RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

SÉCURISATION D'UNE INFRASTRUCTURE VMWARE

LES FONDAMENTAUX

ANSSI-BP-103
02/04/2024

PUBLIC VISÉ :

Développeur | **Administrateur** | **RSSI** | **DSI** | Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI s'intitule **« Sécurisation d'une infrastructure VMware »**. Il est téléchargeable sur le site `cyber.gouv.fr`.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	02/04/2024	Version initiale

Table des matières

1
Préambule

Les technologies de virtualisation sont les sous-jacents d'insfrastructure de l'informatique en nuage (« *Cloud* »). Des briques techniques, appelées communément des « *hyperviseurs* », permettent d'assurer la gestion et de fédérer des ressources d'exécution (« *compute* »), réseau (« *network* ») ou de stockage (« *storage* »).

De fait, les hyperviseurs sont une cible privilégiée pour des attaquants. Dans la mesure où leur compromission permet l'accès à l'ensemble des données et des traitements hébergés, les niveaux de menace étatique et cybercriminel doivent nécessairement être considérés lors du déploiement d'une infrastructure de virtualisation. En fonction du type de menace, les motivations peuvent varier : espionnage ou déstabilisation pour la menace étatique, ou finalités lucratives, voire destruction pour la menace cybercriminelle.

Ce document vise à apporter un éclairage sur la manière de sécuriser les infrastructures virtualisées s'appuyant sur la technologie VMware. Cette dernière fait partie des principales technologies utilisées dans le domaine. Ces recommandations doivent être prises en compte et adaptées au cas par cas, en fonction du contexte d'emploi de l'infrastructure, du type de service porté et de sa criticité. Ce document traite des recommandations les plus importantes en la matière. Il ne vise ni l'exhaustivité ni un niveau de précision détaillé.

2
Principes généraux

Le but de ce chapitre est de définir certains principes généraux de fonctionnement de VMware nécessaires pour comprendre les recommandations du chapitre 3.

2.1 Architecture

Lors de la mise en place d'une infrastructure de virtualisation, il est important de considérer l'infrastructure de virtualisation comme un socle qui doit être indépendant des machines virtuelles qu'il héberge.

L'infrastructure de virtualisation peut être séparée en deux parties :

- le plan de contrôle, responsable du pilotage de l'infrastructure virtuelle ;
- le plan de donnée, qui porte les machines virtuelles.

Cette séparation est une première mesure de sécurité pour protéger l'infrastructure de virtualisation des machines virtuelles qu'elle héberge.

Dans la terminologie VMware utilisée dans les *validated designs* [1], ce découpage s'appelle :

- *Management domain* pour le cluster d'administration ;
- *Workload domain* pour un cluster de production.

2.2 Gestion des privilèges

La gestion des privilèges est importante dans une infrastructure de virtualisation. Il est donc nécessaire de comprendre les mécanismes utilisés pour gérer les accès et les privilèges. Dans vSphere, cette gestion passe par l'usage des rôles [2]. Un rôle est un ensemble de privilèges qui va spécifier des actions autorisées et droits de lecture-écriture sur les propriétés d'un objet. VMware permet de définir une politique d'accès en associant un utilisateur avec un rôle à un objet VMWare (ex. : machine virtuelle, *datastore*, vSwitch, *port group*, etc.).

1. Documentation éditeur sur les designs d'architecture vSphere VCF : https://techdocs.broadcom.com/fr/fr/vmware-cis/vcf/vcf-5-2-and-earlier/5-1/vcf-design-5-1/vmware-cloud-foundation-concepts/vmware-cloud-foundation-architecture-models.html

2. Documentation éditeur sur les rôles, https://techdocs.broadcom.com/fr/fr/vmware-cis/vsphere/vsphere/8-0/vsphere-security/vsphere-permissions-and-user-management-tasks/using-roles-to-assign-privileges.html

2.3 Cloisonnement réseau

Pour permettre de faire communiquer les machines virtuelles entre elles ou avec des machines ou des équipements externes, l'hyperviseur crée un ensemble de périphériques virtuels (commutateur virtuel, carte réseau virtuelle).

Dans une infrastructure vSphere, ces périphériques sont les vSwitch ou dvSwitch (commutateur de niveau 2 virtualisé), les vNic (carte réseau virtuelle).

Les dvSwitch apportent en plus d'une gestion centralisée, des fonctions avancées comme les PVLAN, la capture du trafic et bien d'autres fonctionnalités.

La facilité à segmenter les réseaux dans une infrastructure virtualisée permet d'isoler les machines virtuelles en fonction de leurs usages, leurs expositions, leurs sensibilités.

Afin d'assurer la connectivité entre hyperviseurs ESXi et les différents composants d'une infrastructure virtuelle (autres ESXi, vCenter, NSX, baie de stockage, sauvegarde, supervision...) on utilise les adaptateurs VMKernel [3].

Ces adaptateurs vont porter une adresse IP et vont permettre de gérer le trafic réseau à destination des différents composants de l'infrastructure, il peut y avoir plusieurs adaptateurs VMKernel sur un hyperviseur ESXi.

2.4 Micro-segmentation

La micro-segmentation est une technique de sécurité réseau qui permet de cloisonner les flux de chaque machine virtuelle ou groupe de machines virtuelles à travers des règles de filtrage granulaires et cumulables. Les règles de filtrage sont gérées de manière centralisée et indépendante du système d'exploitation de la machine virtuelle.

La micro-segmentation est une mesure de défense en profondeur qui, bien utilisée, permet :

- de limiter la latéralisation en cas de compromission d'une machine virtuelle ;
- de limiter les flux nord-sud et est-ouest [4] ;
- de rendre le filtrage plus précis (ex. : tags spécifiques sur des VM).

3. Documentation éditeur sur la mise en réseau des ESXi : https://techdocs.broadcom.com/fr/fr/vmware-cis/vsphere/vsphere/8-0/vsphere-networking.html

4. Les termes nord-sud et est-ouest désignent respectivement les flux de communication à l'extérieur de la zone (accès à une autre zone, à une passerelle Internet, etc.) et les flux de communication internes à la zone (entre des serveurs de même sensibilité par exemple).

Attention

Toute solution de micro-segmentation utilisant un agent à l'intérieur de la machine virtuelle pour effectuer les actions de filtrage apporte un niveau de sécurité inférieur aux solutions qui utilisent des composants au niveau de l'hyperviseur (ex. : modules kernel hyperviseur, openvswitch).

Les solutions de micro-segmentation en environnement virtualisé ont chacune leurs spécificités, leurs points forts et leurs faiblesses. Dans l'écosystème VMware vSphere, la micro-segmentation est apportée par la solution NSX. Il est à noter que la solution NSX contient d'autres fonctionnalités de sécurité et n'est pas uniquement dédiée à faire de la micro-segmentation. L'usage de NSX est soumis à licence.

La solution NSX est composée principalement de quatre composants :

- le *NSX manager*, qui permet de créer et de gérer les règles de filtrage de manière centralisée ;
- les *NSX controllers*, qui font partie du plan de contrôle de la solution et s'assurent de la cohérence des règles créées par le *NSX manager* et présentes sur l'infrastructure ;
- un module kernel déployé sur les ESXi afin de créer des pare-feux locaux à chaque interface virtuelle d'une machine virtuelle ;
- des *NSX edges* qui permettent de faire le lien entre l'infrastructure virtuelle et l'extérieur (ex. : autre infrastructure virtuelle, infrastructure physique). Ce composant n'est pas obligatoire et peut être remplacé par des pare-feux physiques pour un meilleur cloisonnement.

La micro-segmentation est un mécanisme de défense en profondeur, son utilisation apporte une ligne de défense supplémentaire contre les attaques informatiques, mais n'est pas suffisante à elle seule.

2.5 Vecteurs d'attaques

Les infrastructures de virtualisation sont fréquemment ciblées par des attaques par rançongiciel. Étant donnée la concentration de machines virtuelles, il s'agit en effet d'une cible de choix.

Parmi les sources et les causes de compromission, on retrouve :

- une attaque par compromission de l'environnement bureautique qui conduit à une latéralisation vers l'infrastructure de virtualisation ;
- une latéralisation par une compromission d'un sous-traitant ;
- l'exploitation d'une vulnérabilité de l'infrastructure de virtualisation ;
- l'usage de binaires compromis ;
- l'absence de maintien en condition de sécurité ;
- l'absence de sécurisation des infrastructures de virtualisation ;

- la mise en place d'un implant sur le stockage utilisé par l'infrastructure de virtualisation ;
- l'exposition sur Internet des hyperviseurs.

3
Recommandations

3.1 Recommandations générales

R1 Le socle de virtualisation doit être maintenu en appliquant au plus vite les mises à jour de sécurité.

R2 Il est recommandé de s'abonner aux bulletins de sécurité liés à toutes les briques logicielles et matérielles qui composent l'infrastructure de virtualisation.

3.2 Recommandations liées à l'architecture

R3 Pour une infrastructure vSphere, il est recommandé de séparer les flux en mettant :

- dans le plan de contrôle, les flux réseau des composants de management de l'infrastructure vSphere (vCenter d'administration, vCenter des *workload*, NSX Manager, NSX Controller, les interfaces d'administration des ESXi) ;
- dans le plan de donnée, les flux réseau des machines hébergées (services, stockage métier, etc.).

Attention

Attention, le port d'administration d'une machine virtuelle ne doit pas être mutualisé avec le plan de contrôle du socle.

R4 Le port d'administration d'une machine virtuelle doit être cloisonné du plan de contrôle du socle, au minimum par un VLAN dédié ;

R5 Les flux réseaux d'administration, de stockage, de sauvegarde doivent être cloisonnés entre eux en utilisant des VLAN dédiés et des adaptateurs VMkernel dédiés ;

R6 Les flux d'administration doivent utiliser un port réseau physique dédié à cet usage.

R7 Afin de sécuriser au mieux l'infrastructure de virtualisation, **il convient d'avoir un cluster dédié à l'administration** *(Management domain)*, séparé des clusters de production. Ce cluster héberge les composants du plan de contrôle, comme par exemple le ou les vCenter du ou des clusters de production *(workload domain)*, ainsi que le vCenter du cluster d'administration.

Information

Pour rationaliser les coûts, un cluster d'administration peut être utilisé pour créer un SI d'administration, comme indiqué dans le guide *Recommandations relatives à l'administration sécurisée des systèmes d'information* de l'ANSSI [4].

R8 Les clusters ou les serveurs de production (*workload domains*) doivent être dédiés par zone de sensibilité ou de confiance.

R9 Chaque zone de sensibilité ou de confiance doit être gérée par un vCenter dédié, hébergé dans la zone d'administration *(management domain)*.

R10 Au sein du cluster d'administration *(management domain)*, une segmentation par VLAN doit être mise en place pour isoler les différents plans de contrôle rattachés à chaque environnement de production *(workload domain)*.

R11 Si le SI d'administration est complexe, il est recommandé d'avoir au sein du SI d'administration un cluster ESXi qui sert de *management domain* et un *workload domain* qui contient les outils d'administration.

La figure 1 illustre un exemple d'architecture mettant en œuvre cette segmentation.

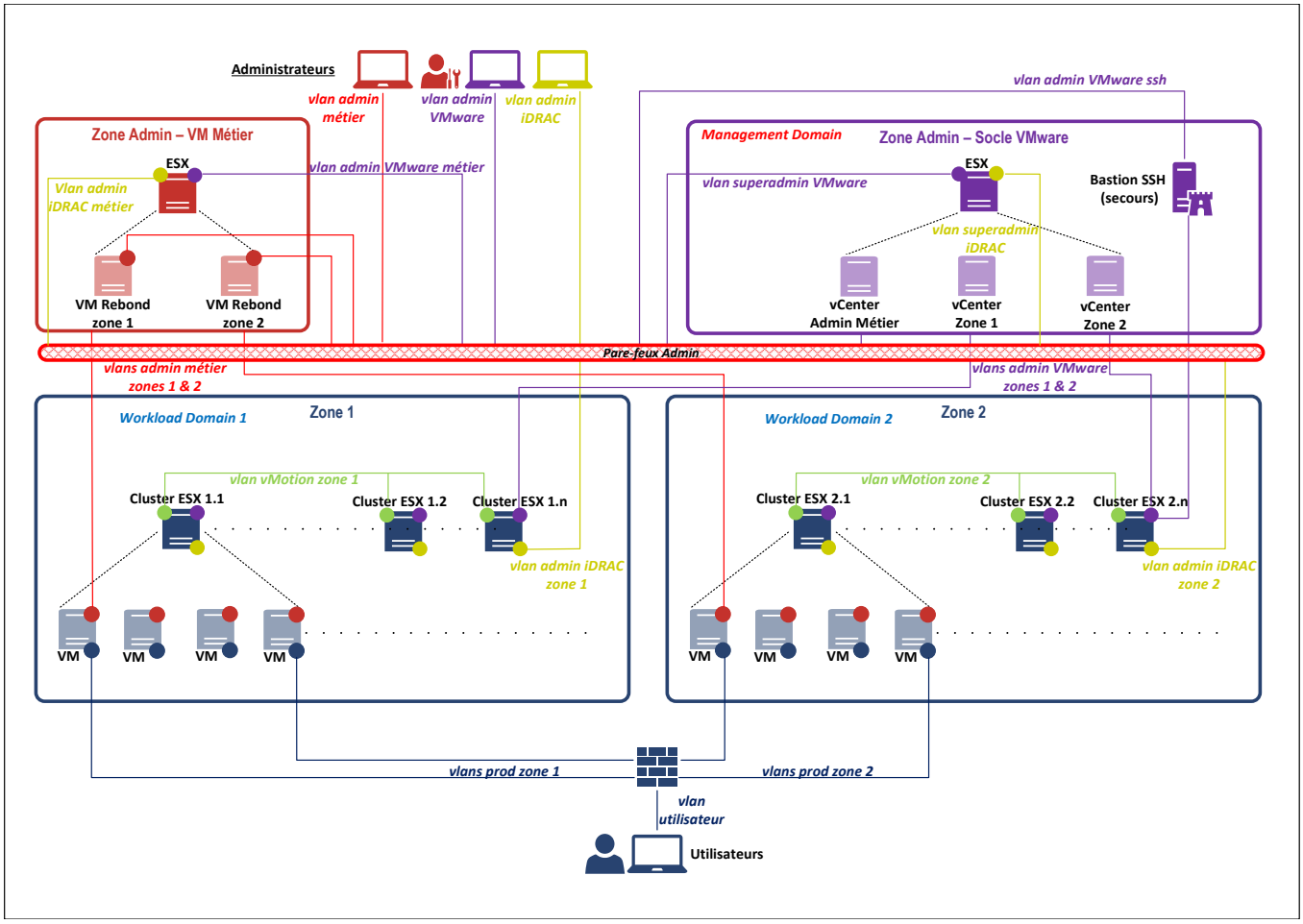

FIGURE 1 – Architecture d'administration VMware

Les grands principes suivants doivent être respectés :

R12 Les zones de confiance doivent être définies en fonction du niveau de sensibilité des ressources (valeurs métier).

R13 L'administration des hyperviseurs ESXi (en violet sur la figure 1) doit être cloisonnée vis-à-vis de l'administration métier des VM (en rouge sur la figure 1).

R14 L'administration de ces zones de confiance doit être cloisonnée en positionnant un système de gestion vCenter par zone pour l'administration du socle (en violet sur la figure 1) et un système de rebond pour l'administration des VM métier (en rouge sur la figure 1) ;

R15 L'administration des cartes de contrôle à distance (ex. : iDRac en jaune dans la figure 1) doit être cloisonnée vis-à-vis du reste de l'administration.

R16 Les flux de transfert vMotion (en vert de la figure 1) doivent être cloisonnés pour chacune des zones de confiance.

Les flux réseau autorisés pour l'administration d'une infrastructure VMware sont les flux bleus sur la figure 2.

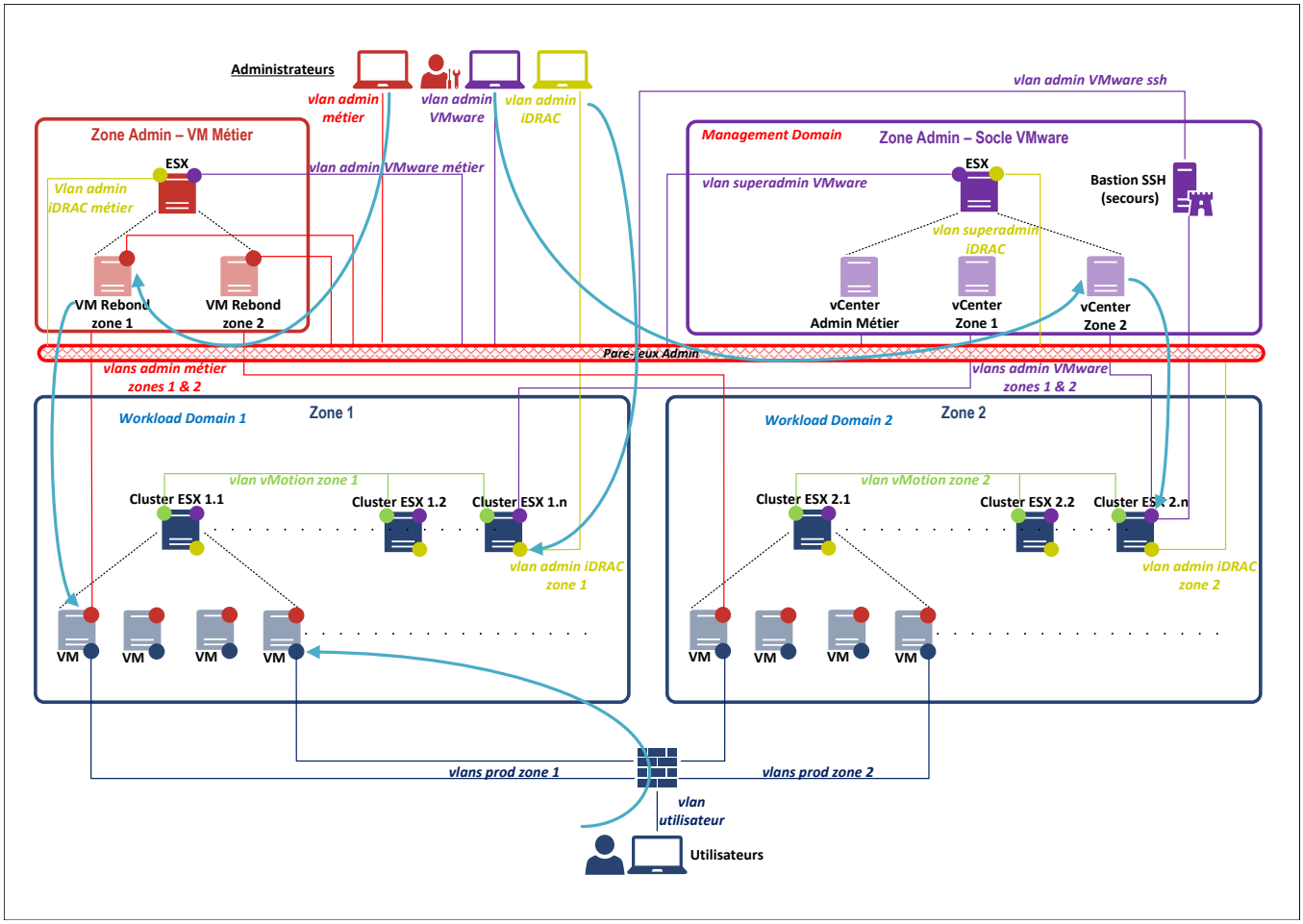

FIGURE 2 – Architecture d'administration VMware - Flux réseau

R17 Il est recommandé de créer les règles de filtrage correspondant aux flux [5] définis dans la figure 2.

5. Documentation éditeur sur les ports utilisés dans les produits VMware : `https://ports.esp.vmware.com/`

R18 Le socle de virtualisation VMware doit être considéré comme une infrastructure critique pour le SI. Ce socle de virtualisation doit bénéficier des mesures de protection adéquates et être intégré au SI d'administration de l'entité.

R19 L'ensemble du matériel en lien avec l'infrastructure VMware doit être administré de façon sécurisée comme décrit ci-dessus. Au-delà des serveurs, cela inclut les interfaces iLO / iDRAC, les baies de stockage, etc.

R20 Une interface réseau doit être dédiée à l'administration pour la gestion des ESXi (accès SSH et les flux de gestion vCenter). Cette interface doit être connectée à un réseau d'administration de l'entité. Elle ne doit surtout pas être accessible depuis un réseau de production.

R21 L'annuaire d'administration de l'infrastructure VMware doit être indépendant des annuaires utilisés en production (ex. : Active Directory). Les chemins de contrôle doivent être vérifiés régulièrement [1], de manière à ce qu'il n'y ait pas de possibilité d'élévation de privilège depuis l'infrastructure VMware vers les annuaires de production et inversement.

R22 Il est recommandé de dédier des clusters ESXi et des *datastores* par niveau de sensibilité des applications et/ou des données hébergées.

R23 Une vérification régulière des configurations des ESXi doit être mise en place en comparant la configuration lors du déploiement via l'utilisation de la fonction *hosts profile* ou par export de configuration via les API vSphere.

R24 Une segmentation réseau par PVLAN doit être mise en place sur les VM quand cela est possible.

R25 La synchronisation horaire des VM doit être configurée avec vigilance. Par exemple, pour des contrôleurs de domaine Active Directory, il est préférable de ne pas configurer comme source l'hyperviseur, afin d'éviter une désynchronisation horaire lors d'un redémarrage de machine virtuelle ou lors d'une prise de *snapshot* pouvant avoir un impact sur les réplications Active Directory [6].

R26 Une fonction proxy doit être dédiée au SI d'administration pour les récupérations de mises à jour sur Internet. Ce proxy doit réaliser un filtrage des URLs VMware par liste d'autorisations [7].

3.3 Actions d'administration

En fonction de la taille des équipes d'administration, deux modèles d'administration des infrastructures de virtualisation peuvent être mis en place :

- soit une équipe est dédiée à l'infrastructure de virtualisation ;
- soit l'équipe est mutualisée entre l'infrastructure de virtualisation et l'administration du système d'information.

R27 Il est recommandé de mettre en place une politique de gestion de droit (RBAC) des comptes d'administration cohérente avec le modèle de délégation de l'entité (taille de l'équipe).

6. Désactivation de la synchronisation via l'hôte d'une machine virtuelle : `https://kb.vmware.com/s/article/1189`
7. Liste d'autorisations des serveurs de mise à jour VMware : `https://kb.vmware.com/s/article/82205`

R28 Le principe du moindre privilège [8] doit être appliqué pour tous les comptes d'administration VMware [9] et les comptes de service (ex. : supervision).

R29 Il est recommandé de mettre en place une authentification multifacteur [5] [10] pour la connexion des administrateurs sur l'interface vSphere / vCenter.

R30 Un ou plusieurs comptes doivent être dédiés aux actions d'administration automatisées utilisant les API vSphere.

R31 Les connexions aux API doivent être supervisées pour permettre d'identifier les sources de connexions légitimes (ex. : serveurs d'orchestration).

R32 L'ensemble des composants doivent être intégrés dans le maintien en condition de sécurité (MCS) : ESXi , *vmware-tools*, vCenter, outils additionnels de l'éditeur VMware et des autres éditeurs tiers, etc.

R33 Les outils additionnels doivent être limités au strict besoin opérationnel. Ceux qui ne sont pas ou plus utilisés doivent être désinstallés.

3.4 Durcissement des ESXi

R34 Il est recommandé de désactiver les accès en SSH sur les ESXi, et d'activer la fonction *lockdown* [11] en « normal mode » avec un accès d'urgence configuré (compte « bris de glace »).

R35 Le *secure boot* doit systématiquement être activé, la signature des VIB pour les ESXi doit systématiquement être vérifiée [12].

R36 Les recommandations du guide *Recommandations de sécurité relatives à TLS* [3] de l'ANSSI doivent être appliquées pour configurer les accès HTTPS de vSphere (interface Web, API) [13] (p. ex. TLS version 1.2 minimum).

R37 Pour la fonction vMotion, TLS doit systématiquement être activé.

R38 Le *tagging* (VLAN) des VM ne doit pas être configuré au sein de la VM, mais au niveau de l'hyperviseur ESX.

R39 Le pare-feu local des ESXi doit être configuré.

R40 L'accès aux interfaces d'administration des machines virtuelles doit impérativement être séparé de l'accès aux interfaces d'administration du socle de virtualisation.

8. Documentation éditeur pour identifier l'ensemble minimal de privilèges : https://techdocs.broadcom.com/fr/fr/vmware-cis/vsphere/vsphere-supervisor/8-0/required-privileges-for-common-tasks.html
9. Documentation éditeur sur la gestion des utilisateurs et des autorisations de vSphere : https://techdocs.broadcom.com/fr/fr/vmware-cis/vsphere/vsphere/8-0/vsphere-authentication.html
10. Documentation éditeur sur l'authentification deux facteurs : https://techdocs.broadcom.com/fr/fr/vmware-cis/vsphere/vsphere/8-0/vsphere-authentication/vsphere-authentication-with-vcenter-single-sign-on-authentication/understanding-vcenter-server-two-factor-authentication-authentication.html
11. Documentation éditeur pour la mise en place du *lockdown* mode : https://techdocs.broadcom.com/fr/fr/vmware-cis/vsphere/vsphere/9-0/vsphere-security/securing-esxi-hosts/customizing-hosts-with-the-security-profile/lockdown-mode.html
12. Documentation éditeur sur le démarrage sécurisé d'ESXi : https://techdocs.broadcom.com/fr/fr/vmware-cis/vsphere/vsphere/9-0/vsphere-security/securing-esxi-hosts/uefi-secure-boot-for-esxi-hosts.html
13. Documentation éditeur sur la configuration de TLS : https://techdocs.broadcom.com/fr/fr/vmware-cis/vsphere/vsphere/8-0/vsphere-security/managing-tls-protocol-configuration-with-the-tls-reconfiguration-utility.html

3.5 Supervision de sécurité

R41 Les évènements de sécurité suivants, liés aux ESXi et aux vCenter, doivent être archivés et supervisés :

- accès aux hôtes ESXi (« auth.log »);
- modification de la configuration des ESXi (paramètre, service) et des VM;
- redémarrage des ESXi;
- connexions au vSphere / vCenter;
- trafic réseau des interfaces (les interfaces d'administration doivent avoir un trafic réseau faible par exemple, un trafic élevé pourrait indiquer une exfiltration de données);
- suspension de VM (*suspended state*, suspicion de dump mémoire);
- arrêt massif de VM (suspicion de chiffrement des vmdk);
- tout événement indiquant l'utilisation des comptes techniques internes à vSphere ou ESXi *vpx-user* et *dcui* (privilèges root);
- historique des commandes interactives « shell.log »;
- opérations de type *guest operations*;
- *upload* et *download* de fichiers sur les *datastores*.

3.6 Micro-segmentation

Dans le cas du recours à la micro-segmentation via la solution NSX, les recommandations suivantes s'appliquent :

R42 Le *NSX manager* et les *NSX controllers* doivent être déployés sur un cluster d'administration uniquement, jamais sur un cluster de production.

R43 La sécurité et l'efficacité de la micro-segmentation reposent sur la non-compromission des composants *NSX Manager* et *NSX Controller*. Il est donc recommandé de sécuriser leur accès, de limiter leurs usages et de mettre en place une politique de contrôle d'accès selon le principe de moindre privilège.

R44 Les règles de filtrage ne doivent pas reposer sur un critère qui peut être modifié ou altéré par la machine virtuelle (ex. : *hostname*, adresse MAC).

R45 Tous les flux qui ne sont pas explicitement autorisés doivent être bloqués.

R46 Il est recommandé d'utiliser des règles génériques en complément de règles plus spécifiques pour une gestion plus souple et maintenable dans le temps.

R47 Il convient de cloisonner correctement son infrastructure en isolant avec des pare-feux physiques les zones de sensibilités différentes.

R48 Dans des infrastructures dynamiques où les machines virtuelles peuvent être créées et supprimées très fréquemment, une bonne approche de la sécurité pourrait être :

- La mise en place des pare-feux physiques qui filtrent les échanges nord-sud (flux interzones de sécurité) de manière plus traditionnelle : IP source, destination, port source, destination.
- La mise en place de la micro-segmentation pour le trafic est-ouest (flux internes à une zone de sécurité) plus fin : IP source, destination, port source, destination, type de VM, tag, système d'exploitation, filtrage TLS, horaire, etc.

3.7 Sauvegarde

R49 Une sauvegarde de l'infrastructure de virtualisation doit être mise en œuvre. Elle doit contenir au moins : les binaires pour installer une infrastructure minimaliste (systèmes d'exploitation, logiciels et leurs correctifs, *firmware* du matériel), les procédures d'import des configurations, ou les scripts de configuration. Les procédures de restauration des machines virtuelles doivent être testées régulièrement.

R50 Une sauvegarde des environnements hébergés sur l'infrastructure de virtualisation doit être mise en place en suivant les recommandations contenues dans *Les Fondamentaux - Sauvegarde des systèmes d'information* [2].

4
Pour aller plus loin

En appliquant les recommandations de ce document, vous aurez les bonnes pratiques pour mettre en place une infrastructure de virtualisation sécurisée. En appliquant les différents guides écrits par l'ANSSI, en faisant une analyse de risques, vous pouvez aller plus loin dans la sécurisation de votre infrastructure de virtualisation utilisant les technologies VMware.

VMware dispose également d'un guide [14] de durcissement qui pourra vous permettre d'affiner votre projet de sécurisation.

14. Guide de durcissement VMware : https://www.vmware.com/security/hardening-guides.html

Bibliographie

[1] *Recommandations relatives à l'administration sécurisée des systèmes d'information reposant sur Microsoft Active Directory*.
Guide ANSSI-BP-099 v1.0, ANSSI, octobre 2023.
https://cyber.gouv.fr/guide-admin-si-ad.

[2] *Sauvegarde des systèmes d'information*.
Guide ANSSI-BP-100 v1.0, ANSSI, octobre 2023.
https://cyber.gouv.fr/publications/fondamentaux-sauvegarde-systemes-dinformation.

[3] *Recommandations de sécurité relatives à TLS*.
Guide ANSSI-PA-035 v1.2, ANSSI, mars 2020.
https://cyber.gouv.fr/guide-tls.

[4] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v3.0, ANSSI, mai 2021.
https://cyber.gouv.fr/guide-admin-si.

[5] *Authentification multifacteurs et mots de passe*.
Guide ANSSI-PG-078 v1.0, ANSSI, octobre 2021.
https://cyber.gouv.fr/guide-authentification.

Version 1.0 - 02/04/2024 - ANSSI-BP-103

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité