

Naam van de G-Clouddienst

ShaD – Shared Directory

01-01-2019

Omschrijving van de G-Clouddienst

ShaD is de centrale identity management oplossing voor G-Cloud diensten. Het systeem laat toe aan gebruikers van verschillende overheidsinstellingen om zich aan G-Cloud toepassingen aan te melden met hun bestaande credentials. En dit met behoud van het eigenaarschap van de eigen lokale directory.

ShaD werd opgezet met volgende principes in gedachten:

- Gemakkelijk gebruikers van verschillende instellingen kunnen identificeren/authentiseren.
- Toelaten om gemeenschappelijke toepassingen te centraliseren op basis van identificatie met AD van de instelling.
- Het beheer van de gebruikersaccounts binnen elke instelling houden.
- Minimale impact op de bestaande AD's van de instellingen.

Op basis van het type applicatie worden verschillende authenticatiemodellen ondersteund:

1. *ShaD Federation Services*

Ondersteunt Single-Sign-On in claims-aware applicaties. Deze service is gebaseerd op een SAML-federatie aan de hand van een AD FS-server die door ShaD wordt onderhouden.

2. *ShaD Online Services*

Verzorgt de connectiviteit naar Azure AD en gebruikersidentificatie in Office 365. Maakt hybride functionaliteiten in UCCaaS mogelijk, waarbij services transparant tussen UCCaaS en Office 365 kunnen gebruikt worden.

Deze dienst is gebaseerd op dezelfde bouwstenen als ShaD Federation op instellingsniveau.

Er is een synchronisatielaag van de AD van een instelling naar Azure AD (Office 365) via Azure AD Connect. Deze diensten worden beheerd door ShaD en moeten gecentraliseerd worden voor G-Cloud Azure AD.

Componenten

Active Directory Federation Services (ShaD-FS)

ShaD onderhoudt een hoogbeschikbare ADFS infrastructuur. Deze infrastructuur biedt authenticatie via het SAML-protocol. Deze service vereist een functionele SAML-server bij de instelling (alleen bereikbaar voor gebruikers).

Het ShaD-team kan ondersteuning en advies geven met betrekking tot de inrichting en het gebruik van de ADFS aan de kant van de instelling, maar neemt geen enkele verantwoordelijkheid met betrekking tot de beschikbaarheid ervan.

Azure AD Connect (ShaD-Online)

ShaD onderhoudt een redundante opstelling van Azure AD Connect. De dienst zal de nodige informatie van uw AD naar Azure AD synchroniseren (enkel de nodige attributen, geen wachtwoorden).

Normale synchronisatie, ook wel Delta synchronisatie genoemd, behandelt alleen verschillen en wordt binnen het uur afgehandeld. In sommige situaties, zoals een upgrade of wijziging in een instellings-AD, is een volledige synchronisatie nodig. Zo'n volledige resync wordt geïnitieerd door ShaD en vereist tot 24 uur.

Service owner

FPD – Luc Coppens – shad@gcloud.belgium.be

Service level agreements

- Beschikbaarheid ShaD FS: 99% (24/7)
- Azure AD Connect Delta Synchronisatie: 1x per uur, 8h/dag, 5d/week (bij volledige synchronisatie 1x / dag)

Kostprijsregeling

Het gebruik van de ShaD-infrastructuur is niet aan kosten onderhevig.

Wat is de voorziene verdere evolutie van de dienst ?

De ShaD dienstverlening zal technologische evoluties en behoeften van G-Cloud volgen.

Een aantal van deze mogelijke evoluties:

- Gebruik van CSAM FAS voor authenticatie
- Vereenvoudigde omgang met gebruikers extern aan ShaD

Praktische info



ShaD-Online vereist een aantal diensten van de AD- en netwerkinfrastructuur van een instelling (eigen AD-controllers op een specifiek netwerk).

Info en aanvragen: shad@gcloud.belgium.be