FICHE TECHNIQUE

Safeguard Authentication Services Single Sign-on for SAP®

Renforcez la sécurité, la confidentialité et la conformité de vos données SAP

Avantages

- Fournit un véritable système d'authentification unique basée sur Active Directory pour les environnements SAP fonctionnant sous Unix ou Linux
- Élimine la transmission des mots de passe des utilisateurs sur le réseau
- Chiffre en toute sécurité les données SAP pendant leur transport sur le réseau
- Fournit une piste d'audit pour les activités d'authentification SAP avec AD
- Simplifie le déploiement sans avoir recours à une infrastructure PKI ou de certificats

Configuration système requise

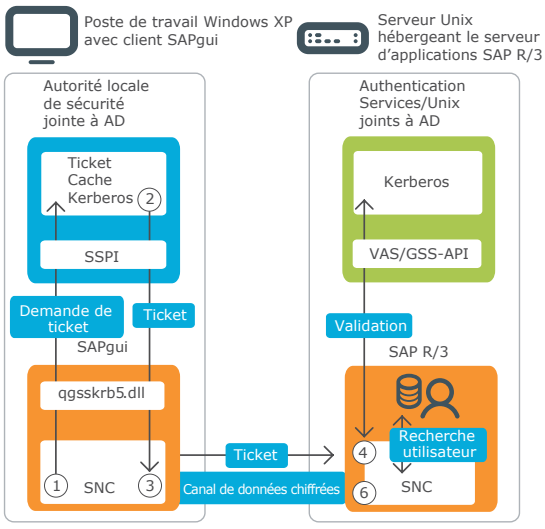
Pour obtenir la liste complète des configurations requises, rendez-vous sur le site www.oneidentity.com/products/safeguard-authentication-services

Pour de nombreuses organisations, les applications et services SAP® sont stratégiques. Toutefois, les applications SAP doivent souvent répondre à des normes strictes exigées par la conformité aux normes en vigueur, les contrôles internes et les bonnes pratiques d'entreprise, notamment :

- S'assurer que seules les bonnes personnes ont accès aux données
- Garantir que ces personnes puissent accéder à SAP
- Sécuriser ces informations stratégiques lorsqu'elles circulent sur le réseau

La solution Single Sign-on for SAP peut aider les organisations à atteindre tous ces objectifs. Malheureusement, l'authentification unique a été difficile à mettre en œuvre, surtout dans les environnements multi-plateformes de plus en plus complexes, du moins jusqu'à aujourd'hui.

One Identity Safeguard Authentication Services Single Sign-on for SAP par Quest fournit une véritable authentification unique pour SAP à l'échelle de l'entreprise. Cette solution permet aux utilisateurs d'authentifier de manière transparente leurs applications SAP sous Windows, Unix et Linux avec les informations d'identification acquises lors de la connexion au réseau, offrant ainsi une alternative économique, éprouvée par les entreprises et standardisée, aux solutions lourdes et complexes de synchronisation ou de méta-annuaire.



1. SAPgui demande un ticket de service Kerberos via le fichier qgsskrb5.dll de One Identity qui traduit les demandes GSS-API vers SSPI.
2. Un ticket généré par le KDC Windows est retourné.
3. Le client SAPgui se connecte au serveur d'applications SAP R/3 en passant le ticket retourné.
4. Le serveur d'applications SAP R/3 valide le ticket via les bibliothèques Authentication Services Unix GSS API.
5. Le nom d'utilisateur principal du ticket Kerberos est associé au compte SAP R/3.
6. Un canal de données chiffrées (facultatif) est établi à l'aide des informations fournies dans le ticket Kerberos.

La solution Safeguard Authentication Services Single Sign-on for SAP fournit une authentification unique sécurisée pour SAP à l'échelle de l'entreprise en permettant aux systèmes Unix ou Linux de « rejoindre » le domaine AD.

Plus précisément, Microsoft® Active Directory® (AD) utilise les standards sectoriels Kerberos et LDAP pour fournir une infrastructure conforme, sécurisée et extensible pour l'authentification, l'autorisation et l'accès. La solution Safeguard Authentication Services Single Sign-on for SAP étend ces fonctionnalités aux utilisateurs de SAP sur les systèmes Unix et Linux en permettant à ces systèmes de « rejoindre » le domaine AD.

La véritable authentification unique qui en résulte élimine les problèmes de gestion des mots de passe, garantissant une expérience utilisateur supérieure, réduisant considérablement la charge de travail administratif et améliorant la sécurité. En outre, la solution Safeguard Authentication Services Single Sign-on for SAP peut protéger les données SAP en transit à l'aide de technologies de chiffrement avancées, ce qui renforce encore la sécurité et la conformité.

Fonctionnalités

Véritable authentification unique pour SAP dans des environnements hétérogènes : Safeguard Authentication Services Single Sign-on for SAP implémente nativement Kerberos et LDAP sur les systèmes Unix et Linux de la même façon que ces normes sont utilisées dans Windows. En créant un « domaine de confiance » unique qui comprend notamment Unix, Linux et Windows, la solution offre une véritable authentification unique pour SAP, et fournit également une piste d'audit pour les activités d'authentification SAP.

Coût total de possession réduit : Safeguard Authentication Services Single Sign-on for SAP étend au reste de l'entreprise la robuste infrastructure AD que vous avez déjà déployée, éliminant ainsi la nécessité d'acheter, déployer et prendre en charge des infrastructures, outils et technologies supplémentaires pour les systèmes non Windows.

Gestion simplifiée des identités : comme les comptes Unix et Windows sont intégrés dans un magasin d'identités (Active Directory) unique, le provisioning et le déprovisioning des comptes Unix peuvent se faire avec les mêmes outils et en même temps que les comptes Windows ; et d'autres fonctionnalités avancées d'administration des identités, telles que la gestion des mots de passe, l'audit et la gestion des rôles, peuvent être centralisées dans AD.

Sécurité robuste et standardisée : l'interface SAP Supply Network Collaboration (SNC) fournit aux clients et serveurs SAP une infrastructure de sécurité et d'authentification indépendante de la plate-forme qui exploite pleinement les mécanismes de sécurité natifs de Windows et Unix. Les clients SAP sous Windows peuvent échanger des jetons d'authentification sécurisés à l'aide de tickets Kerberos avec les serveurs SAP R/3 hébergés sous Unix.

Protection avancée des données : Safeguard Authentication Services Single Sign-on for SAP prend en charge le chiffrement DES et RC4 pour protéger la confidentialité des données lorsqu'elles sont en transit et élimine la nécessité de transmettre les mots de passe des utilisateurs sur le réseau.

Certification SAP : Active Directory et Safeguard Authentication Services Single Sign-on for SAP ont obtenu la certification SAP pour l'interface BC-SNC 4.0. C'est la seule solution SAP certifiée qui assure également l'intégration complète des identités Unix avec Active Directory, ce qui présente l'avantage supplémentaire de permettre aux administrateurs Unix et SAP qui doivent se connecter au serveur R/3 d'utiliser également leurs informations d'identification AD ou de s'authentifier de manière transparente avec un client terminal à authentification unique sur un poste de travail Windows.

À propos de One Identity

One Identity, une entité Quest, aide les organisations à mettre en place une stratégie de sécurité axée sur les identités, aussi bien sur site, dans le Cloud ou dans un environnement hybride. Avec notre vaste portefeuille intégré d'offres de gestion des identités, comprenant la gestion des comptes, l'administration et la gouvernance des identités, ainsi que la gestion des accès à privilèges, les organisations peuvent réaliser tout leur potentiel et bénéficier d'une sécurité efficace grâce à une stratégie axée sur les identités, qui assure un accès adéquat à tous les types d'utilisateurs, tous les systèmes et toutes les données. En savoir plus sur le site OneIdentity.com

Datasheet_SG-AuthServ-SSO4SAP_RS_63084