DELL Technologies

Livre blanc

Livre blanc technique : sécurité cyber-résiliente dans les serveurs Dell EMC PowerEdge

Décembre 2020

Révisions

Date	Description
Janvier 2018	Édition initiale
Novembre 2020	Version révisée

Table des matières

Table des matières

Synthèse

L'approche Dell Technologies de la sécurité est intrinsèque par nature : elle est intégrée à chaque étape à travers le cycle de développement de la sécurité de Dell et non rajoutée par la suite. Nous nous efforçons de faire évoluer en permanence nos contrôles de sécurité, nos fonctionnalités et nos solutions PowerEdge afin de répondre à l'évolution constante des menaces, et nous continuons à ancrer la sécurité à l'aide d'une racine de confiance (« Root of Trust ») gravée dans le silicium. Ce livre détaille les fonctions de sécurité intégrées à la plate-forme PowerEdge cyber-résiliente, dont la plupart sont permises par le Dell Remote Access Controller (iDRAC9). Un grand nombre de nouvelles fonctionnalités ont été ajoutées depuis le précédent livre blanc sur la sécurité PowerEdge, celles-ci recouvrent le contrôle d'accès et le chiffrement des données, mais également l'assurance de la chaîne d'approvisionnement. Voici quelques exemples : Analyse du BIOS en direct, personnalisation du démarrage Secure Boot UEFI, AMF (authentification multifacteur) RSA SecureID, gestion des clés d'entreprise sécurisée (« Secure Enterprise Key Management » ou SEKM), vérification des composants sécurisés (« Secured Component Verification » ou SCV), System Erase amélioré, inscription et renouvellement automatiques des certificats, prise en charge de la sélection du chiffrement et du protocole CNSA. Toutes les fonctionnalités exploitent largement l'intelligence et l'automatisation afin de vous aider à garder une longueur d'avance sur la courbe des menaces et de permettre l'évolutivité requise par les modèles d'utilisation en constante évolution.

1. Introduction

L'écosystème des menaces évoluant en permanence, les professionnels de l'informatique et de la sécurité se trouvent face à des difficultés à gérer les risques pour leurs données et leurs ressources. Les données sont utilisées par de nombreux périphériques, sur site et dans le Cloud, et les violations de données à fort impact continuent de croître. Historiquement, l'accent en matière de sécurité a été mis sur le système d'exploitation (SE), sur les applications, sur les pare-feu et sur les systèmes IPS et IDS (prévention et détection d'intrusion). Tous ces domaines restent importants à prendre en compte. Cependant, étant donné les événements survenus au cours des deux dernières années, qui ont mis au jour des menaces envers le matériel, nous considérons qu'il est tout aussi urgent de sécuriser une infrastructure basée sur le matériel comme le firmware, le BIOS, le contrôleur BMC et d'autres éléments de protection du matériel, comme l'assurance de la chaîne d'approvisionnement.

L'indice 2020 de transformation numérique Dell Technologies a révélé que les préoccupations relatives à la confidentialité des données et à la cybersécurité constituent le premier obstacle à la transformation numérique[1]. 63 % des sociétés ont été confrontées à une compromission de données suite à l'exploitation d'une faille de sécurité[2]. Les dommages au niveau mondial liés à la cybercriminalité atteindront 6 billions de dollars en 2021[3].

Dans la mesure où les serveurs deviennent de plus en plus stratégiques au sein d'une architecture de datacenter software-defined, la sécurité des serveurs devient le fondement de la sécurité d'entreprise globale. Les serveurs doivent mettre l'accent sur la sécurité au niveau du matériel et du firmware en mobilisant une racine de confiance immuable, qui peut être employée pour vérifier les opérations ultérieures au sein du serveur. Ce processus crée une chaîne de confiance qui s'étend tout au long du cycle de vie du serveur, du déploiement à la maintenance, jusqu'au démantèlement.

Les serveurs Dell EMC PowerEdge de 14e et 15e générations dotés d'iDRAC9 offrent cette chaîne de confiance et l'associent à des contrôles de sécurité et à des outils complets de gestion, afin de fournir des couches de sécurité robustes sur l'ensemble du matériel et des firmwares. Il en résulte une architecture cyber-résiliente qui couvre tous les aspects du serveur, y compris le firmware de serveur intégré, les données stockées dans le système, le système d'exploitation, les périphériques et les opérations de gestion qui s'y rapportent. Les organisations peuvent ainsi mettre au point un processus dans le but de protéger leur inestimable infrastructure de serveurs ainsi que les données qui y sont stockées, de détecter les anomalies, les failles ou les opérations non autorisées, et de se remettre d'événements inattendus ou malveillants.

[1] Indice 2020 de transformation numérique Dell Technologies

[2] Correspond aux menaces de sécurité actuelles avec un contrôle au niveau du BIOS. Un document Forrester Consulting sur le leadership d'opinion réalisé à la demande de Dell, 2019

[3] Les attaques par ransomware prévues... Revue « The National Law Review », 2020

2. La voie vers une infrastructure de serveurs sécurisée

Les serveurs Dell EMC PowerEdge offrent une sécurité renforcée depuis plusieurs générations, en utilisant notamment la technologie innovante de sécurité des données basée sur le silicium. Les serveurs Dell EMC PowerEdge de 14e génération ont étendu la sécurité basée sur le silicium pour authentifier le BIOS et le firmware avec une racine de confiance cryptographique pendant le démarrage du serveur. L'équipe produits de Dell EMC a pris en compte plusieurs exigences clés au cours de la conception des serveurs PowerEdge de 14e et 15e générations en réponse aux menaces de sécurité rencontrées dans les environnements informatiques modernes :

- **Protéger :** protéger le serveur dans tous les aspects du cycle de vie, y compris le BIOS, le firmware, les données et le matériel physique
- **Détecter :** détecter les cyber-attaques malveillantes et les modifications non approuvées ; impliquer les administrateurs IT de manière proactive
- **Restaurer :** restaurer le BIOS, le firmware et le système d'exploitation à un état bien connu ; mise au rebut ou réaffectation sécurisée des serveurs

Les serveurs Dell EMC PowerEdge sont conformes aux principales normes du secteur en matière de cryptographie et de sécurité, comme développé dans le présent document, et procèdent au suivi et à la gestion continus des nouvelles failles de sécurité.

Dell EMC a mis en œuvre le processus du cycle de développement de la sécurité, cette dernière étant un élément clé dans tous les aspects du développement, de l'approvisionnement, de la fabrication, de l'expédition et du support, ce qui a abouti à la création d'une architecture cyber-résiliente.

2.1 Cycle de développement de la sécurité

La mise au point de l'architecture cyber-résiliente nécessite une parfaite maîtrise de la sécurité et une grande rigueur à chaque étape du développement. Ce processus est appelé modèle du cycle de développement de la sécurité (« Security Development Lifecycle » ou SDL), dans lequel la sécurité n'est pas un second choix, mais fait plutôt partie intégrante du processus global de conception des serveurs. Ce processus de conception englobe une vue des besoins en matière de sécurité tout au long du cycle de vie du serveur, comme indiqué ci-dessous et présenté dans la figure 1 :

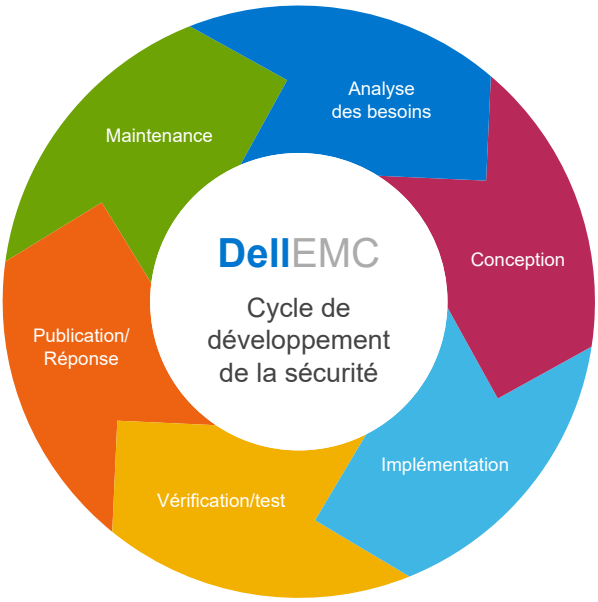


Figure 1 : cycle de développement de la sécurité de Dell EMC

- Les fonctions sont imaginées, conçues, prototypées, mises en œuvre, mises en production, déployées et gérées avec la sécurité comme principale priorité.
- Le micrologiciel du serveur est conçu pour bloquer, empêcher et contrer l'injection de code malveillant pendant toutes les phases du cycle de vie de développement du produit
  - » Modélisation des menaces et couverture des tests d'intrusion pendant le processus de conception
  - » Pratiques de codage sécurisées appliquées à chaque étape du développement du firmware
- Pour les technologies stratégiques, des audits externes complètent le processus SDL interne afin de garantir que le firmware adhère aux pratiques d'excellence connues en matière de sécurité.
- Tests continus et évaluation de nouvelles failles de sécurité potentielles à l'aide des derniers outils d'évaluation de la sécurité.
- Réponse rapide aux failles de sécurité et expositions courantes (« Common Vulnerabilities and Exposures » ou CVE), y compris les mesures correctives recommandées, le cas échéant.

2.2 Architecture cyber-résiliente

Les serveurs Dell EMC PowerEdge de 14e et 15e générations sont dotés d'une architecture cyber-résiliente améliorée qui assure une protection, une détection et une récupération renforcées face aux cyberattaques. Voici quelques-uns des principaux aspects de cette architecture :

- **Protection efficace contre les attaques**
  - » Racine de confiance basée sur le silicium
  - » Secure Boot
  - » Mises à jour de firmware signées
  - » System Lockdown dynamique
  - » Chiffrement du disque dur et gestion des clés d'entreprise
- **Détection d'attaques fiable**
  - » Détection de dérive de la configuration et du firmware
  - » Journalisation des événements persistante
  - » Journalisation des audits et alertes
  - » Détection d'intrusion dans le boîtier
- **Récupération rapide avec une interruption des activités minimale ou inexistante**
  - » Récupération automatisée du BIOS
  - » Restauration rapide de l'OS
  - » Restauration du firmware
  - » System Erase rapide

2.3 Menaces actuelles

Il existe de nombreux vecteurs de menaces dans l'écosystème évolutif actuel. Le tableau 1 résume l'approche de Dell EMC en matière de gestion des menaces critiques pesant sur le serveur principal.

Tableau 1 : réponse de Dell EMC face aux vecteurs de menaces courants

Couches de plate-forme de serveur		
Couche de sécurité	**Vecteur de menace**	**Solution Dell EMC**
Serveur physique	Piratage de serveur/composant	Vérification des composants sécurisés (SCV), détection d'intrusion dans le boîtier
Firmware et logiciels	Corruption du firmware, injection de logiciel malveillant	Racine de confiance basée sur le silicium ; Boot Guard Intel ; racine de confiance AMD sécurisée ; personnalisation du démarrage Secure Boot UEFI Firmware signé et validé de manière chiffrée ;
	Logiciels	Création de rapports CVE ; application de correctifs en fonction des besoins
Fonctions de confiance en matière d'attestation	Usurpation d'identité de serveur	Module TPM, Intel TXT, chaîne de confiance
Gestion de serveurs	Configuration et mises à jour corrompues, attaques sur port ouvert non autorisé	iDRAC9, attestation distante

Couches d'environnement de serveur		
Couche de sécurité	**Vecteur de menace**	**Solution Dell EMC**
Données	Violation de données	Disques durs à chiffrement automatique (« Self Encrypting Drives » ou SED) – norme FIPS ou TCG Opal Disques ISE uniquement (Instant Secure Erase) pour la gestion des clés d'entreprise sécurisée Authentification sécurisée des utilisateurs
Intégrité de la chaîne d'approvisionnement	Composants contrefaits Menaces reposant sur des logiciels malveillants	Certification ISO 9001 pour tous les sites de fabrication de serveurs mondiaux ; vérification des composants sécurisés ; preuve de possession Mesures de sécurité mises en œuvre dans le cadre du processus de cycle de développement de la sécurité (SDL)
Sécurisation de la chaîne d'approvisionnement	Sécurité physique sur les sites de fabrication Vol et piratage pendant le transport	Exigences en matière de sécurité des installations certifiées par l'Association pour la protection des marchandises transportées (TAPA) Partenariat douane-commerce contre le terrorisme (« Customs-Trade Partnership Against Terrorism » ou C-TPAT) ; SCV

3. Protéger

La fonction « Protéger » est un composant clé du cadre de cybersécurité du NIST (« NIST Cybersecurity Framework ») qui protège contre les cyberattaques. Cette fonction comprend plusieurs catégories, notamment le contrôle d'accès, la sécurité des données, la maintenance et la technologie de protection. La principale philosophie sous-jacente suppose que les ressources d'infrastructure doivent fournir une protection robuste contre l'accès non autorisé aux ressources et aux données dans le cadre d'une installation et d'un environnement informatique sécurisés complets. Cela comprend la protection contre les modifications non autorisées de composants stratégiques tels que le BIOS et le firmware. La plate-forme répond aux recommandations actuelles du NIST SP 800-193.

L'architecture cyber-résiliente des serveurs PowerEdge offre un haut niveau de protection de la plate-forme qui inclut les fonctionnalités suivantes :

- Démarrage de confiance vérifié de manière chiffrée
- Sécurité de l'accès de l'utilisateur
- Mises à jour de firmware signées
- Stockage de données chiffrées
- Sécurité physique
- Intégrité et sécurité de la chaîne d'approvisionnement

3.1 Démarrage de confiance vérifié de manière chiffrée

L'un des aspects les plus critiques de la sécurité des serveurs consiste à garantir que le processus de démarrage puisse être vérifié comme étant sécurisé. Ce processus fournit une ancre de confiance pour toutes les opérations ultérieures telles que le démarrage d'un système d'exploitation ou la mise à jour du firmware. Les serveurs PowerEdge utilisent une sécurité basée sur le silicium depuis plusieurs générations pour des fonctions telles que la chambre forte d'identifiants iDRAC (Credential Vault), une mémoire sécurisée chiffrée dans l'iDRAC pour le stockage de données sensibles. Le processus de démarrage est vérifié à l'aide d'une racine de confiance basée sur le silicium afin d'être en conformité avec les recommandations du NIST SP 800-147B (« Directives sur la protection du BIOS pour les serveurs ») et NIST SP 800-155 (« Directives sur l'évaluation de l'intégrité du BIOS »).

3.1.1 Racine de confiance basée sur le silicium

Les serveurs PowerEdge de 14e et 15e générations (basés sur la technologie Intel ou AMD) utilisent désormais une racine de confiance immuable basée sur le silicium pour attester de l'intégrité du BIOS et du firmware de l'iDRAC de manière chiffrée. Cette racine de confiance est fondée sur des clés publiques programmables, en lecture seule et à usage unique, qui assurent une protection contre le piratage par logiciel malveillant. Le processus de démarrage du BIOS utilise la technologie Intel Boot Guard ou la technologie AMD de racine de confiance qui vérifie que la signature numérique du hachage cryptographique de l'image de démarrage correspond à la signature stockée en usine dans le silicium par Dell EMC. Un échec de la vérification entraîne l'arrêt du serveur, une notification de l'utilisateur dans le journal du Lifecycle Controller et le processus de récupération du BIOS peut alors être lancé par l'utilisateur. Si Boot Guard valide l'opération, les autres modules du BIOS sont validés à l'aide d'une procédure de chaîne de confiance, jusqu'à ce que le contrôle soit transmis au SE ou à l'hyperviseur.

Outre le mécanisme de vérification de Boot Guard, iDRAC9 4.10.10.10 ou une version ultérieure fournit un mécanisme de racine de confiance permettant de vérifier l'image du BIOS au moment du démarrage de l'hôte. L'hôte ne peut démarrer qu'une fois l'image du BIOS validée. iDRAC9 fournit également un mécanisme de validation de l'image du BIOS pendant l'exécution, à la demande ou à des intervalles programmés par l'utilisateur.

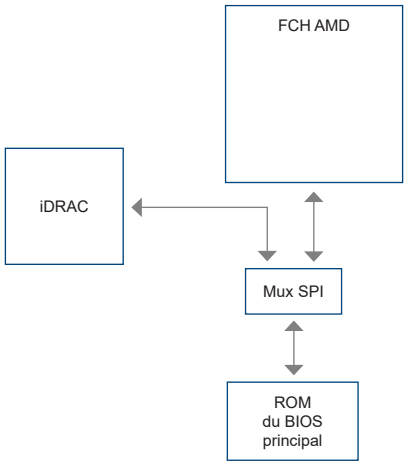
Examinons la chaîne de confiance plus en détail. Chaque module du BIOS contient un hachage du module suivant dans la chaîne. Les principaux modules du BIOS sont les suivants : IBB (« Initial Boot Block » ou bloc de démarrage initial), SEC (sécurité), PEI (« Pre-EFI Initialization » ou initialisation pré-EFI), MRC (« Memory Reference Code » ou code de référence de mémoire), DXE (« Driver Execution Environment » ou environnement d'exécution de pilote) et BDS (« Boot Device Selection » ou sélection de périphérique de démarrage). Si Intel Boot Guard authentifie le module IBB (bloc de démarrage initial), ce dernier valide les modules SEC+PEI avant de leur remettre le contrôle. Les modules SEC+PEI valident ensuite les modules PEI+MRC, qui valident alors les modules DXE+BDS. À cette étape, le contrôle est transmis au Secure Boot UEFI comme expliqué dans la section suivante.

De même, pour les serveurs Dell EMC PowerEdge basés sur la gamme de processeurs AMD EPYC, la technologie AMD Secure Root-of-Trust garantit que les serveurs démarrent uniquement à partir d'images de firmware fiables. En outre, la technologie AMD Secure Run est conçue pour chiffrer les données de la mémoire principale, ce qui l'isole des intrusions malveillantes touchant au matériel. Aucune modification de l'application n'est nécessaire pour utiliser cette fonction et le processeur de sécurité n'expose jamais les clés de chiffrement en dehors du processeur.

L'iDRAC adopte également le rôle de technologie de sécurité basée sur le matériel et accède à la ROM du BIOS principal via le Dell SPI, en plus du chipset Fusion Controller Hub (FCH) d'AMD et exécute le processus de racine de confiance.

iDRAC9 restaure le BIOS dans les conditions suivantes.

1. Échec de la vérification de l'intégrité du BIOS.
2. Échec de la vérification automatique du BIOS.
3. Utilisation de la commande RACADM : **racadm recover BIOS.Setup.1-1**



Le processus de démarrage de l'iDRAC utilise sa propre racine de confiance basée sur le silicium, qui vérifie l'image de son firmware. La racine de confiance de l'iDRAC fournit également une ancre de confiance essentielle pour authentifier les signatures des packages de mise à jour de firmware Dell EMC (« Dell EMC Update Packages » ou DUP).

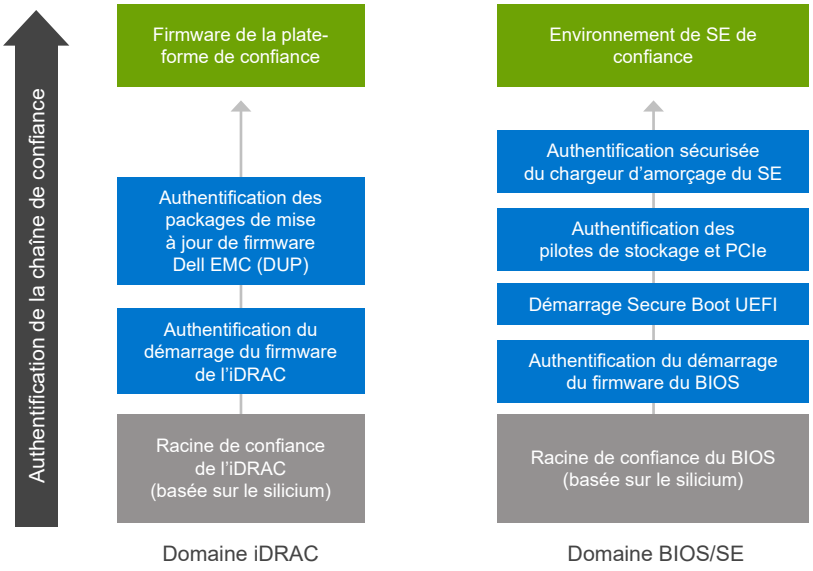


Figure 2 : domaines de racine de confiance basée sur le silicium dans les serveurs PowerEdge

3.1.2 Analyse du BIOS en direct

L'analyse du BIOS en direct vérifie l'intégrité et l'authenticité de l'image du BIOS dans la ROM principale lorsque l'hôte est sous tension, mais pas dans la procédure POST (« Power-On Self-Test » ou auto-test de démarrage). Il s'agit d'une fonction propre à AMD qui est uniquement disponible avec iDRAC9 4.10.10.10 ou une version ultérieure, avec une licence Datacenter. Vous devez disposer de privilèges d'administration ou de privilèges d'opérateur avec le privilège de débogage « Exécuter des commandes de débogage » pour effectuer cette opération. Vous avez la possibilité de planifier l'analyse à l'aide de l'interface utilisateur de l'iDRAC, de la commande RACADM, et des interfaces Redfish.

3.1.3 Personnalisation du démarrage Secure Boot UEFI

Les serveurs PowerEdge prennent également en charge le démarrage Secure Boot UEFI (Unified Extensible Firmware Interface) standard qui effectue une vérification des signatures cryptographiques des pilotes UEFI et d'autres codes chargés avant l'exécution du système d'exploitation. Le démarrage Secure Boot est une norme à l'échelle du secteur pour la sécurité de l'environnement de pré-démarrage. Les fournisseurs de systèmes informatiques, de cartes d'extension et de systèmes d'exploitation collaborent dans le cadre de cette spécification dans le but de promouvoir l'interopérabilité.

Lorsqu'il est activé, le démarrage Secure Boot UEFI empêche le chargement des pilotes de périphériques UEFI non signés (c'est-à-dire, non approuvés), affiche un message d'erreur et ne permet pas au périphérique de fonctionner. Il est nécessaire de désactiver le Secure Boot pour charger des pilotes de périphériques non signés.

De plus, les serveurs PowerEdge de 14e et 15e générations offrent aux clients la flexibilité exclusive de l'utilisation d'un certificat de chargeur d'amorçage personnalisé non signé par Microsoft. Il s'agit principalement d'une fonction destinée aux administrateurs d'environnements Linux qui souhaitent signer leurs propres chargeurs d'amorçage du SE. Les certificats personnalisés peuvent être téléchargés via l'API iDRAC privilégiée pour authentifier le chargeur d'amorçage du SE spécifique au client. Cette méthode de personnalisation de l'UEFI du serveur PowerEdge est citée par la NSA en tant que méthode permettant de minimiser les failles de sécurité de GRUB2 au sein des serveurs.

3.1.4 Prise en charge du module TPM

Les serveurs PowerEdge prennent en charge trois versions du module TPM :

- TPM 1.2 FIPS + critères communs + certifiés TCG (Nuvoton)
- TPM 2.0 FIPS + critères communs + certifiés TCG (Nuvoton)
- TPM 2.0 Chine (NationZ)

Le module TPM peut être employé pour des fonctions de chiffrement de clé publique, des fonctions de calcul du hachage, pour générer, gérer et stocker des clés en toute sécurité, et créer des attestations. La fonction TXT (Trusted Execution Technology) d'Intel et la fonction d'assurance de plate-forme de Microsoft dans Windows Server 2016 sont également prises en charge. Le module TPM peut également être utilisé pour activer la fonction de chiffrement du disque dur BitLocker™ dans Windows Server 2012/2016.

Les solutions d'attestation et d'attestation distante peuvent utiliser le module TPM pour effectuer des mesures au moment du démarrage du matériel, de l'hyperviseur, du BIOS et du SE d'un serveur, et comparer ces dernières de manière sécurisée par chiffrement aux mesures de base stockées dans le module TPM. Si elles ne sont pas identiques, cela signifie que l'identité du serveur a peut-être été compromise et les administrateurs système peuvent le désactiver et le déconnecter localement ou à distance.

Il est possible de commander les serveurs avec ou sans module TPM, mais pour de nombreux systèmes d'exploitation et d'autres dispositions de sécurité, il devient un standard. Le module TPM est activé via une option du BIOS. Il s'agit d'une solution de module plug-in, l'adaptateur Planar est doté d'un connecteur pour ce module enfichable.

3.1.5 Certifications de sécurité

Dell EMC a été certifié pour des normes telles que la FIPS 140-2 du NIST et les critères communs EAL-4. Ces normes sont importantes pour être conforme aux exigences du département de la Défense des États-Unis et aux autres exigences gouvernementales. Les serveurs PowerEdge ont également obtenu les certifications suivantes :

- Plate-forme de serveurs : certifiée critères communs EAL4+ (CC) avec RHEL (Red Hat Enterprise Linux), également utilisée pour prendre en charge les certifications CC du partenaire
- certification iDRAC et Dell CMC FIPS 140-2 niveau 1
- OpenManage Enterprise-Modular est certifié CC EAL2+
- certification FIPS 140-2 et critères communs pour le module TPM 1.2 et 2.0

3.2 Sécurité de l'accès de l'utilisateur

Garantir une authentification et une validation appropriées est un impératif majeur de toute politique de contrôle d'accès moderne. Les interfaces d'accès principales des serveurs PowerEdge sont disponibles via les API, les interfaces de ligne de commande (CLI) ou l'interface graphique de l'iDRAC intégré. Les API et CLI privilégiées pour l'automatisation de la gestion des serveurs sont les suivantes :

- API RESTful iDRAC avec Redfish
- CLI RACADM
- SELinux

Chacune d'entre elles offre une sécurisation élevée des informations d'identification telles que le nom d'utilisateur et le mot de passe, transmise par le biais d'une connexion chiffrée, comme HTTPs, le cas échéant. Le SSH authentifie un utilisateur à l'aide d'un ensemble de clés cryptographiques correspondantes (ce qui évite d'avoir à saisir des mots de passe moins sécurisés). Les anciens protocoles, tels que l'IPMI, sont pris en charge, mais ne sont pas recommandés pour les nouveaux déploiements en raison des divers problèmes de sécurité découverts au cours des dernières années. Nous vous recommandons de tester et de passer à l'API RESTful iDRAC avec Redfish si vous utilisez actuellement le protocole IPMI.

Les **certificats TLS/SSL** peuvent être téléchargés vers l'iDRAC pour authentifier les sessions de navigateur Web. Trois options :

- **Certificat TLS/SSL Dell EMC auto-signé :** le certificat est automatiquement généré et auto-signé par l'iDRAC.
  - » Avantage : il n'est pas nécessaire de conserver une autorité de certification spécifique (voir norme X.509 du groupe de travail PKIX de l'IETF).
- **Certificat TLS/SSL personnalisé :** le certificat est automatiquement généré et signé à l'aide d'une clé privée qui a déjà été téléchargée vers l'iDRAC.
  - » Avantage : une seule autorité de certification de confiance pour tous les contrôleurs iDRAC. Il est possible que votre autorité de certification interne soit déjà approuvée par vos stations de gestion.
- **Certificat TLS/SSL signé par l'autorité de certification :** une demande de signature de certificat (DSC) est créée et envoyée à votre autorité de certification interne ou à une autorité de certification tierce, telle que VeriSign, Thawte et GoDaddy, pour signature.
  - » Avantages : peut utiliser une autorité de certification commerciale (voir les normes X.509 du groupe de travail PKIX de l'IETF). Une seule autorité de certification de confiance pour tous vos contrôleurs iDRAC. Si une autorité de certification commerciale est utilisée, il est fort probable qu'elle soit déjà approuvée par vos stations de gestion.

iDRAC9 s'intègre à l'**Active Directory** et au protocole **LDAP** en utilisant les schémas d'authentification et de validation existants des clients, qui fournissent déjà un accès sécurisé aux serveurs PowerEdge. Il prend également en charge le **contrôle d'accès basé sur les rôles (« Role-Based Access Control » ou RBAC)** pour accorder le niveau d'accès approprié (administrateur, opérateur ou lecture seule), requis pour faire correspondre le rôle de la personne dans les opérations de serveur. Il est vivement recommandé d'utiliser le contrôle RBAC de cette manière et de ne pas simplement accorder le niveau le plus élevé (par exemple, administrateur) à tous les utilisateurs.

iDRAC9 fournit également des moyens supplémentaires de protection contre les accès non autorisés, notamment le **blocage et le filtrage des adresses IP**. Le blocage d'adresse IP détermine de manière dynamique si des échecs de connexion excessifs se produisent à partir d'une adresse IP particulière et bloque (ou empêche) la connexion à iDRAC9 à partir de cette adresse pour une période présélectionnée. Le filtrage d'adresse IP limite la plage d'adresses IP des clients accédant à l'iDRAC. Il compare l'adresse IP d'une connexion entrante à la plage spécifiée et autorise l'accès à l'iDRAC uniquement à partir d'une station de gestion dont l'adresse IP source se trouve dans la plage. Toutes les autres demandes de connexion sont refusées.

L'authentification multifacteur (AMF) est aujourd'hui utilisée plus largement en raison de la vulnérabilité croissante des dispositifs d'authentification à un seul facteur basés sur le nom d'utilisateur et le mot de passe. iDRAC9 permet d'utiliser des cartes à puce pour l'accès distant à l'interface graphique utilisateur et prendra également en charge le jeton RSA. Dans les deux cas, les facteurs multiples vérifient la présence physique de l'appareil ou de la carte et le code PIN associé.

3.2.1 AMF RSA SecurID

RSA SecurID peut constituer un autre moyen d'authentifier un utilisateur sur un système. iDRAC9 commence à prendre en charge RSA SecurID avec la licence Datacenter et le firmware 4.40.00.00, en tant que méthode d'authentification à deux facteurs supplémentaire.

3.2.2 A2F simplifiée

Une autre méthode d'authentification proposée est l'authentification à deux facteurs (A2F) simple, qui envoie un jeton généré de manière aléatoire à la messagerie électronique de l'utilisateur lorsqu'il se connecte à l'iDRAC.

3.2.3 Infrastructure SELinux

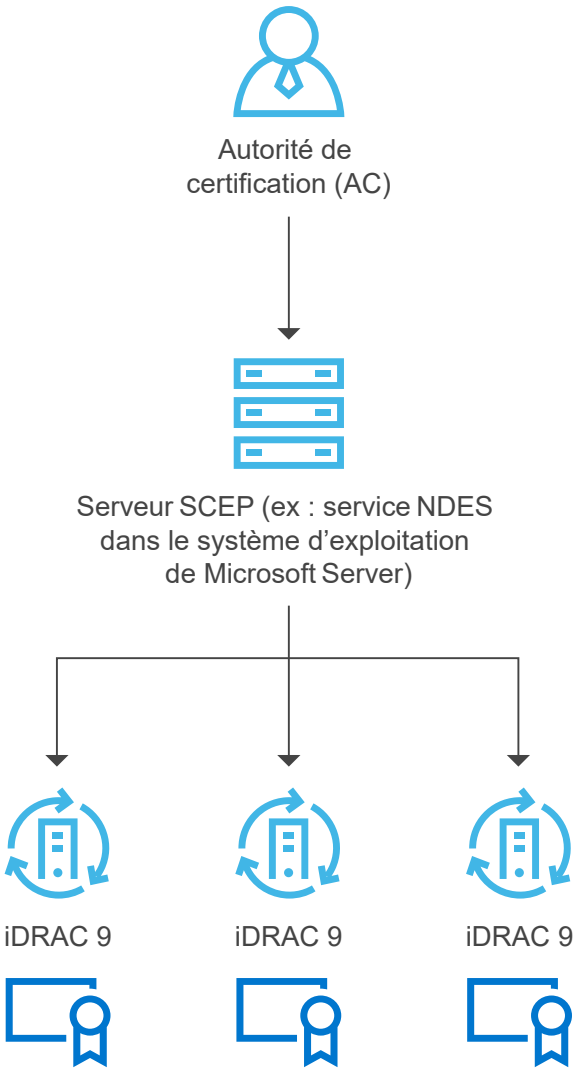
SELinux fonctionne au niveau du noyau central de l'iDRAC et ne nécessite aucune information ni configuration de la part des utilisateurs. SELinux enregistre les messages de sécurité lorsqu'une attaque est détectée. Ces messages de journal indiquent quand et comment un pirate a tenté de pénétrer dans le système. Actuellement, ces journaux sont disponibles via SupportAssist pour les clients inscrits à cette nouvelle fonction. Dans la prochaine version d'iDRAC, ces journaux seront disponibles dans les journaux du Lifecycle Controller.

3.2.4 Privilège minimum requis

Tous les processus internes exécutés dans l'iDRAC s'exécutent avec les privilèges minimum requis ; un concept central de la sécurité UNIX. Cette protection garantit que le processus d'un système susceptible d'être attaqué ne puisse pas accéder à des fichiers ou à du matériel qui sortent du champ d'application de ce processus. Par exemple, le processus qui permet la prise en charge du KVM virtuel ne doit pas être en mesure de modifier la vitesse des ventilateurs. L'exécution de ces deux processus en tant que fonctions séparées permet de protéger le système en empêchant les attaques de se propager d'un processus à un autre.

3.2.5 Inscription et renouvellement automatiques des certificats

iDRAC9 v4.0 a ajouté un client pour la prise en charge du protocole SCEP (Simple Certificate Enrollment Protocol) et nécessite une licence Datacenter. SCEP est une norme de protocole utilisée pour gérer les certificats sur un grand nombre de périphériques réseau à l'aide d'un processus d'inscription automatique. L'iDRAC peut désormais s'intégrer à des serveurs compatibles SCEP tels que le serveur Microsoft NDES, afin de maintenir automatiquement les certificats SSL/TLS. Cette fonction peut servir à l'inscription et à l'actualisation d'un certificat de serveur Web expirant bientôt et peut être utilisée sur la base d'un certificat à la fois dans l'interface graphique de l'iDRAC, définie via le profil de configuration du serveur ou par script à l'aide d'outils tels que RACADM.



3.2.6 Mot de passe par défaut généré en usine

Par défaut, tous les serveurs PowerEdge de 14e génération sont livrés avec un mot de passe iDRAC unique généré en usine afin d'offrir une sécurité supplémentaire. Ce mot de passe est généré en usine et se trouve sur l'étiquette d'information à retirer qui est située à l'avant du boîtier, à côté de l'étiquette d'inventaire du serveur. Les utilisateurs qui choisissent cette option par défaut doivent noter ce mot de passe et l'utiliser pour se connecter à l'iDRAC pour la première fois, plutôt que d'utiliser un mot de passe par défaut universel. Pour des raisons de sécurité, Dell EMC recommande vivement de modifier le mot de passe par défaut.

3.2.7 System Lockdown dynamique

iDRAC9 propose une nouvelle fonction qui « verrouille » la configuration matérielle et du firmware d'un serveur ou de plusieurs serveurs et nécessite une licence Enterprise ou Datacenter. Ce mode peut être activé à l'aide de l'interface graphique utilisateur, d'une CLI comme RACADM, ou dans le cadre du profil de configuration du serveur. Les utilisateurs disposant de privilèges d'administration peuvent définir le mode System Lockdown, qui empêche les utilisateurs disposant de privilèges moindres d'apporter des modifications au serveur. Cette fonction peut être activée/désactivée par l'administrateur informatique. Toute modification apportée lorsque System Lockdown est désactivé est suivie dans le journal du Lifecycle Controller. En activant le mode de verrouillage, vous pouvez empêcher la dérive de la configuration dans votre datacenter lorsque vous utilisez les outils et agents Dell EMC. Vous pouvez également protéger votre système contre les attaques malveillantes ciblant le firmware intégré lors de l'utilisation des packages Dell EMC Update Packages (DUP). Le mode de verrouillage peut être activé de manière dynamique, sans nécessiter de redémarrage du système. iDRAC9 v4.40 introduit des améliorations en plus du verrouillage System Lockdown actuel, qui ne contrôle que les mises à jour à l'aide du package DUP, cette fonctionnalité est étendue à certaines cartes NIC. (REMARQUE : le verrouillage amélioré pour les cartes NIC comprend uniquement le verrouillage du firmware pour empêcher ses mises à jour.) Le verrouillage de la configuration (x-UEFI) n'est pas pris en charge. Lorsque le client configure le système en mode de verrouillage en activant/définissant l'attribut à partir de n'importe quelle interface prise en charge, l'iDRAC réalise les actions complémentaires, en fonction de la configuration du système. Ces actions dépendent des périphériques tiers détectés dans le cadre du processus de détection de l'iDRAC.

3.2.8 Isolation de domaine

Les serveurs PowerEdge de 14e et 15e générations offrent une sécurité supplémentaire via l'**isolation de domaine**, une fonction importante pour les environnements d'hébergement multiclient. Afin de sécuriser la configuration matérielle du serveur, les fournisseurs d'hébergement peuvent souhaiter bloquer toute reconfiguration par les clients. L'isolation de domaine est une option de configuration qui garantit que les applications de gestion du système d'exploitation hôte n'ont pas accès à l'iDRAC hors bande ou aux fonctions du chipset Intel, telles que Management Engine (ME) ou Innovation Engine (IE).

3.3 Mises à jour de firmware signées

Les serveurs PowerEdge utilisent des signatures numériques pour les mises à jour de firmware depuis plusieurs générations afin de garantir que seul le firmware authentique est exécuté sur la plate-forme de serveurs. Nous signons numériquement tous nos packages de firmware à l'aide du hachage SHA-256, avec chiffrement RSA 2 048 bits pour la signature de tous les composants clés du serveur. Il s'agit notamment des firmwares pour l'iDRAC, le BIOS, le contrôleur PERC, les adaptateurs d'E/S et cartes LOM, les blocs d'alimentation, les disques de stockage, les périphériques CPLD et les contrôleurs de fond de panier. L'iDRAC analyse les mises à jour de firmware et compare leurs signatures à ce qui est attendu à l'aide de la racine de confiance basée sur le silicium. Tout package de firmware qui échoue à la validation est abandonné et un message d'erreur est consigné dans le journal du cycle de vie (« Lifecycle Log » ou LCL) afin d'alerter les administrateurs.

L'authentification améliorée du firmware est intégrée à de nombreux périphériques tiers qui assurent la validation des signatures à l'aide de leurs propres mécanismes sur la racine de confiance. Cela empêche l'utilisation d'un outil de mise à jour tiers corrompu pour charger des firmwares malveillants dans, par exemple, une carte NIC ou un disque de stockage (et pour contourner le recours à des DUP signés). La plupart des périphériques PCIe et de stockage tiers expédiés avec les serveurs PowerEdge utilisent une racine de confiance matérielle pour valider leurs mises à jour de firmware respectives.

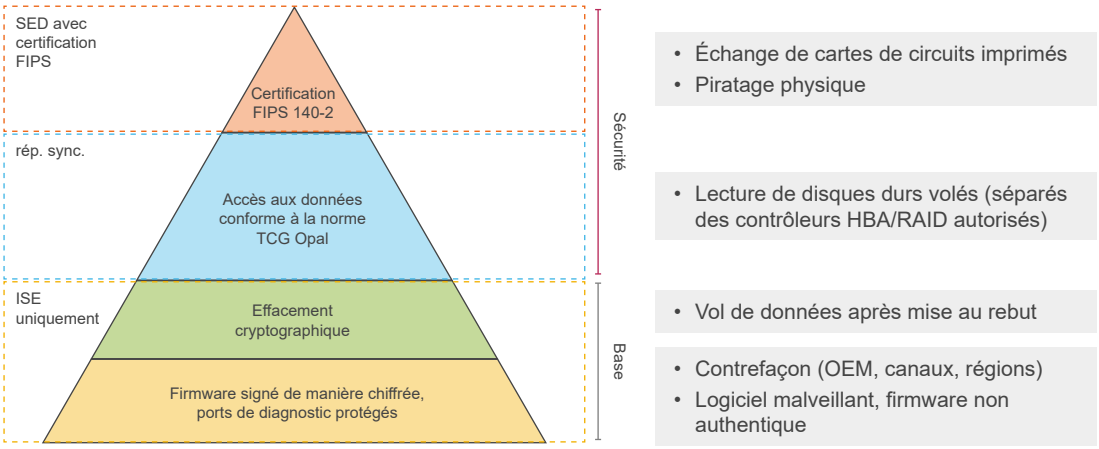
Si le firmware d'un périphérique est soupçonné de comportement malveillant, les administrateurs informatiques ont la possibilité de restaurer la plupart des images de firmware de la plate-forme vers une version antérieure de confiance stockée dans l'iDRAC. Nous conservons 2 versions de firmware du périphérique sur le serveur : la version de production existante (« N ») et une version antérieure de confiance (« N-1 »).

3.4 Stockage de données chiffrées

Les serveurs PowerEdge de 14e et 15e générations proposent plusieurs options de disques de stockage pour sécuriser les données. Comme illustré ci-dessous, les options commencent avec des disques durs qui prennent en charge la technologie ISE (Instant Secure Erase), une nouveauté qui permet d'effacer instantanément et en toute sécurité les données utilisateur. Les serveurs de 14e et 15e générations intègrent des disques durs compatibles ISE par défaut. La technologie ISE est abordée plus en détail ultérieurement dans ce document, dans le cadre de la description de la fonction System Erase (effacement du système).

L'option de sécurité la plus élevée suivante est constituée par les disques durs à chiffrement automatique (« Self-Encrypting Drives » ou SED) qui offrent une protection par verrouillage qui lie le disque dur de stockage au serveur et à la carte RAID utilisée. Cette option permet de se protéger contre le vol de disques par « effraction » et la perte ultérieure de données utilisateur sensibles. Si un voleur tente d'utiliser le disque dur, celui-ci ne connaîtra pas la phrase secrète requise, qui constitue la clé de verrouillage, et sera donc dans l'impossibilité d'accéder aux données du disque chiffré. Les clients peuvent se protéger contre le vol de l'intégralité du serveur à l'aide de la fonction de gestion des clés d'entreprise sécurisée (« Secured Enterprise Key Manager » ou SEKM), abordée plus loin dans ce document.

Le plus haut niveau de protection est assuré par les disques SED certifiés NIST FIPS 140-2. Les disques durs conformes à cette norme ont été accrédités par des laboratoires de test et présentent des étiquettes attestant de leur résistance au piratage. Les disques SED Dell EMC sont certifiés FIPS 140-2 par défaut.



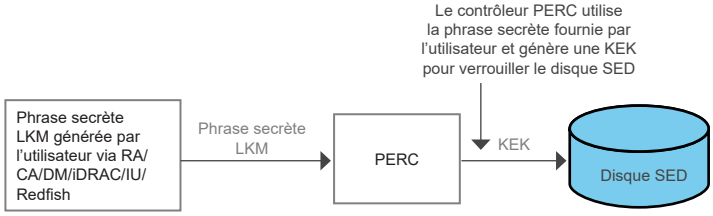
3.4.1 Chambre forte d'identifiants iDRAC

Le processeur de service de l'iDRAC fournit une mémoire de stockage sécurisée qui protège diverses données sensibles, telles que les informations d'identification de l'utilisateur iDRAC et les clés privées pour les certificats SSL auto-signés. Autre exemple de sécurité basée sur le silicium, cette mémoire est chiffrée à l'aide d'une clé racine unique immuable qui est programmée dans chaque puce d'iDRAC au moment de la fabrication. Cette solution offre une protection contre les attaques physiques au cours desquelles le pirate désolidarise la puce afin de tenter d'accéder aux données.

3.4.2 Gestion de clés locales (LKM)

Les serveurs PowerEdge actuels offrent aux utilisateurs la possibilité de sécuriser les disques SED connectés à un contrôleur PERC, à l'aide de la gestion des clés locales (« Local Key Management » ou LKM).

Pour assurer la protection des données utilisateur lorsqu'un disque dur est volé, le disque SED doit être verrouillé à l'aide d'une clé distincte afin qu'il ne déchiffre pas les données utilisateur, à moins que cette clé ne soit fournie. Cette clé est appelée la « clé de chiffrement de clé » (« Key Encryption Key » ou KEK). Pour ce faire, un utilisateur définit un ID de clé ou une phrase secrète sur le contrôleur PERC auquel le disque SED est connecté et le contrôleur PERC génère une KEK à l'aide de la phrase secrète, puis l'utilise pour verrouiller le disque SED. Dès lors que le disque dur est mis sous tension, il apparaît en tant que disque SED verrouillé et chiffrera/déchiffrera les données utilisateur uniquement lorsque la KEK est fournie pour le déverrouiller. Le contrôleur PERC fournit la KEK au disque pour le déverrouiller. Ainsi, si le disque dur est volé, il apparaît comme « verrouillé », et si le pirate est dans l'impossibilité de fournir la KEK, les données utilisateur sont alors protégées. La gestion est considérée comme locale, car la phrase secrète et la KEK sont stockées localement sur le contrôleur PERC. Le schéma suivant présente la solution LKM.

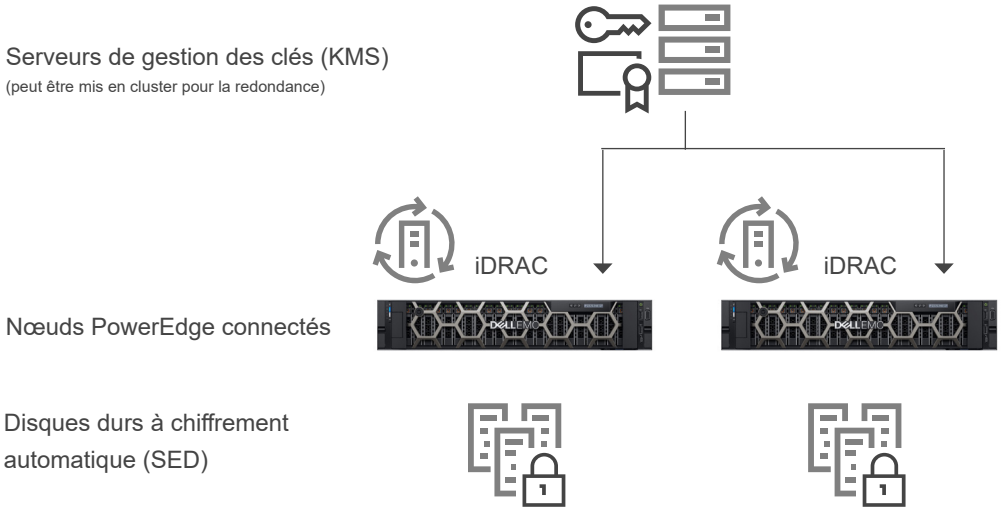


3.4.3 Gestion des clés d'entreprise sécurisée (SEKM)

La gestion des clés d'entreprise sécurisée d'OpenManage offre une solution de gestion des clés centralisée permettant de gérer les données au repos au sein de l'organisation. Cette solution permet au client d'utiliser un serveur de gestion des clés (« Key Management Server » ou KMS) externe afin de gérer les clés susceptibles d'être utilisées par l'iDRAC pour verrouiller et déverrouiller les périphériques de stockage sur un serveur Dell EMC PowerEdge. À l'aide du code intégré et activé au moyen d'une licence spéciale, l'iDRAC demande au serveur KMS de créer une clé pour chaque contrôleur de stockage, qu'il extrait et fournit à ce contrôleur à chaque démarrage de l'hôte, afin qu'il puisse déverrouiller le ou les disques durs à chiffrement automatique (SED).

Les avantages de l'utilisation de la SEKM plutôt que de la gestion de clés locales (LKM) sont les suivants :

- Protection contre le « vol d'un serveur », car les clés ne sont pas stockées sur le serveur, mais stockées en externe et extraites par les nœuds du serveur PowerEdge connectés (via l'iDRAC)
- Gestion des clés centralisée et évolutive pour les périphériques chiffrés avec une haute disponibilité
- Prise en charge du protocole KMIP standard, permettant ainsi l'utilisation d'autres périphériques compatibles KMIP
- Protection des données au repos lorsque les disques durs ou l'intégralité du serveur sont compromis
- Évolutivité des performances de chiffrement sur disque en fonction du nombre de disques durs



3.5 Sécurité matérielle

La sécurité matérielle fait partie intégrante de toute solution de sécurité complète. Certains clients souhaitent limiter l'accès aux ports d'entrée, comme les ports USB. Un boîtier de serveur n'a généralement pas besoin d'être ouvert une fois qu'il a été mis en production. Dans tous les cas, les clients souhaitent au minimum suivre et enregistrer de telles activités. L'objectif global est de décourager et de limiter toute intrusion physique.

3.5.1 Alerte d'intrusion dans le boîtier

Les serveurs PowerEdge proposent la détection et la journalisation des intrusions dans le matériel, avec une détection qui fonctionne même si aucune alimentation secteur n'est disponible. Les capteurs situés sur le boîtier détectent toute ouverture ou altération du boîtier, même pendant le transport. Les serveurs qui ont été ouverts lors de leur transport génèrent une entrée dans le journal du cycle de vie iDRAC une fois qu'ils sont mis sous tension.

3.5.2 Gestion dynamique des ports USB

Pour davantage de sécurité, vous pouvez désactiver complètement les ports USB. Vous avez également la possibilité de désactiver uniquement les ports USB situés en façade. Par exemple, les ports USB peuvent être désactivés pour une utilisation en production, puis temporairement activés pour fournir un accès d'urgence à une console à des fins de débogage.

3.5.3 iDRAC Direct

iDRAC Direct est un port USB spécial qui est relié par un câble au processeur de service iDRAC pour le débogage et la gestion depuis le serveur, à partir de la face avant du serveur (allée froide). Il permet à un utilisateur de connecter un câble USB standard micro-AB à ce port et l'autre extrémité (type A) à un ordinateur portable. Un navigateur Web standard peut ensuite accéder à l'interface graphique de l'iDRAC pour un débogage et une gestion étendus du serveur. Si une licence iDRAC Enterprise est installée, l'utilisateur peut même accéder au bureau du système d'exploitation via la fonction de console virtuelle de l'iDRAC.

Puisque des informations d'identification iDRAC classiques sont utilisées pour la connexion, iDRAC Direct agit comme un accès d'urgence sécurisé avec l'avantage supplémentaire de la gestion matérielle étendue et des diagnostics de service. Cela peut s'avérer être une option intéressante pour sécuriser l'accès physique au serveur sur les sites distants (les ports USB et les sorties VGA de l'hôte peuvent être désactivés dans ce cas).

3.5.4 Vue de connexion iDRAC avec géolocalisation

La vue de connexion permet à l'iDRAC de signaler les commutateurs externes et les ports connectés aux E/S du serveur. Il s'agit d'une fonction présente sur certains périphériques de gestion de réseau qui nécessite l'activation du protocole LLDP (Link Layer Discovery Protocol) sur les commutateurs connectés.

Voici quelques-uns des avantages de la vue de connexion :

- Vérifier à distance et rapidement si les modules d'E/S du serveur (LOM, NDC et les cartes d'extension PCIe) sont connectés aux commutateurs et aux ports adéquats
- Éviter l'envoi coûteux de techniciens sur place pour corriger les erreurs de câblage
- Plus de retraçage des câbles dans les allées chaudes de la salle serveur
- Peut être effectué via l'interface graphique utilisateur ou les commandes RACADM, peut fournir des informations pour toutes les connexions sur serveur de 14e génération

Au-delà des économies de temps et d'argent évidentes, la vue de connexion offre un avantage supplémentaire : fournir une géolocalisation en temps réel d'un serveur physique ou d'une machine virtuelle. À l'aide de la vue de connexion de l'iDRAC, les administrateurs peuvent localiser un serveur pour déterminer précisément quels commutateurs et quels ports y sont connectés, ce qui permet de sécuriser les serveurs qui sont connectés à des réseaux et à des périphériques qui ne sont pas conformes aux directives de sécurité ou aux pratiques d'excellence de l'entreprise.

La vue de connexion valide indirectement l'emplacement du serveur en indiquant l'identité des commutateurs auxquels il est connecté. L'identité du commutateur permet de déterminer la géolocalisation et de s'assurer que le serveur n'est pas un usurpateur sur un site non autorisé, ce qui fournit une couche de sécurité physique supplémentaire. Cela permet également de valider le fait qu'une application ou une machine virtuelle n'a pas « traversé » les frontières du pays et qu'elle s'exécute dans un environnement sécurisé et approuvé.

3.6 Intégrité et sécurité de la chaîne d'approvisionnement

L'intégrité de la chaîne d'approvisionnement concerne deux enjeux majeurs :

1. Maintenir l'intégrité du matériel : garantir qu'aucun piratage de produit ou insertion de composants contrefaits n'ait lieu avant l'envoi du produit au client ;
2. Maintenir l'intégrité des logiciels : garantir qu'aucun logiciel malveillant n'est inséré dans le firmware ou dans les pilotes de périphériques avant l'envoi du produit au client et éviter toute faille de sécurité dans le codage.

Dell EMC définit la sécurité de la chaîne d'approvisionnement comme la pratique et l'application de mesures de contrôle de prévention et de détection destinées à protéger les actifs physiques, l'inventaire, les informations, la propriété intellectuelle et les personnes. Ces mesures de sécurité permettent également de garantir l'intégrité et l'assurance de la chaîne d'approvisionnement en réduisant les possibilités d'introduction malveillante ou négligente de logiciels malveillants et de composants contrefaits dans la chaîne d'approvisionnement.

3.6.1 Intégrité matérielle et logicielle

Dell EMC s'attache à veiller à ce que les processus de contrôle de la qualité soient en place afin de minimiser les risques d'introduction de composants contrefaits dans sa chaîne d'approvisionnement. Les contrôles mis en place par Dell EMC couvrent la sélection des fournisseurs, l'approvisionnement, les processus de production et la gouvernance par le biais d'audits et de tests. Une fois qu'un fournisseur a été sélectionné, le nouveau processus d'introduction de produit vérifie que l'ensemble des ressources utilisées pendant toutes les étapes de construction proviennent d'une source figurant sur la liste des fournisseurs approuvés et correspondent à la nomenclature selon les besoins. Les inspections des ressources au cours de la production permettent d'identifier les composants marqués de manière inadéquate, s'écartant des paramètres de performances normaux ou contenant un identifiant électronique incorrect.

Lorsque cela est possible, les pièces sont achetées directement auprès du producteur de concepts d'origine (« Original Design Manufacturer » ou ODM) ou du fabricant de composant d'origine (« Original Component Manufacturer » ou OCM). L'inspection des ressources qui a lieu au cours du processus d'introduction du nouveau produit offre de nombreuses occasions d'identifier les composants contrefaits ou corrompus susceptibles d'avoir infiltré la chaîne d'approvisionnement.

En outre, Dell EMC maintient la certification ISO 9001 pour tous les sites de fabrication mondiaux. Le strict respect de ces processus et contrôles permet de minimiser le risque d'intégration de composants contrefaits au sein des produits Dell EMC, ou d'infiltration de logiciels malveillants dans les firmwares ou les pilotes de périphériques. Ces mesures sont mises en œuvre dans le cadre du processus de cycle de développement logiciel (« Software Development Lifecycle » ou SDL).

3.6.2 Sécurité physique

Dell EMC a, de longue date, mis en place diverses pratiques clés qui établissent et maintiennent la sécurité au sein des installations de fabrication et des réseaux logistiques. Par exemple, nous demandons à certaines usines dans lesquelles les produits Dell EMC sont fabriqués de répondre aux exigences de sécurité des installations de l'Association pour la protection des marchandises transportée (« Transported Asset Protection Association » ou TAPA), notamment de recourir à des caméras contrôlées en circuit fermé dans les zones clés, des contrôles d'accès et à la surveillance continue des entrées et sorties. Des mesures de protection ont également été mises en place pour protéger les produits contre le vol et le piratage pendant le transport dans le cadre d'un programme logistique leader sur le marché. Ce programme propose un centre de commande permanent afin de surveiller certaines expéditions entrantes et sortantes dans le monde entier et de garantir qu'elles transitent d'une destination à une autre sans interruption.

Dell EMC participe également activement à plusieurs programmes et initiatives volontaires de sécurité de la chaîne d'approvisionnement. L'une de ces initiatives concerne le Partenariat douane-commerce contre le terrorisme (« Customs-Trade Partnership Against Terrorism » ou C-TPAT), lancé par le gouvernement des États-Unis après les événements du 11 septembre 2001, pour contribuer à réduire le risque terroriste grâce à des mesures renforcées de sécurité de la chaîne d'approvisionnement et des frontières. Dans le cadre de cette initiative, le Service des douanes et de la protection des frontières des États-Unis demande aux membres participants de garantir l'intégrité de leurs pratiques en matière de sécurité et de communiquer leurs consignes de sécurité à leurs partenaires commerciaux au sein de la chaîne d'approvisionnement. Dell EMC est un participant actif depuis 2002 et conserve le statut de membre le plus élevé.

3.6.3 Dell Technologies Secured Component Verification (SCV) pour serveur PowerEdge

Dell Technologies Secured Component Verification (SCV) pour serveur PowerEdge est une offre d'assurance de la chaîne d'approvisionnement qui permet aux clients Dell EMC de vérifier qu'un serveur PowerEdge reçu correspond à ce qui a été fabriqué en usine. Afin de valider les composants de manière sécurisée par chiffrement, un certificat, qui contient les ID de composants uniques pour un serveur spécifique, est généré en usine au cours du processus de fabrication. Ce certificat est signé dans l'usine Dell Technologies et stocké dans l'iDRAC, puis utilisé ultérieurement par le client dans l'application SCV. Le client utilise l'application SCV pour récupérer l'inventaire courant du système, y compris les ID de composants uniques, et le valide après comparaison avec l'inventaire figurant dans le certificat SCV.

Le rapport généré par l'application SCV vérifie quels composants correspondent et quels composants diffèrent par rapport à ce qui a été installé en usine. Il vérifie également le certificat et la chaîne de confiance, ainsi que la preuve de possession de la clé privée SCV pour l'iDRAC. L'implémentation actuelle prend en charge les clients en expédition directe, mais n'inclut pas les scénarios liés aux revendeurs à valeur ajoutée (RVA) ou de remplacement des pièces.

4. Détection

Il est essentiel de disposer d'une fonctionnalité de détection qui offre une visibilité complète sur la configuration, l'état de santé et les événements de modification au sein d'un système de serveur. Cette visibilité doit également être en mesure de détecter les modifications malveillantes ou autres apportées au BIOS, au firmware et aux mémoires ROM facultatives au cours du processus de démarrage et d'exécution du système d'exploitation. L'interrogation proactive doit être associée à la possibilité d'envoyer des alertes pour tous les événements se déroulant au sein du système. Les journaux doivent fournir des informations complètes concernant l'accès et les modifications apportées au serveur. Plus important encore, le serveur doit étendre ces fonctionnalités à tous les composants.

4.1 Surveillance complète via l'iDRAC

Plutôt que de dépendre des agents du système d'exploitation pour communiquer avec les ressources gérées d'un serveur, l'iDRAC utilise un chemin d'accès direct à bande latérale vers chaque périphérique. Dell EMC a utilisé des protocoles standard tels que MCTP, NC-SI et NVMe-MI pour communiquer avec des périphériques comme les contrôleurs RAID PERC, les cartes NIC Ethernet, les adaptateurs HBA Fibre Channel, les adaptateurs HBA SAS et les disques NVMe. Cette architecture est le fruit de longs partenariats pluriannuels avec des fournisseurs leaders sur le marché ayant pour finalité de proposer une gestion des périphériques sans agent dans nos serveurs PowerEdge. Les opérations de configuration et de mise à jour de firmware tirent également parti des puissantes fonctions UEFI et HII prises en charge par Dell EMC et ses partenaires.

Avec cette fonctionnalité, l'iDRAC peut surveiller le système en se concentrant sur les événements de configuration, les événements d'intrusion (comme la détection des intrusions dans le boîtier mentionnée précédemment dans ce document) et les changements de l'état de santé. Les événements de configuration sont directement liés à l'identité de l'utilisateur qui a initié la modification, qu'il s'agisse d'un utilisateur de l'interface graphique, de l'API ou de la console.

4.1.1 Journal du cycle de vie

Le journal du cycle de vie est constitué d'un ensemble d'événements se produisant au sein d'un serveur sur une période donnée. Le journal du cycle de vie fournit une description des événements avec des horodatages, la gravité, l'ID utilisateur ou la source, les actions recommandées et d'autres informations techniques qui pourraient s'avérer très utiles à des fins de surveillance ou d'alerte.

Les différents types d'informations enregistrées dans le journal du cycle de vie (« Lifecycle Log » ou LCL) sont les suivants :

- Modifications de configuration des composants matériels du système
- Modifications de configuration de l'iDRAC, du BIOS, de la carte NIC et du RAID
- Journaux de toutes les opérations distantes
- Historique des mises à jour de firmware en fonction du périphérique, de la version et de la date
- Informations sur les pièces remplacées
- Informations sur les pièces défectueuses
- ID d'événement et de message d'erreur
- Événements liés à l'alimentation de l'hôte
- Erreurs POST
- Événements de connexion utilisateur
- Événements de modification de l'état d'un capteur

4.1.2 Alertes

L'iDRAC offre la possibilité de configurer différentes alertes d'événements ainsi que les actions à effectuer lorsqu'un événement particulier de journaux de cycle de vie se produit. Lorsqu'un événement est généré, il est transféré vers les destinations configurées à l'aide des mécanismes de type d'alerte sélectionnés. Il est possible d'activer ou de désactiver les alertes via l'interface Web de l'iDRAC, la commande RACADM ou avec l'utilitaire des paramètres iDRAC.

L'iDRAC prend en charge différents types d'alertes, telles que :

- Alerte par e-mail ou IPMI
- Trap SNMP
- Journaux du système d'exploitation et du système distant
- Événement Redfish

Les alertes peuvent également être classées par gravité : critique, avertissement ou information.

Les filtres suivants peuvent être appliqués aux alertes :

- Santé du système : par exemple, la température, la tension ou les erreurs de périphérique
- Santé du stockage : par exemple, erreurs de contrôleur, erreurs de disque physique ou virtuel
- Modifications de configuration : par exemple, modification de la configuration RAID, retrait de la carte PCIe
- Journaux d'audit : par exemple, échec de l'authentification par mot de passe
- Firmware/pilote : par exemple, mises à niveau ou retour à une version antérieure

Enfin, l'administrateur informatique a la possibilité de définir différentes actions pour les alertes : redémarrage, cycle d'alimentation, mise hors tension ou aucune action.

4.2 Détection de dérive

En appliquant des configurations standardisées et en adoptant une politique de « tolérance zéro » pour toute modification, les organisations peuvent réduire le risque d'exploitation. La console Dell EMC OpenManage Enterprise permet au client de définir sa propre référence en matière de configuration des serveurs, puis de surveiller leurs dérives par rapport à ces références. La référence peut être élaborée en fonction de différents critères permettant de s'ajuster à différentes exécutions de production, telles que la sécurité et les performances. OpenManage Enterprise peut signaler tout écart par rapport à la référence et, en option, réparer l'écart avec un workflow simple pour cadrer les modifications sur l'iDRAC hors bande. Les modifications peuvent alors avoir lieu lors des fenêtres de maintenance suivantes, pendant que les serveurs redémarrent afin de retrouver la conformité de l'environnement de production. Ce processus échelonné permet au client de déployer les modifications de configuration en production sans aucune interruption de service du serveur au cours des heures de maintenance. Il améliore la disponibilité du serveur sans compromettre la facilité de maintenance ni la sécurité.

5. Récupération

Les solutions de serveurs doivent prendre en charge la récupération vers un état connu et cohérent en réponse à divers événements :

- Failles de sécurité nouvellement découvertes
- Attaques malveillantes et piratage de données
- Corruption du firmware en raison d'une défaillance de la mémoire ou de procédures de mise à jour inadéquates
- Remplacement des composants du serveur
- Mise au rebut ou réaffectation d'un serveur

Ci-dessous, nous allons aborder en détail les réponses que nous apportons face aux nouvelles failles de sécurité et aux problèmes de corruption, ainsi que nos solutions de restauration du serveur à son état d'origine, le cas échéant.

5.1 Réponse rapide aux nouvelles failles de sécurité

Les failles de sécurité et expositions courantes (« Common Vulnerabilities and Exposures » ou CVE) correspondent à des vecteurs d'attaque nouvellement détectés qui compromettent les produits logiciels et matériels. La plupart des sociétés requièrent des réponses opportunes aux CVE afin de pouvoir évaluer rapidement leur exposition et prendre les mesures appropriées.

Les CVE peuvent être émises en réponse aux nouvelles failles de sécurité identifiées dans de nombreux éléments, notamment :

- Code Open Source, tel que OpenSSL
- Navigateurs Web et autres logiciels d'accès à Internet
- Matériel et firmware des produits de fournisseurs
- Systèmes d'exploitation et hyperviseurs

Dell EMC travaille sans relâche pour répondre rapidement aux nouvelles CVE de ses serveurs PowerEdge et fournir aux clients des informations appropriées, notamment :

- Les produits concernés
- Les mesures correctives à engager
- Si nécessaire, la date de mise à disposition des mises à jour afin de traiter la CVE

5.2 Récupération du BIOS et du SE

Les serveurs Dell EMC PowerEdge de 14e et 15e générations intègrent deux types de récupération : la récupération du BIOS et la récupération rapide du système d'exploitation (OS). Ces fonctionnalités permettent une récupération rapide à partir d'images corrompues du BIOS ou du système d'exploitation. Dans les deux cas, une zone de stockage spéciale est masquée par le logiciel d'exécution (BIOS, système d'exploitation, firmware de périphérique, etc.). Ces zones de stockage contiennent des images non compromises qui peuvent être utilisées comme alternative au logiciel principal compromis.

La récupération rapide de système d'exploitation permet une récupération rapide à partir d'une image de SE corrompue (ou d'une image de SE suspectée d'avoir subi une falsification malveillante). La récupération peut être réalisée via une carte SD interne, des ports SATA, des disques M.2 ou un port USB interne. Le périphérique sélectionné peut être exposé à la liste de démarrage et au système d'exploitation pour l'installation de l'image de récupération. Il peut ensuite être désactivé et dissimulé à la liste de démarrage et au système d'exploitation. Dans l'état dissimulé, le BIOS désactive le périphérique pour qu'il ne soit pas accessible par le système d'exploitation. Dans le cas d'une image de système d'exploitation corrompue, l'emplacement de récupération peut alors être activé pour le démarrage. Ces paramètres sont accessibles via le BIOS ou l'interface iDRAC.

Dans les cas extrêmes, si le BIOS est corrompu (soit en raison d'une attaque malveillante, soit en raison d'une perte d'alimentation au cours du processus de mise à jour, soit en raison d'un autre événement imprévu), il est important de fournir un moyen de restaurer le BIOS vers son état d'origine. Une image de sauvegarde du BIOS est stockée dans l'iDRAC afin de pouvoir récupérer l'image du BIOS si nécessaire. L'iDRAC orchestre l'intégralité du processus de récupération de bout en bout.

- La récupération automatique du BIOS est lancée par le BIOS lui-même.
- La récupération du BIOS à la demande peut être lancée par les utilisateurs à l'aide de la commande CLI RACADM.

5.3 Restauration du firmware

Il est recommandé d'avoir un firmware à jour afin de s'assurer de disposer des dernières fonctionnalités et mises à jour de sécurité. Cependant, il peut être nécessaire de restaurer une mise à jour ou d'installer une version antérieure si des problèmes apparaissent après une mise à jour. Si vous effectuez une restauration vers une version précédente, la signature du firmware fait également l'objet d'une vérification.

La restauration du firmware à partir de la version de production existante « N » vers une version antérieure « N-1 » est actuellement prise en charge pour les images de firmware suivantes :

- BIOS
- iDRAC avec Lifecycle Controller
- Carte d'interface réseau (NIC)
- Contrôleur RAID PowerEdge (PERC)
- Bloc d'alimentation
- Fond de panier

Vous pouvez restaurer le firmware sur la version précédemment installée (« N-1 ») à l'aide de l'une des méthodes suivantes :

- Interface Web de l'iDRAC
- Interface Web Dell CMC
- CLI RACADM – iDRAC et CMC
- Interface graphique du Lifecycle Controller
- Services Lifecycle Controller à distance

Il est possible de restaurer le firmware de l'iDRAC ou de tout autre périphérique pris en charge par Lifecycle Controller, même si la mise à niveau a été effectuée auparavant à l'aide d'une autre interface. Par exemple, si le firmware a été mis à niveau à l'aide de l'interface graphique du Lifecycle Controller, vous pouvez le restaurer à l'aide de l'interface Web de l'iDRAC. Vous pouvez restaurer le firmware de plusieurs périphériques grâce à un seul redémarrage du système.

Sur les serveurs PowerEdge de 14e et 15e générations dotés d'un seul firmware pour l'iDRAC et le Lifecycle Controller, le fait de restaurer le firmware de l'iDRAC restaure également le firmware du Lifecycle Controller.

5.4 Restauration de la configuration du serveur après la maintenance du matériel

La mise en place de mesures correctives face aux événements de service est un élément essentiel de toute opération informatique. La capacité à atteindre les objectifs de temps de reprise et les objectifs de perte de données maximale admissible a des implications directes sur la sécurité de la solution. La restauration de la configuration et du firmware du serveur garantit automatiquement le respect des politiques de sécurité en matière de fonctionnement du serveur.

Les serveurs PowerEdge proposent une fonction de restauration rapide de la configuration du serveur dans les situations suivantes :

- Remplacement de pièces individuelles
- Remplacement de la carte mère (sauvegarde et restauration complètes du profil du serveur)
- Remplacement de la carte mère (Easy Restore)

5.4.1 Remplacement des pièces

L'iDRAC enregistre automatiquement l'image du firmware et les paramètres de configuration pour les cartes NIC, les contrôleurs RAID et les blocs d'alimentation. En cas de remplacement de ces pièces sur site, l'iDRAC détecte automatiquement la nouvelle carte et restaure le firmware et la configuration sur cette dernière. Cette fonctionnalité permet d'économiser un temps précieux et de garantir la cohérence de la configuration et de la politique de sécurité. La mise à jour s'effectue automatiquement lors du redémarrage du système après le remplacement de la pièce prise en charge.

5.4.2 Easy Restore (pour le remplacement de la carte mère)

Le remplacement de la carte mère peut prendre du temps et affecter la productivité. L'iDRAC offre la possibilité de sauvegarder et de restaurer la configuration et le firmware d'un serveur PowerEdge afin de minimiser les efforts nécessaires au remplacement d'une carte mère défaillante.

Le serveur PowerEdge dispose de deux moyens pour effectuer des sauvegardes et des restaurations :

1. Les serveurs PowerEdge sauvegardent automatiquement les paramètres de configuration du système (BIOS, iDRAC, NIC), le numéro de série, l'application de diagnostic UEFI et d'autres données sous licence sur la mémoire Flash.

   Après avoir remplacé la carte mère de votre serveur, la fonction Easy Restore vous invite à restaurer automatiquement ces données.

2. Pour une sauvegarde plus complète, un utilisateur a la possibilité de sauvegarder la configuration du système, y compris les images de firmware installées sur différents composants tels que le BIOS, les contrôleurs RAID, les cartes NIC, l'iDRAC, le Lifecycle Controller et les cartes filles réseau (« Network Daughter Cards » ou NDC), ainsi que les paramètres de configuration de ces composants. L'opération de sauvegarde inclut également les données de configuration du disque dur, la carte mère et les pièces remplacées. La sauvegarde crée un fichier unique que vous pouvez enregistrer sur une carte SD vFlash ou un partage réseau (CIFS, NFS, HTTP ou HTTPs).

   Cette sauvegarde de profil peut être restaurée à tout moment par l'utilisateur. Dell EMC vous recommande d'effectuer l'opération de sauvegarde pour chaque profil de système que vous pensez devoir restaurer à un moment donné.

5.5 System Erase

À la fin du cycle de vie d'un système, celui-ci doit être retiré ou réaffecté. L'objectif de System Erase est d'effacer les données et les paramètres sensibles des périphériques de stockage du serveur et des magasins non volatils du serveur, tels que les mémoires cache et les journaux, de façon à ce qu'aucune information confidentielle ne soit divulguée de manière involontaire. Il s'agit d'un utilitaire de Lifecycle Controller conçu pour effacer les journaux, les données de configuration, les données de stockage, la mémoire cache et toutes les applications intégrées.

Les périphériques, paramètres de configuration et applications suivants peuvent être supprimés à l'aide de la fonction System Erase :

- iDRAC réinitialisé à sa valeur par défaut
- Données de Lifecycle Controller (LC)
- BIOS
- Packs intégrés de diagnostic et de pilotes de système d'exploitation
- iSM
- Rapports de collecte SupportAssist

En outre, les composants suivants peuvent également être supprimés :

- Cache du matériel (effacement de la mémoire NVCache du contrôleur PERC)
- Carte SD vFlash (initialisation de la carte) (Remarque : vFlash n'est pas disponible sur les serveurs de 15e génération ou ultérieurs.)

Les données des composants suivants sont supprimées de manière cryptographique par System Erase, comme décrit ci-dessous :

- Disques à chiffrement automatique (SED)
- Disques ISE uniquement (Instant Secure Erase)
- Périphériques NVM (mémoires Apache Pass, NVDIMM)

De plus, les disques durs SATA non ISE peuvent être effacés par écrasement des données.

Notez que la fonction Instant Secure Erase (ISE) détruit la clé de chiffrement interne utilisée dans les disques des serveurs de 14e et 15e générations, rendant ainsi les données utilisateur irrécupérables. ISE est une méthode reconnue d'effacement de données sur les disques de stockage qui est évoquée dans la publication spéciale du NIST 800-88 « Guidelines for Media Sanitization » (directives pour le nettoyage des données présentes sur les supports).

Les avantages de la nouvelle fonction ISE avec System Erase sont les suivants :

- **Vitesse :** bien plus rapide que les techniques d'écrasement des données telles que la méthode 5220.22-M du département de la Défense des États-Unis (quelques secondes contre plusieurs heures)
- **Efficacité :** ISE rend toutes les données du disque dur, y compris les blocs réservés, complètement illisibles
- **Meilleur coût TCO :** les périphériques de stockage peuvent être réutilisés au lieu d'être écrasés ou physiquement détruits

L'opération System Erase peut être effectuée avec les méthodes suivantes :

- Interface graphique Lifecycle Controller (F10)
- CLI RACADM
- Redfish

5.6 Sélection du chiffrement d'iDRAC9

La sélection de la suite de chiffrement peut permettre de limiter les chiffrements utilisés par le navigateur Web pour communiquer avec l'iDRAC. Elle peut également
déterminer le niveau de sécurité de la connexion. Ces paramètres peuvent être configurés via l'interface Web de l'iDRAC, la commande RACADM et Redfish. Cette fonctionnalité est disponible sur plusieurs versions d'iDRAC : iDRAC7, iDRAC8 (2.60.60.60 et ultérieure) et l'iDRAC9 actuel (3.30.30.30 et versions ultérieures).

5.7 Prise en charge CNSA

Les chiffrements pris en charge disponibles dans iDRAC9 avec TLS1.2 et le chiffrement 256 bits sont indiqués dans la capture d'écran ci-dessous. Les chiffrements disponibles sont inclus dans l'ensemble approuvé par le protocole CNSA.

5.8 Cycle d'alimentation complet

Au cours d'un cycle d'alimentation complet, le serveur ainsi que tous ses composants sont redémarrés. Cette opération draine l'alimentation principale et auxiliaire du serveur et de tous les composants. Toutes les données contenues dans la mémoire volatile sont également effacées.

Un cycle d'alimentation complet physique nécessite de retirer le câble d'alimentation secteur, d'attendre 30 secondes, puis de remettre le câble en place. Cela pose un problème lorsqu'il s'agit d'un système distant. Une nouvelle fonctionnalité des serveurs de 14e et 15e générations vous permet d'effectuer un cycle d'alimentation complet efficace à partir du module de service iDRAC (iSM), de l'interface graphique de l'iDRAC, du BIOS ou d'un script. Le cycle d'alimentation complet prend effet au cycle d'alimentation suivant.

La fonction de cycle d'alimentation complet supprime la nécessité de la présence physique d'une personne dans le datacenter, réduisant ainsi la durée du dépannage. Elle est capable d'éliminer, par exemple, tout logiciel malveillant qui réside encore dans la mémoire.

6. Résumé

La sécurité des datacenters est primordiale pour la réussite de l'entreprise et la sécurité de l'infrastructure de serveurs sous-jacente est essentielle. Les cyberattaques peuvent provoquer de longues interruptions de service des systèmes et de l'activité, une perte de chiffre d'affaires et de clients, des préjudices juridiques et une réputation d'entreprise ternie. Pour se protéger des cyberattaques ciblant le matériel, les détecter et s'en remettre, la sécurité doit être intégrée à la conception matérielle du serveur et non ajoutée par la suite.

Dell EMC a été un leader de l'utilisation d'une solution de sécurité basée sur le silicium pour sécuriser le firmware et protéger les données utilisateur sensibles des serveurs PowerEdge des deux dernières générations. Les lignes de produits PowerEdge de 14e et 15e générations sont dotées d'une architecture cyber-résiliente améliorée qui utilise une racine de confiance basée sur le silicium pour renforcer la sécurité des serveurs, avec notamment les fonctions suivantes :

- **Démarrage de confiance vérifié de manière chiffrée :** ancre la sécurité du serveur de bout en bout et la sécurité globale du datacenter. Il comprend des fonctions telles que la racine de confiance basée sur le silicium, le firmware signé numériquement et la récupération automatique du BIOS.
- **Secure Boot :** vérifie les signatures cryptographiques des pilotes UEFI et d'autres codes chargés avant l'exécution du système d'exploitation.
- **Chambre forte d'identifiants iDRAC :** espace de stockage sécurisé pour les informations d'identification, les certificats et les autres données sensibles chiffrées à l'aide d'une clé à base de silicium qui est propre à chaque serveur.
- **System Lockdown dynamique :** une fonctionnalité propre à PowerEdge, cette fonction contribue à sécuriser la configuration et le firmware de n'importe quel système face aux modifications malveillantes ou involontaires, tout en alertant les utilisateurs de toute tentative de modification du système.
- **Gestion des clés d'entreprise :** offre une solution de gestion des clés centralisée permettant de gérer les données au repos au sein de l'organisation.
- **System Erase :** permet aux utilisateurs de procéder au retrait ou de réaffecter facilement leurs serveurs PowerEdge de 14e et 15e générations en effaçant les données de manière sécurisée et rapide des disques de stockage et autres modules de mémoire non volatile intégrés.
- **Sécurité de la chaîne d'approvisionnement :** fournit une assurance de la chaîne d'approvisionnement en veillant à ce qu'aucun produit ne soit piraté ou qu'aucun composant ne soit contrefait avant l'envoi des produits aux clients.

En conclusion, les serveurs PowerEdge de 14e et 15e générations, avec leur sécurité leader sur le marché, constituent une base de confiance pour la transformation de l'IT, sur laquelle les clients pourront exécuter leurs opérations informatiques et leurs charges applicatives en toute sécurité.

A. Annexe : Autres lectures

Livres blancs et documents sur la sécurité

- (Direct from Development) SYSTEM ERASE SUR LES SERVEURS POWEREDGE
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444242
- SÉCURISATION DES SERVEURS DELL EMC POWEREDGE DE 14E GÉNÉRATION AVEC SYSTEM ERASE
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444269
- (Direct from Development) SÉCURITÉ DANS LA CONCEPTION DE SERVEURS
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444243
- (Direct from Development) LA CYBER-RÉSILIENCE COMMENCE AU NIVEAU DU CHIPSET ET DU BIOS
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444061
- MOT DE PASSE IDRAC9 PAR DÉFAUT GÉNÉRÉ EN USINE
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444368
- RÉPONSE DE DELL EMC AVEC l'IDRAC À L'ATTAQUE CVE-2017-1000251 « BLUEBORNE »
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444605
- (Vidéo) CONFIGURATION DE SECURE BOOT ET GESTION DES CERTIFICATS À L'AIDE DE RACADM
  https://youtu.be/mrIIN4X380c
- GESTION DE SECURE BOOT SUR LES SERVEURS DELL EMC POWEREDGE
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444259/download
- Signature d'images UEFI pour la fonction Secure Boot dans les serveurs Dell EMC PowerEdge de 14e et 15e générations et versions ultérieures
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444255
- RÉCUPÉRATION RAPIDE DU SYSTÈME D'EXPLOITATION
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444249
- Gestion des alertes d'événements iDRAC9 sur les serveurs Dell EMC PowerEdge de 14e génération (14G)
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444266
- Personnalisation du Secure Boot UEFI
  https://media.defense.gov/2020/Sep/15/2002497594/-1/-1/0/CTR-UEFI-Secure-Boot-Customization-UOO168873-20.PDF

Livres blancs PowerEdge

- Présentation de l'iDRAC
  http://www.DellTechCenter.com/iDRAC
- Présentation de la console OpenManage
  http://www.DellTechCenter.com/OME
- Présentation de la solution OpenManage Mobile
  http://www.DellTechCenter.com/OMM
- Remplacement de pièces du Lifecycle Controller
  http://en.community.dell.com/techcenter/extras/m/white_papers/20276457
- Remplacement de la carte mère
  http://en.community.dell.com/techcenter/extras/m/white_papers/20168832
- Inscription automatique des certificats iDRAC
  https://www.dellemc.com/resources/fr-fr/asset/white-papers/products/software/direct-from-development-idrac-automatic-certificate-enrollment.pdf
- Amélioration des fonctions de sécurité des serveurs dans iDRAC9 à l'aide de SELinux
  https://downloads.dell.com/manuals/all-products/esuprt_solutions_int/esuprt_solutions_int_solutions_resources/dell-management-solution-resources_white-papers20_fr-fr.pdf
- Sélection du chiffrement iDRAC9 – amélioration de la sécurité des serveurs Dell EMC PowerEdge
  https://downloads.dell.com/manuals/all-products/esuprt_software_int/esuprt_software_ent_systems_mgmt/idrac9-lifecycle-controller-v33-series_white-papers11_fr-fr.pdf

En savoir plus sur les serveurs PowerEdge

En savoir plus sur nos nouveaux serveurs PowerEdge

En savoir plus sur nos solutions de gestion des systèmes

Effectuer une recherche dans notre bibliothèque de ressources

Suivre les serveurs PowerEdge sur Twitter

Contacter un expert Dell Technologies pour une question sur les ventes ou le support

DELL Technologies