. Iso Active Directory infra
- Menossa kuitenkin modernisointia mahdollisuuksien mukaan ja erityisesti tietoturva parannuksia
- Kallis ja iso legacy järjestelmä joka vatiin LDAP:n, mutta vain ”muutamia” käyttäjiä
- Ratkaisu
  - Otettiin Entra DS käyttöön
  - Testattiin että saadaan järjestelmä päivitettyä LDAP -> LDAPS
  - Määritettiin pieni rajoitettu ryhmä tunnuksia jotka synkataan Entra DS:ään
  - Vaikka olisi voitu tehdä myös Onpremise AD:ta vasten niin nyt saatiin rajoitettu suppea AD vain niille ketkä sitä oikeasti tarvii ja päivitettyä samalla se LDAPS. Ei tarvinnut avata verkkoyhteyksiä AD palvelimille eikä tehdä muutoksia AD ympäristöön. Lopputulos hyvin kustannustehokas ja pyörii käytännössä itsellään.

# Yhteenveto

- Hallittu AD DS ympäristö pilvestä
- Riittää moneen muutta on kuitenkin rajoitteita
- Voi nopeuttaa on-prem AD:n alasajoa, vähentää monimutkaisuutta, lisätä joustavuutta
- Maailma ei ole mustavalkoinen ”AD ikuisesti vs. kaikki legacy heti pois”. Entra DS voi auttaa tuossa välissä
- Jos kamppailette AD riippuvuuksien kanssa tutustukaa Entra Domain Servicesiin, voi olla se puuttuva palanen mistä ette olleet tietoisia.
- Modernisoikaa kuitenkin aina kun mahdollista, ei kannata Entra DS:ää pitää tekosyynä pitää kiinni vanhasta loputtomiin
- Entra DS ei ole määränpää, vaan väline. Se mahdollistaa siirtymävaiheen, jossa voimme luopua on-prem AD:sta hallitusti – mutta samalla jatkaa modernisointia kohti täysin pilvipohjaista ympäristöä. Kun viimeinenkin legacy-sovellus on korvattu, myös Entra DS voidaan sammuttaa.

- Kun tietää, että tällainenkin työkalu on olemassa, meillä on yksi kynnys vähemmän matkalla kohti kokonaan pilvipohjaista ja yksinkertaisempaa IT-ympäristöä.

# THANK YOU ALL AND
# A SPECIAL THANKS TO OUR SPONSORS!

PATCH MY PC

Microsoft

PLENTICS

Metropolia

twoday

NETOX

DELL

Workplace Ninja
User Group Finland

intel

# Thank you!