TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Livre Blanc de Securité

L'Agent HelloID

Table des matières

Introduction

HelloID est une plateforme de gestion des identités (IDaaS) basée sur le cloud. Elle facilite le contrôle d'accès (SSO et MFA) et provisionne les comptes utilisateurs dans les applications et les systèmes informatiques.

Si votre entreprise est basée à 100% sur le cloud, HelloID fonctionne en cloud également.
Pour les organisations qui disposent encore d'un centre de données local (Active Directory, Serveur de fichiers, système de messagerie on-premises, applications métiers, etc.), HelloID propose un **agent** installé sur site.

Cet agent est composé d'un ensemble leger de services Windows installés sur un serveur à l'intérieur du réseau de votre organisation. Il permet la communication avec HelloID. Pour simplifier, il fait office de courtier entre le tenant Helloid dans le cloud et les systèmes locaux. Cela inclut le "load balancing", le "failover" et la supervision.

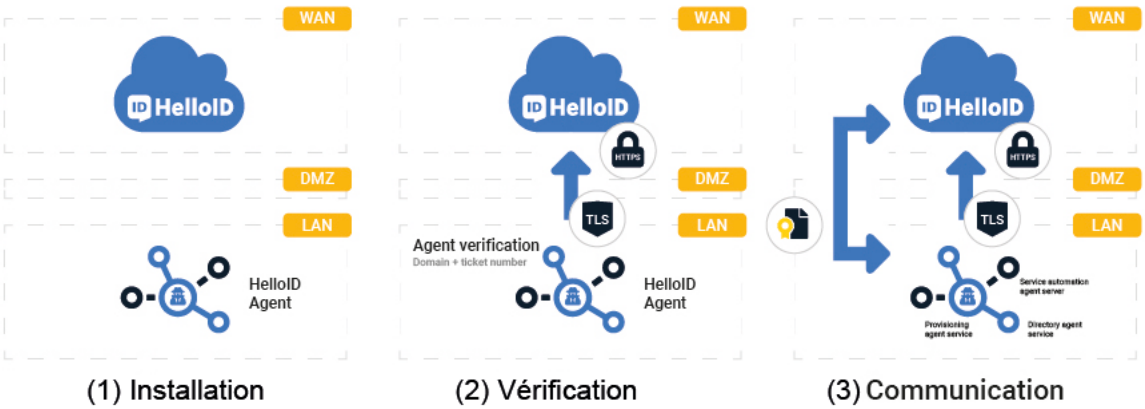
Ce document explique les mesures de sécurité intégrées et appliquées à l'agent, notamment :

- La vérification des jetons avant toute communication,
- Une communication via HTTPS avec cryptage TLS 1.2,
- Et l'authentification par certificat pour tous les points de terminaison.

Pour les prérequis techniques et les procédures d'installation de l'agent, reportez-vous à notre site de documentation technique https://docs.helloid.com. Pour plus de ressources, notamment notre livre blanc sur la sécurité et les garanties des tests de pénétration Deloitte, visitez notre site www.tools4ever.fr/resources

Configuration, vérification et communication de l'Agent

Un processus de configuration décomposé en 3 étapes garantit un chemin de communication sécurisé entre HelloID et l'agent :



Installation

La première étape consiste à installer l'agent (https://docs.helloid.com/hc/en-us/articles/360001597494-Install-or-manage-an-Agent) sur un serveur dans le réseau. Il peut s'agir de n'importe quel serveur membre du domaine avec un accès HTTPS à HelloID. En règle générale, il doit s'agir d'un serveur qui n'est pas un contrôleur de domaine, pour éviter les conflits avec les stratégies de sécurité locales. Les services de l'agent s'exécuteront avec un compte de domaine ayant les droits d'administrateur local du serveur et les droits nécessaires aux actions attendues par chacun des services.

Note : Une ou plusieurs instances d'agents peuvent être installées dans un ou plusieurs pools d'agents. Cela permet une gestion automatique de l'équilibrage de charge et la séparation des tâches.

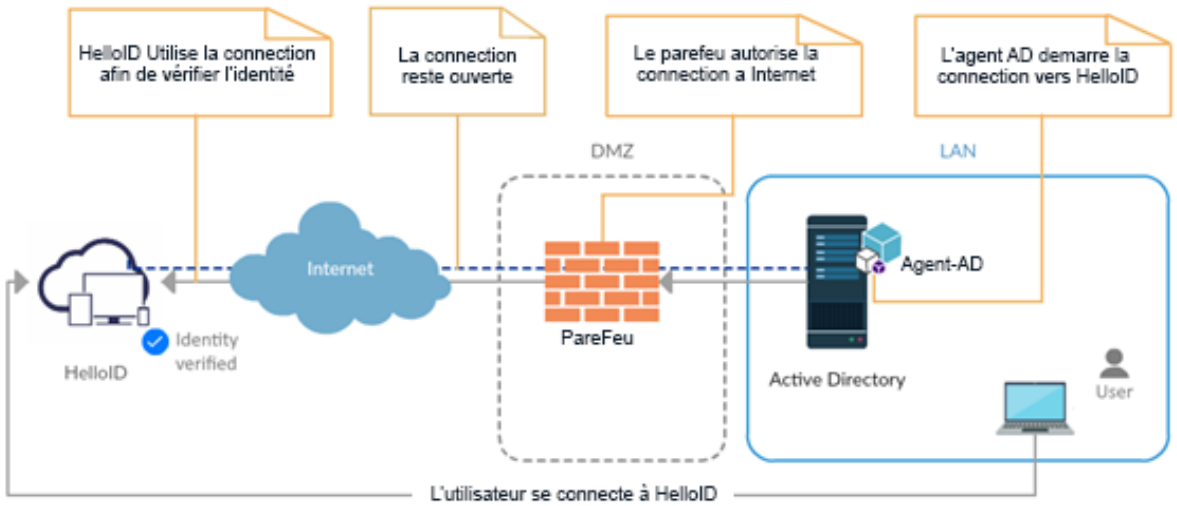
Vérification

Nous nous assurons que votre portail HelloID approuve uniquement la bonne instance de l'agent. Lors de l'installation de l'agent, HelloID génère un numéro de ticket OTP. Ce numéro ne peut être utilisé qu'une seule fois, et seulement dans les 10 minutes suivant sa création. L'administrateur HelloID fournit ce numéro au programme d'installation de l'agent. Un certificat partagé est généré en fonction d'une combinaison de l'OTP, de l'URL du portail et du GUID de l'agent. Par la suite, ce certificat valide chaque tentative de communication entre HelloID et l'agent. Si le certificat ne correspond pas ou si le GUID de l'agent a changé, la communication est impossible.
Si le certificat ou l'agent est copié ou déplacé, la confiance est immédiatement révoquée.

Cette procédure de vérification ne peut être effectuée que par les administrateurs HelloID autorisés à ajouter des agents dans le tableau de bord d'administration HelloID. Pour une sécurité maximale, aucun autre scénario n'est autorisé.

Communication

Après vérification, le portail HelloID et l'agent peuvent communiquer. L'agent HelloID est passif et unidirectionnel. Lorsque l'agent répond à une demande, HelloID vérifie l'adresse IP d'origine. S'il ne correspond pas à l'adresse IP utilisée lors de la vérification, la commande est rejetée et la confiance est immédiatement révoqué.
Aucune ouverture de port de pare-feu ou configuration DMZ spéciale n'est requise.
L'agent communique via le port TCP standard 443. Cependant si vous souhaitez n'accorder que les droits internet à des domaines spécifiques vous trouverez ici (https://docs.helloid.com/hc/en-us/articles/360013014280-Whitelist-Domains) la liste des domaines à approuver par votre proxy.



Les services de l'Agent

L'agent comprend trois services Windows distincts (https://docs.helloid.com/hc/en-us/articles/360013121280) - un pour chaque module HelloID (Provisioning, Service Automation et Access Management). Chaque service peut être exécuté sous son propre compte, avec des paramètres de sécurité différentiels en fonction des besoins de votre organisation.

Access Management

Le service AM utilise HTTPS avec une longue interrogation. Chaque demande reste ouverte pendant 30 secondes. Pendant cet intervalle, le service répond toutes les cinq secondes. La plupart des demandes reçoivent une réponse en moins d'une seconde. Toutes les communications sont cryptées avec des certificats HelloID via TLS 1.2. Chaque demande est vérifiée en fonction du certificat de l'agent et du GUID. Cela garantit que la communication est immédiatement interrompue si l'agent est supprimé dans le tableau de bord d'administration HelloID. Ce service est optimisé pour la stabilité.

Provisioning

Le service Provisioning utilise des **WebSockets** sécurisés pour maintenir une communication ouverte et en temps quasi réel avec HelloID. Une demande HTTPS initiale adressée au portail HelloID est mise à niveau vers un WebSocket sécurisé. Le WebSocket est recyclé toutes les trois heures et dispose d'un battement de 60 secondes pour vérifier si la connexion doit rester ouverte. Toutes les communications sont cryptées avec des certificats HelloID via TLS 1.2.
Chaque demande est vérifiée en fonction du certificat de l'agent et du GUID. Ce service est optimisé pour une communication en temps quasi réel, la stabilité et les performances des demandes en masse.

Service Automation

Le service SA partage les caractéristiques de sécurité du Provisioning. Il est optimisé pour un temps de réponse rapide, afin de proposer aux utilisateurs finaux une expérience dynamique des formulaires HelloID.

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

T4E.FR

Adresse 10-12 Bd Marius Vivier Merle
69003 LYON
FRANCE

Standard + 33 4 78 95 37 98
Fax + 33 4 78 95 38 37

Sales frsales@tools4ever.com
Support frsupport@tools4ever.com

TOOLS4E SOUTH EUROPE

Adresse Ramon Turró 169
08005 BARCELONE
ESPAGNE

Standard + 34 622 213 732

Sales sesales@tools4ever.com
Support frsupport@tools4ever.com