La Securitée de VMware V-Center

Realisée Par:
Wissal BOUTAYEB

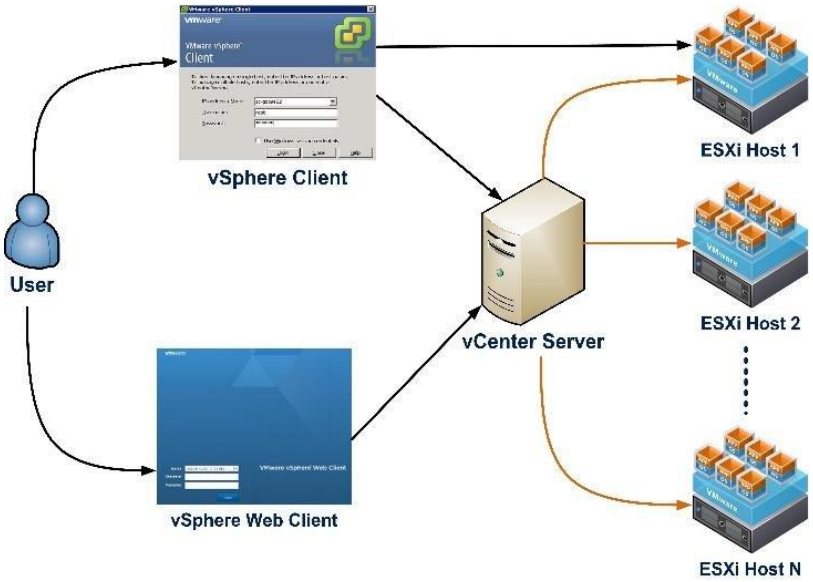
Encadree Par:
M.AMAMOU Ahmed

Sommaire

Dans l'infrastructure informatique contemporaine, la virtualisation représente un élément vital, permettant une gestion agile et efficace des ressources. Au cœur de cet écosystème se trouve VMware vCenter, une plateforme cruciale pour la gestion des environnements virtualisés. Toutefois, avec l'évolution constante des menaces en ligne, la sécurité de VMware vCenter est devenue une priorité majeure pour les organisations cherchant à protéger leurs données et leurs opérations.

Ce rapport se concentre sur l'évaluation et la recommandation des meilleures pratiques de sécurité pour VMware vCenter. Notre objectif est d'identifier les vulnérabilités potentielles, d'explorer les stratégies de configuration et de gestion des accès, et de proposer des mesures concrètes pour garantir la sécurité et l'intégrité de l'infrastructure virtualisée.

- **Contexte et Description de VMware vCenter :**



VMware vCenter se démarque en tant que plateforme de gestion centrale pour les environnements virtualisés. Cette solution permet aux entreprises de simplifier la gestion de leurs ressources informatiques en consolidant et en optimisant l'utilisation de leurs serveurs physiques. Grâce à VMware vCenter, les administrateurs peuvent efficacement créer, déployer, surveiller et gérer des machines virtuelles, garantissant ainsi une infrastructure informatique robuste et agile.

- **Points Essentiels pour Maintenir la Sécurité de VMware vCenter**

1. Sécurisation de l'hyperviseur ESXi :

Limiter l'accès à ESXi :

Par défaut, les services ESXi Shell et SSH ne s'exécutent pas et seul l'utilisateur racine peut se connecter à l'interface utilisateur de la console directe (DCUI). Si nous décidons d'activer l'accès à ESXi ou SSH, nous pouvons définir des délais d'expiration pour limiter le risque d'accès non autorisé.

Gestion des comptes utilisateurs :

Créent des comptes utilisateur distincts avec des privilèges appropriés et limitant l'accès uniquement aux administrateurs nécessaires. Toute en Évitant l'utilisation du compte root sauf lorsque c'est absolument nécessaire.

Réduire le nombre de ports de pare-feu ESXi ouverts :

ESXi contient un pare-feu activé par défaut.

Au moment de l'installation, le pare-feu ESXi est configuré pour bloquer le trafic entrant et sortant, sauf le trafic des services activés dans le profil de sécurité de l'hôte.

Réfléchissons bien avant d'ouvrir des ports sur le pare-feu, car l'accès illimité aux services qui s'exécutent sur un hôte ESXi peut exposer ce dernier aux attaques extérieures et aux accès non autorisés. Pour minimiser les risques, configurant le pare-feu ESXi de manière à autoriser l'accès uniquement depuis les réseaux autorisés.

Gérer les paramètres du pare-feu ESXi :

Nous pouvons configurer les connexions de pare-feu entrantes et sortantes pour un agent de service ou de gestion dans vSphere Client ou sur la ligne de commande.

Ajouter des adresses IP autorisées pour un hôte ESXi :

Par défaut, le pare-feu de chaque service autorise l'accès à toutes les adresses IP. Pour restreindre le trafic, modifions chaque service pour autoriser uniquement le trafic provenant de notre sous-réseau de gestion. Nous pouvons également annuler la sélection de certains services si notre environnement ne les utilise pas

Gérer les certificats ESXi :

Utilisation des certificats signés par une CA de confiance : L'Obtention des certificats signés par une CA de confiance pour nos hôtes ESXi. Cela garantit que les certificats sont émis par une source fiable et permet aux clients et aux utilisateurs de vérifier l'authenticité de notre environnement ESXI.

Renouveler ou actualiser des certificats ESXi : Si l'autorité de certification VMware (VMCA) attribue des certificats à nos hôtes ESXi (6.0 et version ultérieure), nous pouvons renouveler ces certificats à partir de vSphere Client. Nous pouvons également actualiser tous les certificats du magasin TRUSTED_ROOTS associés à vCenter Server.

Envisager l'authentification par carte à puce :

Nous pouvons utiliser l'authentification par carte à puce pour se connecter à l'interface DCUI (Direct Console User Interface) ESXi à l'aide d'une carte à puce PIV (Personal Identity Verification), CAC (Common Access Card) ou SC650 au lieu d'entrer un nom d'utilisateur et un mot de passe.

Une carte à puce est une petite carte en plastique dotée d'une puce de circuit intégré. Beaucoup d'organismes publics et de grandes entreprises utilisent l'authentification à deux facteurs basée sur carte à puce pour renforcer la sécurité de leurs systèmes et respecter les réglementations de sécurité.

Lorsque l'authentification par carte à puce est activée sur un hôte ESXi, l'interface DCUI vous invite à entrer une combinaison valide de carte à puce et de code PIN. Cette invite remplace l'invite par défaut qui demande d'entrer un nom d'utilisateur et un mot de passe.

1. Lorsque nous insérant la carte à puce dans le lecteur de carte à puce, l'hôte ESXi lit les informations d'identification qui s'y trouvent.
2. L'interface DCUI ESXi affiche notre ID de connexion et nous invite à entrer notre code PIN.

3. Une fois que nous avons entré le PIN, l'hôte ESXi établit la correspondance entre celui-ci et le PIN stocké sur la carte à puce et vérifie le certificat de la carte à puce à l'aide d'Active Directory.
4. Une fois le certificat de la carte à puce vérifié, ESXi nous connecte à l'interface DCUI.

2. Sécurisation des systèmes vCenter Server et services associés :

VCenter et communication chiffrée :

V-Sphere utilise deux niveaux de chiffrement sous la forme d'une clé de chiffrement de clés (KEK) et d'une clé de chiffrement des données (DEK). Brièvement, un hôte ESXi génère une clé DEK pour chiffrer les machines virtuelles et les disques. La clé KEK est fournie par un serveur de clés et chiffre (ou « encapsule ») la clé DEK. La clé KEK est chiffrée à l'aide de l'algorithme AES256 et la clé DEK est chiffrée à l'aide de l'algorithme XTS-AES-256. Selon le type de fournisseur de clés, différentes méthodes sont utilisées pour créer et gérer les clés DEK et KEK.

Le fournisseur de clés standard fonctionne comme suit.

1. L'hôte ESXi génère et utilise des clés internes pour chiffrer des machines virtuelles et des disques. Ces clés sont utilisées comme clés DEK.
2. vCenter Server demande les clés au serveur de clés (KMS). Ces clés sont utilisées comme clés KEK. vCenter Server stocke uniquement l'identifiant de chaque KEK et non la clé elle-même.
3. ESXi utilise la clé KEK pour chiffrer les clés internes et stocke la clé interne chiffrée sur le disque. ESXi ne stocke pas la clé KEK sur le disque. Lorsqu'un hôte redémarre, vCenter Server demande la clé KEK avec l'ID correspondant au serveur de clés et la met à la disposition du produit ESXi. ESXi peut alors déchiffrer les clés internes si nécessaire.

Le fournisseur de clés approuvé Autorité d'approbation vSphere fonctionne comme suit.

1. L'instance de vCenter Server du cluster approuvé vérifie si le fournisseur de clés approuvé par défaut est accessible à l'hôte ESXi sur lequel la machine virtuelle chiffrée doit être créée.
2. L'instance de vCenter Server du cluster approuvé ajoute le fournisseur de clés approuvé à la machine virtuelle ConfigSpec.
3. La demande de création de la machine virtuelle est envoyée à l'hôte ESXi.
4. Si un jeton d'attestation n'est pas déjà disponible pour l'hôte ESXi, il en demande un à partir du service d'attestation.
5. Le service de fournisseur de clés valide le jeton d'attestation et crée une KEK à envoyer à l'hôte ESXi. La clé KEK est encapsulée (chiffrée) avec la clé principale qui est configurée sur le fournisseur de clés. Les deux types de texte chiffré KEK et de texte brut KEK sont renvoyés à l'hôte approuvé.
6. L'hôte ESXi génère une clé DEK pour chiffrer les disques de la machine virtuelle.
7. La clé KEK est utilisé pour encapsuler les DEK générés par l'hôte ESXi et le texte chiffré du fournisseur de clés est stocké avec les données chiffrées.
8. La machine virtuelle est chiffrée et écrite dans le stockage.

Configuration de PTP ou NTP :

1. Synchronisation précise de l'heure : En assurant une synchronisation précise de l'heure sur tous les hôtes ESXi via PTP ou NTP, nous garantissons que les horloges système sont uniformément alignées. Cela est crucial pour les mécanismes de sécurité tels que les certificats SSL/TLS, qui dépendent d'une horloge précise pour les processus de chiffrement et de déchiffrement.
2. Prévention des attaques de rejeu : Les protocoles de sécurité, tels que Kerberos, utilisent souvent l'heure système pour générer des jetons d'authentification. Si les horloges des hôtes ESXi ne sont pas synchronisées, cela pourrait permettre des attaques de rejeu où un attaquant utilise un jeton d'authentification généré à un moment donné pour accéder illégalement à un système à un moment ultérieur.
3. Audit et conformité : Dans de nombreux environnements réglementés, tels que ceux soumis à des normes de conformité PCI DSS, HIPAA ou GDPR, la synchronisation précise de l'heure est une exigence de sécurité. La configuration de PTP ou NTP garantit que vous êtes en conformité avec ces exigences en matière de sécurité et vous aide à passer avec succès les audits de conformité.
4. Fiabilité des logs d'audit : Les logs d'audit sont essentiels pour la détection des menaces et la réponse aux incidents. Des horloges synchronisées garantissent que les événements sont correctement horodatés, ce qui facilite l'analyse des logs pour détecter les activités suspectes ou malveillantes.
5. Sécurité des transactions et des processus critiques : Dans un environnement vCenter où des opérations sensibles, telles que le déploiement de machines virtuelles ou la migration de charges de travail, sont effectuées, la synchronisation précise de l'heure garantit la cohérence des transactions et des processus critiques, renforçant ainsi la sécurité globale de l'environnement.

Limiter l'accès au réseau de vCenter Server :

1. Segmentation réseau : Placement de vCenter Server dans un segment réseau dédié, isolé des autres systèmes et services non essentiels. Utilisation des pare-feux et des règles de sécurité pour limiter le trafic réseau entrant et sortant vers vCenter Server.
2. Liste de contrôle d'accès (ACL) : Utilisation des ACL pour contrôler quelles adresses IP ou sous-réseaux sont autorisés à communiquer avec vCenter Server. Limitez l'accès uniquement aux systèmes et aux administrateurs système autorisés.
3. VPN ou accès sécurisé : Si nous avons besoin d'accéder à vCenter Server depuis un réseau distant ou non sécurisé, utilisation d'un VPN (Virtual Private Network) ou des connexions sécurisées telles que SSH (Secure Shell) ou SSL VPN pour crypter le trafic et sécuriser les communications.
4. Authentification forte : Mettez en œuvre des mécanismes d'authentification forte, tels que l'authentification à deux facteurs, pour renforcer la sécurité des connexions avec vCenter Server. Cela garantit que seules les personnes autorisées peuvent accéder à l'interface de gestion.
5. Surveillance du trafic réseau : Utilisation des outils de surveillance du trafic réseau pour détecter et analyser les activités suspectes ou non autorisées. Surveillez les journaux d'audit pour détecter les tentatives d'accès non autorisé ou les violations de la politique de sécurité.
6. Mises à jour et correctifs : Assurons-nous que vCenter Server et tous ses composants sont régulièrement mis à jour avec les derniers correctifs de sécurité pour atténuer les vulnérabilités connues et réduire les risques d'exploitation.

Sécurisation des canaux de communication :

Utilisation de protocoles sécurisés : Configurez vCenter Server pour utiliser des protocoles de communication sécurisés tels que HTTPS (HTTP sécurisé) pour les connexions Web et SSL/TLS (Secure Sockets Layer/Transport Layer Security) pour les communications réseau. Ces protocoles cryptent le trafic pour empêcher les interceptions non autorisées.

Certificats SSL/TLS : Utilisation des certificats SSL/TLS valides émis par une autorité de certification (CA) de confiance pour sécuriser les connexions avec vCenter Server. Assurons-nous que les certificats sont correctement configurés et renouvelés régulièrement pour garantir la sécurité des communications.

Configuration des protocoles : Configurons les paramètres de vCenter Server pour utiliser des ciphers (algorithmes de chiffrement) forts et des protocoles sécurisés pour les connexions SSL/TLS. Désactivez les anciens protocoles et ciphers faibles pour renforcer la sécurité.

Surveillance du trafic réseau : Utilisation des outils de surveillance du trafic réseau pour détecter et analyser les activités suspectes ou non autorisées. Surveillez les journaux d'audit pour détecter les tentatives d'accès non autorisé ou les violations de la politique de sécurité.

Chiffrement de bout en bout : Si nous avons besoin d'une sécurité supplémentaire pour les données sensibles, envisagez d'utiliser le chiffrement de bout en bout pour chiffrer les données au niveau de l'application avant leur transmission et de les déchiffrer uniquement lorsqu'elles atteignent leur destination finale.