ADSelfService Plus

Architecture de la solution

ManageEngine
ADSelfService Plus

Contenu de ce document

Ce document fournit un aperçu détaillé de l'architecture et des options de déploiement d'ADSelfService Plus. Après avoir lu ce document, vous aurez une meilleure compréhension des différents composants nécessaires au déploiement d'ADSelfService Plus, de l'objectif de chaque composant et de la manière dont ils communiquent entre eux pour activer les différentes fonctionnalités d'ADSelfService Plus.

1. À propos d'ADSelfService Plus

ManageEngine ADSelfService Plus est une solution intégrée de gestion des mots de passe en libre-service et d'authentification unique. Elle offre la réinitialisation des mots de passe et le déverrouillage des comptes en libre-service, l'authentification multifacteur des terminaux, l'authentification unique aux applications d'entreprise, la synchronisation des mots de passe multiplateforme basée sur l'Active Directory, la notification d'expiration des mots de passe et l'application de la stratégie de mot de passe. Elle fournit également des applications mobiles Android et iOS qui facilitent le libre-service pour les utilisateurs finaux, partout et à tout moment.

Il existe différentes méthodes de déploiement pour installer ADSelfService Plus dans votre environnement. En fonction de vos besoins et de la structure de votre réseau, vous pouvez choisir une méthode de déploiement. Ce guide d'architecture a pour objectif de vous présenter les différents composants nécessaires au déploiement d'ADSelfService Plus. Divers scénarios de déploiement du produit ont également été abordés.

2. Composants et pré-requis nécessaires au déploiement d'ADSelfService Plus

Serveur

C'est ici qu'ADSelfService Plus est installé. Le serveur peut être un serveur membre ou un contrôleur de domaine.

Si vous configurez un environnement de haute disponibilité, vous aurez besoin d'un serveur primaire et d'un serveur secondaire. Les deux serveurs doivent avoir installé ADSelfService Plus.

Pour activer l'équilibrage des charges, un serveur primaire et un ou plusieurs serveurs secondaires doivent être configurés. Tous les serveurs doivent avoir installé ADSelfService Plus.

En savoir plus sur les pré-requis matériels et logiciels pour installer ADSelfService Plus.

Base de données

ADSelfService Plus utilise une base de données pour stocker des informations telles que les détails des attributs Active Directory, les données d'audit, les données de configuration du produit, les données d'inscription, etc. Le produit est livré avec une base de données PostgreSQL intégrée. Vous pouvez également utiliser une base de données MS SQL autonome ou une base de données PostgreSQL.

Intégration avec l'Active Directory

L'Active Directory constitue la pierre angulaire d'ADSelfService Plus. La synchronisation programmée des données entre ADSelfService Plus et l'Active Directory est nécessaire pour permettre aux administrateurs de créer diverses stratégies de libre-service et de les appliquer aux OU et aux groupes, d'installer l'agent de connexion sur les ordinateurs du domaine et de configurer diverses fonctions et paramètres à partir du portail du produit. La synchronisation avec l'Active Directory est également nécessaire pour que les utilisateurs finaux puissent effectuer les différentes actions en libre-service.

Portail web ADSelfService Plus

Il existe deux types de portails web ADSelfService Plus :

Portail administrateur : Le portail administrateur permet à l'administrateur de la solution de configurer les paramètres du domaine et de connexion (SSL, serveur proxy, etc.), de créer et d'appliquer diverses stratégies, de déployer l'authentification multifacteur, d'intégrer les applications on-premises et cloud avec la synchronisation des mots de passe et l'authentification unique, et bien plus encore

Portail utilisateur : Le portail utilisateur permet aux utilisateurs de s'inscrire à ADSelfService Plus, d'effectuer les différentes actions en libre-service, de rechercher des employés, de consulter l'organigramme, etc

Composants optionnels et pré-requis

Agent de connexion ADSelfService Plus

L'agent de connexion ADSelfService Plus est un logiciel qui, lorsqu'il est installé sur les ordinateurs du domaine Windows, macOS et Linux, offre aux utilisateurs la possibilité de réinitialiser les mots de passe Active Directory et de déverrouiller les comptes à partir de leur écran de connexion. L'installation de l'agent de connexion active également la fonction d'authentification multifacteur des terminaux pour les connexions Windows, macOS et Linux.

L'agent de connexion peut être poussé sur les ordinateurs clients à l'aide du portail administrateur, des GPO de l'Active Directory, de Microsoft System Center Configuration Manager (SCCM), des solutions tierces de gestion des terminaux comme Desktop Central, ou être installé manuellement.

Agent de synchronisation des mots de passe ADSelfService Plus

L'agent de synchronisation des mots de passe ADSelfService Plus synchronise les changements de mots de passe natifs (changement de mots de passe à l'aide de l'option Ctrl+Alt+Del et réinitialisation de mots de passe à l'aide de la console Active Directory Users and Computers) à travers toutes les applications d'entreprise qui sont intégrées à ADSelfService Plus pour la synchronisation des mots de passe. Il est également utilisé pour appliquer la stratégie de mot de passe personnalisée créée dans ADSelfService Plus lors de ces changements de mots de passe natifs. L'agent de synchronisation des mots de passe doit être installé sur tous les contrôleurs de domaine dans un domaine configuré.

Application mobile ADSelfService Plus

L'application mobile ADSelfService Plus permet aux utilisateurs du domaine d'effectuer des réinitialisations de mots de passe Active Directory et des déverrouillages de comptes à l'aide de leur appareil mobile. Elle permet également aux utilisateurs de s'inscrire à certaines méthodes d'authentification multifacteur. L'application mobile est également utilisée pour recevoir des notifications push pour :

- Notifier les utilisateurs lors de la réussite des actions en libre-service.
- Mots de passe et expiration du compte imminent
- Rappels d'inscription

Intégration avec les applications d'entreprise

Via la synchronisation des mots de passe et l'authentification unique, ADSelfService Plus s'intègre avec diverses applications d'entreprise telles que G Suite, Salesforce, Microsoft 365 et Dropbox. Lorsque la synchronisation des mots de passe est activée, toute modification des mots de passe de domaine des utilisateurs est synchronisée sur toutes les applications intégrées, permettant ainsi à l'utilisateur d'accéder à ces dernières avec un seul mot de passe. Dans le cas de l'authentification unique, si l'utilisateur s'est connecté à son compte ADSelfService Plus, il est automatiquement connecté à ces applications cloud sans avoir à fournir ses identifiants d'utilisateur.

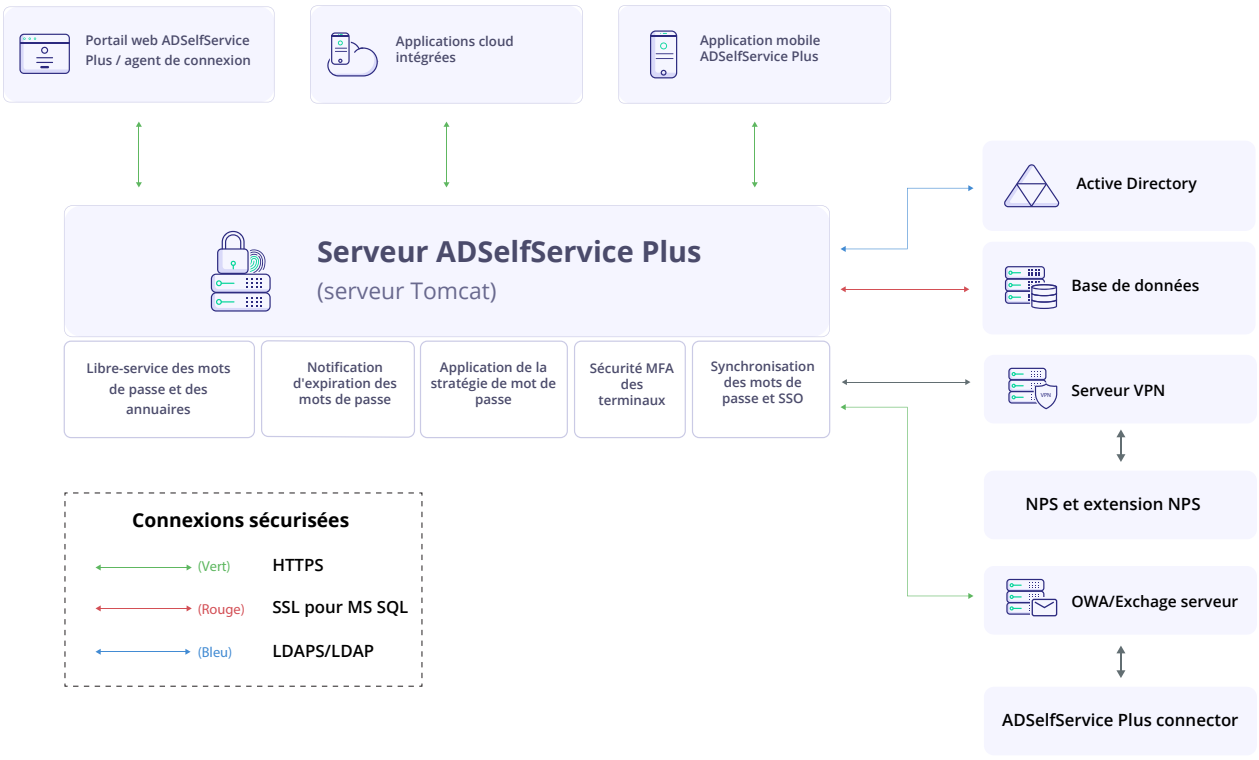
Serveur Microsoft Exchange

Pour configurer le MFA de ADSelfService Plus pour les connexions à Outlook Web Access (OWA) et Exchange admin center (EAC), le connecteur ADSelfService Plus doit être installé dans le serveur OWA/Exchange. Ce connecteur sert d'intermédiaire entre OWA ou EAC et ADSelfService Plus pour activer l'AMF pendant les connexions.

Serveur VPN et NPS

Pour sécuriser vos VPN utilisant la fonctionnalité MFA d'ADSelfService Plus, le serveur VPN doit utiliser un serveur NPS (Network Policy Server) pour configurer l'authentification RADIUS, et l'extension NPS d'ADSelfService Plus doit être installée dans le NPS. Cette extension sert de lien entre le NPS et ADSelfService Plus pour activer la MFA lors des connexions VPN.

Voici une illustration d'un environnement avec ADSelfService Plus déployé :

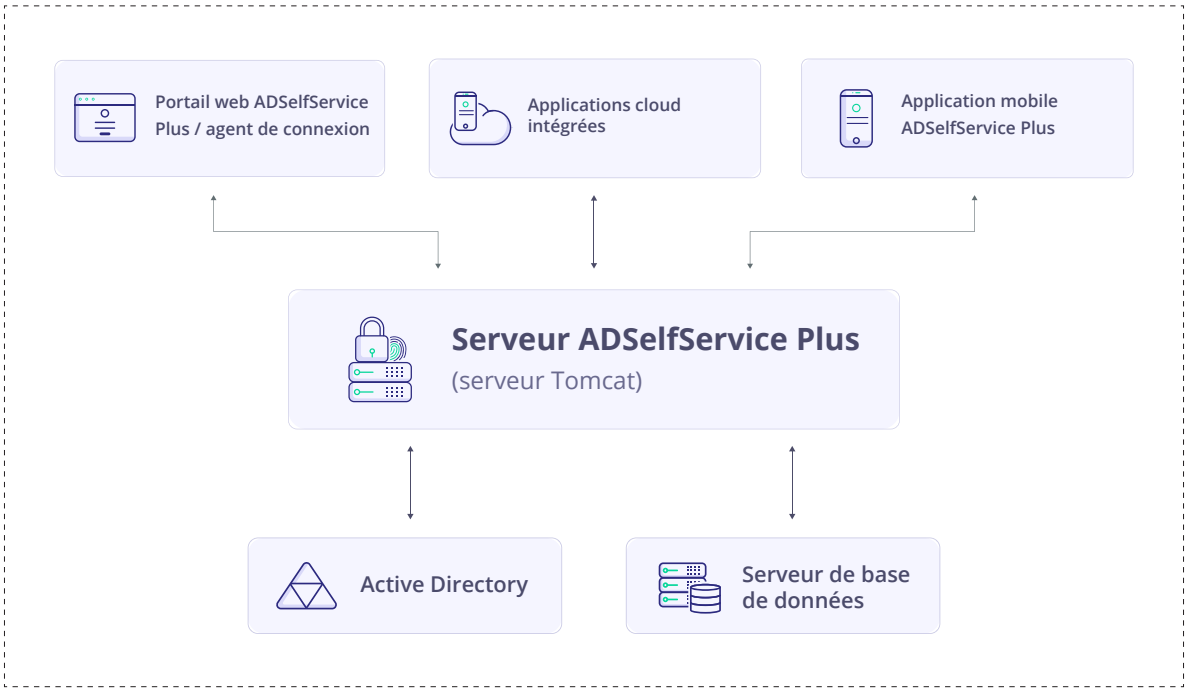


3. Scénarios de déploiement

Voici cinq scénarios qui illustrent les différentes méthodes de déploiement d'ADSelfService Plus :

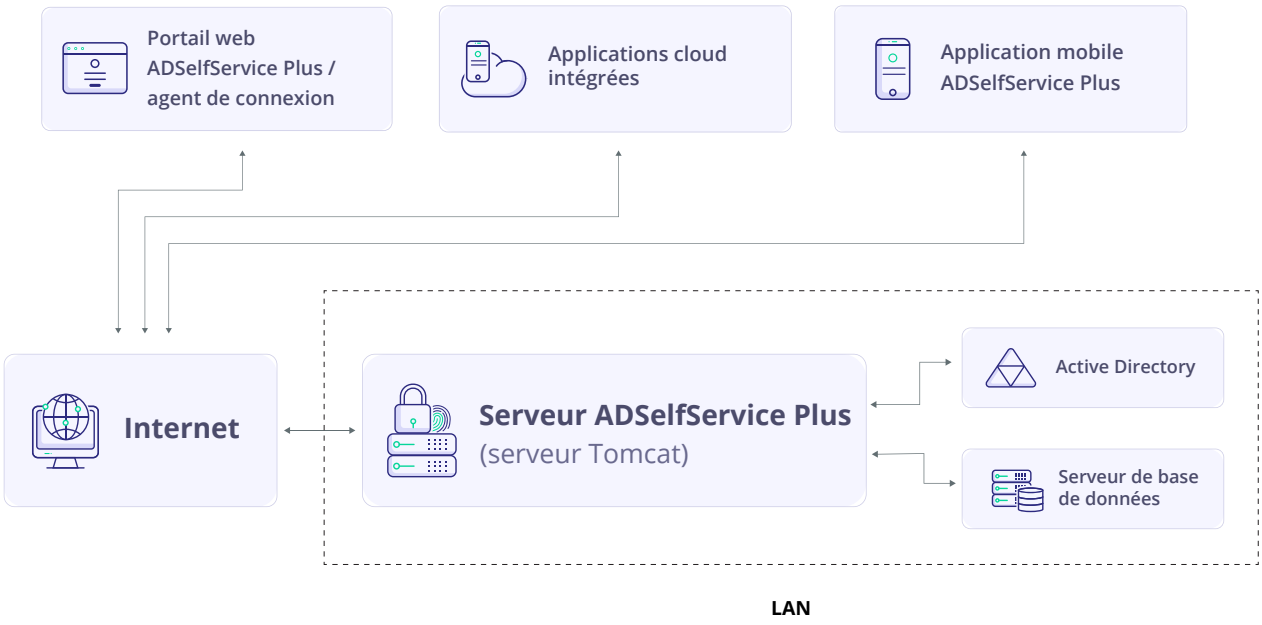
1. Déploiement sur un Intranet

Il est standard de déployer ADSelfService Plus dans l'Intranet de l'entreprise. Dans cette méthode, le portail web ADSelfService Plus, l'agent de connexion et l'application mobile ne sont accessibles que lorsque l'utilisateur est connecté à l'Intranet. Vous trouverez ci-dessous une représentation du déploiement d'ADSelfService Plus sur l'Intranet :



2. Déploiement sur Internet

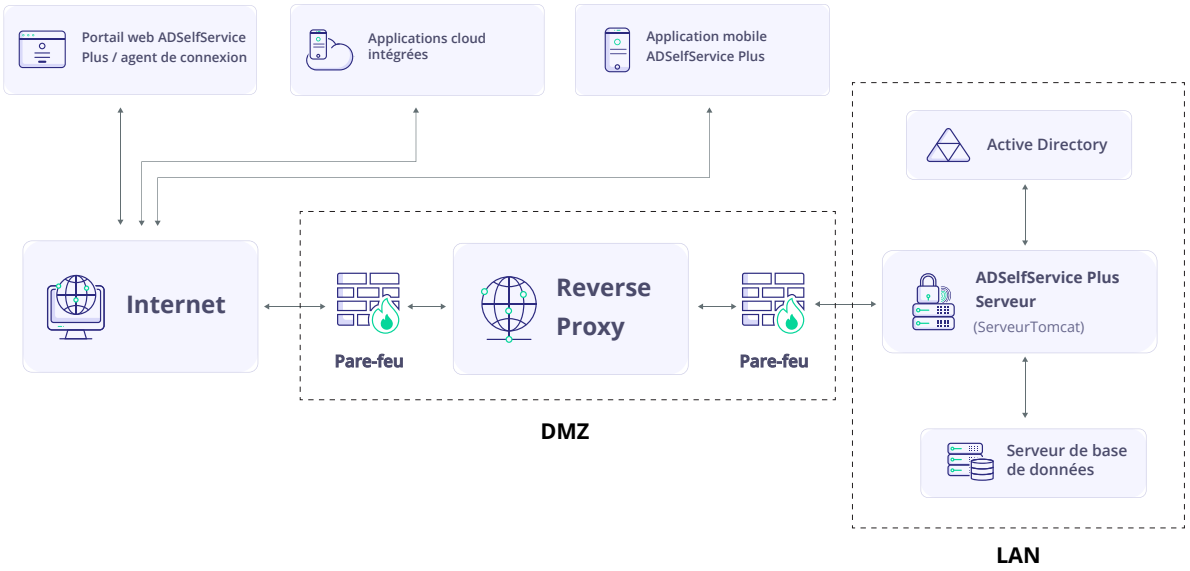
Lorsque ADSelfService Plus est déployé sur Internet, les utilisateurs finaux peuvent se connecter au portail web ADSelfService et à l'application mobile via n'importe quel réseau externe. Il est recommandé que le réseau interne avec le serveur ADSelfService Plus, la base de données et les autres entités déployées soient protégés de l'accès client via Internet en utilisant une DMZ ou un reverse proxy. Voici une illustration du déploiement d'ADSelfService Plus sur Internet :



a. Configuration DMZ

Une DMZ est un sous-réseau qui empêche les clients d'accéder directement au serveur, et par conséquent au LAN interne où le serveur et d'autres composants sont déployés. La DMZ agit comme une barrière entre Internet et le LAN interne où se trouvent le serveur ADSelfService Plus, la base de données et l'Active Directory.

Voici une représentation d'ADSelfService Plus déployé à l'aide de la DMZ :

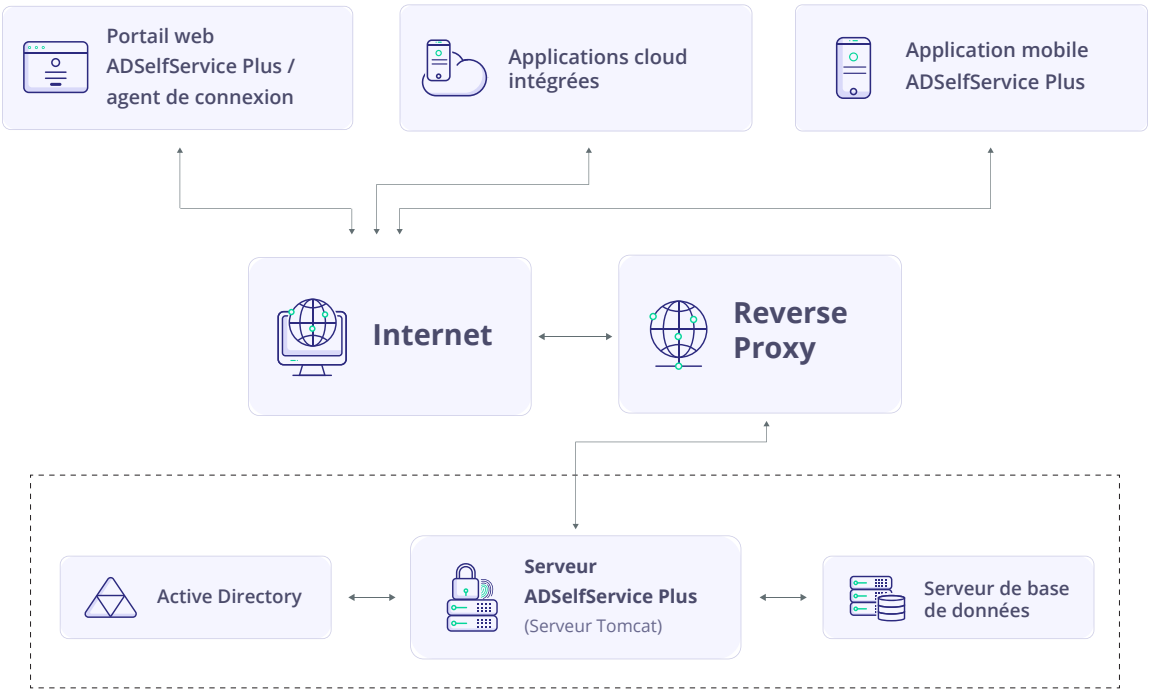


Ici, la configuration DMZ consiste en un reverse proxy qui est protégé des deux côtés par un pare-feu. Le premier pare-feu est configuré uniquement pour autoriser le trafic en provenance d'Internet vers le reverse proxy et le second pare-feu est configuré uniquement pour recevoir les connexions du LAN de l'entreprise vers le reverse proxy.

b. Reverse proxy

Un reverse proxy est un type de serveur proxy qui récupère des ressources au nom d'un client à partir d'un serveur. Ces ressources sont ensuite renvoyées au client, apparaissant comme si elles provenaient du reverse proxy lui-même. Ainsi, le site web ou le service n'a jamais besoin de révéler l'adresse IP de son serveur d'origine. Le reverse proxy dissimule le serveur ADSelfService Plus, les autres composants et le LAN dans lequel ils sont situés des attaques de tiers.

Voici un exemple de déploiement d'ADSelfService Plus avec un reverse proxy :

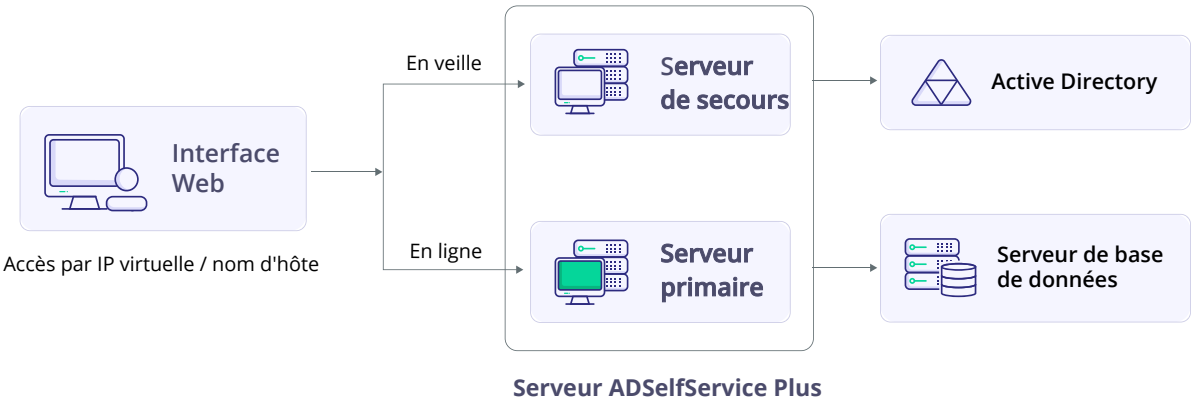


Ici, le reverse proxy a été placé derrière le pare-feu qui sécurise le LAN. Lorsqu'une demande entrante au serveur ADSelfService Plus arrive, le reverse proxy intercepte et envoie la requête au serveur. Il récupère ensuite la réponse et l'envoie au client au nom du serveur.

3. Haute disponibilité

La haute disponibilité est configurée dans ADSelfService Plus pour assurer le basculement en cas de défaillance du système ou de l'application. La haute disponibilité est obtenue par un basculement automatique, c'est-à-dire que lorsque le service s'exécutant sur un serveur tombe en panne, une autre instance du service s'exécutant sur un autre serveur prendra le relais.

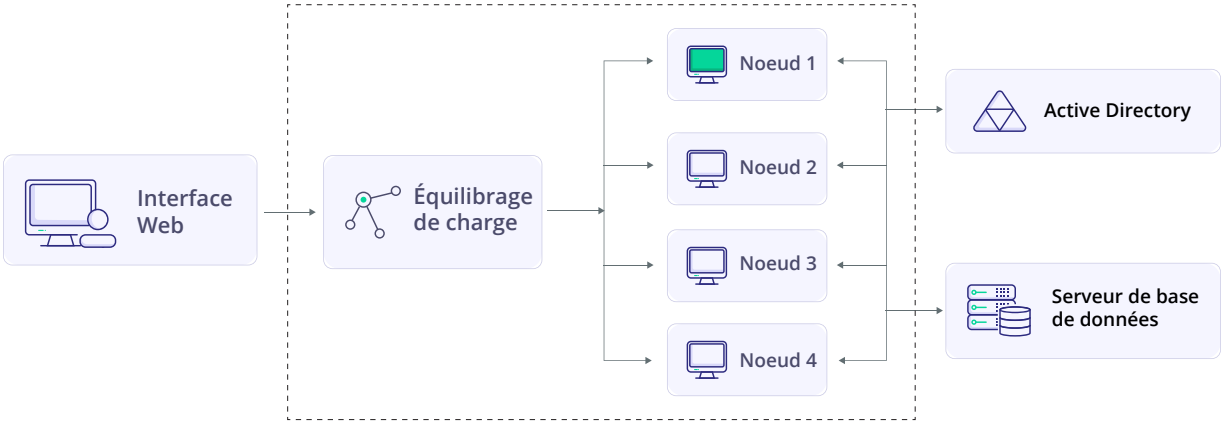
Voici une représentation de l'architecture de l'environnement ADSelfService Plus lorsque la haute disponibilité est configurée :



Lorsque le serveur primaire ne fonctionne plus, l'instance qui s'exécute sur le serveur secondaire prend le relais. Comme les données du serveur primaire sont clonées sur le serveur secondaire lors de la configuration, le basculement est automatique et sans problème. La haute disponibilité permet aux administrateurs et aux utilisateurs finaux d'avoir un accès continu à ADSelfService Plus.

4. Équilibrage de charge

Avec l'équilibrage de charge, les demandes entrantes à ADSelfService Plus sont réparties entre plusieurs nœuds de serveur. Pour activer l'équilibrage de charge dans ADSelfService Plus, un nœud primaire et plusieurs nœuds secondaires doivent être configurés. Voici comment le nœud primaire et les nœuds secondaires sont placés dans l'architecture ADSelfService Plus :



Lorsque des demandes sont adressées à ADSelfService Plus, le nœud primaire répartit les demandes entre les nœuds secondaires à l'aide de la méthode round-robin. L'équilibrage de charge permet d'atténuer la dégradation des performances due à un trafic important et d'améliorer l'expérience des utilisateurs.

Les scénarios expliqués ci-dessus sont un bref guide sur les différentes manières dont ADSelfService Plus peut être déployé dans un réseau. Si vous avez besoin d'aide pour déployer ADSelfService Plus, contactez-nous à helpdesk@pgsoftware.support

À propos ADSelfService Plus

ManageEngine ADSelfService Plus est une solution intégrée de gestion des mots de passe en libre-service et d'authentification unique. Elle offre la réinitialisation des mots de passe et le déverrouillage de comptes en libre-service, l'authentification multifacteur pour les machines et les connexions VPN, l'authentification unique pour les applications d'entreprise, la synchronisation des mots de passe multiplateforme basée sur l'Active Directory, la notification d'expiration des mots de passe et l'application de la stratégie de mot de passe. Elle fournit également des applications mobiles Android et iOS qui facilitent le libre-service pour les utilisateurs finaux, partout et à tout moment. ADSelfService Plus permet de réduire les dépenses informatiques liées aux appels helpdesk, d'améliorer la sécurité des comptes d'utilisateurs et d'épargner aux utilisateurs finaux la frustration due aux temps d'arrêt de leur ordinateur. Pour plus d'informations sur ADSelfService Plus, visitez...

https://www.manageengine.fr/ads

$ Obtenir un devis

Télécharger

+33 805 296 540 Service & appel gratuits

PG Software EUROPE