Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 25 mai 2016

N° DAT-NT-34/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 19

Note technique

Recommandations de sécurité pour les architectures basées sur VMware vSphere ESXi

Public visé :

Développeur	
Administrateur	✓
RSSI	✓
DSI	✓
Utilisateur	

Informations

Avertissement

Ce document rédigé par l'ANSSI présente les « **Recommandations de sécurité pour les architectures basées sur VMware vSphere ESXi** ». Il est téléchargeable sur le site www.ssi.gouv.fr. Il constitue une production originale de l'ANSSI. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab (www.etalab.gouv.fr). Il est par conséquent diffusable sans restriction.

Ces recommandations sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Personnes ayant contribué à la rédaction de ce document :

Contributeurs	Rédigé par	Approuvé par	Date
BSS	BAS	SDE	25 mai 2016

Évolutions du document :

Version	Date	Nature des modifications
1.0	25 mai 2016	Version initiale

Pour toute question :

Contact	Adresse	@mél
Division Assistance Technique de l'ANSSI	51 bd de La Tour-Maubourg 75700 Paris Cedex 07 SP	conseil.technique@ssi.gouv.fr

Table des matières

1 Introduction

Les technologies de virtualisation sont de plus en plus utilisées pour l'hébergement mutualisé de services dans les Datacenter.

VMware est un des principaux éditeurs de solutions de virtualisation et propose, à ce titre, une gamme de produits relativement étendue.

Seuls certains produits ont été étudiés et testés par l'ANSSI et sont décrits dans cette note technique :
- VMware vSphere ESXi 5.5 (ESX) ;
- VMware vCenter Server 5.5 ;
- VMware vSphere Client 5.5.

Il convient de préciser que ces produits n'ont fait l'objet d'aucune évaluation ou certification de sécurité par l'ANSSI. L'ANSSI n'est donc pas en mesure de formuler un avis sur le niveau d'assurance sécurité des solutions VMware.

Les recommandations de sécurité mentionnées dans ce document visent à diminuer autant que possible la surface d'attaque de telles solutions.

2 Les termes utilisés dans cette note

La *machine hôte* ou *l'hôte* héberge des *machines virtuelles (VM)*.

L'*hyperviseur* est le composant logiciel qui joue le rôle d'interface entre les machines virtuelles et l'hôte.

Un *cluster* est un regroupement d'hôtes ESX dont les ressources peuvent être gérées, optimisées et supervisées selon des règles spécifiques.

3 Description des produits

3.1 vSphere ESXi

ESXi (ESX) est la solution de virtualisation proprement dite.

C'est un système d'exploitation à part entière, basé sur un noyau de type POSIX [1], appelé VMkernel. Ce dernier assume le rôle d'hyperviseur. Il permet d'allouer les ressources matérielles de l'hôte aux différentes machines virtuelles (VM). Le partage de ressources obéit à des règles configurables relativement précises (temps CPU, mémoire vive, priorités réseau, entrées sorties disque, etc.).

Les machines virtuelles peuvent communiquer entre elles grâce à des switchs virtuels (vSwitchs) gérés par la solution. Les vSwitchs peuvent aussi être connectés aux interfaces physiques des serveurs et ainsi permettre la communication entre les machines virtuelles et le réseau local physique de manière transparente.

Très concrètement, ESX permet :
- de cloner une machine en quelques clics ;
- de créer des modèles de machines déployables ;

1. POSIX (Portable System Operating Interface) est un standard définissant les interfaces communes à tous les systèmes de type Unix.

– de sauvegarder un ou plusieurs états d'une machine virtuelle, pour ensuite pouvoir revenir à des états antérieurs (ce qui s'avère pratique lors des tests ou montées de version) ;
– etc.

En outre, la mise en « cluster » de plusieurs serveurs ESX rend par exemple possible :
– la migration d'une machine virtuelle d'un serveur à un autre sans interruption de service (fonctionnalité vMotion) ;
– la haute disponibilité et la réplication automatique des machines virtuelles ;

En fonction de la licence acquise, des fonctionnalités plus ou moins avancées sont disponibles : planification de tâches, switchs distribués DVS (switchs partagés entre plusieurs hôtes ESX), duplications et réplications automatiques, déploiement assisté d'hôtes ESX, etc.

3.2 vCenter Server

VCenter Server permet la gestion centralisée des hôtes ESX, et rend ainsi transparente l'administration de multiples serveurs en une seule interface consolidée.

Il permet entre autres :
– la gestion de rôles et de droits, pour définir des périmètres d'administration spécifiques à différents groupes d'administrateurs ;
– l'authentification unique (l'administrateur s'authentifie sur VCenter Server et se trouve connecté à l'ensemble des serveurs ESX) ; il est également possible de s'authentifier via un annuaire Active Directory ;
– la gestion de l'optimisation des ressources des serveurs (pour les ressources pouvant être gérées ou allouées dynamiquement) ;
– l'automatisation de tâches d'administration.

Une des spécificités de VMware est que l'administration des hôtes, des VM, mais aussi du stockage et une partie du réseau (vSwitch ou DVS) se fait à partir du serveur vCenter.

VCenter Server s'avère donc incontournable lorsqu'il est question d'administrer plusieurs hôtes ESX.

3.3 vSphere Client

Pour l'administration d'un hôte ESX, les seules manipulations graphiques pouvant être réalisées en local sont limitées à sa configuration IP ainsi qu'au changement du mot de passe root. Pour le reste, il est possible d'y ouvrir une session shell et de procéder à la maintenance du serveur par ligne de commandes.

Pour une administration par interface graphique, l'utilisation du client lourd vSphere Client est incontournable jusqu'à ESX 5.0. Ce client permet de se connecter au serveur vCenter ou directement à un hôte ESX à des fins d'administration. Il permet entre autres :
– de monter une clé USB locale sur une VM à travers le réseau ;
– de monter un CD/DVD local, ou une image ISO sur une VM à travers le réseau ;
– de modifier tous les paramètres de configuration d'ESX et des VM ;
– d'effectuer la prise en main de bureau à distance des VM (ce qui revient à voir l'écran virtuel d'une VM dans une fenêtre) ;
– d'accéder aux espaces de stockage des serveurs ESX (pour envoi/téléchargement de fichiers ou dossiers).

Depuis ESX 5.1, le client léger vSphere Web Client tend à se substituer à vSphere Client puisque les nouvelles fonctionnalités d'ESX ne sont pas accessibles depuis le client lourd. VSphere Web Client

s'impose alors comme le nouveau mode d'administration à utiliser. Il est toutefois à noter que ce dernier ne permet pas d'administrer directement un serveur ESX, et requiert donc de passer par un serveur VCenter Server.

4 Recommandations de sécurité

Dans une solution de virtualisation, l'hyperviseur contrôle l'accès aux ressources de l'hôte et est responsable du cloisonnement entre les machines virtuelles. Ce composant logiciel est donc critique du point de vue de la sécurité.

En exploitant une ou plusieurs vulnérabilités [2] de l'hyperviseur, un attaquant peut compromettre l'intégralité de la machine hôte, c'est-à-dire le système de l'hôte et les VM qu'il héberge.

Les recommandations qui suivent s'appuient sur des principes couramment utilisés en sécurité des systèmes d'information (cloisonnement, réduction de la surface d'attaque, etc.) ainsi que sur des paramétrages sécurisés de la solution.

4.1 Mutualisation des ressources

Les mécanismes de cloisonnement de l'hyperviseur sont les éléments critiques de toute solution de virtualisation. En l'absence d'évaluation de sécurité, tâche qui est difficile à mener sur ce genre d'hyperviseur, il convient de faire l'hypothèse qu'ils ne sont pas suffisamment robustes pour héberger sur un même hôte des machines virtuelles dont les niveaux de sensibilité sont différents.

Ainsi, par mesure de précaution, on mutualisera un équipement ou une machine pour n'y héberger que des environnements dont le niveau de sensibilité est similaire, c'est-à-dire des environnements pour lesquels l'éventuelle compromission de l'un a le même impact que si les autres étaient eux-même compromis.

Le niveau de sensibilité d'un environnement sera d'abord évalué au regard de **la criticité** du (ou des) service(s) qu'il héberge, cette dernière étant fonction de leurs besoins de sécurité [3].

En fonction du contexte, d'autres paramètres devraient également être pris en compte :
- **l'exposition** de la machine virtuelle (une VM accessible publiquement sur Internet est naturellement plus exposée qu'une VM seulement accessible sur un réseau filtré ou cloisonné) ;
- **la surface d'attaque** de la machine virtuelle qui dépend du nombre de services qu'elle héberge et des vulnérabilités potentielles ou avérées de ces services (on peut considérer qu'un système d'exploitation obsolète ou une application web mal développée ont une grande surface d'attaque).

R1

Pour les raisons évoquées précédemment, il ne faut en aucun cas mutualiser les ressources d'un même hôte entre des environnements de niveaux de sensibilité différents.

Cette recommandation de sécurité vaut également dans le cas où des interfaces réseau et des vSwitchs seraient affectés à des environnements de niveaux de sensibilité différents.

2. Comme tout logiciel, les hyperviseurs font l'objet de vulnérabilités, certaines pouvant être critiques (élévation de privilèges, exécution de code arbitraire, déni de service, etc.).

3. Les besoins de sécurité sont directement liés à la nature des impacts (opérationnels, financiers, juridiques, etc.) qui découlent d'une atteinte aux critères de sécurité habituellement considérés (disponibilité, intégrité, confidentialité).

R2

Pour les mêmes raisons, les fonctions de routage et de filtrage concernant des environnements de sensibilités différentes doivent être assurées par des équipements dédiés à l'usage de chacun des environnements.

4.2 Maintien en condition de sécurité

Les solutions de virtualisation sont des produits pour lesquels la sécurité est une composante importante. Le MCS (maintien en condition de sécurité) de telles architectures est donc primordial.

R3

Il est recommandé de s'abonner au service de notification des alertes de sécurité de l'éditeur (VMware Security Advisories).

R4

Il faut toujours maintenir les hôtes ESX et vCenter Server à jour de leurs correctifs de sécurité. Cette recommandation s'applique également à l'ensemble des briques logicielles de vSphere ainsi qu'aux systèmes d'exploitation qui les supportent, et aux systèmes d'exploitation des VM.

R5

Afin de disposer des pilotes spécifiques au matériel utilisé, il est préférable de récupérer les supports d'installation des hôtes ESX sur les sites des constructeurs. Il faut toujours vérifier l'authenticité des images (vérification des empreintes) avant de procéder à leur installation.

Certains constructeurs (comme DELL ou HP) proposent sur leurs sites des images d'installation de vSphere ESXi intégrant leurs pilotes respectifs, mais la mise à disposition de ces dernières n'est toutefois pas immédiate après la sortie de nouvelles versions par VMware.

R6

Seuls des modules [4] signés par VMware doivent être chargés dans le noyau (VMkernel).

R7

La mise à jour du socle logiciel d'un serveur VCenter devrait toujours être validée préalablement sur un environnement de test ou de pré-production.

4. Les modules permettent d'ajouter des fonctionnalités au noyau : pilotes de périphériques matériels, protocoles, etc.

La mise à jour d'un serveur VCenter peut s'avérer fastidieuse voire très problématique dans certains cas (mise à jour de la version 5.0 vers 5.5 par exemple). Il convient donc de ne pas considérer cette tâche comme une simple procédure du type « Point and click ». Parfois, l'installation d'un nouveau serveur VCenter sera préférable.

En revanche, la mise à jour des serveurs ESX ne présente pas de difficulté particulière.

4.2.1 VMware Update Manager

VMware met à disposition un composant spécialement conçu pour le déploiement des mises à jour : VMware Update Manager (VUM).

VUM est un outil dont le rôle est crucial. Par ailleurs, VUM a besoin de communiquer avec le serveur vCenter, qui est une autre brique logicielle sensible.

R8

Lors de l'installation de VUM, des privilèges élevés sont requis pour configurer la base de données des utilisateurs de ce dernier. Certains de ces privilèges ne sont plus nécessaires une fois l'installation terminée : ils doivent par conséquent être révoqués.

Les privilèges nécessaires et suffisants sont précisés dans le guide de durcissement [5], en fonction du système de gestion de base de données utilisé (Oracle, SQL server, etc).

R9

VUM ne doit pas être exposé sur Internet. Pour récupérer les mises à jour, il convient d'utiliser le service UMDS (Update Manager Download Services). Ces dernières pourront ensuite être copiées vers un serveur web local ou sur un disque amovible (clé USB, CD-ROM) afin que VUM puisse les récupérer.

R10

La machine hébergeant le service UMDS, qui effectue le téléchargement des mises à jour sur Internet, doit être protégée par un pare-feu dit « stateful ». Ce dernier doit être configuré pour n'autoriser que les flux depuis cette machine vers les adresses IP des services de mises à jour officiels sur les ports associés.

5. Les guides de durcissement de vSphere peuvent être téléchargés à l'adresse suivante : http://www/VMware.com/fr/security/hardening-guides.

R11

Le serveur sur lequel est installé VUM doit être tenu à jour de ses correctifs de sécurité. Il doit être durci le plus possible (désactiver les services inutiles, configurer des restrictions logicielles, restrictions et filtrage sur les supports USB, etc.).

R12

Compte-tenu du rôle crucial de VUM, les accès à celui-ci doivent être réservés aux administrateurs les plus privilégiés, dits « de confiance ». Il est également recommandé d'auditer régulièrement les accès au VUM.

Bien qu'il soit possible d'installer VUM et vCenter dans des machines virtuelles, cette pratique est déconseillée pour les raisons suivantes :

- si vCenter et VUM sont virtualisés sur un même hôte ESX, la mise à jour par VUM de ses propres VM peut avoir des effets inattendus ;
- compte-tenu du rôle crucial de VUM et vCenter dans la sécurité de l'infrastructure vSphere, il n'est pas souhaitable qu'ils reposent sur cette même infrastructure.

R13

Au même titre que vCenter, VUM ne doit pas être hébergé dans une machine virtuelle, mais sur un serveur physique.

4.3 Désactivation de composants non utilisés

R14

Les services non utilisés des hôtes ESX doivent être arrêtés et configurés pour ne pas se lancer automatiquement lors du démarrage des hôtes.

Dans la liste des services décrits ci-dessous, certains peuvent être désactivés :

- snmpd : gère la partie SNMP ; si la supervision n'est pas mise en œuvre, la désactivation peut se faire par la commande `esxcli system snmp set -enable false` ;
- lbtd : gère le Load Balancing ; il peut être désactivé si le Load Balancing n'est pas utilisé ;
- vpxa : gère les agents d'administration et permet la communication entre les serveurs ESX et VCenter Server ; ce service est indispensable ;
- Serveur CIM : permet de superviser l'état de santé des hôtes physiques (capteurs matériels) ; ce service est indispensable ;
- vprobed : permet la supervision des hôtes et les VM ; ce service est indispensable.

Les machines virtuelles VMware sont conçues pour fonctionner sur d'autres plate-formes de virtualisation comme Fusion [6] ou Workstation [7]. Lorsque les machines virtuelles sont utilisées avec

6. Solution de VMware permettant d'exécuter plusieurs systèmes d'exploitation sur les ordinateurs MAC OS X avec processeurs Intel.

7. Solution de VMware permettant d'exécuter plusieurs systèmes d'exploitation x86 sur un même PC.

VSphere (cas présent), un certain nombre paramètres peuvent être désactivés.

R15

La surface d'attaque d'ESX peut être réduite en désactivant les paramètres de compatibilité des machines virtuelles. Pour ce faire, les paramètres suivants devraient être positionnés à la valeur VRAI :
- disable-unexposed-features-autologon
- disable-unexposed-features-biosbbs
- disable-unexposed-features-getcreds
- disable-unexposed-features-launchmenu
- disable-unexposed-features-memsfss
- disable-unexposed-features-protocolhandler
- disable-unexposed-features-shellaction
- disable-unexposed-features-toporequest
- disable-unexposed-features-trashfolderstate
- disable-unexposed-features-trayicon
- disable-unexposed-features-unity
- disable-unexposed-features-unity-interlock
- disable-unexposed-features-unity-taskbar
- disable-unexposed-features-unity-unityactive
- disable-unexposed-features-unity-windowcontents
- disable-unexposed-features-unitypush
- disable-unexposed-features-versionget
- disable-unexposed-features-versionset

4.4 Sécurité de l'administration

L'accès à l'interface d'administration d'ESX par une personne malveillante engendre d'importants risques de sécurité puisqu'il est alors possible d'exploiter des vulnérabilités du service d'administration et ainsi d'avoir un contrôle total de la plate-forme de virtualisation.

Par défaut, le service d'administration d'ESX écoute sur l'interface réseau principale d'un ESX.

R16

Sur chaque ESX, une interface réseau doit être dédiée à son administration (VSwitch dédié et interface physique dédiée), pour bien séparer administration et accès réseau des machines virtuelles.

L'administration ne sera donc possible que depuis un réseau physiquement dédié, a minima depuis des adresses IP ou des VLAN spécifiques.

R17

Afin de bloquer d'éventuelles tentatives de connexions illégitimes en provenance des hôtes ESX et à destination du serveur vCenter ou des postes d'administration, le serveur vCenterServer et les postes d'administration doivent être isolés dans deux zones distinctes et sécurisées (de type DMZ).

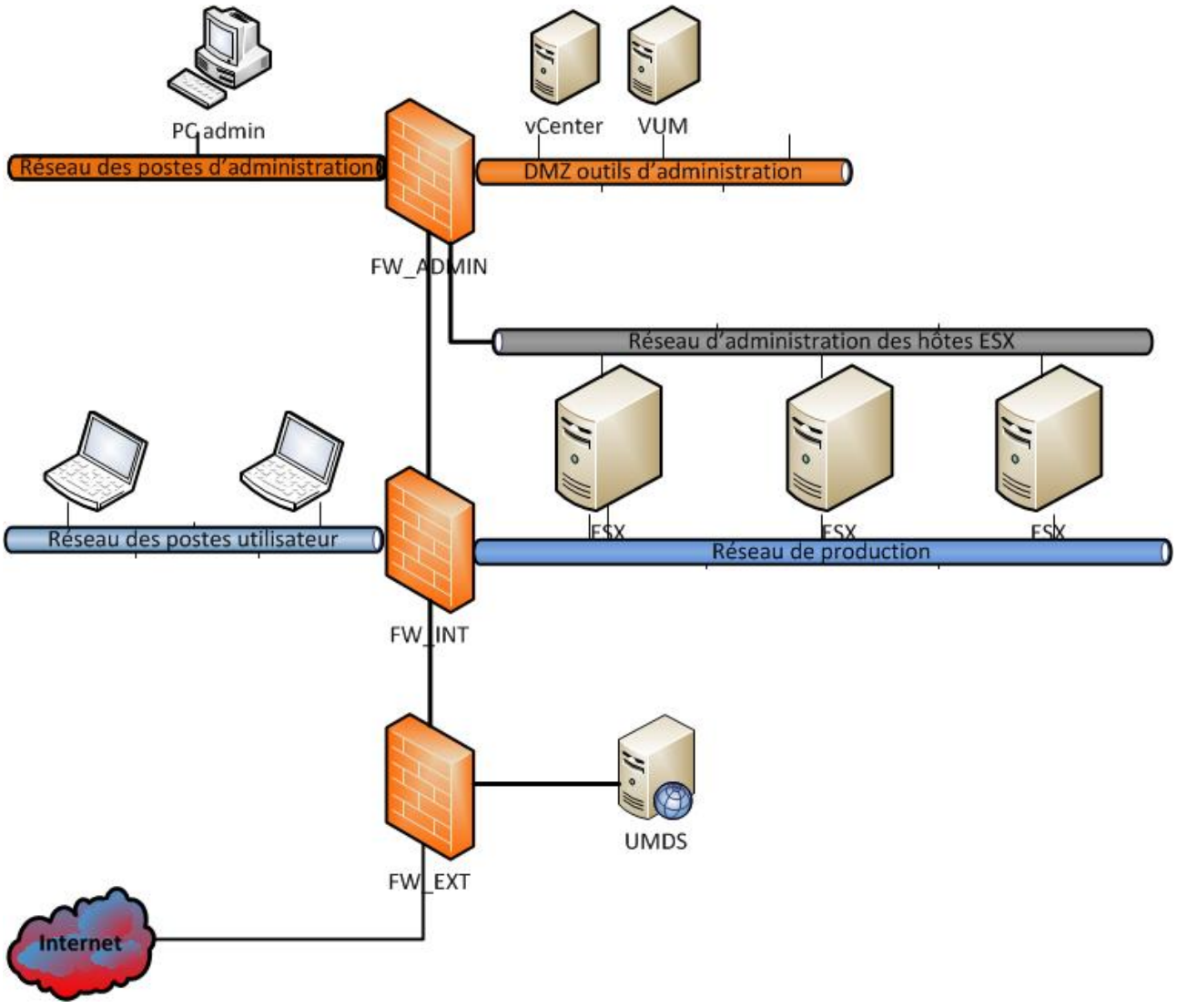

FIGURE 1 – Architecture recommandée pour l'administration de vSphere

Comme cela a été évoqué précédemment, une des spécificités de VMware est que l'administration des hôtes et des VM, mais aussi du stockage et une partie du réseau (vSwitch ou DVS) se fait à partir du serveur vCenter.

En vertu du principe de « séparation des rôles » et du principe de « moindre privilège », il est essentiel de bien définir les rôles et privilèges associés aux différents périmètres de responsabilité des administrateurs. À titre d'exemple, il n'est pas concevable que l'administrateur d'une machine virtuelle dispose également des privilèges d'administration de l'hôte qui les héberge. Le cas échéant, si cette machine virtuelle venait à être compromise, les autres machines virtuelles de l'hôte le seraient également. Pour les mêmes raisons, il convient également de créer des rôles spécifiques à la gestion du

stockage et la gestion du réseau.

Puisque l'ensemble des tâches d'administration sont réalisées à partir du même outil, la différenciation des accès devra obligatoirement être faite sur l'interface d'accès de l'unique vCenter.

R18

Les droits octroyés aux comptes des administrateurs doivent suivre le principe de séparation des privilèges. Les privilèges accordés aux administrateurs se feront en fonction du juste besoin opérationnel.

Le serveur vCenter est une brique logicielle critique qui requiert des privilèges d'administration locaux pour s'exécuter. Néanmoins, ce dernier n'a pas besoin de privilèges aussi élevés que le compte « system » de Microsoft Windows pour s'exécuter.

R19

Pour exécuter vServer, il est préférable d'utiliser un compte utilisateur du domaine, ou compte de service, avec les privilèges nécessaires et suffisants.

4.5 Sécurisation des accès

Les accès réalisés à travers la DCUI (*Direct Console User Interface*, console accessible physiquement sur les hôtes), ou bien par l'ESXi Shell via SSH, ou même encore à travers le MOB (*Managed Object Browser*) contournent tous les mécanismes de contrôle d'accès (rôles et droits d'accès) ainsi que les mécanismes d'audit et de journalisation d'ESX.

R20

En temps normal, les accès à travers la DCUI, l'ESXi Shell et la MOB doivent être désactivés. Pour la résolution de problèmes graves, seul un nombre limité d'administrateurs de confiance doivent pouvoir les réactiver temporairement.

R21

La désactivation du service SSH est également recommandée. L'administration d'ESX ne devrait se faire que depuis le client VSphere, les outils en ligne de commande (vCLI, PowerCLI) ou les APIs éventuellement publiés.

Le mode « lockdown » peut également être envisagé pour désactiver tout accès direct à l'hôte. Si SSH reste malgré tout utilisé, il est préférable d'utiliser la connexion par clés (`/etc/ssh/keys-root/authorized_keys`) et de réduire le timeout de session (`ESXiShellInteractiveTimeOut`).

R22

Le compte root des hôtes ESX ne doit pas être partagé. Il ne devrait pas non plus être utilisé, sauf en cas de nécessité absolue. Il faut lui définir un mot de passe robuste et différent par hôte, puis n'utiliser que des comptes nominatifs d'administration.

R23

Il est préconisé de définir un délai d'expiration (session timeout) pour les sessions demeurées inactives.

Durant l'installation de vSphere, des certificats auto-signés sont automatiquement générés pour permettre les accès sécurisés par les procédés SSL/TLS (Hôtes ESX, vCenter, SSO, Update Manager, etc.).

Ces certificats n'étant pas signés par une autorité de certification dite « de confiance », un avertissement de sécurité sera systématiquement affiché lors de la connexion. Afin d'éviter l'affichage de ce message d'avertissement à chaque connexion, la plupart des utilisateurs cocheront très probalement l'option permettant d'ignorer les vérifications à venir. Que l'utilisateur choisisse ou non de désactiver ces avertissements, le fait d'utiliser des certificats auto-signés enlève toute possibilité de détection des attaques de type MITM (Man In The Middle).

R24

Il est fortement recommandé de remplacer tous les certificats auto-signés par des certificats issus d'une autorité de certification de confiance, et ce, dès la fin de l'installation des composants de vSphere.

R25

Les administrateurs doivent recevoir la consigne de ne pas cocher la case permettant d'ignorer les avertissements de sécurité. Un administrateur devrait également être sensibilisé au fait qu'un tel avertissement constitue un incident de sécurité devant être rapporté au responsable de la sécurité de l'exploitation.

R26

Lors de son installation, le service de SSO (Single Sign On) de vSphere requiert des privilèges élevés pour configurer la base de données des utilisateurs. Dès lors que l'installation est terminée, certains de ces privilèges ne sont plus nécessaires : ils doivent par conséquent être révoqués.

Les privilèges nécessaires et suffisants sont précisés dans le guide de durcissement de vSphere [8], en fonction du système de gestion de base de données utilisé (Oracle, SQL server, etc).

R27

Le mot de passe utilisé par le SSO pour interagir avec la base de données doit être noté et conservé dans un endroit sûr.

Il est possible d'intégrer les hôtes ESX à un domaine Active Directory (AD). L'authentification se fait dès lors au moyen des comptes membres du groupe « ESX Admins », qui disposent des privilèges d'administrateur sur tous les hôtes ESX du domaine.

Cette approche permet d'éviter la création et la gestion de comptes utilisateur propres à ESX et permet de bénéficier d'une stratégie de groupe [9] applicable à ces comptes (fréquence de renouvellement et complexité du mot de passe, verrouillage, etc).

Le rattachement des hôtes ESX à un AD facilite donc la gestion des comptes ESX. Néanmoins, en cas de compromission d'un compte utilisateur membre du groupe « ESX Admins », l'attaquant est en mesure de prendre le contrôle de tous les hôtes ESX.

R28

Le choix de rattacher les hôtes ESX à un domaine Active Directory ne devrait être fait qu'aux conditions suivantes :
- utiliser le vSphere Authentication Proxy (afin d'éviter que les authentifiants ne soient stockés dans le profil de l'hôte et transmis sur le réseau) ;
- au sein de l'environnement Active Directory, s'assurer que les bonnes pratiques sont mises en œuvre [10] ;
- disposer d'un réseau d'administration dédié à l'administration du système d'information de l'entité et de postes exclusivement dédiés à cette fonction ;
- respecter les bonnes pratiques en matière d'administration des systèmes windows ;
- s'assurer que seul un nombre limité d'utilisateurs (administrateurs de confiance) sont membres du groupe « ESX Admins ».

4.6 Sécurité du réseau

R29

Configurer le pare-feu local des hôtes ESX pour restreindre l'accès aux services (ssh, vsphere web, http, etc.) depuis les adresses IP autorisées.

R30

Les composants critiques comme vCenter et VMware Update Manager (VUM) doivent être placés dans une DMZ dont le pare-feu devrait n'autoriser que les connexions depuis les machines utilisées pour réaliser les tâches d'administration.

8. Les guides de durcissement de vSphere peuvent être téléchargés à l'adresse suivante : http://www/vmware.com/fr/security/hardening-guides.
9. Au sens Active Directory : une fonction de gestion centralisée.
10. Se référer à la note intitulée « Recommandations de sécurité relatives à Active Directory » publiée sur le site de l'ANSSI.

Afin d'éviter les erreurs de configuration, et donc des problèmes potentiels de sécurité, il est indispensable de définir des principes de gestion et de configuration du réseau.

R31

Toutes les briques réseau virtuelles (vSwitch, D-vSwitchs, Portgroups, VLANs, Private VLAN, etc.) doivent être nommées et documentées de façon claire de sorte qu'il n'y ait aucune ambiguïté.

À titre d'exemple, un de ces principes pourrait être de toujours dédier un équipement physique ou virtuel à une fonction particulière (un vSwitch pour l'administration, un vswitch pour la production, etc.)

On portera ainsi une attention particulière :
- aux liens de type trunk entre les switchs virtuels et switchs physiques, pour éviter de faire passer des VLAN correspondant à des fonctions différentes dans un même trunk ;
- à la fonctionnalité de « port mirroring » des switchs distribués, pour éviter que le trafic soit dupliqué sur un port correspondant à un VLAN d'une fonction différente ;
- à la fonctionnalité de « Netflow » des switchs distribués, pour éviter que le trafic soit dirigé vers des adresses IP correspondant à des fonctions différentes.

Les copies ou migration de VM entres les hôtes ESX sont effectuées à travers le réseau par le service NFC (*Network File Copy*). Par défaut, ce dernier utilise SSL pour la phase d'authentification, mais pas pour le transfert des données.

R32

Il est recommandé d'activer SSL pour les transferts de données NFC.

L'activation se fait avec le paramètre avancé `config.nfc.useSSL`.

4.7 Sécurité des machines virtuelles

Les machines virtuelles et les services qu'elles hébergent doivent faire l'objet des mêmes mesures de durcissement que celles préconisées sur un serveur physique.

R33

À ce titre, il convient :
- de minimiser la surface d'attaque des machines virtuelles (installation des composants strictement nécessaires, désactivation des services inutiles, etc.) ;
- d'appliquer, tant que possible, les règles de durcissement du système d'exploitation de la machine virtuelle ;
- d'appliquer les correctifs de sécurité concernant les systèmes d'exploitation et les composants tiers.

R34

L'instanciation des machines virtuelles devrait toujours être réalisée à partir de modèles (« template ») préconfigurés et durcis en fonction du type de services hébergés. Cette approche permet d'industrialiser le processus de déploiement d'environnements pré-durcis sans occasionner une charge supplémentaire.

Dans la mesure où les machines virtuelles se partagent les ressources matérielles de l'hôte, une attaque par déni de service visant une machine virtuelle peut entraîner l'indisponibilité de toutes les machines virtuelles hébergées sur l'hôte.

R35

Afin de limiter les impacts des attaques par déni de service, il est recommandé de limiter les ressources physiques (mémoire, CPU) allouées à une machine virtuelle en fonction de ses besoins.

L'utilisation de composants additionnels - VMware tools - au sein des machines virtuelles fournit des fonctionnalités supplémentaires et améliore les performances, mais présente également des risques non négligeables pour la sécurité de l'hôte. En effet, l'exploitation de vulnérabilités affectant des composants additionnels a déjà permis par le passé de réaliser des exploits de type « VM Escape ».

R36

Il est recommandé de n'installer que les composants additionnels strictement nécessaires. En outre, le paramètre disable-autoinstall empêche l'installation automatique de composants et permet d'éviter le redémarrage automatique des machines virtuelles. Vérifier que ce dernier est activé.

4.8 Stockage NAS/SAN

Si un stockage en réseau sur SAN (Storage Area Network) ou NAS (Network Attached Storage) est utilisé, et partagé entre plusieurs serveurs ou clusters, il est primordial de configurer le zonage et le masquage des LUN de manière adéquate.

R37

Il ne faut en aucun cas mutualiser une zone de stockage pour des hôtes ayant des besoins de sécurité hétérogènes (par exemple un serveur de développement et un serveur de production).

R38

Le réseau SAN / NAS devrait être physiquement dédié (switchs compris) pour éviter tout risque d'accès frauduleux au réseau.

R39

Il est recommandé d'activer le protocole CHAP avec authentification mutuelle de l'hôte et de la cible iSCSI.

R40

Lorsqu'une VM traite des données sensibles, il est recommandé d'écrire des zéro sur ses disques virtuels (VMDK) avant leur suppression ou leur réutilisation par une autre VM. Toutefois, ce procédé n'est pas suffisant pour les données classifiées de défense ou portant la mention Diffusion Restreinte. Dans ce cas, il est impératif de recourir à un procédé ayant fait l'objet d'un agrément au niveau de confidentialité adéquat.

L'écriture de zeros sur les disques virtuels peut être réalisée avec la commande `vmkfstools -writezeroes`.

4.9 Audit et journalisation

Par défaut `/scratch` est un lien vers le répertoire temporaire `/tmp/scratch` et les journaux sont donc perdus au redémarrage de l'hôte. Il convient donc de changer a minima le paramètre `Syslog.global.LogDir` pour chaque hôte dans les paramètres systèmes avancés.

R41

Afin de ne pas perdre les journaux d'évènements au redémarrage des hôtes ESXi, il est nécessaire de configurer un stockage persistant de ces derniers.

R42

Afin de faciliter l'analyse des journaux, il convient de mettre en œuvre une synchronisation de l'heure de tous les serveurs hébergeant les briques logicielles de la suite vSphere.

La configuration relative à l'utilisation du protocole Network Time Protocol (NTP) se trouve dans le fichier `/etc/ntp.conf`.

R43

Afin de préserver l'intégrité des journaux en toutes circonstances, il est recommandé de centraliser les journaux des hôtes ESX.

La centralisation des journaux peut se faire via un serveur Syslog qui sera alors spécifié par le paramètre `Syslog.global.logHost` (cela se fait graphiquement dans les options logicielles avancées

des hôtes. Le paramètre logHost à préférer est « ssl ://ip :1514 »).

Le service VMware Syslog Collector peut être utilisé comme serveur Syslog. Il se configure via le fichier `vmconfig-syslog.xml` présent dans son dossier d'installation et dans lequel il est possible de spécifier : chemin des journaux, adresse et port du serveur web, ainsi que les ports syslog TCP, UDP et SSL.

4.10 Supervision

R44

Si le protocole SNMP n'est pas utilisé, il est préférable de le désactiver. Dans le cas contraire, il faut proscrire SNMP v1 et v2, et choisir SNMP v3 avec authentification et chiffrement.

La configuration de SNMP se trouve dans `/etc/vmware/snmp.xml`.

R45

Il est recommandé de configurer des profils d'hôtes (configurations de référence) pour superviser et détecter toute déviation de configuration d'un hôte par rapport à sa référence (*Host Profile*).

R46

La supervision matérielle par le biais de l'interface CIM (*Common Information Model*) doit utiliser un compte utilisateur spécifique limité au privilège *CIM interaction*. Dans le cas contraire, cette fonctionnalité pourrait devenir une porte dérobée sur les hôtes ESX.