UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PUBLIQUE)

Guide d'endurcissement VMWARE

CESI

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PUBLIQUE)

TABLE DES MATIERES

INTRODUCTION

MISE EN CONTEXTE

Le virage infonuagique est très avancé dans le monde des entreprises et les établissements du réseau des Universités du Québec (UQ), n'en font pas exception. Les enjeux de sécurité autrefois orientés sur les architectures traditionnelles ont également évolué. Bon nombre d'établissements ont optés pour des architectures hybrides comprenant une partie privée orientée VMware ESXi. Nous allons, dans ce document, nous intéresser à la sécurité du cloud privé bâti avec les solutions du fournisseur VMware.

L'utilisation des hosts ESXi fait naitre le besoin d'avoir un guide de référence pour l'endurcissement de VMware. Il s'agit de donner des orientations de configuration pour rehausser et garantir le niveau de sécurité.

OBJECTIF

Ce guide a pour objectif de décrire les exigences de sécurité au niveau de la configuration des serveurs VMware ESXi dans l'écosystèmes des universités du Québec afin d'assurer un niveau adéquat d'endurcissement. Ce guide présente les exigences communes, puis les exigences spécifiques à VMware ESXi.

PORTÉE, LIMITES ET EXCLUSIONS

Ce document s'adresse à tous les établissements d'enseignement supérieur, aux responsables et administrateurs d'infrastructure cloud VMware ESXi, aux professionnels de la sécurité de l'information et à toutes les ressources intervenant dans la gestion des hyperviseurs ESXi.

Les exigences décrites dans ce document s'appliques à tous les systèmes utilisant VMware ESXi. Pour chaque exigence, le ou les contextes ciblés sont indiqués.

La version analysée est la version 7 de l'hyperviseur présentement utilisée pour le fournisseur VMware.

Lorsqu'utilisé, le terme "système" réfère à un environnement hébergeant VMware ESXi.

Ce guide de sécurité doit être appliqué à :

- Tous les nouveaux équipements installés dans tous les environnements informatique (Production ou développement ou test) après la date d'entrée en vigueur de ce guide.
- Tous les équipements installés dans tous les environnements informatiques (production, développement) avant la date d'entrée en vigueur de ce guide quand ils :

- Sont réinstallés pour évolution
- Subissent un changement substantiel
- Sont de nature critique

Remarque : L'application de ce guide doit être considère comme le minimum de sécurité requis dans le cadre d'une entité pédagogique et universitaire.

ENTRÉE EN VIGUEUR ET MESURES TRANSITOIRES

Les mesures de sécurité indiquées dans ce guide sont des recommandations du CESI pour le réseau des universités du Québec. Il peut servir d'orientations dans le cadre d'un rehaussement de sécurité VMware.

FONCTIONNEMENT DU DOCUMENT

Le contenu de ce guide est tiré/adapté du guide d'endurcissement de VMware ESXi v7 fourni par WMware ainsi que du guide de référence CIS Benchmarks. Les url du document de VMware et CIS sont indiquée au besoin dans la section Références de chaque point.

Si une configuration particulière requise pour répondre à une exigence n'est pas fournie dans ce guide, la méthode de configuration utilisée afin de remplir cette exigence est au choix de l'administrateur.

Les références de type CCE (Common Configuration Énumération) fournissent des références plus précises sur comment procéder pour obtenir le comportement visé a titre informatif seulement, afin d'aider à la compréhension des comportements désirés.

Champ d'intervention						
X.X.X.X	Cette exigence est un exemple seulement. L'exigence est décrite ici.	**P**	**C**	**T**	**D**
Spécificités	Si l'exigence demande un comportement spécifique, il est decrit ici. Par exemple, une exigence peut demander a ce que certains évènements soient journalises. La liste de ces évènements serait ici.				
Références	Des liens vers des documents ou des numéros CCE sont ivi lorsque c'est applicable.				
Exceptions	Les exceptions existantes se retrouvent ici. Certaines exceptions peuvent couvrir une version d'un OS, un environnement spécifique un cas précis.				

Les case P C T D indiquent si l'exigence s'applique en production, Certification, Test ou Développement. Par exemple, si les lettres P et C sont les seules, cette exigence est applicable à la production et la certification seulement. Il est bien sur

permis de configurer les autres environnements de la même façon pour des besoins de tests, consistance dans les configurations, mais pour les lettres qui ne sont pas inscrites, il n'y a pas d'obligation de configuration pour ces environnements.

Attention : Si un environnement de laboratoire est complètement isolé, ces exigences ne s'appliquent pas, et les équipements peuvent être configurés soit en utilisant ce guide comme référence ou d'une autre façon pour permettre. Certains tests. Si un laboratoire 'n'est pas isolé, les exigences s'appliquant aux environnement Développement s'appliquent.

Pour les fins de ce guide, aucune exigence ne sera incluse concernant l'endurcissement sous forme de protection physique (périmètre), de communication avec d'autres actifs configurables et non configurables ou de séparation des taches de gestion.

L'endurcissement (c.-à-d. : bastionnage ou renforcement de la sécurité), consiste principalement à rehausser le niveau de sécurité d'un actif configurable en appliquant les derniers correctifs de sécurité, en désactivant les composants inutilisés, en activant les mesures de sécurité optionnelles et en resserrant les accès sur des ressources critiques en plus d'une application stricte de la norme de contrôle d'accès.

EXIGENCES DE SÉCURITÉ À VMWARE ESXI (VSPHERE)

Recommandations Systèmes

Le "**Security Configuration Guide**" de vSphere (**SCG**) est la référence pour les conseils de renforcement et d'audit pour VMware. Lancé il y a plus de dix ans, il a longtemps servi de guide aux administrateurs vSphere cherchant à protéger leur infrastructure.

Le Guide de configuration de la sécurité est destiné à être un ensemble de bonnes pratiques de sécurité de base qui informent les efforts de sécurité d'un administrateur vSphere d'une manière générale qui examine les compromis à portée de main. L'activation de toutes les fonctionnalités de sécurité à leurs niveaux les plus élevés peut être préjudiciable, entravant les efforts quotidiens des administrateurs pour exploiter, corriger et surveiller leurs environnements. Le SCG n'est pas un catalogue de tous les contrôles de sécurité disponibles, c'est simplement une base de référence à partir de laquelle nous pouvons opérer.

SCG ID	Description
design-7.administration-client-plugins	Réduisez ou éliminez les plugins vCenter Server tiers.
design-7.centralized-authentication	Rester prudent lorsque vous connectez des interfaces de gestion d'infrastructure à des sources d'authentification et d'autorisation à usage général.
design-7.enable-vsphere-drs	Activez vSphere Distributed Resource Scheduler (DRS) en mode entièrement automatisé.
design-7.enable-vsphere-ha	Activez vSphere High Availability (HA).
design-7.evc	Activez la compatibilité vMotion améliorée (EVC).
design-7.hardware-physical-security	Assurez-vous que les systèmes hôtes ESXi et les composants de stockage et de mise en réseau associés sont protégés contre la falsification, l'accès non autorisé et le retrait non autorisé, ainsi que contre les dommages causés par des facteurs environnementaux tels que les inondations, les températures extrêmes (basses ou élevées) et la poussière et les débris.
design-7.network-isolation-management	Assurez-vous que les interfaces de gestion de l'infrastructure informatique sont isolées sur leur propre segment de réseau ou dans le cadre d'un réseau de gestion isolé.
design-7.storage-lun-masking	Assurez-vous que les systèmes de stockage utilisent le masquage LUN, le zonage et d'autres techniques de sécurité côté stockage pour garantir que les allocations de stockage ne sont visibles que pour le cluster vSphere dans lequel elles doivent être utilisées.
design-7.storage-fabric-isolation	Assurez-vous que les connexions de la structure de stockage utilisent le chiffrement des données en transit ou sont isolées sur leurs propres segments de réseau ou SAN qui ont des contrôles de périmètre.
design-7.network-isolation-vmotion	Assurez-vous que vMotion utilise le chiffrement des données en transit (défini sur "Requis" pour les machines virtuelles) ou que les interfaces réseau VMkernel utilisées pour vMotion sont isolées sur leurs propres segments de réseau qui ont des contrôles de périmètre.
design-7.network-isolation-vsan	Assurez-vous que vSAN utilise le chiffrement des données en transit ou que les interfaces réseau VMkernel utilisées pour vSAN sont isolées sur leurs propres segments de réseau qui ont des contrôles de périmètre.
design-7.vcsa-firewall	Envisagez l'utilisation du pare-feu de l'appliance VCSA pour limiter les connexions aux systèmes et administrateurs autorisés.
design-7.naming	Assurez-vous que les objets dans vSphere sont nommés de manière descriptive, en modifiant les noms par défaut des objets pour garantir l'exactitude et réduire la confusion.
design-7.network-untagged-traffic	Assurez-vous que les liaisons montantes des commutateurs physiques des hôtes ESXi sont configurées en tant que « ports d'accès » attribués à un seul VLAN ou en tant que troncs de VLAN 802.1q balisés sans VLAN natif. Assurez-vous que les groupes de ports vSphere n'autorisent pas l'accès au VLAN 1 ou aux VLAN natifs non balisés

INSTALLATION

Les exigences de sécurité concernant une installation d'un hyperviseur ESXi.

Installation					
2.1.1	L'installation d'un système d'exploitation doit se faire à partir d'une source normalisée.	**P**	**C**	**T**	**D**
Spécificités	Doit être décrit dans le processus d'installation. Une image standard ou des médias d'origine doivent être utilisés pour les serveurs de PROD ou CERTIF. Faire une image d'un serveur similaire, déjà en opération et la modifier au besoin peut servir pour des serveurs dans les environnements de TEST ou DEV. Le profil d'image ESXi ne doit autoriser que les VIB (vSphere Installation Bundle) signés, car un VIB non signé représente un code non testé installé sur un hôte ESXi. De plus, l'utilisation de VIB non signés entraînera l'échec de la configuration du démarrage sécurisé de l'hyperviseur. Les VIB pris en charge par la communauté n'ont pas de signature numérique. Pour protéger la sécurité et l'intégrité de vos hôtes ESXi, n'autorisez pas l'installation de VIB non signés (CommunitySupported) sur vos hôtes. **Impact**: Les VIB non signés (pris en charge par la communauté) ne pourront pas être utilisés sur un hôte. `# Set the Software AcceptanceLevel for each host<span>` `Foreach ($VMHost in Get-VMHost ) {` `  $ESXCli = Get-EsxCli -VMHost $VMHost` `  $ESXCli.software.acceptance.Set("PartnerSupported")` `}`				
Références	Guide de configuration de sécurité VMware https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html				
Exceptions					
2.1.2	Le service NTPd doit être configuré et activé automatiquement	**P**	**C**	**T**	**D**
Spécificités	Démontrer dans la documentation d'installation l'utilisation des sources de temps normalisé. Depuis le client Web vSphere, sélectionnez l'hôte et cliquez sur "Configure" -> "Time Configuration" et cliquez sur le bouton "Edit...". Indiquez le nom/IP de vos serveurs NTP, démarrez le service NTP et modifiez la politique de démarrage en "Start and stop with host". Notes: vérifiez que les ports du pare-feu NTP sont ouverts. Il est recommandé de synchroniser l'horloge ESXi avec un serveur de temps situé sur le réseau de gestion plutôt que directement avec un serveur de temps sur un réseau public. Ce serveur de temps peut alors se synchroniser avec une source publique via une connexion réseau strictement contrôlée avec un pare-feu.				

Références	Guide de configuration de sécurité VMware Guideline-ID : ESXi.config-ntp				
Exceptions					
2.1.3	Garder les servers ESX à jour avec les rustines	**P**	**C**	**T**	**D**
Spécificités	Délai d'installation de rustines à valider selon sévérité Dans le client Web vSphere, sélectionnez l'hôte et cliquez sur " Summary ". Développez "Configuration" et vérifiez les chaînes " ESX/ESXi Version" et " Image Profile ". Ces chaînes vous indiqueraient la version actuelle de l'image de l'hôte. Assurez-vous que la version de l'image est la dernière fournie par VMware. En restant à jour sur les correctifs ESXi, les vulnérabilités de l'hyperviseur peuvent être atténuées. Un attaquant averti peut exploiter des vulnérabilités connues lorsqu'il tente d'accéder ou d'élever des privilèges sur un hôte ESXi. **Impact**: Les serveurs ESXi doivent être en mode maintenance pour appliquer les correctifs. Cela implique que toutes les machines virtuelles doivent être déplacées ou mises hors tension sur le serveur ESXi, de sorte que le processus de correction peut nécessiter de brèves interruptions. `Foreach ($VMHost in Get-VMHost ) {` `  $EsxCli = Get-EsxCli -VMHost $VMHost -V2` `  $EsxCli.software.vib.list.invoke() \| Select-Object` `@{N="VMHost";E={$VMHost}},*` `}`				
Références	Guide de configuration de sécurité VMware : Guideline-ID : ESXi.apply.patches https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere-lifecycle-manager.doc/GUID-74295A37-E8BB-4EB9-BFBA-47B78F0C570D.html CIS controls : Deploy Automated Operating System Patch Management Tools				
Exceptions					
2.1.4	Assurer la bonne configuration de SNMP. SNMP doit etre soit désactivé, ou bien ne doit pas avoir une configuration par defaut.	**P**	**C**	**T**	
Spécificités	Il faut changer les community strings des configurations par defaut. Trap destination == [selon emplacement du serveur ESXi] From the vSphere web client select the host and click "Manage" -> "Setting" -> "Security Profile". Look for "SNMP Server" under "Services" section. Its status should be "Stopped" until and unless you re using in your environment.				

	Depuis le client Web vSphere, sélectionnez l'hôte et cliquez sur "Manage" -> "Setting" -> "Security Profile". Recherchez " SNMP Server" dans la section "Services". Son statut doit être "Stopped" jusqu'à ce que vous l'utilisiez dans votre environnement. ESXi Shell Command : **# Configure Community String** esxcli system snmp set --communities [COMMUNITY] **# Configure SNMP Target** esxcli system snmp set --targets [TARGET]@[PORT]/[COMMUNITY] **# Enable SNMP** esxcli system snmp set --enable true"				
Références	Guide de configuration de sécurité VMware Guideline-ID : ESXi.config-snmp Document additionnel : https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-8EF36D7D-59B6-4C74-B1AA-4A9D18AB6250.html				
Exceptions					
2.1.5	Configuration de la bannière de connexion	**P**	**C**	**T**	**D**
Spécificités	Le texte doit être approuvé par les administrateurs. **ESX** : /etc/motd Sur **ESXi** : Utiliser la méthode appropriée à la version (esxcli, vCli, etc..)				
Références					
Exceptions					
2.1.6	La bannière de connexion doit s'afficher lors des connexions SSH	**P**	**C**	**T**	**D**
Spécificités	L'option PrintMotd doit être activée en tout temps pour ESX, et lorsque SSH est activé sur ESXi				
Références					
Exceptions					
2.1.7	Assurez-vous qu'Intel TXT est activé, s'il est disponible dans le micrologiciel du système	**P**	**C**	**T**	**D**
Spécificités					

	Les plates-formes de processeurs évolutifs Intel Xeon disposent de la technologie d'exécution sécurisée, ou TXT, qui aide à renforcer les systèmes contre les logiciels malveillants, les rootkits, les attaques du BIOS et du micrologiciel, etc. Lorsqu'il est activé, ESXi tirera parti des avantages de sécurité offerts par cette technologie. **Valeur par défaut à l'installation :** *Not Configured* **Valeur recommandée sécuritaire :** *Enabled* **Section de configuration :** *Hardware Management & Firmware*				
Références	Guide de configuration de sécurité VMware Guideline-ID : hw-7.hardware-cpu-intel-txt				
Exceptions					
2.1.8	Assurez-vous que le démarrage sécurisé UEFI est activé.	**P**	**C**	**T**	**D**
Spécificités	L'activation du démarrage sécurisé UEFI sur le matériel de l'hôte ESXi permet d'empêcher les logiciels malveillants et les configurations non approuvées. **Valeur par défaut à l'installation :** *Not Configured* **Valeur recommandée sécuritaire :** *Enabled* **Section de configuration :** *Hardware Management & Firmware*				
Références	Guide de configuration de sécurité VMware Guideline-ID : hw-7.hardware-secure-boot				
Exceptions					
2.1.9	Assurez-vous qu'un TPM 2.0 est installé et activé sur l'hôte.	**P**	**C**	**T**	**D**
Spécificités	ESXi peut utiliser Trusted Platform Modules (TPM) 2.0 pour activer des fonctions de sécurité avancées qui empêchent les logiciels malveillants, suppriment les dépendances et sécurisent les opérations du cycle de vie du matériel. Nous recommandons fortement que tous les serveurs soient configurés avec un TPM 2.0 et que le TPM soit activé dans le micrologiciel du système. **Valeur par défaut à l'installation :** *Not Configured* **Valeur recommandée sécuritaire :** *TPM 2.0 installed, enabled.* *SHA-256 hashing, TIS/FIFO interface* **Section de configuration :** *Hardware Management & Firmware*				

Références	Guide de configuration de sécurité VMware Guideline-ID : hw-7.hardware-tpm				
Exceptions					
2.1.10	Durée en secondes pour verrouiller le compte d'un utilisateur après avoir dépassé le nombre maximal de tentatives de connexion infructueuses autorisées.	**P**	**C**	**T**	**D**
Spécificités	**Détails**: Plusieurs échecs de connexion à un même compte peuvent indiquer un problème de sécurité. De telles tentatives de brute force sur le système doivent être limitées en verrouillant le compte après avoir atteint un seuil. Cependant, comme cela peut être utilisé pour refuser le service, une période de déverrouillage est souvent spécifiée. **Valeur par défaut à l'installation :** *120* **Valeur recommandée sécuritaire :** *900* **Section de configuration :** *ESXi Advanced System Settings* **Configuration Parameter** : *Security.AccountUnlockTime* **PowerCLI Command Assessment** : *Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.AccountUnlockTime*				
Références	Guide de configuration de sécurité VMware Guideline-ID : esxi-7.account-auto-unlock-time				
Exceptions					
2.1.11	Nombre maximal de tentatives de connexion infructueuses autorisées avant de verrouiller le compte d'un utilisateur.	**P**	**C**	**T**	**D**
Spécificités	**Détails** : Plusieurs échecs de connexion à un même compte peuvent indiquer un problème de sécurité. De telles tentatives de brute force sur le système doivent être limitées en verrouillant le compte après avoir atteint un seuil. Il convient de veiller à ce que ce paramètre soit suffisamment élevé pour qu'un client SSH ou un autre système qui tente de se reconnecter automatiquement ne verrouille pas le compte. Un faible nombre d'échecs de connexion fournit une méthode pour les attaques par déni de service, intentionnellement ou non. **Valeur par défaut à l'installation :** *10*				

	Valeur recommandée sécuritaire : *5* **Section de configuration :** *ESXi Advanced System Settings* **Configuration Parameter**: *Security.AccountLockFailures* **PowerCLI Command Assessment**: *Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.AccountLockFailures*				
Références	Guide de configuration de sécurité VMware Guideline-ID : esxi-7.account-lockout				
Exceptions					
2.1.12	Bloquer les transmissions BPDU du système d'exploitation invité	**P**	**C**	**T**	**D**
Spécificités	**Détails** : BPDU Guard et Portfast sont généralement activés sur le commutateur physique auquel l'hôte ESXi est directement connecté pour réduire le délai de convergence Spanning Tree. Si un paquet BPDU est envoyé depuis une machine virtuelle sur l'hôte ESXi vers le commutateur physique ainsi configuré, un verrouillage en cascade de toutes les interfaces de liaison montante de l'hôte ESXi peut se produire. Pour empêcher ce type de verrouillage, le filtre BPDU peut être activé sur l'hôte ESXi pour supprimer tous les paquets BPDU envoyés au commutateur physique. Certaines charges de travail orientées réseau peuvent légitimement générer des paquets BPDU. L'administrateur doit vérifier qu'il n'y a pas de paquets BPDU légitimes générés par des machines virtuelles sur l'hôte ESXi avant d'activer le filtre BPDU. Si le filtre BPDU est activé dans cette situation, l'activation de Reject Forged Transmits sur le groupe de ports du commutateur virtuel ajoute une protection contre les boucles Spanning Tree. **Valeur par défaut à l'installation :** *0* **Valeur recommandée sécuritaire :** *1* **Section de configuration :** *ESXi Advanced System Settings* **Configuration Parameter** : *Net.BlockGuestBPDU* **PowerCLI Command Assessment** : *Get-VMHost -Name $ESXi | Get-AdvancedSetting Net.BlockGuestBPDU*				

Références	Guide de configuration de sécurité VMware Guideline-ID : esxi-7.network-bpdu				
Exceptions					
2.1.13	Assurez-vous que seul TLS 1.2 est activé	**P**	**C**	**T**	**D**
Spécificités	**Détails** : ESXi 7 est livré avec TLS 1.2 activé mais peut avoir d'autres protocoles réactivés. **Valeur par défaut à l'installation :** *sslv3,tlsv1,tlsv1.1* **Valeur recommandée sécuritaire :** *Is default - sslv3,tlsv1,tlsv1.1* **Section de configuration :** *ESXi Advanced System Settings* **Configuration Parameter** : *UserVars.ESXiVPsDisabledProtocols* **PowerCLI Command Assessment** : *Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.ESXiVPsDisabledProtocols*				
Références	Guide de configuration de sécurité VMware Guideline-ID : esxi-7.tls-protocols				
Exceptions					
2.1.14	Assurez-vous qu'aucun module de noyau non autorisé n'est chargé sur l'hôte	**P**	**C**	**T**	**D**
Spécificités	**Détails** : Par défaut, les hôtes ESXi n'autorisent pas le chargement de modules de noyau dépourvus de signatures numériques valides. Cette fonctionnalité peut être remplacée, ce qui permettrait le chargement de modules de noyau non autorisés. VMware fournit des signatures numériques pour les modules du noyau. Des modules de noyau non testés ou malveillants chargés sur l'hôte ESXi peuvent exposer l'hôte à un risque d'instabilité et/ou d'exploitation. **Impact**: C'est le comportement par défaut, donc l'impact est faible à nul. Sécurisez l'hôte en désactivant les modules non signés et en supprimant les VIB incriminés de l'hôte. Pour implémenter l'état de configuration recommandé, exécutez la commande PowerCLI suivante : `# To disable a module:` `$ESXCli = Get-EsxCli -VMHost "MyHostName_or_IPaddress"` `$ESXCli.system.module.set($false, $false, "MyModuleName")`				

Références	1. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-E9B71B85-FBA3-447C-8A60-DEE2AE1A405A.html 2. http://kb.vmware.com/kb/2042473				
Exceptions					
2.1.15	Assurez-vous que la valeur par défaut du sel individuel par machine virtuelle est configurée	**P**	**C**	**T**	**D**
Spécificités	**Détails** : Le concept de salage a été introduit pour aider à répondre aux préoccupations que les administrateurs système peuvent avoir concernant les implications de sécurité du partage de page transparent, autrement connu sous le nom de TPS. Selon l'implémentation TPS d'origine, plusieurs machines virtuelles pouvaient partager des pages lorsque le contenu des pages était le même. Avec les nouveaux paramètres de salage, les machines virtuelles peuvent partager des pages uniquement si la valeur de salage et le contenu des pages sont identiques. Une nouvelle option de configuration d'hôte Mem.ShareForceSalting est introduite pour activer ou désactiver le salage. Par défaut, le salage est activé (**Mem.ShareForceSalting=2**) et chaque machine virtuelle a un sel différent. Cela signifie que le partage de pages ne se produit pas sur les machines virtuelles (TPS inter-VM) et ne se produit qu'à l'intérieur d'une machine virtuelle (intra VM). Intra-VM signifie que TPS dédupliquera les pages de mémoire identiques au sein d'une machine virtuelle, mais ne partagera pas les pages avec d'autres machines virtuelles. S'assurer que le paramètre par défaut est en place afin que le partage de page ne se produise qu'à l'intérieur d'une machine virtuelle est la meilleure option ici. **Impact**: Il existe un potentiel d'impact sur les performances concernant ce paramètre, chaque environnement et l'impact sur celui-ci varieront. `Get-VMHost | Get-AdvancedSetting -Name Mem.ShareForceSalting | Set-AdvancedSetting -Value`				
Références	1. https://kb.vmware.com/s/article/2097593 2. https://blogs.vmware.com/vsphere/2015/01/assess-the-performance-impact-of-the-security-change-in-transparent-page-sharing-behaviour.html				
Exceptions					

COMMUNICATION

Les exigences de sécurité concernant les flux de communication en provenance, en destination ou via l'hyperviseur.

Communication					
2.2.1	Assurez-vous que le pare-feu de l'hôte ESXi est configuré pour restreindre l'accès aux services exécutés sur l'hôte	**P**	**C**	**T**	**D**
Spécificités	**Details** : Le pare-feu ESXi est activé par défaut et autorise le ping (ICMP) et la communication avec les clients DHCP/DNS. L'accès aux services ne doit être autorisé qu'aux adresses IP/réseaux autorisés. L'accès illimité aux services exécutés sur un hôte ESXi peut exposer un hôte à des attaques extérieures et à un accès non autorisé. Réduisez les risques en configurant le pare-feu ESXi pour n'autoriser l'accès qu'à partir d'adresses IP et de réseaux autorisés. **Impact**: Les connexions à partir d'adresses IP et de plages qui ne sont pas explicitement définies seront refusées. Assurez-vous que les plages d'adresses IP/IP appropriées sont autorisées. Vérification : `# List all services for a host` `Get-VMHost HOST1 | Get-VMHostService` `# List the services which are enabled and have rules defined for specific IP ranges to access the service` `Get-VMHost HOST1 | Get-VMHostFirewallException | Where {$_.Enabled -and (-not $_.ExtensionData.AllowedHosts.AllIP)}` `# List the services which are enabled and do not have rules defined for specific IP ranges to access the service` `Get-VMHost HOST1 \| Get-VMHostFirewallException \| Where {$_.Enabled -and ($_.ExtensionData.AllowedHosts.AllIP)}` **Correction**: 1. Sélectionnez un hôte 2. Cliquez sur Configurer puis développez Système puis sélectionnez Pare-feu. 3. Cliquez sur Modifier pour afficher les services activés (indiqués par une coche). 4. Pour chaque service activé (par exemple, ssh, vSphere Web Access, client http), fournissez une liste d'adresses IP autorisées. 5. Cliquez sur OK.				

Références	Guide de configuration de sécurité VMware https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-8912DD42-C6EA-4299-9B10-5F3AEA52C605.html				
Exceptions					
2.2.2	Assurez-vous que le Managed Object Browser (MOB) est désactivé	**P**	**C**	**T**	**D**
Spécificités	**Details** : Le Managed Object Browser (MOB) est une application serveur basée sur le Web qui vous permet d'examiner les objets qui existent côté serveur, d'explorer le modèle d'objet utilisé par le noyau VM pour gérer l'hôte et de modifier les configurations. Il est installé et démarré automatiquement lorsque vCenter est installé. Le MOB est destiné à être utilisé principalement pour le débogage du SDK vSphere. Comme il n'y a pas de contrôle d'accès, le MOB peut également être utilisé comme méthode pour obtenir des informations sur un hôte ciblé pour un accès non autorisé. **Impact**: Certains outils tiers peuvent utiliser le navigateur d'objets gérés (MOB), ce qui signifie que sa désactivation entraînera un dysfonctionnement de ces outils. **Vérification** : #ESXi Shell vim-cmd proxysvc/service_list #PowerCLI Get-VMHost | Get-AdvancedSetting -Name Config.HostAgent.plugins.solo.enableMob **Correction**: 1. Sélectionnez un hôte 2. Cliquez sur Configurer puis développez Système puis sélectionnez Paramètres système avancés. 3. Cliquez sur Modifier puis recherchez Config.HostAgent.plugins.solo.enableMob 4. Définissez la valeur sur false. 5. Cliquez sur OK. Note : 1- Vous ne pouvez pas désactiver le MOB lorsqu'un hôte est en mode verrouillage. 2- Vous devez désactiver MOB à partir de l'interface vSphere et non via la commande vim-cmd.				
Références	https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-0EF83EA7-277C-400B-B697-04BDC9173EA3.html				
Exceptions					

2.2.3	Assurez-vous que le certificat auto-signé par défaut pour la communication ESXi n'est pas utilisé	P	C		
Spécificités	**Détails** : Le certificat par défaut est auto-signé et non signé par une autorité de certification (CA) approuvée. Il doit être remplacé par un certificat valide émis par une autorité de certification de confiance. Il convient de noter que les certificats sont générés au moment de l'installation, ce qui diffère légèrement de certaines solutions de certificats auto-signés. L'utilisation du certificat auto-signé par défaut peut augmenter le risque lié aux attaques de l'homme du milieu (MITM). **Impact**: Le remplacement du certificat par défaut peut entraîner l'arrêt de la gestion de l'hôte par vCenter Server. Déconnectez et reconnectez l'hôte si vCenter Server ne peut pas vérifier le nouveau certificat. **Correction** : Sauvegardez et remplacez les détails du certificat SSL présenté par l'hôte ESXi et déterminez s'il est émis par une autorité de certification approuvée : 1- Connectez-vous à ESXi Shell, soit directement à partir de la DCUI, soit à partir d'un client SSH, en tant qu'utilisateur avec des privilèges d'administrateur. 2- Dans le répertoire /etc/vmware/ssl, renommez les certificats existants à l'aide des commandes suivantes : `mv rui.crt orig.rui.crt` `mv rui.key orig.rui.key` 3- Copiez les certificats que vous souhaitez utiliser dans /etc/vmware/ssl. 4- Renommez le nouveau certificat et la clé en rui.crt et rui.key. 5- Redémarrez l'hôte après avoir installé le nouveau certificat. Note : Vous pouvez également mettre l'hôte en mode maintenance, installer le nouveau certificat, utiliser l'interface utilisateur de la console directe (DCUI) pour redémarrer les agents de gestion et configurer l'hôte pour qu'il quitte le mode maintenance.				
Références	Guide de configuration de sécurité VMware 1. https://kb.vmware.com/s/article/2111219 2. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-AC7E6DD7-F984-4E0F-983A-463031BA5FE7.html				

Exceptions					
2.2.4	Assurez-vous que l'API dvfilter n'est pas configurée si elle n'est pas utilisée	**P**	**C**	**T**	**D**
Spécificités	**Details** : L'API réseau dvfilter est utilisée par certains produits (par exemple, VMSafe). S'il n'est pas utilisé, il ne doit pas être configuré pour envoyer des informations réseau à une machine virtuelle. Si l'API réseau dvfilter est activée à l'avenir et qu'elle est déjà configurée, un attaquant pourrait tenter d'y connecter une machine virtuelle, fournissant ainsi potentiellement un accès au réseau d'autres machines virtuelles sur l'hôte. **Impact**: Cela empêchera une appliance de sécurité réseau basée sur dvfilter, telle qu'un pare-feu, de fonctionner si elle n'est pas configurée correctement. **Valeur par défaut à l'installation :** *Not configured* **Valeur recommandée sécuritaire :** Pour supprimer la configuration de l'API réseau dvfilter, procédez comme suit à partir du client Web vSphere : 1. À partir du client Web vSphere, sélectionnez l'hôte et cliquez sur Configurer, puis développez Système 2. Cliquez sur Paramètres système avancés puis sur Modifier. 3. Recherchez Net.DVFilterBindIpAddress dans le filtre. 4. Mettre Net.DVFilterBindIpAddress a une valeur vide. 5. Si une appliance est utilisée, assurez-vous que la valeur de ce paramètre est définie sur la bonne adresse IP. 6. Entrez l'adresse IP appropriée. 1- 7. Cliquez sur OK. **PowerCLI Command Assessment** : # Set Net.DVFilterBindIpAddress to null on all hosts Get-VMHost HOST1 | Foreach { Set-AdvancedSetting -VMHost $_ -Name Net.DVFilterBindIpAddress -IPValue "" }				
Références	Guide de configuration de sécurité VMware https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-CD0783C9-1734-4B9A-B821-ED17A77B0206.html				
Exceptions					

2.2.5	Assurez-vous que les certificats SSL expirés et révoqués sont supprimés du serveur ESXi	**P**	**C**	**T**	**D**
Spécificités	**Details** : Par défaut, les hôtes ESXi ne disposent pas de la vérification de la liste de révocation de certificats (CRL). Par conséquent, les certificats SSL expirés et révoqués doivent être vérifiés et supprimés manuellement. Laisser des certificats expirés et révoqués sur votre système vCenter Server peut compromettre votre environnement. Le remplacement des certificats évitera aux utilisateurs de s'habituer à cliquer sur les avertissements du navigateur. L'avertissement peut être une indication d'une attaque de l'homme du milieu, et seule l'inspection du certificat et de l'empreinte digitale peut se prémunir contre de telles attaques.				
Références	1. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-AC7E6DD7-F984-4E0F-983A-463031BA5FE7.html 2. http://en-us.sysadmins.lv/Lists/Posts/Post.aspx?List=332991f0-bfed-4143-9eea-f521167d287c&ID=60				
Exceptions					
2.2.6	Assurez-vous que vSphere Authentication Proxy est utilisé lors de l'ajout d'hôtes à Active Directory	**P**	**C**	**T**	**D**
Spécificités	**Détails** : vSphere Authentication Proxy permet aux hôtes ESXi de rejoindre un domaine sans utiliser les informations d'identification Active Directory. vSphere Authentication Proxy améliore la sécurité des hôtes démarrés par PXE et des hôtes qui sont provisionnés à l'aide des profils Auto Deploy et Host, en supprimant la nécessité de stocker les informations d'identification Active Directory dans la configuration de l'hôte. Le service vSphere Authentication Proxy se lie à une adresse IPv4 pour communiquer avec vCenter Server et ne prend pas en charge IPv6. Le vCenter Server peut se trouver sur une machine hôte dans un environnement réseau IPv4 uniquement, IPv4/IPv6 en mode mixte ou IPv6 uniquement, mais la machine qui se connecte au vCenter Server via vSphere Client doit avoir une adresse IPv4 pour vSphere Service d'authentification Proxy pour fonctionner. Si vous configurez votre hôte pour rejoindre un domaine Active Directory à l'aide de profils d'hôte, les informations d'identification Active Directory sont enregistrées dans le profil d'hôte et sont transmises sur le réseau. Pour éviter d'avoir à enregistrer les informations d'identification Active Directory dans le profil d'hôte et pour éviter de transmettre les informations d'identification Active Directory sur le réseau, utilisez vSphere Authentication Proxy. **Correction** : Pour configurer correctement vSphere Authentication Proxy via les profils d'hôte : 1. Dans vSphere Web Client, accédez à Accueil dans le menu.				

	2. Cliquez sur Politiques et profils suivi de Profils d'hôte. 3. Choisissez le profil d'hôte approprié 4. Sélectionnez Configure suivi de Edit Host Profile... puis développez Security and Services suivi de Security Settings, puis Authentication configuration. 5. Sélectionnez la configuration d'Active Directory. 6. Définissez la méthode JoinDomain est configurée sur Utiliser vSphere Authentication Proxy pour ajouter l'hôte au domaine. 7. Cliquez sur Enregistrer.				
Références	https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-084B74BD-40A5-4A4B-A82C-0C9912D580DC.html				
Exceptions					
2.2.7	Assurez-vous que la vérification de l'état du VDS est désactivée	**P**	**C**	**T**	**D**
Spécificités	**Détails** : La prise en charge de la vérification de l'état dans VDS vous aide à identifier et à résoudre les erreurs de configuration dans un vSphere Distributed Switch. Il est recommandé de désactiver la vérification de l'état par défaut et de confirmer qu'elle est désactivée une fois le dépannage terminé. Une fois activé, le contrôle de santé du commutateur vSphere Distributed collecte les paquets contenant des informations sur l'hôte #, vds # port #, qu'un attaquant trouverait utiles. **Correction** : Utilisation de vSphere Web Client pour chaque VDS : 1. Sélectionnez un VDS 2. Accédez à Configurer, développez Paramètres, puis sélectionnez Bilan de santé. 3. Cliquez sur Modifier. 4. Définissez l'état VLAN et MTU sur Désactivé. 5. Définissez l'état d'association et de basculement sur Désactivé. 6. Cliquez sur OK. De plus, la commande **PowerCLI** suivante peut être utilisée : Get-View -ViewType DistributedVirtualSwitch | ?{($_.config.HealthCheckConfig \| ?{$_.enable -notmatch "False"})}| %{$_.UpdateDVSHealthCheckConfig(@((New-Object Vmware.Vim.VMwareDVSVlanMtuHealthCheckConfig -property @{enable=0}),(New-Object Vmware.Vim.VMwareDVSTeamingHealthCheckConfig -property @{enable=0})))}				
Références	Guide de configuration de sécurité VMware https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-4A6C1E1C-8577-4AE6-8459-EEB942779A82.html				

Exceptions	

AUTORISATION

Les exigences de sécurité concernant les autorisations d'un hyperviseur ESXi.

Autorisation					
2.3.1	Utiliser le paramètre DCUI.Access pour assurer un accès au serveur ESXi pour ldes admins autorisés au cas ou le serveur ESXi se trouve isolé de vCenter Server. Configurer une valeur de temporisation afin que des usagers connectés et inactifs soient déconnectés.	**P**	**C**	**T**	**D**
Spécificités	DCUI.Access – Une liste de comptes admins autorisés. UserVars.DCUITimeOut = 600 From the vSphere web client select the host and click "Manage" -> "Setting" -> "System" -> "Advanced System Setting". Enter "DCUI.Access" in the filter. Enter comma separated user accounts who are authorized to access DCUI even in cas of lockdown mode.				
Références	Guide de configuration de sécurité VMware				
Exceptions					
2.3.2	Limiter le nombre de connexions concurrentes administraeur	**P**	**C**	**T**	**D**
Spécificités	Limiter le nombre de connexions concurrentes de type Administrateur à se connecter à la console d'une VM				
Références	Guide de configuration de sécurité VMware Guideline-ID : RemoteDisplay.maxConnetions=1 (PROD) RemoteDisplay.maxConnetions=5 (DEV)				
Exceptions					

JOURNALISATION

Les exigences de sécurité concernant la journalisation.

Journalisation						
2.4.1	Assurez-vous qu'un emplacement centralisé est configuré pour collecter les vidages de mémoire de l'hôte ESXi	**P**	**C**	**T**	**D**	
Spécificités	**Details** : Le service VMware vSphere Network Dump Collector permet de collecter des informations de diagnostic à partir d'un hôte qui rencontre une panne critique. Ce service fournit un emplacement centralisé pour la collecte des vidages de mémoire de l'hôte ESXi. Lorsqu'un hôte tombe en panne, une analyse du vidage de mémoire résultant est essentielle pour pouvoir identifier la cause du plantage et déterminer une résolution. L'installation d'un collecteur de vidage centralisé permet de garantir que les fichiers principaux sont correctement enregistrés et mis à disposition au cas où un hôte ESXi paniquerait. **Impact**: Les connexions à partir d'adresses IP et de plages qui ne sont pas explicitement définies seront refusées. Assurez-vous que les plages d'adresses IP/IP appropriées sont autorisées. **Correction** : Pour implémenter l'état de configuration recommandé, exécutez les commandes shell ESXi suivantes : # Configure remote Dump Collector Server esxcli system coredump network set -v [VMK#] -i [DUMP_SERVER] -o [PORT] # Enable remote Dump Collector esxcli system coredump network set -e true					
Références	Support VMware http://kb.vmware.com/kb/1032051					
Exceptions						
2.4.2	Assurez-vous que la journalisation persistante est configurée pour tous les hôtes ESXi	**P**	**C**	**T**	**D**	
Spécificités	**Details** : ESXi peut être configuré pour stocker les fichiers journaux sur un système de fichiers en mémoire. Cela se produit lorsque la propriété Syslog.global.LogDir de l'hôte est définie sur un emplacement non persistant, tel que /scratch. Lorsque cela est fait, une seule journée de journaux est stockée à tout moment. De plus, les fichiers journaux seront réinitialisés à chaque redémarrage.					

	La journalisation non persistante présente un risque de sécurité car l'activité de l'utilisateur connecté à l'hôte n'est stockée que temporairement et ne sera pas conservée lors des redémarrages. Cela peut également compliquer l'audit et compliquer la surveillance des événements et le diagnostic des problèmes. La journalisation de l'hôte ESXi doit toujours être configurée sur une banque de données persistante. **Correction**: Pour configurer correctement la journalisation persistante, procédez comme suit à partir du client Web vSphere : 1. Sélectionnez l'hôte 2. Cliquez sur Configurer puis développez Système puis sélectionnez Paramètres système avancés. 3. Sélectionnez Modifier, puis saisissez Syslog.global.LogDir dans le filtre. 4. Définissez Syslog.global.logDir sur un emplacement persistant spécifié comme [datastorename] path_to_file où le chemin est relatif au datastore. Par exemple, [datastore1] /systemlogs. 5. Cliquez sur OK. Vous pouvez également exécuter la commande PowerCLI suivante : # Set Syslog.global.logDir for each host Get-VMHost | Foreach { Set-AdvancedConfiguration -VMHost $_ -Name Syslog.global.logDir -Value "<NewLocation>" } Note : Syslog.global.LogDir doit être défini pour chaque hôte. Les paramètres syslog de l'hôte peuvent également être configurés à l'aide de vCLI ou PowerCLI, ou à l'aide d'un client API.					
Références	1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-9F67DB52-F469-451F-B6C8-DAE8D95976E7.html 2. http://kb.vmware.com/kb/1033696					
Exceptions						
2.4.3	Assurez-vous que la journalisation à distance est configurée pour les hôtes ESXi	**P**	**C**			
Spécificités	**Détails** : Par défaut, les journaux ESXI sont stockés sur un volume de travail local ou un disque virtuel. Pour conserver les journaux, configurez également la journalisation à distance sur un hôte de journal central pour les hôtes ESXI. La journalisation à distance sur un hôte de journal central fournit un magasin sécurisé et centralisé pour les journaux ESXi. Vous pouvez surveiller plus facilement tous les hôtes avec un seul outil. Vous pouvez également effectuer une analyse et une recherche agrégées pour rechercher des éléments tels que des					

	attaques coordonnées sur plusieurs hôtes. La connexion à un serveur de journaux sécurisé et centralisé permet d'éviter la falsification des journaux et fournit un enregistrement d'audit à long terme. **Correction**: Pour configurer correctement la journalisation à distance, procédez comme suit à partir du client Web vSphere : 1. Sélectionnez l'hôte 2. Cliquez sur Configurer puis développez Système puis sélectionnez Paramètres système avancés. 3. Sélectionnez Modifier puis saisissez Syslog.global.logHost dans le filtre. 4. Définissez Syslog.global.logHost sur le nom d'hôte ou l'adresse IP du serveur de journalisation central. 5. Cliquez sur OK. Vous pouvez également exécuter la commande PowerCLI suivante : # Set Syslog.global.logHost for each host Get-VMHost | Foreach { Set-AdvancedSetting -VMHost $_ -Name Syslog.global.logHost -Value "<NewLocation>" } Note : lors de la configuration d'un hôte de journal distant, il est également recommandé de définir "Syslog.global.logDirUnique" sur true. Vous devez configurer les paramètres syslog pour chaque hôte.
Références	Guide de configuration de sécurité VMware https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-9F67DB52-F469-451F-B6C8-DAE8D95976E7.html
Exceptions	

CONSOLE

Les exigences de sécurité concernant la console d'administration.

Console					
2.5.1	Assurez-vous que le shell ESXi est désactivé	**P**	**C**	**T**	**D**
Spécificités	**Details** : Le shell ESXi est un environnement de ligne de commande interactif disponible à partir de l'interface utilisateur de la console directe (DCUI) ou à distance via SSH. Le shell ESXi ne doit être activé sur un hôte que lors de l'exécution de diagnostics ou de dépannage. Les activités effectuées à partir du shell ESXi contournent vCenter RBAC et les contrôles d'audit, de sorte que le shell ESXi ne doit être activé que lorsque cela est nécessaire pour dépanner/résoudre les problèmes qui ne peuvent pas être résolus via le client Web vSphere ou vCLI/PowerCLI. **Correction** : Pour désactiver le shell ESXi, procédez comme suit : 1. Dans vSphere Web Client, sélectionnez l'hôte. 2. Sélectionnez Configurer puis développez Système et sélectionnez Services. 3. Cliquez sur ESXi Shell, puis sur Modifier la stratégie de démarrage. 4. Définissez la stratégie de démarrage sur Démarrer et arrêter manuellement. 5. Cliquez sur OK. Vous pouvez également utiliser la commande **PowerCLI** suivante : # Set the ESXi shell to start manually rather than automatically for all hosts Get-VMHost | Get-VMHostService | Where { $_.key -eq "TSM" } | Set-VMHostService -Policy Off				
Références	1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-B5144CE9-F8BB-494D-8F5D-0D5621D65DAE.html 2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-DFA67697-232E-4F7D-860F-96C0819570A8.html				
Exceptions					
2.5.2	Assurez-vous que SSH est désactivé	**P**	**C**	**T**	**D**
Spécificités	**Details** : Le shell ESXi, lorsqu'il est activé, est accessible directement depuis la console hôte via l'interface DCUI ou à distance via SSH. Désactivez Secure Shell (SSH) pour chaque hôte ESXi afin d'empêcher l'accès à distance au shell ESXi et n'activez SSH que lorsque cela est nécessaire pour le dépannage ou les diagnostics.				

	L'accès à distance à l'hôte doit être limité à vSphere Client, aux outils de ligne de commande à distance (vCLI/PowerCLI) et via les API publiées. Dans des circonstances normales, l'accès à distance à l'hôte à l'aide de SSH doit être désactivé. **Impact**: Dans les scénarios de dépannage et d'évaluation, la désactivation de SSH, qui est la valeur par défaut, peut empêcher les connexions à l'hôte par des outils ou via d'autres méthodes. **Correction**: Pour désactiver SSH, procédez comme suit : 1. Dans vSphere Web Client, sélectionnez l'hôte. 2. Sélectionnez Configurer puis développez Système et sélectionnez Services. 3. Cliquez sur SSH puis cliquez sur Modifier la stratégie de démarrage. 4. Définissez la stratégie de démarrage sur Démarrer et arrêter manuellement. 5. Cliquez sur OK. 6. Tandis qu'ESXi Shell est toujours sélectionné, cliquez sur Arrêter. Vous pouvez également utiliser la commande **PowerCLI** suivante : # Set SSH to start manually rather than automatically for all hosts Get-VMHost | Get-VMHostService | Where { $_.key -eq "TSM-SSH" } | Set-VMHostService -Policy Off Note : Syslog.global.LogDir doit être défini pour chaque hôte. Les paramètres syslog de l'hôte peuvent également être configurés à l'aide de vCLI ou PowerCLI, ou à l'aide d'un client API.
Références	https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-12E27BF3-3769-4665-8769-DA76C2BC9FFE.html
Exceptions	
2.4.3	Assurez-vous que la journalisation à distance est configurée pour les hôtes ESXi — **P** **C**
Spécificités	**Détails** : Par défaut, les journaux ESXI sont stockés sur un volume de travail local ou un disque virtuel. Pour conserver les journaux, configurez également la journalisation à distance sur un hôte de journal central pour les hôtes ESXI. La journalisation à distance sur un hôte de journal central fournit un magasin sécurisé et centralisé pour les journaux ESXi. Vous pouvez surveiller plus facilement tous les hôtes avec un seul outil. Vous pouvez également effectuer une analyse et une recherche agrégées pour rechercher des éléments tels que des

	attaques coordonnées sur plusieurs hôtes. La connexion à un serveur de journaux sécurisé et centralisé permet d'éviter la falsification des journaux et fournit un enregistrement d'audit à long terme. **Correction**: Pour configurer correctement la journalisation à distance, procédez comme suit à partir du client Web vSphere : 1. Sélectionnez l'hôte 2. Cliquez sur Configurer puis développez Système puis sélectionnez Paramètres système avancés. 3. Sélectionnez Modifier puis saisissez Syslog.global.logHost dans le filtre. 4. Définissez Syslog.global.logHost sur le nom d'hôte ou l'adresse IP du serveur de journalisation central. 5. Cliquez sur OK. Vous pouvez également exécuter la commande PowerCLI suivante : # Set Syslog.global.logHost for each host Get-VMHost | Foreach { Set-AdvancedSetting -VMHost $_ -Name Syslog.global.logHost -Value "<NewLocation>" } Note : lors de la configuration d'un hôte de journal distant, il est également recommandé de définir "Syslog.global.logDirUnique" sur true. Vous devez configurer les paramètres syslog pour chaque hôte.
Références	Guide de configuration de sécurité VMware https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-9F67DB52-F469-451F-B6C8-DAE8D95976E7.html
Exceptions	

STOCKAGE

Les exigences de sécurité concernant le stockage.

Stockage					
2.5.1	Assurez-vous que les ressources du réseau de stockage (SAN) sont correctement séparées	**P**	**C**	**T**	**D**
Spécificités	**Details** : Utilisez le zonage et le masquage de numéro d'unité logique (LUN) pour séparer l'activité du réseau de stockage (SAN). Le zonage fournit un contrôle d'accès dans la topologie SAN. Le zonage définit quels adaptateurs de bus hôte (HBA) peuvent se connecter à quelles cibles. Les périphériques à l'extérieur d'une zone ne sont pas visibles pour les périphériques à l'intérieur de la zone lorsque le zonage SAN est configuré. Par exemple, les zones définies pour les tests doivent être gérées indépendamment au sein du SAN afin qu'elles n'interfèrent pas avec l'activité dans les zones de production. De même, vous pouvez configurer différentes zones pour différents départements. Le zonage doit prendre en compte tous les groupes d'hôtes qui ont été configurés sur le périphérique SAN. Le masquage de LUN est un processus qui rend un LUN disponible pour certains hôtes et indisponible pour d'autres hôtes. La séparation de l'activité SAN peut réduire la surface d'attaque du SAN, empêcher les systèmes non ESXi d'accéder aux SAN et séparer les environnements, par exemple, les environnements de test et de production. **Correction** : Les procédures de correction pour séparer correctement l'activité SAN sont spécifiques au fournisseur ou au produit SAN. En général, avec les hôtes ESXi, utilisez une segmentation à un seul initiateur ou une segmentation à un seul initiateur et à une seule cible. Cette dernière est une pratique de zonage privilégiée. L'utilisation du zonage plus restrictif évite les problèmes et les erreurs de configuration qui peuvent survenir sur le SAN.				
Références	1. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.storage.doc/GUID-6029358F-8EE8-4143-9BB0-16ABB3CA0FE3.html 2. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-BFE9046A-2278-4026-809A-ED8F9D8FDACE.html 3. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.storage.doc/GUID-39A4551F-4B03-43A6-BEDF-FAB1528C070D.html				
Exceptions					
2.5.2	Assurez-vous que l'authentification CHAP bidirectionnelle pour le trafic iSCSI est activée	**P**	**C**	**T**	**D**

Spécificités	

Details :
vSphere permet l'utilisation de l'authentification bidirectionnelle de la cible et de l'hôte iSCSI. Le protocole CHAP (Bidirectional Challenge-Handshake Authentication Protocol), également connu sous le nom de CHAP mutuel, doit être activé pour fournir une authentification bidirectionnelle.

En n'authentifiant pas à la fois la cible iSCSI et l'hôte, il existe un risque d'attaque de l'homme du milieu dans laquelle un attaquant pourrait se faire passer pour l'un ou l'autre côté de la connexion pour voler des données. L'authentification bidirectionnelle peut atténuer ce risque.
Remarque : choisir de ne pas appliquer l'authentification bidirectionnelle peut être judicieux si vous créez un réseau ou un VLAN dédié pour desservir tous vos périphériques iSCSI. Si l'installation iSCSI est isolée du trafic réseau général, elle est moins vulnérable à l'exploitation.

Correction :

Pour activer l'authentification CHAP bidirectionnelle pour le trafic iSCSI, procédez comme suit :

1. Dans vSphere Web Client, sélectionnez l'hôte.
2. Cliquez sur Configurer puis développez Stockage.
3. Sélectionnez Adaptateurs de stockage, puis sélectionnez l'adaptateur iSCSI.
4. Sous Propriétés, cliquez sur Modifier à côté d'Authentification.
5. En regard de Méthode d'authentification, sélectionnez Utiliser CHAP bidirectionnel dans la liste déroulante.
6. Spécifiez le nom CHAP sortant.

-Assurez-vous que le nom que vous spécifiez correspond au nom configuré côté stockage.
-Pour définir le nom CHAP sur le nom de l'adaptateur iSCSI, sélectionnez "Utiliser le nom de l'initiateur".
-Pour définir le nom CHAP sur autre chose que le nom de l'initiateur iSCSI, désélectionnez "Utiliser le nom de l'initiateur" et saisissez un nom dans la zone de texte Nom.

8. Entrez un secret CHAP sortant à utiliser dans le cadre de l'authentification. Utilisez le même secret que votre secret côté stockage.
9. Spécifiez les informations d'identification CHAP entrantes. Assurez-vous que vos secrets sortants et entrants ne correspondent pas.
10. Cliquez sur OK.
11. Cliquez sur l'avant-dernier symbole intitulé Rescan Adapter.

Vous pouvez également exécuter la commande PowerCLI suivante :

```
# Set the Chap settings for the Iscsi Adapter Get-VMHost | Get-VMHostHba | Where {$_.Type -eq "Iscsi"} | Set-VMHostHba # Use desired parameters here
```

	Note : Avant de configurer les paramètres CHAP pour le logiciel ou le matériel iSCSI dépendant, déterminez s'il faut configurer le CHAP unidirectionnel ou bidirectionnel. Les adaptateurs iSCSI matériels indépendants ne prennent pas en charge CHAP bidirectionnel. 1. Vérifiez les paramètres CHAP configurés côté stockage. Les paramètres que vous configurez doivent correspondre à ceux côté stockage. 2. Privilège requis : Host.Configuration.Storage Partition Configuration				
Références	1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-AC65D747-728F-4109-96DD-49B433E2F266.html 2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-2F1E64DB-20BB-4D18-A083-8E65FE380899.html				
Exceptions					
2.5.3	Garantir l'unicité des secrets d'authentification CHAP pour le trafic iSCSI	**P**	**C**	**T**	**D**
Spécificités	**Details** : Le protocole CHAP (Challenge-Handshake Authentication Protocol) exige que le client et l'hôte connaissent le secret (mot de passe) pour établir une connexion. Chaque secret d'authentification mutuelle doit être unique. Raisonnement: Si tous les secrets d'authentification mutuelle sont uniques, la compromission d'un secret ne permet pas à un attaquant de s'authentifier auprès d'autres hôtes ou clients utilisant ce même secret. **Correction** : Pour modifier les valeurs des secrets CHAP afin qu'ils soient uniques, procédez comme suit : 1. Dans vSphere Web Client, sélectionnez l'hôte. 2. Cliquez sur Configurer puis développez Stockage. 3. Sélectionnez Adaptateurs de stockage, puis sélectionnez l'adaptateur iSCSI. 4. Sous Propriétés, cliquez sur Modifier à côté d'Authentification. 5. En regard de Méthode d'authentification, spécifiez la méthode d'authentification dans la liste déroulante. sur une o Utiliser le CHAP unidirectionnel si requis par la cible o Utiliser le CHAP unidirectionnel à moins que la cible ne l'interdise o Utiliser le CHAP unidirectionnel o Utiliser le CHAP bidirectionnel 6. Spécifiez le nom CHAP sortant. o Assurez-vous que le nom que vous spécifiez correspond au nom configuré côté stockage. o Pour définir le nom CHAP sur le nom de l'adaptateur iSCSI, sélectionnez "Utiliser le nom de l'initiateur".				

	o Pour définir le nom CHAP sur autre chose que le nom de l'initiateur iSCSI, désélectionnez "Utiliser le nom de l'initiateur" et saisissez un nom dans la zone de texte Nom. 8. Entrez un secret CHAP sortant à utiliser dans le cadre de l'authentification. Utilisez le même secret que votre secret côté stockage. 9. En cas de configuration avec CHAP bidirectionnel, spécifiez les informations d'identification CHAP entrantes. Assurez-vous que vos secrets sortants et entrants ne correspondent pas. 10. En cas de configuration avec CHAP bidirectionnel, spécifiez les informations d'identification CHAP entrantes. Assurez-vous que vos secrets sortants et entrants ne correspondent pas. 11. Cliquez sur OK. 12. Cliquez sur l'avant-dernier symbole intitulé Rescan Adapter .
Références	1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-AC65D747-728F-4109-96DD-49B433E2F266.html 2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-2F1E64DB-20BB-4D18-A083-8E65FE380899.html
Exceptions	

VNETWORK

Les exigences de sécurité concernant les connexions réseaux.

vNetwork					
2.6.1	Assurez-vous que la stratégie vSwitch Forged Transmits est définie sur Reject	**P**	**C**	**T**	**D**
Spécificités	**Details** : Définissez la stratégie vSwitch Forged Transmits sur Rejeter pour chaque vSwitch. Reject Forged Transmit peut être défini au niveau du vSwitch et/ou du groupe de ports. Vous pouvez remplacer les paramètres au niveau du commutateur au niveau du groupe de ports. Si le système d'exploitation de la machine virtuelle modifie l'adresse MAC, le système d'exploitation peut envoyer des trames avec une adresse MAC source usurpée à tout moment. Cela permet à un système d'exploitation d'organiser des attaques malveillantes sur les appareils d'un réseau en se faisant passer pour une carte réseau autorisée par le réseau récepteur. Définir les transmissions falsifiées sur accepter signifie que le commutateur virtuel ne compare pas les adresses MAC source et effective. Pour se protéger contre l'usurpation d'identité d'adresse MAC, tous les commutateurs virtuels doivent avoir des transmissions falsifiées définies sur rejeter. **Impact**: Cela empêchera les machines virtuelles de modifier leur adresse MAC effective. Cela affectera les applications qui nécessitent cette fonctionnalité, telles que Microsoft Clustering, qui nécessite que les systèmes partagent efficacement une adresse MAC. Cela affectera le fonctionnement d'un pont de couche 2. Cela affectera également les applications qui nécessitent une adresse MAC spécifique pour la licence. Une exception doit être faite pour les groupes de ports auxquels ces applications sont connectées. **Correction** : Pour définir la stratégie afin de rejeter les transmissions falsifiées, procédez comme suit : 1. Dans vSphere Web Client, sélectionnez l'hôte. 2. Cliquez sur Configurer puis développez Mise en réseau. 3. Sélectionnez Commutateurs virtuels, puis cliquez sur Modifier. 4. Cliquez sur Sécurité. 5. Définissez les transmissions falsifiées sur Rejeter dans la liste déroulante. 6. Cliquez sur OK. Alternativement, la commande shell ESXi suivante peut être utilisée : # esxcli network vswitch standard policy security set -v vSwitch2 -f false				

Références	https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-891147DD-3E2E-45A1-9B50-7717C3443DD7.html				
Exceptions					
2.6.2	Assurez-vous que la stratégie de changement d'adresse MAC vSwitch est définie sur rejeter	**P**	**C**	**T**	**D**
Spécificités	**Details** : Assurez-vous que la politique de changement d'adresse MAC dans le vSwitch est définie sur rejeter. Le rejet des modifications MAC peut être défini au niveau du vSwitch et/ou du groupe de ports. Vous pouvez remplacer les paramètres au niveau du commutateur au niveau du groupe de ports. Si le système d'exploitation de la machine virtuelle modifie l'adresse MAC, il peut envoyer des trames avec une adresse MAC source usurpée à tout moment. Cela lui permet d'organiser des attaques malveillantes sur les appareils d'un réseau en se faisant passer pour une carte réseau autorisée par le réseau récepteur. **Impact**: Cela empêchera les machines virtuelles de modifier leur adresse MAC effective. Cela affectera les applications qui nécessitent cette fonctionnalité, telles que Microsoft Clustering, qui nécessite que les systèmes partagent efficacement une adresse MAC. Cela affectera le fonctionnement d'un pont de couche 2. Cela affectera également les applications qui nécessitent une adresse MAC spécifique pour la licence. Une exception doit être faite pour les groupes de ports auxquels ces applications sont connectées. **Correction**: Pour définir la stratégie sur Rejeter, procédez comme suit : 1. Dans vSphere Web Client, sélectionnez l'hôte. 2. Cliquez sur Configurer puis développez Mise en réseau. 3. Sélectionnez Commutateurs virtuels, puis cliquez sur Modifier. 4. Cliquez sur Sécurité. 5. Définissez les changements d'adresse MAC sur Rejeter dans la liste déroulante. 6. Cliquez sur OK. Vous pouvez également effectuer les opérations suivantes à l'aide du shell ESXi : # esxcli network vswitch standard policy security set -v vSwitch2 -m false				
Références	https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-891147DD-3E2E-45A1-9B50-7717C3443DD7.html				

Exceptions					
2.6.3	Assurez-vous que la stratégie vSwitch Promiscuous Mode est définie sur Rejeter	**P**	**C**		
Spécificités	**Détails** : Assurez-vous que la politique de mode promiscuité dans le vSwitch est définie sur rejeter. Le mode promiscuité peut être défini au niveau du vSwitch et/ou du groupe de ports. Vous pouvez remplacer les paramètres au niveau du commutateur au niveau du groupe de ports. Lorsque le mode promiscuité est activé pour un commutateur virtuel, toutes les machines virtuelles connectées au dvPortgroup ont le potentiel de lire tous les paquets traversant ce réseau. Cela pourrait permettre un accès non autorisé au contenu de ces paquets. Impact: Il peut y avoir une raison légitime d'activer le mode promiscuité pour des raisons de débogage, de surveillance ou de dépannage. Les dispositifs de sécurité peuvent nécessiter la possibilité de voir tous les paquets sur un vSwitch. Une exception doit être faite pour les dvPortgroups auxquels ces applications sont connectées afin de permettre une visibilité permanente du trafic sur ce dvPortgroup. **Correction**: Pour définir la stratégie sur Rejeter, procédez comme suit : 1. Dans vSphere Web Client, sélectionnez l'hôte. 2. Cliquez sur Configurer puis développez Mise en réseau. 3. Sélectionnez Commutateurs virtuels, puis cliquez sur Modifier. 4. Cliquez sur Sécurité. 5. Définissez Mode promiscuité sur Rejeter dans la liste déroulante. 6. Cliquez sur OK. Vous pouvez également effectuer les opérations suivantes via le shell ESXi :. Vous pouvez également exécuter la commande PowerCLI suivante : # esxcli network vswitch standard policy security set -v vSwitch2 -p false				
Références	Guide de configuration de sécurité VMware https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-891147DD-3E2E-45A1-9B50-7717C3443DD7.html				
Exceptions					
2.6.4	Assurez-vous que les groupes de ports ne sont pas configurés sur la valeur du VLAN natif	**P**	**C**	**T**	**D**

Spécificités	**Details** : ESXi n'utilise pas le concept de VLAN natif, donc ne configurez pas les groupes de ports pour utiliser l'ID de VLAN natif. Si la valeur par défaut de 1 pour le VLAN natif est utilisée, les groupes de ports du commutateur virtuel ESXi Server doivent être configurés avec n'importe quelle valeur comprise entre 2 et 4094. Sinon, assurez-vous que le groupe de ports n'est pas configuré pour utiliser la valeur définie pour le VLAN natif. Les trames avec VLAN spécifié dans le groupe de ports auront une étiquette, mais les trames sans VLAN spécifié dans le groupe de ports ne sont pas étiquetées et finiront donc par appartenir au VLAN natif du commutateur physique. Par exemple, les trames sur le VLAN 1 d'un commutateur physique Cisco ne seront pas marquées, car elles sont considérées comme le VLAN natif. Cependant, les trames d'ESXi spécifiées comme VLAN 1 seront marquées d'un « 1 » ; par conséquent, le trafic d'ESXi destiné au VLAN natif ne sera pas correctement acheminé (car il est étiqueté avec un « 1 » au lieu d'être non étiqueté), et le trafic du commutateur physique provenant du VLAN natif ne sera pas visible (car il n'est pas marqué). Si le groupe de ports du commutateur virtuel ESXi utilise l'ID de VLAN natif, le trafic de ces machines virtuelles ne sera pas visible pour le VLAN natif sur le commutateur, car le commutateur attend un trafic non balisé. **Correction** : Pour vérifier que l'ID de VLAN natif n'est pas utilisé pour les groupes de ports, procédez comme suit : # Répertorier tous les vSwitches, leurs groupes de ports et leurs ID VLAN Get-VirtualPortGroup -Standard | Sélectionnez virtualSwitch, Nom, VlanID Pour arrêter d'utiliser l'ID de VLAN natif pour les groupes de ports, procédez comme suit : 1. Dans vSphere Web Client, sélectionnez l'hôte. 2. Cliquez sur Configurer puis développez Mise en réseau. 3. Sélectionnez Commutateurs virtuels. 4. Développez le vSwitch standard. 5. Affichez le diagramme de topologie du commutateur, qui montre les différents groupes de ports associés à ce commutateur. 6. Pour chaque groupe de ports sur le vSwitch, vérifiez et enregistrez les ID VLAN utilisés. 7. Si une modification de l'ID VLAN est nécessaire, cliquez sur le nom du groupe de ports dans le diagramme de topologie du commutateur virtuel. 8. Cliquez sur l'option Modifier les paramètres. 9. Dans la section Propriétés, saisissez un nom approprié dans le champ Nom du réseau. 10. Dans la liste déroulante VLAN ID, sélectionnez ou saisissez un nouveau VLAN. 11. Cliquez sur OK.
Références	https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-3A9D9911-3632-4B81-9D2E-A2F9F2D01180.html

Exceptions					
2.6.5	Assurez-vous que les groupes de ports ne sont pas configurés sur les valeurs VLAN réservées par les commutateurs physiques en amont	**P**	**C**	**T**	**D**
Spécificités	**Details** : Assurez-vous que les groupes de ports ne sont pas configurés sur des valeurs VLAN réservées par des commutateurs physiques en amont. Certains commutateurs physiques réservent certains ID VLAN à des fins internes et interdisent souvent le trafic configuré avec ces valeurs. Par exemple, les commutateurs Cisco Catalyst réservent généralement les VLAN 1001 à 1024 et 4094, tandis que les commutateurs Nexus réservent généralement 3968 à 4047 et 4094. Consultez la documentation de votre commutateur spécifique. L'utilisation d'un VLAN réservé peut entraîner un déni de service sur le réseau. **Correction**: Pour remplacer les valeurs VLAN des groupes de ports par des valeurs non réservées, procédez comme suit : 1. Dans vSphere Web Client, sélectionnez l'hôte. 2. Cliquez sur Configurer puis développez Mise en réseau. 3. Sélectionnez Commutateurs virtuels. 4. Développez le vSwitch standard. 5. Affichez le diagramme de topologie du commutateur, qui montre les différents groupes de ports associés à ce commutateur. 6. Pour chaque groupe de ports sur le vSwitch, vérifiez et enregistrez les ID VLAN utilisés. 7. Si une modification de l'ID VLAN est nécessaire, cliquez sur le nom du groupe de ports dans le diagramme de topologie du commutateur virtuel. 8. Cliquez sur l'option Modifier les paramètres. 9. Dans la section Propriétés, saisissez un nom approprié dans le champ Nom du réseau. 10. Dans la liste déroulante VLAN ID, sélectionnez ou saisissez un nouveau VLAN. 11. Cliquez sur OK.				
Références	http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/20ew/configuration/guide/config/vlans.html#wp1038758				
Exceptions					

MACHINES VIRTUELLES - VM

Les contrôles de sécurité concernant les Machines Virtuelles VM.

Machines Virtuelles - VM						
2.7.1	Assurez-vous que les messages d'information de la machine virtuelle au fichier VMX sont limités	**P**	**C**	**T**	**D**	
Spécificités	**Details** : Limitez les messages d'information de la machine virtuelle (VM) au fichier d'extensions de machine virtuelle (VMX) pour éviter de remplir la banque de données. Le fichier de configuration contenant ces paires nom-valeur est limité à une taille de 1 Mo par défaut. Cela devrait être suffisant dans la plupart des cas, mais vous pouvez modifier cette valeur si nécessaire, par exemple si de grandes quantités d'informations personnalisées sont stockées dans le fichier de configuration. Remplir le magasin de données avec des messages d'information de la VM vers le fichier VMX pourrait entraîner un déni de service. **Correction** : Définissez cette configuration comme suit : Exécutez la commande PowerCLI suivante : # Ajoutez le paramètre à toutes les VM Get-VM | New-AdvancedSetting -Name "tools.setInfo.sizeLimit" -value 1048576 **Valeur par défaut:** 1048576					
Références	https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-91BF834E-CB92-4014-8CF7-29CE40F3E8A3.html					
Exceptions						
2.7.2	Assurez-vous qu'une seule connexion de console distante est autorisée à une machine virtuelle à tout moment	**P**	**C**	**T**	**D**	
Spécificités	**Details** : Par défaut, les sessions de console distante peuvent être connectées par plusieurs utilisateurs à la fois. Autorisez une seule connexion de console distante à une machine virtuelle à la fois. Les autres tentatives seront rejetées jusqu'à ce que la première connexion se déconnecte. Lorsque plusieurs sessions sont activées, chaque fenêtre de terminal reçoit une notification concernant la nouvelle session. Si un administrateur de la VM se connecte à l'aide d'une console distante VMware pendant sa session, un non-administrateur de la VM peut se connecter à la console et observer les actions de l'administrateur. En outre, cela pourrait entraîner la perte de l'accès de la console à une machine virtuelle par un administrateur. Par exemple, si une boîte de jonction est utilisée pour une					

	session de console ouverte et que l'administrateur perd une connexion à cette boîte, la session de console reste ouverte. Autoriser deux sessions de console permet le débogage via une session partagée. Pour une sécurité maximale, une seule session de console distante à la fois doit être autorisée. **Correction**: Pour définir cette configuration, utilisez l'interface vSphere comme suit : 1. Sélectionnez la machine virtuelle, puis sélectionnez Actions suivi de Modifier les paramètres. 2. Cliquez sur l'onglet Options VM puis développez Avancé. 3. Cliquez sur MODIFIER LA CONFIGURATION. 4. Cliquez sur AJOUTER DES PARAMÈTRES DE CONFIGURATION puis saisissez RemoteDisplay.maxConnections avec une valeur de 1. 5. Cliquez sur OK, puis à nouveau sur OK. Vous pouvez également exécuter la commande PowerCLI suivante pour les VM qui ne spécifient pas le paramètre : # Ajoutez le paramètre à toutes les VM Get-VM | New-AdvancedSetting -Name "RemoteDisplay.maxConnections" -value 1 Exécutez la commande PowerCLI suivante pour les machines virtuelles qui spécifient le paramètre mais dont la valeur est incorrecte : # Ajoutez le paramètre à toutes les machines virtuelles Get-VM | New-AdvancedSetting -Name "RemoteDisplay.maxConnections" -value 1 -Force					
Références	1. http://www.ibenit.com/post/85227299008/security-benchmark-hardening-guide-policies-and-profile 2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-27A340F5-DE98-41A8-AC73-01ED4949EEF2.html 3. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-7FED3B17-E2E9-4360-AAC6-B70F9A9AEB84.html					
Exceptions						
2.7.3	Assurez-vous que la modification et la déconnexion non autorisées des appareils sont désactivées	**P**	**C**			
Spécificités	**Détails** : Dans une machine virtuelle, les utilisateurs et les processus sans privilèges racine ou administrateur peuvent connecter des périphériques, tels que des adaptateurs réseau et des lecteurs de CD-ROM. Cela devrait être évité.					

	La désactivation de la connexion non autorisée des appareils permet d'empêcher les modifications non autorisées au sein du système d'exploitation invité, qui pourraient être utilisées pour obtenir un accès non autorisé, provoquer des conditions de déni de service et autrement affecter négativement la sécurité du système d'exploitation invité. **Correction**: Pour empêcher les connexions de périphériques non autorisées, exécutez la commande PowerCLI suivante : # Ajoutez le paramètre à toutes les machines virtuelles Get-VM | New-AdvancedSetting -Name "isolation.device.connectable.disable" -value $true
Références	Guide de configuration de sécurité VMware https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-F88A5FED-552B-44F9-A168-C62D9306DBD6.html
Exceptions	

SURVEILLANCE

Les contrôles de sécurité concernant la surveillance.

Surveillance						
2.8.1	Assurez-vous que l'accès aux machines virtuelles via les API réseau dvfilter est correctement configuré	**P**	**C**	**T**	**D**	
Spécificités	**Details** : Une machine virtuelle doit être configurée explicitement pour accepter l'accès par l'API réseau dvfilter. Seules les machines virtuelles qui doivent être accessibles par cette API doivent être configurées pour accepter un tel accès. Un attaquant pourrait compromettre une machine virtuelle en utilisant l'API dvfilter. **Correction** : Pour définir cette configuration, utilisez l'interface vSphere comme suit : 1. Sélectionnez la machine virtuelle, puis sélectionnez Actions suivi de Modifier les paramètres. 2. Cliquez sur l'onglet Options VM puis développez Avancé. 3. Cliquez sur MODIFIER LA CONFIGURATION. 4. Supprimez la valeur de ethernet0.filter1.name = dv-filter. - Les paramètres sont supprimés lorsqu'aucune valeur n'est présente 5. Cliquez sur OK. Vous pouvez également configurer une VM pour autoriser l'accès à dvfilter via la méthode suivante dans le fichier VMX : 1. Configurez les éléments suivants dans le fichier VMX : ethernet0.filter1.name = dv-filter1 où ethernet0 est l'interface de la carte réseau de la machine virtuelle à protéger, filter1 est le numéro du filtre utilisé et dv -filter1 est le nom du module de noyau de chemin de données particulier qui protège la machine virtuelle. - Si l'accès à dvfilter ne doit pas être autorisé : Supprimez les éléments suivants de son fichier VMX : ethernet0.filter1.name = dv-filter1. 2. Définissez correctement le nom du noyau du chemin de données.						
Références	1. http://kb.vmware.com/kb/1714 2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-CD0783C9-1734-4B9A-B821-ED17A77B0206.html					
Exceptions						
2.8.2	Assurez-vous que la connexion automatique est désactivée	**P**	**C**	**T**	**D**	

Spécificités	**Details** : La connexion automatique doit être désactivée si elle n'est pas nécessaire. Certains paramètres VMX ne s'appliquent pas sur vSphere, car les machines virtuelles VMware fonctionnent sur vSphere et sur des plates-formes de virtualisation hébergées telles que Workstation et Fusion. Les chemins de code pour ces fonctionnalités ne sont pas implémentés dans ESXi. La désactivation explicite de ces fonctionnalités, telles que la connexion automatique, réduit le risque de vulnérabilités, car elle réduit le nombre de façons dont un invité peut affecter l'hôte. Notez que ceux-ci sont référencés pour les organisations qui insistent sur le fait que tout paramètre documenté, qu'il soit implémenté dans le code ou non, doit avoir une valeur. **Correction**: Pour définir cette configuration, utilisez l'interface vSphere comme suit : 1. Sélectionnez la machine virtuelle, puis sélectionnez Actions suivi de Modifier les paramètres. 2. Cliquez sur l'onglet Options VM puis développez Avancé. 3. Cliquez sur MODIFIER LA CONFIGURATION. 4. Cliquez sur ADD CONFIGURATION PARAMS puis saisissez isolation.tools.ghi.autologon.disable avec la valeur TRUE. 5. Cliquez sur OK, puis à nouveau sur OK. Vous pouvez également exécuter la commande PowerCLI suivante : # Ajoutez le paramètre à toutes les machines virtuelles Get-VM | New-AdvancedSetting -Name "isolation.tools.ghi.autologon.disable" -value $true					
Références	https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html					
Exceptions						
2.8.3	Assurez-vous que Shell Action est désactivée	**P**	**C**			
Spécificités	**Détails** : La fonctionnalité Shell Action doit être désactivée si elle n'est pas nécessaire. Certains paramètres VMX ne s'appliquent pas sur vSphere, car les machines virtuelles VMware fonctionnent sur vSphere et sur des plates-formes de virtualisation hébergées telles que Workstation et Fusion. Les chemins de code pour ces fonctionnalités ne sont pas implémentés dans ESXi. La désactivation explicite de ces fonctionnalités, telles que la fonctionnalité Shell Action, réduit le potentiel de vulnérabilités, car elle réduit le nombre de façons dont un invité peut affecter l'hôte. Notez que ceux-					

	ci sont référencés pour les organisations qui insistent sur le fait que tout paramètre documenté, qu'il soit implémenté dans le code ou non, doit avoir une valeur. **Impact**: Certains outils et processus automatisés peuvent cesser de fonctionner. **Correction**: Pour définir cette configuration, utilisez l'interface vSphere comme suit : 1. Sélectionnez la machine virtuelle, puis sélectionnez Actions suivi de Modifier les paramètres. 2. Cliquez sur l'onglet Options VM puis développez Avancé. 3. Cliquez sur MODIFIER LA CONFIGURATION. 4. Cliquez sur ADD CONFIGURATION PARAMS puis saisissez isolation.ghi.host.shellAction.disable avec la valeur TRUE. 5. Cliquez sur OK, puis à nouveau sur OK. Pour désactiver la fonctionnalité Shell Action, exécutez la commande PowerCLI suivante : # Ajoutez le paramètre à toutes les machines virtuelles Get-VM | New-AdvancedSetting -Name "isolation.ghi.host.shellAction.disable" -value $true
Références	Guide de configuration de sécurité VMware ICI
Exceptions	

RÉFÉRENCES

Site officiel VMware pour les guides d'endurcissement :
https://www.vmware.com/ca/security/hardening-guides.html

CIS Center of Security - Benchmarks
https://www.cisecurity.org/benchmark/vmware

CIS Center of Security - Guide
https://downloads.cisecurity.org/#/

GLOSSAIRE

vSphere : Plateforme de virtualisation de serveurs de VMware qui permet de gérer les machines virtuelles et les ressources informatiques.
ESXi : Système d'exploitation bare-metal de VMware qui fournit une plateforme pour les machines virtuelles.
vCenter Server : Produit central de gestion pour vSphere qui permet de surveiller et de gérer les ressources informatiques.
vMotion : Technologie de VMware qui permet de déplacer des machines virtuelles en cours d'exécution d'un serveur physique à un autre sans interruption.
vSAN : Stockage défini par logiciel de VMware qui permet de créer un pool de stockage partagé pour les machines virtuelles.

vSphere Client : Interface graphique pour vCenter Server qui permet de gérer les ressources informatiques et les machines virtuelles.
vCenter Server Appliance : Version pré-configurée de vCenter Server qui s'exécute sur une machine virtuelle.
Datacenter : Unité de gestion de vCenter Server qui regroupe des ressources informatiques telles que des serveurs et du stockage.
Cluster : Ensemble de serveurs vSphere qui partagent des ressources informatiques telles que le processeur et la mémoire pour exécuter des machines virtuelles.
Host : Serveur physique exécutant le système d'exploitation ESXi et hébergeant des machines virtuelles.
Virtual Machine : Machine virtuelle qui s'exécute sur un hôte et qui peut être déplacée entre les hôtes avec vMotion.
Template : Image de machine virtuelle préconfigurée qui peut être utilisée pour déployer rapidement de nouvelles machines virtuelles.
Snapshot : Instantané d'une machine virtuelle qui peut être utilisé pour restaurer la machine virtuelle à un état antérieur.
Resource Pool : Ensemble de ressources informatiques telles que le processeur et la mémoire qui peuvent être assignées à des machines virtuelles.
Distributed Resource Scheduler (DRS) : Technologie de vCenter Server qui permet d'équilibrer automatiquement les charges de travail entre les hôtes dans un cluster.

Virtual Machine Disk (VMDK) : Format de fichier utilisé pour les disques durs virtuels des machines virtuelles.
Virtual Network Interface Card (vNIC) : Carte réseau virtuelle qui permet à une machine virtuelle de communiquer avec le réseau.
Virtual SCSI Controller : Contrôleur SCSI virtuel qui permet à une machine virtuelle d'accéder au stockage.
Virtual CPU (vCPU) : Unité de traitement virtuelle qui peut être assignée à une machine virtuelle pour exécuter des tâches.
Virtual Memory (vRAM) : Mémoire virtuelle qui peut être assignée à une machine virtuelle pour exécuter des applications.
Virtual Disk : Disque dur virtuel qui peut être utilisé par une machine virtuelle pour stocker des données.

Virtual BIOS : BIOS virtuel qui permet à une machine virtuelle de démarrer et de s'exécuter.
Virtual USB Controller : Contrôleur USB virtuel qui permet à une machine virtuelle d'utiliser des périphériques USB.
Virtual CD/DVD Drive : Lecteur CD/DVD virtuel qui peut être utilisé par une machine virtuelle pour lire des disques optiques.
Virtual Machine Monitor (VMM) : Logiciel qui gère les machines virtuelles et qui fournit des ressources telles que le processeur, la mémoire et le stockage.

Virtual Switch : Commutateur virtuel qui permet de connecter des machines virtuelles à un réseau physique.
Port Group : Groupe de ports logiques qui regroupent des ports de switch virtuel pour des besoins de gestion et de sécurité.
Virtual Network Interface Card (vNIC) : Carte réseau virtuelle qui permet à une machine virtuelle de communiquer avec le réseau.
Virtual LAN (VLAN) : Réseau local virtuel qui permet de séparer les trafics réseau pour des besoins de sécurité et de gestion.
Virtual Distributed Switch (VDS) : Commutateur distribué virtuel qui permet de gérer des commutateurs virtuels sur plusieurs hôtes vSphere.
Network I/O Control : Technologie qui permet de contrôler les entrées/sorties réseau pour éviter les congestions et les erreurs.
Virtual Network Adapters : Adaptateurs réseau virtuels qui permettent à une machine virtuelle de se connecter à un réseau physique ou virtuel.
Virtual Network Segments : Segments de réseau virtuel qui permettent de séparer les trafics réseau pour des besoins de sécurité et de gestion.
Virtual Network Traffic Shaping : Technologie qui permet de contrôler la vitesse de transmission des données sur un réseau virtuel.
Virtual Router : Routeur virtuel qui permet de connecter des réseaux virtuels entre eux et à des réseaux physiques.

Virtual SCSI Controller : Contrôleur SCSI virtuel qui permet à une machine virtuelle d'accéder au stockage.
Raw Device Mapping (RDM) : Mapping direct entre un périphérique de stockage physique et une machine virtuelle.
Storage DRS : Technologie de vCenter Server qui permet de gérer automatiquement les charges de travail de stockage entre les datastores.
Storage vMotion : Technologie de vCenter Server qui permet de déplacer des disques virtuels entre des datastores sans interruption.
Virtual Disk : Disque dur virtuel qui peut être utilisé par une machine virtuelle pour stocker des données.
Virtual SAN : Stockage défini par logiciel de VMware qui permet de créer un pool de stockage partagé pour les machines virtuelles.
NFS : Protocole de partage de fichiers qui permet de partager des données entre des systèmes d'exploitation différents.
iSCSI : Protocole de stockage en réseau qui permet de connecter des systèmes d'exploitation à un stockage distant.

vCenter Server Installer : Logiciel d'installation de vCenter Server qui permet de configurer et d'installer vCenter Server.
Single Sign-On (SSO) : Technologie qui permet d'authentifier les utilisateurs une seule fois pour accéder à plusieurs produits et services.
Inventory Service : Service qui stocke les informations sur les ressources informatiques gérées par vCenter Server.
vCenter Server Database : Base de données qui stocke les informations sur les ressources informatiques gérées par vCenter Server.
Platform Services Controller (PSC) : Composant de vCenter Server qui gère les services de plateforme tels que SSO et Inventory Service.
Linked Mode : Mode de vCenter Server qui permet de gérer plusieurs instances de vCenter Server comme une seule.
External PSC : Instance externe de PSC qui peut être utilisée pour gérer plusieurs instances de vCenter Server.
Embedded PSC : Instance intégrée de PSC qui est installée avec vCenter Server et qui peut être utilisée pour gérer une seule instance de vCenter Server.

RÉVISIONS

Date	Action	Auteur	Ver.
2022-11-03	Version initiale	Aboubakar - CESI de l'UQ	0.1
2022-11-07	Table des matières	Aboubakar - CESI de l'UQ	0.2
2022-11-17	Analyse Guide SCG version 6, version 7	Aboubakar - CESI de l'UQ	0.3
2022-12-04	Recommandation systèmes	Aboubakar - CESI de l'UQ	0.4
2022-12-16	SCG unifié	Aboubakar - CESI de l'UQ	0.5
2023-02-06	Contrôle de sécurité Stockage, Journalisation	Aboubakar - CESI de l'UQ	0.6
2023-02-10	Introduction, Contrôle de sécurité Réseau	Aboubakar - CESI de l'UQ	0.7
2023-02-28	Correction linguistique	BOUILLON, Marie-Josée	0.8
2023-03-13	Observations internes et validation	CESI de l'UQ	0.9
2023-03-20	Version prête pour publication	CESI de l'UQ	1.0