DOSSIER SOLUTION

Comment protéger les identifiants à forts privilèges dans les data centers traditionnels et virtuels, les Clouds privés et publics, et les environnements hybrides ?

ca technologies

La gestion et la protection des identifiants à forts privilèges est indispensable pour limiter les risques et répondre aux exigences de conformité.
Les organisations doivent évaluer l'ampleur des contrôles, l'étendue de la couverture et le degré de correspondance avec le Cloud proposés dans les solutions de gestion des mots de passe à forts privilèges. CA Privileged Access Manager répond à ces trois aspects grâce à une solution nouvelle génération de gestion des identifiants à forts privilèges qui réduit les risques informatiques, renforce l'efficacité opérationnelle et protège les investissements d'une organisation en prenant en charge tant les infrastructures traditionnelles, virtualisées que de Cloud hybride.

Résumé

Défi

La virtualisation et l'adoption du Cloud Computing accentuent l'importance et la complexité d'un problème récurrent : comment gérer et protéger efficacement les mots de passe des comptes à forts privilèges ? La gestion des mots de passe à forts privilèges dans les infrastructures traditionnelles (conteneur réseau sécurisé, serveurs, mainframes, etc.) est un problème de longue date en termes de sécurité et de conformité. La multitude d'identifiants à forts privilèges codés de manière irréversible dans les applications rend ce problème d'autant plus complexe. Parmi ces identifiants, citons les paires de clés SSH et les clés chiffrées au format PEM qui permettent d'accéder aux ressources AWS (Amazon Web Services).

Solution

Grâce à une protection efficace des identifiants à forts privilèges dans une entreprise hybride, une organisation peut limiter les risques d'exploitations externes et internes provenant respectivement de pirates informatiques ou de personnes malveillantes. Aujourd'hui, les organisations qui adoptent des approches de gestion des accès à forts privilèges répondant aux 12 impératifs présentés dans ce document peuvent se prémunir contre de très nombreux risques, ayant tous un rapport avec des comptes à forts privilèges non protégés. Il s'agit notamment des risques liés aux échecs d'audits et aux violations de conformité, à la perte de données stratégiques et aux interruptions de services coûteuses.

Avantages

CA Privileged Access Manager inclut un ensemble complet de commandes permettant de protéger et de gérer tous les types d'identifiants de tous les types de ressources, où qu'elles se trouvent et au fur et à mesure de l'évolution des environnements de Cloud hybride. Les organisations peuvent ainsi réduire les risques, le coût de possession et le coût opérationnel de façon plus importante qu'avec les autres approches, dépourvues de commandes et d'une couverture comparables, et d'un tel alignement avec le Cloud Computing.

Section 1

Notions de base concernant la gestion des mots de passe à forts privilèges

Les mots de passe des utilisateurs à forts privilèges (ci-après dénommés mots de passe à forts privilèges) se distinguent des mots de passe des utilisateurs finaux ordinaires dans la mesure où ils donnent uniformément accès aux ressources les plus sensibles d'une organisation, à savoir les comptes d'administration (admin, root, SYS et sa) et les fonctionnalités connexes utilisées pour configurer et contrôler l'infrastructure informatique d'une organisation. Étant donné les risques encourus, la gestion et la protection de ces identifiants sont bien entendu importantes. Ce point est d'ailleurs confirmé par les nombreuses obligations connexes codifiées dans les standards et réglementations de sécurité couramment invoqués, comme la norme NIST Special Publication 800-53 et la norme PCI-DSS (Payment Card Industry Data Security Standard).

Outre les aspects réglementaires, la gestion des mots de passe à forts privilèges est non seulement intéressante en termes de gestion des risques, mais également indispensable pour endiguer la pléthore de pratiques non fiables couramment rencontrées dans les organisations. Parmi les problèmes les plus fréquents, citons les mots de passe faibles, hors service ou aisément accessibles (car notés sur un post-it ou dans une feuille de calcul), la multiplicité ou la divulgation des mots de passe, l'absence d'attribution claire des comptes partagés, l'impossibilité d'une authentification forte ou d'une révocation centralisée.

D'après le rapport 2015 « Verizon Data Breach Investigations Report », 95 % des violations de sécurité seraient dues à des identifiants volés. Dix autres pour cent résultent d'une utilisation abusive de ces informations par des membres internes « de confiance ».[1]

Le problème ne repose pas tant sur ces mots de passe que sur les risques qu'ils induisent, tels que les attaques par hameçonnage, les attaques ciblées et, en fin de compte, les vols de données, sans parler des violations de conformité. Toujours sceptique ? D'après le rapport 2015 « Verizon Data Breach Investigations Report », 95 % des violations de sécurité seraient dues à des vols d'identifiants. Dix autres pour cent résultent d'une utilisation abusive de ces informations par des membres « de confiance ».[1] Ces conclusions montrent sans équivoque pourquoi il est important que les organisations s'appuient aujourd'hui sur une solution d'entreprise comme CA Privileged Access Manager pour gérer et protéger les identifiants à forts privilèges et pour les contrôles d'accès.

L'impact du Cloud hybride

Les problèmes traditionnels énoncés précédemment ne sont que la partie émergée de l'iceberg. Au vu des nombreux avantages en termes de coût, d'adaptabilité et de réactivité des configurations de Cloud hybride, dans lesquelles les services informatiques et les applications s'appuient sur une infrastructure traditionnelle et virtualisée englobant l'entreprise et les data centers du Cloud, leur adoption massive ne fait aucun doute. Malgré tous ces avantages, les Clouds hybrides font apparaître de nouvelles problématiques en matière de gestion des mots de passe à forts privilèges :

- Augmentation du volume/de l'évolutivité : avec les exigences opérationnelles et la facilité de déploiement des machines virtuelles, un nombre croissant d'entités ont besoin d'accès à forts privilèges (et par conséquent, de mots de passe à forts privilèges)
- Périmètre étendu : la puissance conjuguée des consoles de gestion de la virtualisation et du Cloud introduisent un nouveau type de ressource/compte à forts privilèges
- Dynamisme accru : il est désormais possible d'ajouter de nouveaux serveurs/systèmes à la demande, voire en bloc (10, 20 ou plus en même temps)
- Possibilité de créer des blocs d'identités puisque chaque service Cloud dispose de son propre référentiel d'identités et de sa propre infrastructure[2]

Au-delà des problèmes posés par le Cloud hybride, les responsables de la sécurité informatique doivent également tenir compte de deux autres aspects des mots de passe à forts privilèges lors de l'évaluation des solutions. Tout d'abord, ils doivent tenir compte des cas d'utilisation poste-à-poste et application-à-application (A2A) dans lesquels les mots de passe utilisés par un système ou une application pour accéder à un autre système ou à une autre application sont codés de façon irréversible dans l'application initiale ou mis à sa disposition dans un fichier de configuration en texte brut. La seconde difficulté, trop souvent négligée, résulte du fait que la plupart des organisations peuvent également disposer de milliers de clés (par exemple, pour les implémentations SSH). Or, même s'il ne s'agit pas de mots de passe traditionnels basés sur des phrases, ces clés continuent à servir d'identifiants pour accéder aux comptes à forts privilèges et, par conséquent, doivent encore faire l'objet d'une gestion et d'une protection pour limiter les risques qui leur sont associés.

En conséquence, à l'heure des Clouds hybrides, la gestion des mots de passe à forts privilèges s'avère aujourd'hui plus importante et complexe que jamais.

Section 2

La solution de gestion des accès à forts privilèges de CA Technologies

CA Privileged Access Manager est une solution complète de gestion des identités à forts privilèges. De ce fait, outre les fonctionnalités de contrôle d'accès, de supervision et de consignation des activités des utilisateurs à forts privilèges dans des environnements de Cloud hybride, CA Privileged Access Manager intègre les fonctionnalités indispensables d'une solution nouvelle génération pour la gestion des mots de passe à forts privilèges. En fait, il est important que les équipes de sécurité informatique admettent que, bien que la gestion et la protection des mots de passe soient pertinentes en soi, elles permettent d'atteindre un objectif bien plus vaste. Ces deux opérations constituent plus exactement la première étape (ou une étape complémentaire) d'un processus plus large, mais tout aussi important, qui consiste à contrôler et à gérer les accès aux ressources à haut risque. Si la distinction semble subtile, c'est surtout parce que, dans la pratique, les implémentations fonctionnelles de mécanismes d'authentification (comme les mots de passe) et de contrôle d'accès vont rarement l'un sans l'autre. Elles sont donc souvent associées dans notre esprit.

Quoi qu'il en soit, les objectifs des fonctionnalités de gestion des mots de passe à forts privilèges de CA Privileged Access Manager sont par définition identiques à ceux appliqués dans le reste de la solution. Nous cherchons plus particulièrement à proposer une solution offrant un ensemble complet de commandes et de fonctionnalités applicables à un ensemble exhaustif de cibles et de cas d'utilisation, mais surtout de façon cohérente avec les options, pratiques et architectures de livraison propres à l'ère du Cloud.

Des contrôles exhaustifs

Pour évaluer les solutions de gestion des mots de passe à forts privilèges, nous vous recommandons de vérifier en premier lieu si elles intègrent un ensemble complet de commandes qui permettront à l'équipe de sécurité d'éviter les risques induits par les approches traditionnelles en matière de création, de gestion et d'utilisation des identifiants administratifs stratégiques. Il est plus particulièrement important d'examiner les fonctionnalités de détection, de mise en chambre forte, d'application des politiques et de récupération, et la capacité à prendre en charge en toute transparence l'implémentation d'une solution complète de gestion des accès à forts privilèges.

Section 3

Les 12 fonctionnalités indispensables en matière de gestion des accès à forts privilèges

N° 1. Détection automatisée/facilitée

Sans dispositif de détection automatisée ou facilitée, la gestion des mots de passe à forts privilèges peut être coûteuse. Elle peut également conduire à des situations délicates quand, en raison d'erreurs ou d'omissions, l'environnement informatique d'une organisation peut facilement devenir la cible d'attaques sophistiquées. Pour cette raison, CA Privileged Access Manager inclut différentes méthodes de détection des appareils, des systèmes, des applications, des services et des comptes, et elle s'appuie notamment sur les associations de ports connues, les informations d'annuaire, les consoles de gestion et les API. CA Privileged Access Manager exploite ainsi les API disponibles pour les solutions de gestion de la virtualisation et du Cloud prises en charge afin d'alerter les administrateurs de la création de nouvelles machines virtuelles. Par ailleurs, cette solution facilite l'importation en bloc des listes système à partir de fichiers texte et la création d'entrées ad hoc via la console de gestion. Pour finir, il convient de comprendre que, par définition, nous avons choisi d'écarter les techniques de détection moins fiables (et potentiellement plus risquées) basées sur des agents qui s'accrochent à la pile TCP locale ou la bloquent.

N° 2. Mise en chambre forte/stockage sécurisé

Une chambre forte chiffrée offre un point de contrôle centralisé et permet d'éliminer les méthodes de stockage non sécurisées (comme les feuilles de calcul) par le biais desquelles les identifiants sont facilement partagés et usurpés. La chambre forte CA Privileged Access Manager est une solution conforme à la norme FIPS 140-2 de niveau 1 qui offre un espace sécurisé. Elle s'appuie en effet sur le chiffrement AES 256 bits pour sécuriser tous les types d'identifiants et pas uniquement les mots de passe. Autres fonctionnalités remarquables de la solution :

- Possibilité d'utiliser les modules de sécurité matérielle (HSM) intégrés, comme ceux de SafeNet et de Thales, pour réaliser une implémentation FIPS 140-2 de niveau 2 ou 3. Cette fonctionnalité est particulièrement utile pour les clients prudents ou très exposés et dans certains cas, pour les clients impliqués dans des systèmes bancaires et financiers pour lesquels il est judicieux de stocker séparément les identifiants chiffrés et les clés utilisées pour ce faire. Plusieurs possibilités de déploiement sont supportées : appliances matérielles CA Privileged Access Manager avec cartes PCI intégrées, appliances virtuelles CA Privileged Access Manager appelant des appliances HSM liées au réseau, et appliances CA Privileged Access Manager de tout type appelant une offre HSM-As-A-Service AWS.
- Des routines cryptographiques en boîte blanche éprouvées protègent les clés de chiffrement pendant leur utilisation (c'est-à-dire, en mémoire) sur un système. Cette approche entend empêcher les pirates informatiques de saisir/dérober les clés en supervisant les API cryptographiques standard et la mémoire, et en déjouant les alternatives inférieures basées sur la fragmentation ou le simple masquage des clés. L'ajout de cette technologie est particulièrement important pour les scénarios d'utilisation A2A dans lesquels le système accédant doit également mettre en chambre forte les identifiants et est davantage susceptible d'être usurpé (en raison de sa relative exposition).

N° 3. Application automatisée des règles

CA Privileged Access Manager automatise la création, l'utilisation et la modification des mots de passe, éliminant ainsi la tendance qu'ont les utilisateurs à réutiliser des mots de passe ou à employer des mots de passe faibles (faciles à mémoriser). Avec CA Privileged Access Manager, des règles flexibles peuvent être paramétrées pour renforcer la complexité des mots de passe, implémenter les obligations de changement comme le renouvellement des mots de passe après un certain délai (par exemple, tous les jours ou toutes les semaines) ou en réponse à un événement spécifique (par exemple, après chaque utilisation). Des règles peuvent être également définies pour régir l'utilisation des mots de passe (par exemple, en autorisant l'accès uniquement pendant les créneaux spécifiés ou en demandant plusieurs autorisations pour accéder au mot de passe). Comme ces règles peuvent être appliquées de façon hiérarchique à des groupes de ressources cibles, il est possible de prendre en charge diverses obligations et fonctionnalités pour des cibles différentes. Leur application est également dynamique puisque toutes les ressources ajoutées à un groupe héritent automatiquement des règles de ce groupe. En arrière-plan, CA Privileged Access Manager interagit aussi directement avec les ressources cibles concernées pour veiller à ce que les identifiants restent synchronisés (lorsqu'ils sont modifiés d'un côté, la modification est prise en compte de l'autre).

N° 4. Récupération, présentation et utilisation sécurisées

La mise en chambre forte d'identifiants à forts privilèges est inutile si ces informations ne peuvent pas être également récupérées et utilisées de façon sécurisée. La première étape de cette procédure consiste à authentifier de façon précise qui ou ce qui (dans le cas d'applications et de scripts) cherche à accéder aux identifiant ou à les utiliser. Pour ce faire, CA Privileged Access Manager s'appuie pleinement sur votre infrastructure d'identité existante, via une intégration à Active Directory et à des annuaires LDAP, ainsi que sur des systèmes d'authentification RADIUS. Le support est également assuré pour les éléments suivants :

- Jetons à deux facteurs (par exemple, via CA Advanced Authentication ou d'autres solutions comme RSA et SafeNet)
- Certificats X.509/PKI
- Des cartes PIV (Privileged Identity Verification, vérification des identités à forts privilèges) ou CAC (Common Access Card, carte d'accès commun) sont nécessaires pour la mise en conformité avec les réglementations HSPD-12 et OMB-11-11 du secteur fédéral
- SAML
- Techniques multifacteurs composites (par exemple, combinaison de mots de passe avec des jetons RSA)

Selon le mode de fonctionnement choisi, CA Privileged Access Manager présente ensuite les identifiants demandés au système cible pour le compte de l'entité demandant l'accès (utilisateur ou application). Cette approche présente d'autres avantages en termes de sécurité. Tout d'abord, contrairement aux solutions d'archivage et d'extraction simples, les identifiants ne sont jamais divulgués ni présentés à l'entité qui demande l'accès. Le risque d'exposition est ainsi considérablement réduit. Par ailleurs, comme l'authentification auprès du système cible est entièrement automatisée et que les utilisateurs n'ont jamais à gérer ni à mémoriser leurs mots de passe, des règles peuvent être mises en œuvre pour renforcer considérablement la complexité des mots de passe. Comme tous les accès passent par CA Privileged Access Manager, cette solution peut également assurer l'attribution complète des activités des utilisateurs à forts privilèges, même pour des comptes administrateur partagés.

Pour être complet, notons également que toutes les communications réseau entre les entités demandant un accès, CA Privileged Access Manager et les cibles gérées font l'objet d'un chiffrement SSL. Par ailleurs, CA Privileged Access Manager prend en charge un autre mode de fonctionnement dans lequel les entités demandant un accès peuvent récupérer et envoyer directement les identifiants demandés aux systèmes cibles.

N° 5. Transition transparente vers une gestion complète des accès à forts privilèges

CA Privileged Access Manager met à la disposition des organisations initialement axées sur la seule gestion des mots de passe tout ce dont elles ont besoin pour évoluer vers une gestion des accès à forts privilèges et ce, dès qu'elles en

éprouvent le besoin. Exemples de fonctionnalités les plus notables mises à la disposition des services de sécurité informatique :

- Contrôle granulaire des accès basé sur les rôles et workflows associés (par exemple, pour demander ou valider des autorisations supplémentaires)
- Établissement automatisé de la connexion/session avec les ressources cibles (avec support pour RDP, SSH, Web ainsi que pour plusieurs autres modes/options d'accès)
- Supervision en temps réel des sessions utilisateur à forts privilèges et application, sur la base de règles, des activités autorisées et refusées (par exemple, commandes pouvant être utilisées par un utilisateur donné)
- Journalisation, avec intégration SIEM syslog
- Enregistrement complet d'une session à l'aide de commandes de lecture rappelant celles d'un lecteur de DVD et permettant de passer directement aux événements recherchés
- Prévention des sauts qui empêche les utilisateurs de contourner leurs autorisations en s'appuyant sur des cibles accessibles afin d'accéder à d'autres cibles non autorisées

L'implémentation de ces fonctionnalités supplémentaires est très simple. CA Privileged Access Manager propose l'ensemble de ces fonctionnalités de gestion des mots de passe à forts privilèges et de contrôle d'accès dans une solution unique, étroitement intégrée. CA Privileged Access Manager assure également une gestion unifiée des règles dans l'ensemble de la solution, pour une simplification accrue de l'implémentation et de l'administration.

Couverture étendue

Le second aspect qu'il est important d'examiner avant de choisir une solution de gestion des mots de passe à forts privilèges est l'étendue de la couverture proposée. Autrement dit, pour l'ensemble de commandes identifiées précédemment, quels types d'entités en attente d'un accès, d'identifiants et de système cible la solution prend-elle en charge ?

N° 6. Couverture complète pour les cibles traditionnelles

CA Privileged Access Manager inclut un large éventail de connecteurs système cibles assurant l'intégration immédiate de tous les types d'infrastructures informatiques, périphériques réseau, systèmes et applications :

- Domaine Windows®, Administrateur local et Comptes de services
- Distributions Linux® et UNIX® courantes
- AS/400
- Périphériques réseau Cisco et Juniper
- Systèmes Telnet/SSH
- SAP
- Remedy
- Bases de données ODBC/JDBC
- Systèmes et serveurs d'applications

CA Privileged Access Manager est une solution extensible qui inclut également des fonctionnalités de personnalisation souples pour permettre aux organisations d'étendre plus facilement leur support aux systèmes propriétaires et développés en interne.

N° 7. Prise en charge des consoles de gestion de la virtualisation et du Cloud

Les possibilités immédiates de gestion et de protection des identifiants de CA Privileged Access Manager ne se limitent pas aux cibles traditionnelles. Elles s'étendent également aux solutions de virtualisation et de Cloud populaires comme VMware vSphere, VMware NSX, Amazon Web Services et Microsoft® Online Services. Par ailleurs, les fonctionnalités applicables à ces solutions ne sont pas limitées aux seules instances des machines virtuelles, applications et services associés. Leur couverture s'étend également aux consoles de gestion correspondantes qui, en raison de la puissance commandée, doivent être reconnues de plein droit en tant que ressources à forts privilèges.

N° 8. Prise en charge de l'authentification poste-à-poste

Comme évoqué précédemment, l'homme n'est pas le seul à utiliser des identifiants à forts privilèges. Dans la plupart des organisations, un grand nombre d'applications et de systèmes sont aussi autorisés à accéder à des ressources stratégiques, tels que d'autres applications ou des bases de données. Pour ce faire, les identifiants associés sont généralement intégrés dans le code de l'application demandant un accès ou mis à disposition au démarrage via un fichier de configuration. Notez qu'aucune de ces solutions n'est réellement sécurisée ni facile à gérer. CA Privileged Access Manager propose une couverture pour ces scénarios d'utilisation d'application-à-application en permettant aux développeurs d'injecter un client léger CA Privileged Access Manager dans leurs applications. Cette approche donne lieu à des applications à forts privilèges comprenant tous les composants nécessaires à leur enregistrement auprès de CA Privileged Access Manager, à la récupération dynamique des mots de passe demandés et à leur protection en mémoire sur le système local. Par ailleurs, plusieurs mécanismes permettent d'authentifier ces applications à forts privilèges et de vérifier leur intégrité avant que CA Privileged Access Manager ne diffuse les identifiants demandés.

En s'appuyant sur CA Privileged Access Manager pour les scénarios A2A, les organisations peuvent éliminer les identifiants A2A exposés ou non fiables en les regroupant dans une chambre forte, automatiser la gestion des identifiants A2A et l'application des règles, et simplifier les activités d'audit et de mise en conformité.

N° 9. Prise en charge de la gestion des clés

Parallèlement à la prise en charge des opérations cryptographiques, un grand nombre de types de clés servent également de jetons pour confirmer les identités. Bien que ces clés ne constituent pas des mots de passe à proprement parler, elles agissent comme tel et restent soumises aux mêmes menaces, risques et problématiques, comme leur copie, leur partage, leur exposition fortuite et peuvent être des portes dérobées non auditées. Ces clés étant généralement intégrées ou utilisées de façon transparente dans les solutions pour masquer leur complexité aux utilisateurs, elles ont également plus de chances de ne plus être utilisées et/ou de proliférer avec le temps. Il est donc recommandé d'appliquer bon nombre des contrôles utilisés pour gérer et protéger les mots de passe à ces nouveaux identifiants. Meilleures pratiques recommandées pour déjouer les menaces connexes :

- Déplacer les clés autorisées dans des emplacements protégés
- Procéder régulièrement au renouvellement de toutes les clés (pour garantir la fin éventuelle d'un accès en cas de perte de clés)
- Application de restrictions de sources pour les clés autorisées[3]
- Application de restrictions de commandes pour les clés autorisées

CA Privileged Access Manager inclut des commandes et d'autres fonctionnalités permettant de prendre en compte des types d'identifiants supplémentaires comme les clés SSH et les clés PEM utilisées pour accéder aux ressources AWS et aux consoles de gestion. CA Privileged Access Manager peut donc utiliser les types d'identifiants suivants : (1) mis en chambre forte, (2) renouvelés et contrôlés par des règles configurées et (3) récupérés, puis utilisés de manière à minimiser les risques de vol ou d'exposition.

Fourniture à l'ère du Cloud

À l'ère du Cloud hybride, l'efficacité d'une solution de gestion des mots de passe à forts privilèges repose également sur un facteur très important : sa capacité d'adaptation non seulement d'un point de vue physique, mais également en termes d'alignement avec les besoins et capacités réseau du Cloud.

N° 10. Options de livraison sur site, sur une machine virtuelle et dans le Cloud

CA Privileged Access Manager propose trois possibilités de déploiement pratiques pour aider les organisations à s'adapter aux architectures de Cloud hybrides complexes :

- Appliance physique renforcée, disponible dans plusieurs modèles pour le montage en rack traditionnel dans le data center de l'entreprise
- Instance AMI (Amazon Machine Instance) préconfigurée en vue d'un déplacement avec l'infrastructure Amazon EC2
- Appliance virtuelle OVF, prête à l'emploi et préconfigurée pour un déploiement dans des environnements VMware

Indépendamment des options de déploiement retenues, les organisations disposent d'une solution pour gérer l'intégralité de leur infrastructure Cloud hybride.

N° 11. Architecture et approche alignées sur le Cloud

L'architecture de CA Privileged Access Manager a été spécialement conçue pour intégrer de nombreuses fonctionnalités, ce qui fait de cette solution un composant intéressant dans les environnements de Cloud hybrides. Voici trois exemples :

- Détection et protection automatiques : dans les environnements Cloud hybrides, les opérateurs peuvent créer (ou supprimer) le nombre de systèmes voulus à l'aide d'une seule commande. CA Privileged Access Manager tient compte de cette situation en exploitant les API applicables pour détecter automatiquement les ressources virtualisées et Cloud, puis fournir (ou retirer) les identifiants et les règles de gestion des accès appropriées.
- Suppression des blocs d'identité (par exemple, fédération des identités). Pour éliminer les blocs d'informations d'identité, CA Privileged Access Manager tire pleinement parti de l'infrastructure d'identité utilisée dans l'organisation. Pour les implémentations AWS, il est également possible de supporter des utilisateurs provisoires. Cette approche permet aux organisations de ne pas devoir conserver des informations d'identité séparées dans le sous-système de gestion des accès et des identités AWS.
- Activation de l'automatisation : une API complète autorise l'accès et l'automatisation des programmes de l'ensemble des fonctions de CA Privileged Access Manager (par exemple, par des systèmes de gestion et de coordination externes).

N° 12. Évolutivité et fiabilité compatibles avec le Cloud

La gestion des identifiants à forts privilèges est un élément crucial de l'infrastructure informatique d'une organisation. Ce point est doublement vrai lorsque l'implémentation est étendue de façon à supporter les scénarios d'utilisation d'application-à-application, qui fonctionnent de façon totalement automatisée. Dans cette optique, CA Privileged Access Manager inclut des fonctionnalités natives de mise en cluster et de distribution des charges pour répondre aux demandes d'évolutivité et de haute disponibilité des environnements les plus exigeants et les plus vastes. Contrairement aux alternatives traditionnelles, CA Privileged Access Manager ne vous oblige pas à investir dans des équilibreurs de charge externes distincts. Il n'existe par ailleurs aucun retard de performances comme c'est le cas dans les approches actives/passives. Enfin, il n'est pas nécessaire d'acheter sous licence des fonctionnalités « en option » supplémentaires. Si vous le souhaitez et sous réserve de compatibilité opérationnelle en termes de latence, les clusters CA Privileged Access Manager peuvent même être configurés de façon à activer la redondance dans des environnements de Cloud et des data centers éloignés géographiquement.

CA Privileged Access Manager propose une solution nouvelle génération de gestion des identifiants à forts privilèges, conçue pour réduire les risques de sécurité et renforcer l'efficacité opérationnelle dans l'infrastructure métier hybride.

Section 4

Conclusion : Adoption de la gestion des identifiants à forts privilèges à l'ère du Cloud

La gestion et la protection des identifiants à forts privilèges sont indispensables pour limiter les risques et répondre aux exigences réglementaires connexes. Ce problème devient de plus en plus important et complexe, car les environnements Cloud hybrides introduisent des consoles de gestion aux performances jusque-là inégalées et permettent d'ajouter/de supprimer des centaines de systèmes cibles en quelques clics.

Les organisations qui souhaitent s'attaquer à ce pan essentiel de leur stratégie de sécurité des informations doivent évaluer les différentes solutions proposées. Il convient à cet égard d'analyser l'ampleur des commandes, l'étendue de la couverture et le degré d'alignement avec le Cloud proposé. Comme indiqué précédemment, CA Privileged Access Manager répond à ces trois aspects afin de proposer aux organisations d'aujourd'hui ce dont elles ont exactement besoin : une solution nouvelle génération de gestion des identifiants à forts privilèges conçue pour réduire les risques informatiques, renforcer l'efficacité opérationnelle et protéger les investissements d'une organisation en prenant en charge tant les infrastructures traditionnelles, virtualisées que de Cloud hybride.

ca technologies

Restez connecté à CA Technologies sur ca.com/fr

CA Technologies (NASDAQ : CA) fournit les logiciels qui aident les entreprises à opérer leur transformation numérique. Dans tous les secteurs, les modèles économiques des entreprises sont redéfinis par les applications. Partout, une application sert d'interface entre une entreprise et un utilisateur. CA Technologies aide ces entreprises à saisir les opportunités créées par cette révolution numérique et à naviguer dans « l'Économie des applications ». Grâce à ses logiciels pour planifier, développer, gérer la performance et la sécurité des applications, CA Technologies aide ainsi ces entreprises à devenir plus productives, à offrir une meilleure qualité d'expérience à leurs utilisateurs, et leur ouvre de nouveaux relais de croissance et de compétitivité sur tous les environnements : mobile, Cloud, distribué ou mainframe. Pour en savoir plus, rendez-vous sur www.ca.com/fr.

1 Rapport 2015 Verizon Data Breach Investigations Report

2 *« New Platforms, New Requirements. Privileged Identity Management for the Hybrid Cloud »*, Livre blanc CA, mars 2013

3 *« Managing SSH Keys for Automated Access - Current Recommended Practice »*, version préliminaire IETF, avril 2013

CS200-169152_1215