AD integratie

todo



-bestaande AD groepen nakijken, hernoemen en lid maken van de groep Users/Jumpcloud

context

Als je al een werkende AD hebt draaien, ga je geen stap terug zetten. JumpCloud kan niet wat AD kan. Nog niet in de verste verte. Wel kan je AD met JumpCloud laten samenwerken om het beste van 2 werelden te hebben. Zo kan je makkelijker niet-verbonden clients bedienen, LDAP-as-a-service blijven gebruiken voor SSO. Hieronder even de werking uitleggen. Installeren doen we in een afzonderlijk artikel.

werking

Alle import gebeurt via een flinterdun stukje software: **ADImport** (te downloaden op je Jumpcloud portal). Het ding leeft onder C:\Program Files\JumpCloud AD Bridge en heeft:

1. adint.exe: het uitvoerbaar bestand
2. adint.config.json: het configuratiebestand
3. C:\Windows\Temp\JumpCloud_AD_Integration.log: het logboek
4. JumpCloud AD Bridge Agent: de Windows service

Een beetje grafische interface ontbreekt, zodat je alle wijziging moet doen door configuratiebestand aan te passen en de service te herstarten.
Standaard wordt bv logrotatie De waarheid vind je steeds in het logboek.

ADImport importeert AD gebruikers & groepen naar de Jumpcloud directory. Hij synchroniseert daarna onderstaande attributen:

1. naam en voornaam
2. emailadres
3. gebruikersnaam

Nu kan je de gebruikers nakijken in de JC **webconsole** > **Users**.
De eigenlijke bewerkingen kan je nakijken in **INSIGHTS** > **Directory**

Import betekent dat AD PDC de **master** blijft. Alle aanpassingen gebeuren nog steeds in **gebruikers&computers**.

Wachtwoorden

1. elke **wachtwoordwijziging** dient op de Windows clients te gebeuren en wordt doorgegeven aan JumpCloud.
2. van **nieuwe** AD-gebruikers wordt het wachtwoord correct ingelezen door JumpCloud
3. **bestaande** AD-gebruikers die worden geïmporteerd, dienen een **wachtwoordwijziging** te initiëren alvorens het AD-wachtwoord in JumpCloud gekend is.

Gebruikersstatus

- gebruikers die je blokkeert in AD worden **verwijderd** uit Jumpcloud!

Groepen

1. elke ADgroep die je lid maakt van de AD-groep **Jumpcloud** zal via ADImport ook in JumpCloud terechtkomen.

Warning: Je moet de groep dan nog toevoegen aan de Jumpcloud LDAP user directory!!!
Anders zal die niet in LDAP terechtkomen en zal je die niet kunnen gebruikern in LDAP-gebaseerde toepassignen.

Dankzij de ADImport kun je de luxe van je AD behouden en toch de voordelen van LDAP-as-a-service genieten. Je kunt je AD zelfs zo inrichten dat hij gebruikers bevat die niet op je Windows domein aanmelden, maar die je wil in je LDAP moet kunnen opnemen om bv toegang te geven tot een LDAP-enabled web toepassing. Voorzie voor die gebruikers een afzonderlijke OU. Ze kunnen onmiddellijk aanmelden met het wachtwoord dat je voor hen in AD hebt ingesteld en ze kunnen het wachtwoord wijzigen via het JumpCloud gebruiker portaal door aan te melden met het emailadres dat je in AD hebt ingevuld. Kennen ze hun wachtwoord niet meer, dan kan jij het eenvoudig resetten vanuit … AD!

problemen,problemen

wachtwoord AD gebruiker wordt niet bijgewerkt in JumpCloud

logboek toont:

```
ADINT:2019/09/08 11:52:51 jcmap.go:568: Could not update user for
'id=[5d74af5bcc2e4752b2c32a4c] - userName=[pieter] -
email=[pieter@jackland.net] - externally_managed=[true] - sudo=[false]'
err='ERROR: Could not post new JCUser object, err='JumpCloud HTTP response
status='400 Bad Request', body={"status":400,"error":"Password does not
satisfy complexity requirements due to missing special character."}''
```

oorzaak:wachtwoordbeleid in AD verschilt van dat in JumpCloud (dat in dit geval een speciaal teken verwacht).

oplossing: zet het wachtwoordbeleid in JumpCloud gelijk aan dat van AD.

AD gebruiker wordt niet in JumpCloud geïmporteerd.

logboek toont:

```
ADINT:2019/09/08 13:11:28 jcmap.go:533: Could not add a user 'id=[] -
userName=[charel] - email=[charel@jackland.net] - externally_managed=[true]
- sudo=[false]' to JumpCloud, err='ERROR: Could not post new JCUser object,
err='JumpCloud HTTP response status='400 Bad Request', body={"message":"Your
system user count of 10 has been exceeded. Please sign up for paid JumpCloud
service."}''
```

oorzaak:je hebt je maximaal aantal gebruikers bereikt.
oplossing: verwijder onnodige gebruikers of breid je licentie uit

meer weten

- zie JumpCloud KB

From:
https://www.louslab.be/ - **Lou's lab**

Permanent link:
https://www.louslab.be/doku.php?id=jumpcloud:adintegratie

Last update: **2024/11/16 18:14**