

Vintela Authentication Services

GESTION INTÉGRÉE DES IDENTITÉS ET DE L'AUTHENTIFICATION EN ENVIRONNEMENT MULTI PLATEFORMES VIA ACTIVE DIRECTORY

«En à peine quinze minutes, j'ai pu étendre le schéma Active Directory, configurer un utilisateur, ajouter un serveur Linux sur le domaine et constater que tout fonctionnait bien lorsqu'un utilisateur s'est connecté à ce serveur Linux en utilisant son identité Active Directory. C'est très impressionnant, surtout lorsque l'on se souvient à quel point ces tâches sont complexes à réaliser manuellement. Aujourd'hui, j'ai réellement le sentiment de disposer d'une solution pour mettre en œuvre l'authentification unifiée à l'échelle de l'entreprise, et pour l'ensemble des plateformes existantes.»

— Bob McCoy
Microsoft Consulting

- **Étend les fonctions d'administration des utilisateurs et des groupes Active Directory aux environnements Unix et Linux**
- **Permet la mise en œuvre effective de l'authentification unique (single sign-on) pour l'ensemble des systèmes**
- **Permet la mise en œuvre d'une politique de gestion des identités au niveau de l'entreprise**
- **Simplifie la gestion des identités**
- **Améliore la sécurité des environnements multi plateformes**
- **Contribue à la mise en conformité du SI aux obligations réglementaires**
- **Constitue la base d'une gestion par règles des configurations Unix et Linux**

Gestion intégrée de l'authentification et des droits d'accès aux ressources Windows, Unix et Linux via Active Directory

Vintela Authentication Services de Quest Software permet la mise en œuvre effective, à l'échelle de l'entreprise, de services d'authentification unifiés (single sign-on — SSO) pour les systèmes Unix et Linux, en s'appuyant sur l'infrastructure de gestion des ressources Windows existantes: Active Directory(AD). Cette solution permet d'intégrer des ressources non-Windows à la zone de confiance «trusted zone» d'Active Directory. Il devient dès lors possible d'étendre aux systèmes Unix et Linux le bénéfice de la sécurité renforcée, d'une gestion unifiée et de règles avancées d'authentification d'Active Directory, à l'échelle de l'entreprise.

Vintela Authentication Services est une solution basée sur les standards. Elle constitue ainsi une alternative particulièrement efficace aux solutions souvent lourdes et complexes de synchronisation des données ou de méta annuaires. Elle permet d'utiliser la même infrastructure, les mêmes procédures et les mêmes compétences mises en place pour la gestion des ressources Windows, pour prendre en compte l'ensemble des ressources Windows, Unix et Linux. L'entreprise y gagne non seulement une sécurité globale renforcée, mais elle prépare aussi efficacement la mise en conformité de sa gestion avec les directives d'entreprise ou les obligations réglementaires en matière de traçabilité et de sécurité.

Avec Vintela Authentication Services, les systèmes Unix et Linux deviennent des membres à part entière de l'infrastructure contrôlée par Active Directory. Facile à déployer, la solution n'exige pas de couche administrative supplémentaire ou spécifique, éliminant ainsi les coûts et la complexité de gestion de technologies dédiées à chaque environnement système existant dans l'entreprise. Vintela Authentication Services contribue à améliorer la productivité des services informatiques tout en réduisant les coûts d'exploitation. La sécurité globale de l'infrastructure, ainsi que sa conformité aux directives d'entreprise ou aux obligations réglementaires, s'en trouvent renforcées. Vintela Authentication Services est en outre livré avec Vintela Group Policy. Cet outil permet de gérer de façon unifiée la gestion des stratégies de configuration des systèmes Windows, Unix et Linux, via le composant Windows Group Policy d'Active Directory (GPO).

Les bénéfices de la solution

Vintela Authentication Services est une solution, facile à déployer, pour étendre es fonctionnalités d'Active Directory aux ressources Unix et Linux.



Vintela Authentication Services

GESTION INTÉGRÉE DES IDENTITÉS ET DE L'AUTHENTIFICATION EN ENVIRONNEMENT MULTI PLATEFORMES VIA ACTIVE DIRECTORY

Extension des stratégies de gestion des utilisateurs et des groupes d'Active Directory aux environnements Unix et Linux

Vintela Authentication Services intègre de façon native les systèmes Unix et Linux, qui deviennent membres à part entière de l'infrastructure Active Directory. Vintela Authentication Services gère l'intégration des systèmes Unix et Linux à des architectures multi domaines, la prise en charge de plusieurs contrôleurs de domaines, et l'authentification entre domaines. La solution étend également aux systèmes Unix et Linux les fonctions de gestion de zones de réplication (Sites) et de groupes imbriqués (nested groups).

Conçue pour simplifier la mise en œuvre d'une solution unifiée d'authentification (SSO) à l'échelle de l'entreprise, Vintela Authentication Services standardise l'exploitation de ces protocoles sur le modèle défini par Active Directory pour la gestion des environnements Windows. De cette façon, les systèmes Linux et Unix sont intégrés à la zone de confiance Active Directory. Les ressources Unix et Linux sont simplement rattachées au domaine Active Directory. L'hôte Unix ou Linux est un membre principal d'Active Directory, capable de s'authentifier auprès d'Active Directory de la même façon qu'un hôte Windows.

Exploitation de l'infrastructure existante pour une stratégie d'entreprise de gestion des identités

Vintela Authentication Services permet d'étendre simplement l'infrastructure Active Directory à toutes les ressources système de l'entreprise. Au lieu de devoir acquérir, déployer et maintenir des composants d'infrastructure et des outils spécifiques pour chaque type de système non-Windows, Vintela Authentication Services fournit aux services informatiques le moyen de consolider les accès aux ressources à l'échelle de l'entreprise, pour une gestion unifiée des authentifications via Active Directory.

Simplification de la gestion des identités

Les solutions de synchronisation des annuaires, ou de méta annuaires induisent mécaniquement de la complexité, une nouvelle couche d'infrastructure et de nouvelles procédures d'administration. Avec Vintela Authentication Services, l'entreprise peut tirer parti de son investissement Active Directory, en y incluant les ressources Unix et Linux. A partir d'une infrastructure déjà déployée, dûment testée et pour laquelle l'entreprise dispose des compétences administratives nécessaires, Vintela Authentication Services permet la mise en place d'une solution puissante, sécurisée et évolutive de gestion des identités et d'authentification à l'échelle de l'entreprise.

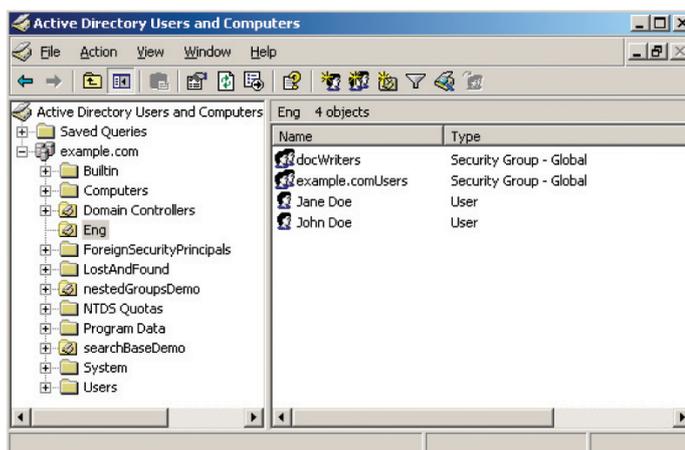
Sécurité renforcée des environnements multi plateformes

En implémentant en mode natif les standards de sécurité d'Active Directory — Kerberos et LDAP —, sur chaque ressource Unix ou Linux, Vintela Authentication Services garantit que toutes les ressources non-Windows bénéficieront du même niveau de sécurité que l'infrastructure Windows gérée par Active Directory, réduisant ainsi l'exposition globale de l'entreprise aux risques de sécurité.

Conformité des systèmes et conformité réglementaire

L'accès sécurisé à un nombre croissant de ressources hétérogènes constitue l'un des défis majeurs auxquels sont confrontés aujourd'hui les entreprises, soumises à des directives internes ou à des obligations réglementaires de plus en plus rigoureuses.

En standardisant au moindre coût, sur Active Directory la gestion des droits d'accès et de l'authentification pour les systèmes Windows, Linux et Unix, Vintela Authentication Services aide l'entreprise à consolider sa stratégie de sécurité et facilite la mise en conformité du système d'information aux obligations réglementaires, notamment en termes d'audit de traçabilité. Contrairement à d'autres solutions, l'approche native de Vintela Authentication Services ne nécessite qu'un investissement minimal, tant en technologies qu'en ressources humaines, et ne modifie ni les procédures ni l'infrastructure mis en place pour gérer l'environnement Windows.



Bases pour une gestion par règles des systèmes Unix et Linux

Vintela Authentication Services intègre une plateforme permettant la mise en œuvre d'une gestion par règles des systèmes Unix et Linux, via Active Directory. Vintela Group Policy, de Quest Software, étend pour la première fois les possibilités de gestion des Group Policy Objects (GPO) d'Active Directory aux systèmes Unix et Linux.

Intégration native des systèmes Unix et Linux dans Active Directory

Microsoft Active Directory est un environnement idéal pour la gestion des identités des droits d'accès aux ressources, parce qu'il met en œuvre efficacement des standards reconnus. Vintela Authentication Services implémente ces mêmes standards — Kerberos et LDAP —. Pour garantir la cohérence de l'ensemble, Vintela Services Authentication associe ces standards Active Directory à des protocoles standardisés, dont Simple Authentication and Security Layer (SASL), Generic Security Services API (GSSAPI), Pluggable Authentication Modules (PAM), Name Service Switch (NSS), et enfin LDAP comme service d'information de réseau (RFC 2307).

Vintela Integration Architecture

Vintela Integration Architecture repose sur l'intégration native de protocoles standards, à l'exclusion de tout autre, seule façon de réaliser la prise en charge des environnements non-Windows par les technologies d'administration Windows. Cette approche autorise la consolidation de l'administration des systèmes autour d'un nombre limité d'outils Microsoft, déjà largement déployés dans les entreprises. L'unification des procédures d'administration simplifie d'autant la mise en conformité des systèmes avec les directives internes ou les obligations réglementaires. La diversité des plateformes, nécessaire à l'évolutivité des systèmes d'information, est préservée sans pour autant compromettre la sécurité globale du système d'information et sans augmenter le coût total de possession (TCO) ou la complexité d'administration. Plus important encore, ce résultat est obtenu sans remettre en cause les caractéristiques fonctionnelles spécifiques aux systèmes non-Windows, et sans modifier ces environnements, grâce à une implémentation native des technologies adaptées à chaque plateforme non-Windows.

Vintela Authentication Services

GESTION INTÉGRÉE DES IDENTITÉS ET DE L'AUTHENTIFICATION EN ENVIRONNEMENT MULTI PLATEFORMES VIA ACTIVE DIRECTORY

Principales Fonctionnalités

Gestion des Sites Active Directory

Les systèmes Unix et Linux rattachés à Active Directory via Vintela Authentication Services détectent automatiquement leur Site Active Directory d'appartenance. Vintela Authentication Services établit la communication avec les contrôleurs de domaines dont il est le plus proche, facilitant l'ajout, sans configuration manuelle spécifique, des ressources Unix et Linux aux topologies de sites Active Directory.

Compatibilité avec Active Directory Nested Group

Les administrateurs d'Active Directory peuvent simplifier l'administration du contrôle d'accès et des droits sur les fichiers Unix en utilisant les groupes imbriqués (nested group) d'Active Directory. Vintela Authentication Services traite de façon transparente les informations des groupes Unix, utilisant l'information PAC des tickets Kerberos délivrés par Active Directory.

Compatibilité avec les stratégies de gestion des mots de passe d'Active Directory

Vintela Authentication Services applique de façon automatisée les stratégies de mot de passe de domaine définies par Active Directory aux systèmes Unix et Linux. Active Directory étant considéré comme le serveur d'authentification, les règles Active Directory relatives à la complexité du mot de passe, ou à la gestion de l'historique, sont appliquées automatiquement, de même que la fonction d'expiration du mot de passe. Comme les ressources Windows, les systèmes Unix et Linux utilisant Vintela Authentication Services relaye l'obligation faite aux utilisateurs de changer son mot de passe au moment de la connexion.

Intégration à la console MMC Active Directory

Vintela Authentication Services est accessible via un composant d'extension (snapin) standard de la console d'administration Microsoft Management Console (MMC) d'Active Directory, tant pour ce qui concerne les utilisateurs que pour ce qui touche aux systèmes. Les administrateurs peuvent ainsi gérer les comptes d'utilisateurs et les groupes Unix à partir de la même interface MMC qu'ils utilisent pour les ressources Windows. Le composant MMC de Vintela Authentication Services intègre un assistant de résolution des conflits d'identifiants Unix, un profil entièrement configurable d'utilisateur par défaut, et des fonctions avancées de filtrage pour appliquer des règles spécifiques aux paramètres des comptes Unix.

Support de domaines multiples Active Directory

Vintela Authentication Services détecte automatiquement l'arborescence des forêts Active Directory, permettant aux utilisateurs de se connecter à des ressources Unix ou Linux appartenant à un autre domaine que le leur. Vintela Authentication Services permet également l'authentification d'utilisateurs rattachés à une forêt Active Directory différente. Ces fonctionnalités garantissent la flexibilité de l'authentification dans le cas d'architectures Active Directory distribuées en domaines de ressources.

Fonctions d'authentification forte Active Directory

Vintela Authentication Services utilise les standards d'authentification forte compatibles avec Active Directory, et notamment les clés de chiffrement 128-bit, plus sécurisées que les clés DES 56-bit utilisées en standard pour Kerberos.

Support automatique de TCP Failover

Les tickets Kerberos délivrés par Active Directory sont en général trop volumineux pour être transmis via UDP, notamment en raison des informations PAC ajoutées au ticket par Active Directory. Vintela Authentication Services offre de façon automatisée une voie de transmission alternative par le protocole TCP lorsque le ticket Kerberos est trop volumineux pour être transmis en UDP.

Contrôle d'accès centralisé

Vintela Authentication Services permet de configurer des règles de contrôle d'accès au niveau des ressources systèmes Unix et Linux, mais également au niveau de chaque service applicatif exécuté sur ces systèmes. Ces règles peuvent être gérées de façon centralisée via Active Directory et sa gestion d'appartenance à des groupes, des domaines ou des unités organisationnelles. Pour l'application de règles spécifiques aux systèmes Unix et Linux, Vintela Authentication Services intègre en outre un composant d'administration dédié, Vintela Group Policy.

Compatibilité avec le mode hors connexion

Vintela Authentication Services utilise une architecture de cache intelligent qui permet aux systèmes Unix et Linux de rester pleinement opérationnels même en cas d'indisponibilité des contrôleurs de domaines. Par ailleurs, l'authentification hors connexion maintient l'accès des utilisateurs à leurs ressources Unix et Linux, même lorsqu'ils sont déconnectés du réseau. Cette fonctionnalité permet de déployer Unix ou Linux sur des postes mobiles, qui continueront à bénéficier hors connexion du même niveau de sécurité.

Support natif Unix et Linux

Le client logiciel de Vintela Authentication Services s'intègre de façon native aux systèmes Linux, HP-UX, Solaris, et AIX platforms, simplifiant ainsi les déploiements et les mises à jour. Les administrateurs peuvent ainsi continuer à utiliser leurs outils habituels pour déployer et configurer le client Vintela Authentication Services.

LDAP sans SSL

Toutes les communications LDAP d'Active Directory sont sécurisées via Kerberos, ce qui élimine l'obligation de recourir à une configuration spécifique de SSL pour Active Directory, et de distribuer des certificats SSL sur les systèmes Unix et Linux.

Compatibilité NIS

Vintela Authentication Services permet aux administrateurs de migrer les informations NIS vers Active Directory (y compris les topologies NIS), tout en maintenant la compatibilité pour les applications NIS clientes, et cela sans remettre en cause la sécurité de l'ensemble.

Compatibilité avec les schémas AD

Vintela Authentication Services est compatible avec plusieurs schémas d'extension Active Directory pour le stockage des informations utilisateurs Unix. La solution de Quest Software est également compatible, sans extension complémentaire, avec les installations existantes Microsoft Services pour Unix. Vintela Authentication Services permet aussi de personnaliser le schéma pour l'adapter à un schéma existant.

Vintela Authentication Services

GESTION INTÉGRÉE DES IDENTITÉS ET DE L'AUTHENTIFICATION EN ENVIRONNEMENT MULTI PLATEFORMES VIA ACTIVE DIRECTORY

Support multi plateformes étendu

Compatibilité Vintela Authentication Services est compatible avec les systèmes Unix/Linux suivants:

- AIX 4.3.3, 5.1, 5.2, et 5.3
- AIX 64 bit pour les versions 5.1 et supérieures
- HP-UX 11i v1 (B.11.11/PA-RISC)
- HP-UX 11i v1.6 (b.11.22/IA-64)
- HP-UX 11.0 (PA-RISC)
- HP-UX 64-bit pour toutes les versions HP-UX
- Solaris 2.6, 2.7, 8, et 9 (Sparc)
- Solaris 8 et 9 (x86)
- Solaris 64-bit pour Solaris 2.7 Sparc et supérieur
- SuSE 8.0, 9.0, et supérieur (x86)
- Suse Linux Enterprise Server 8.0 (IBM P-Series)
- Red Hat 7.3 et supérieur (x86)
- Red Hat Enterprise Linux 2.1/3.0 (x86)

Quest Software France

79, avenue Edouard Vaillant
Bâtiment D
F-92100 Boulogne-Billancourt
Tel : +33 (0)1 41 31 96 96
info@fr.quest.com
www.quest.com



Compatibilité avec les systèmes Kerberos tiers

Vintela Authentication Services permet d'identifier rapidement les applications utilisant l'authentification Kerberos. De plus, Vintela Authentication Services permet le renouvellement de tickets d'authentification pour garantir la validité des scripts à longue durée de vie.

Configuration de groupes non-Unix

Vintela Authentication Services évite les problèmes liés aux capacités limitées d'appartenance à des groupes Unix, en autorisant l'utilisation de groupes non-Unix dans des listes de contrôle d'accès.

Utilitaires de migration des groupes et des utilisateurs

Vintela Authentication Services intègre un outil de génération de script pour créer des utilisateurs et des groupes dans Active Directory, migrer des paramètres de comptes Unix vers Active Directory, ou créer des scripts personnalisés de migration.

Support des identités Unix alternatives

Pour les environnements dans lesquels les utilisateurs disposent de plusieurs configurations de comptes pour des accès différenciés à des ressources ou à des groupes de ressources Unix, Vintela Authentication Services intègre un mécanisme pour personnaliser des paramètres tels que le répertoire racine de l'utilisateur. Ces paramètres personnalisés peuvent être gérés par Active Directory via des stratégies de groupe, ou déployés de façon centralisée avec Vintela Groupe Policy, l'outil de gestion des stratégies fourni avec Vintela Authentication Services.

A propos de Quest Software

Afin d'aider ses clients à faire face à la complexité croissante de leur système d'information et à concilier gain de productivité, adaptabilité et sécurité, Quest Software fournit des solutions logicielles pour simplifier l'administration, optimiser les performances et assurer la disponibilité de leurs applications, bases de données et infrastructures.

Plus de 18.000 clients font confiance à Quest Software dont 1.000 en France.
Pour plus d'information: www.quest.com



©2006 Quest Software, Inc. Tous droits réservés. Vintela Authentication Services, Vintela Group Policy et Vintela Integration Architecture sont des marques déposées de Quest Software. Toutes les autres marques ou noms de produits sont des marques déposées de leurs sociétés respectives. Document non contractuel.

IMG_VAS_DS_AD_01102006