jmy37
GitHub : https://github.com/jmy37/infrathome

DESCRIPTIF	
Description du projet Infr@home	
Infr@home_DESC_01-Descriptif-projet	
Version 1.3	**Date d'application : 17/12/2020**
Projet/SI : Infr@home	

1. HISTORIQUE DES MODIFICATIONS

Version	Date	Auteur	Objet de la modification
1.0	30/11/2020	jmy37	Création du document
1.1	03/12/2020	jmy37	Ajout du serveur VLSUPDACS01 au titre 4.4.2
1.2	10/12/2020	jmy37	Ajout du serveur VLSLOGACS02 au titre 4.4.2 Ajout du serveur VLSMONACS01 au titre 4.4.2 Ajout de la configuration syslog pour Linux au titre 5.2.3.7 Ajout de la désactivation des dépôts d'origine (titre 5.2.3.8) Ajout de la configuration NTP (titre 5.2.3.9)
1.3	17/12/2020	jmy37	Ajout du guide de configuration de la supervision au titre 4.3 Ajout de la configuration de Zabbix au titre 5.2.3.10

Tableau 1 : Historique des modifications

2. RÉFÉRENCES

2.1. Table des matières

2.2. Liste des tableaux

2.3. Liste des figures

3. PRÉAMBULE

Ce document précise les objectifs, l'architecture globale, les règles communes et l'ordre d'application des procédures du projet « Infr@home ».

4. PRÉSENTATION

4.1. Le projet Infr@home

L'objectif d'Infr@home est de proposer une architecture simple, résiliente et abordable de système d'information permettant de suivre les standards en termes d'organisation et de cybersécurité. Le projet est totalement virtualisé en environnement VMware, mais peut facilement être converti sur d'autres hyperviseurs, voire en environnement physique.

4.2. Conventions

4.2.1. Conventions d'écriture

Différentes conventions d'écriture sont appliquées sur l'ensemble des documents :

```
Cette convention représente une commande à saisir.
```

Cette convention représente un élément important.

Cette convention représente une information.

4.2.2. Conventions techniques

4.2.2.1. Convention de réseaux

La séparation des réseaux est effective telle que présentée sur le Tableau 2.

Numéro VLAN	Nom du VLAN	Adresse réseau	Usage
10	DMZ	192.168.1.0 /24	DMZ (serveurs de dépôt et frontend)
20	CORESVC	172.16.20.0 /24	Serveurs et équipements réseaux
100	CLIENTS	172.16.100.0 /24	Postes clients
110	ADMIN	172.16.110.0 /24	Postes d'administration
254	FIREWALL_HA	172.16.254.0 /30	Haute disponibilité entre les pares-feux

Tableau 2 : Affectation des VLANs

La dernière adresse IP de chaque VLAN est réservée à l'adresse virtuelle de passerelle. L'avant-dernière adresse IP de chaque VLAN est réservée à l'adresse du deuxième pare-feu. L'antépénultième adresse IP de chaque VLAN est réservée à l'adresse du premier pare-feu. La première adresse IP de chaque VLAN ne sera pas utilisée. Le réseau DMZ est spécifique et sera présenté de manière plus détaillée au titre 4.4.1.

4.2.2.2. Nomenclature des équipements et adresses IP

La nomenclature des équipements se réalise de la manière suivante :

<TYPE><OS><ENV><USAGE><SITE><SI>[01-99]
avec [01-99] un numéro incrémental allant de « 01 » à « 99 ».

La nomenclature des adresses IP virtuelles se réalise de la manière suivante :

<TYPE><OS><ENV><USAGE><SITE><SI><n1><n2>
avec <n1> et <n2> les numéros incrémentaux des hôtes cibles.

La nomenclature complète est présentée dans le Tableau 3.

TYPE	OS	ENV	USAGE	SITE	SI
P (physique)	L (Linux)	P (Production)	AVS (antivirus)	A (site A)	CS (Core services)
V (virtuel)	N (sans OS)	S (Staging)	DBS (bases de données)	B (site B)	
	V (VMware)	L (Lab)	DEP (dépôt)		
	W (Windows)		FWL (firewall)		
			IEM (SIEM)		
			ITM (ITSM)		
			LOG (journaux)		
			MON (supervision)		
			SAV (sauvegarde)		
			UPD (mises à jour)		
			VAS (scanner de vulnérabilités)		

Tableau 3 : Nomenclature des équipements

4.3. Présentation des fonctionnalités attendues

L'architecture présentée est en mesure de réaliser de nombreuses fonctionnalités. Le Tableau 4 présente l'association entre les guides d'installation et les fonctionnalités attendues.

Fonctionnalité	Guide d'installation
Filtrage de flux	Infr@home_GUI-INST_01-Firewall
Dépôts externes	Infr@home_GUI-INST_02-DMZ-repository
Gestion des systèmes d'information (ITSM)	Infr@home_GUI-INST_04-ITSM
Gestion des journaux d'évènements	Infr@home_GUI-INST_05-Syslog
Mises à jour des différents systèmes (Windows/Linux)	Infr@home_GUI-INST_06-Linux-updates-and-configurations
Supervision	Infr@home_GUI-INST_07-Monitoring
Console antivirale	
Scanner de vulnérabilités	
Authentification des clients par le protocole 802.1x	
Gestion des certificats machines	

Tableau 4 : Association des fonctionnalités et des guides d'installation

L'application partielle implique un potentiel non-fonctionnement. Les guides doivent être suivis dans l'ordre. Les points présentés en annexes ne sont pas nécessairement réalisables immédiatement, et peuvent demander l'application de guides à suivre.

4.4. Présentation des VLANs

4.4.1. DMZ (VLAN 10)

Le VLAN 10 est l'interface entre le réseau sécurisé (postes clients, postes d'administration, serveurs) et Internet. Son adressage IP est spécifique compte tenu des impératifs imposés par l'opérateur. Il est représenté par la Figure 1.

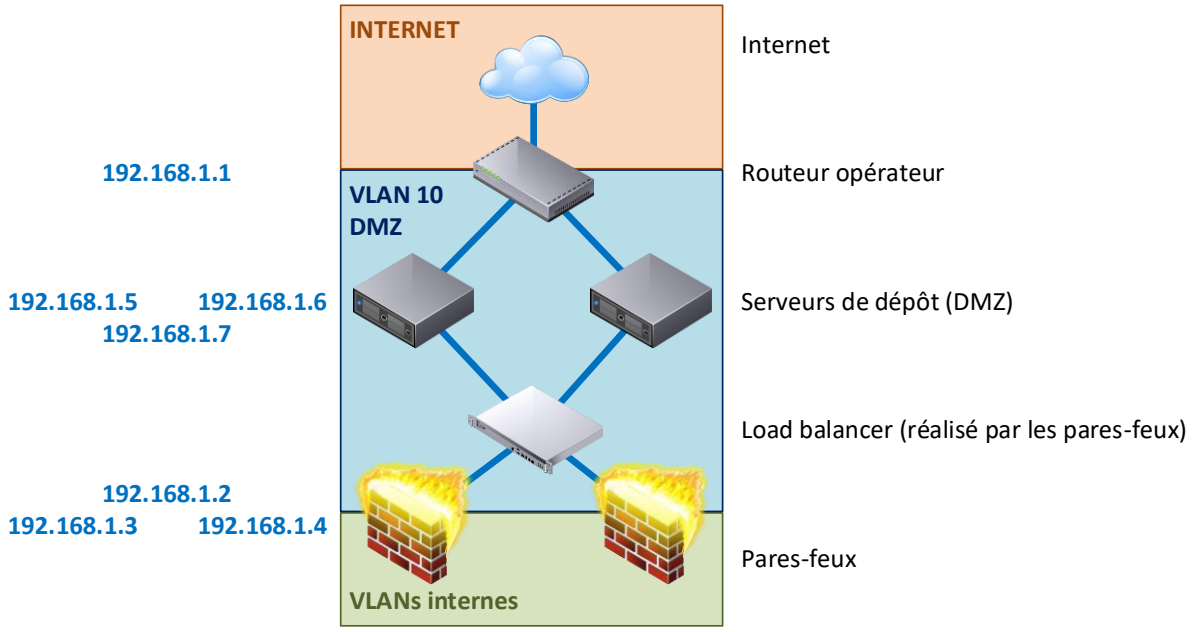

Figure 1 : Présentation du VLAN "DMZ"

Le routeur opérateur effectue également un rôle de pare-feu et est en mesure de rediriger tout le trafic interne (172.16.0.0 /16) vers les pares-feux. Les seuls serveurs qui se trouvent sur ce VLAN sont les serveurs de dépôt, qui récupèrent les mises à jour des différents composants sur Internet et les mettent à disposition.

Le Tableau 5 présente l'adressage IP de ce VLAN.

Adresse IP	Nom DNS	Fonctionnalité
192.168.1.1 /24	gateway	Routeur opérateur
192.168.1.2 /24	vlsfwlacs0102	Passerelle - pare-feu (VIP)
192.168.1.3 /24	vlsfwlacs01	Passerelle - pare-feu
192.168.1.4 /24	vlsfwlacs02	Passerelle - pare-feu
192.168.1.5 /24	vlsdepacs01	Serveur de dépôt
192.168.1.6 /24	vlsdepacs02	Serveur de dépôt
192.168.1.7 /24	vlsdepacs0102	Serveur de dépôt (VIP)

Tableau 5 : Affectation des adresses IP du VLAN "DMZ"

4.4.2. CORESVC (VLAN 20)

Le VLAN 20 est celui qui héberge tous les serveurs et les services réseaux. Aucun poste de travail n'y est admis. Dans le principe de défense en profondeur, les pares-feux locaux sont tous configurés de manière à limiter les risques d'attaques. Le Tableau 6 présente l'adressage IP de ce VLAN.

Adresse IP	Nom DNS	Fonctionnalité
172.16.20.3 /24	vlsitmacs01	ITSM
172.16.20.6 /24	vlslogacs01	Gestion des logs
172.16.20.7 /24	vlslogacs02	Gestion des logs
172.16.20.9 /24	vlsupdacs01	Gestion des mises à jour et configurations Linux
172.16.20.12 /24	vlsmonacs01	Supervision
172.16.20.252 /24	vlsfwlacs01	Passerelle - pare-feu
172.16.20.253 /24	vlsfwlacs02	Passerelle - pare-feu
172.16.20.254 /24	vlsfwlacs0102	Passerelle - pare-feu (VIP)

Tableau 6 : Affectation des adresses IP du VLAN "CORESVC"

4.4.3. CLIENTS (VLAN 100)

Ce VLAN dispose des adresses réservées pour les pares-feux, et d'une étendue DHCP allant de 172.16.100.100 à 172.16.100.150.

4.4.4. ADMIN (VLAN 110)

Ce VLAN dispose des adresses réservées pour les pares-feux, et d'une étendue DHCP allant de 172.16.110.100 à 172.16.110.110.

4.4.5. FIREWALL_HA (VLAN 254)

Ce VLAN permet exclusivement aux pares-feux de synchroniser les règles, les états et de contrôler le bon fonctionnement. Le Tableau 7 présente l'adressage IP de ce VLAN.

Adresse IP	Nom DNS	Fonctionnalité
172.16.254.1 /30	vlsfwlacs01	Pare-feu
172.16.254.2 /30	vlsfwlacs02	Pare-feu

Tableau 7 : Affectation des adresses IP du VLAN "FIREWALL_HA"

5. RÈGLES DE DURCISSEMENT

5.1. Configuration des machines virtuelles

5.1.1. Configuration matérielle

La configuration matérielle est systématiquement adaptée aux machines. Les éléments qui s'y trouvent sont :

- Mémoire vive
- Processeur
- Disques durs configurés en NVMe
- Carte réseau
- Affichage

Tous les autres éléments sont supprimés.

5.1.2. Options et UEFI

Les options sont systématiquement adaptées aux machines, tout en prenant en compte les impératifs de performances et de sécurité. Les configurations suivantes sont systématiquement appliquées :

- Sélection du système d'exploitation adapté
- Désactivation de la synchronisation horaire par les VMware Tools
- Désactivation de la mise à jour automatique des VMware Tools
- Utilisation de l'UEFI
- Configuration du démarrage exclusivement sur le système d'exploitation installé

5.2. Configuration des systèmes CentOS

5.2.1. Installation

Un serveur Linux CentOS doit impérativement être installé avec une sélection logiciel « Installation minimale (fonctionnalité de base) ». Le fuseau horaire doit impérativement être configuré. Les serveurs NTP sont obligatoirement les pares-feux, qui eux-mêmes se synchroniseront sur des sources fiables. Le partitionnement retenu pour les partitions systèmes se réalise via LVM et doit au moins correspondre à celui présenté dans le Tableau 8.

Point de montage	Capacité	Système de fichiers	Groupe de volumes	Volume logique
/boot	1Gio	ext4	Non-concerné	Non-concerné
/boot/efi	1Gio	EFI System Partition	Non-concerné	Non-concerné
/var/cache	3Gio	xfs	VG_System	LV_var_cache
/var/spool	2Gio	xfs	VG_System	LV_var_spool
/var/log	2Gio	xfs	VG_System	LV_var_log
/opt	2Gio	xfs	VG_System	LV_opt
/var	3Gio	xfs	VG_System	LV_var
/	2Gio	xfs	VG_System	LV_root
/usr	5Gio	xfs	VG_System	LV_usr
/tmp	2Gio	xfs	VG_System	LV_tmp
/home	2Gio	xfs	VG_System	LV_home
swap	Voir Tableau 9	swap	VG_System	LV_swap

Tableau 8 : Partitionnement pour un système CentOS

La taille du volume logique « swap » est définie suivant les standards de RedHat[1], rappelés dans le Tableau 9.

Mémoire vive du serveur	Taille de swap recommandée (sans hibernation)	Taille de swap recommandée (hibernation activée)
≤ 2Gio	Mémoire vive multipliée par 2	Mémoire vive multipliée par 3
> 2Gio et ≤ 8Gio	= mémoire vive	Mémoire vive multipliée par 2
> 8Gio et ≤ 64Gio	Au moins 4Gio	Mémoire vive multipliée par 1,5
> 64Gio	Au moins 4Gio	Hibernation non-recommandée

Tableau 9 : Calcul de la taille du swap

5.2.2. Paquets à installer

Certains paquets systèmes utiles ne sont pas intégrés à CentOS, et doivent être installés manuellement.

```
dnf -y install drpm net-tools open-vm-tools mlocate rsyslog
```

5.2.3. Configurations supplémentaires

5.2.3.1. Désactivation du nommage consistent des interfaces

Le nommage consistent implique des noms d'interfaces réseaux variables, rendant plus complexe la gestion de serveurs par scripts et la supervision.

```
mv /etc/sysconfig/network-scripts/ifcfg-ens32 /etc/sysconfig/network-
scripts/ifcfg-eth0

sed -i -- 's/ens32/eth0/g' /etc/sysconfig/network-scripts/ifcfg-eth0
ln -s /dev/null /etc/udev/rules.d/80-net-name-slot.rules
```

L'application de ce paramètre implique un redémarrage, qui ne doit être effectué qu'après la recompilation du noyau Linux détaillée au titre 5.2.3.2.

5.2.3.2. Recompilation du noyau Linux

L'audit du kernel permet de détecter d'éventuelles compromissions du noyau. IPv6 n'étant pas activé dans ce projet, la stratégie de défense en profondeur implique de désactiver IPv6 dans le noyau. Le nommage consistent des interfaces est lui aussi une option du noyau.

```
sed -i '/^GRUB_CMDLINE_LINUX/d' /etc/default/grub

echo -e 'GRUB_CMDLINE_LINUX="crashkernel=auto resume=/dev/mapper/VG_System-
LV_swap rd.lvm.lv=VG_System/LV_root rd.lvm.lv=VG_System/LV_swap
rd.lvm.lv=VG_System/LV_usr rhgb quiet audit=1 ipv6.disable=1 net.ifnames=0
biosdevname=0"' >> /etc/default/grub

grub2-mkconfig -o /boot/efi/EFI/centos/grub.cfg
```

L'application de ce paramètre implique un redémarrage, qui ne doit être effectué qu'après la désactivation du nommage consistent des interfaces détaillé au titre 5.2.3.1.

[1] https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/storage_administration_guide/ch-swapspace

5.2.3.3. Bannières

La bannière a un caractère légal, définissant clairement qu'il est interdit de se connecter à l'équipement. Il est également judicieux, afin de rendre plus difficile l'exploitation d'une éventuelle faille de sécurité, de ne pas y exposer son système d'exploitation ou la version de son noyau.

```
echo "---- UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED       ----
---- LES ACCES NON-AUTORISES A CET EQUIPEMENT SONT PROHIBES ----

You must have explicit, authorized permission to access or configure this
device. Unauthorized attempts and actions to access or use this system may
result in civil and/or criminal penalties. All activities performed on this
device are logged and monitored.

Vous devez avoir une autorisation explicite afin d'acceder ou de configurer
cet equipement. Les tentatives non-autorisees et les actions pour acceder
ou utiliser ce systeme peuvent conduire a des poursuites civiles et/ou
penales. Toutes les activites realisees sur cet equipement sont
enregistrees et supervisees.\n" > /etc/issue
```

La bannière doit ensuite être déployée pour les connexions SSH.

```
sed -i -- 's+#Banner none+Banner /etc/issue+g' /etc/ssh/sshd_config
```

5.2.3.4. Configuration SSH

La configuration en tant que serveur SSH ne peut pas être réalisée par des fichiers annexes. Les Ciphers et Macs autorisés sont pour certains obsolètes, ne garantissant pas une sécurité optimale, et doivent être spécifiés à la main.

```
sed -i -- 's/# For more information, see manual page for update-crypto-
policies(8)./# For more information, see manual page for update-crypto-
policies(8).\nCiphers=aes128-ctr,aes192-ctr,aes256-ctr\nMacs=hmac-sha2-
256,hmac-sha2-512/g' /etc/ssh/sshd_config
```

En tant que client SSH, cette modification peut se mettre en œuvre par un fichier de configuration annexe.

```
echo "# Disabling weak ciphers/Macs
Ciphers=aes128-ctr,aes192-ctr,aes256-ctr
Macs=hmac-sha2-256,hmac-sha2-512" > /etc/ssh/ssh_config.d/10-disable-weak-
ciphers-and-mac.conf
```

5.2.3.5. Configuration système

Le renforcement de la configuration du système se réalise par l'intermédiaire d'un fichier de configuration additionnel.

```
echo "net.ipv4.ip_forward = 0
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.ipv4.route.flush = 1
net.ipv4.tcp_syncookies = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.log_martians = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.secure_redirects = 0
net.ipv4.conf.default.send_redirects = 0" > /etc/sysctl.d/10-hardening.conf
```

5.2.3.6. Configuration réseau

Un paramètre réseau permet de rendre la résolution DNS bien plus rapide, élément qui se ressent d'autant plus lors des connexions.

```
echo -e 'RES_OPTIONS="single-request-reopen timeout:1 attempts:1"' >>
/etc/sysconfig/network
```

5.2.3.7. Configuration de syslog

La configuration de syslog ne sera effective que lorsque les serveurs seront installés. Cependant, les logs ne seront pas perdus, mais stockés en attente de transmission.

```
echo -e '$ActionQueueFileName queue
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
*.* @@vlslogacs01:514

$ActionQueueFileName queue
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
*.* @@vlslogacs02:514' > /etc/rsyslog.d/00-client.conf
```

5.2.3.8. Désactivation des dépôts originaux

Les dépôts utilisés étant ceux du projet, les dépôts préexistants doivent être désactivés. En effet, si les fichiers sont supprimés, ils seront remis en place s'ils sont modifiés par une mise à jour ultérieure, et donc réactivés.

```
sed -i -- '+s+enabled=1+enabled=0+g' /etc/yum.repos.d/CentOS-*
```

5.2.3.9. Configuration des serveurs NTP

Si aucun serveur NTP n'est configuré en local, il faut alors en configurer à l'extérieur de l'organisation. Quatre à cinq références différentes sont recommandées.

- Supprimer toutes les références aux serveurs pré-existants
- Insérer les serveurs NTP
- Redémarrer chrony

```
sed -i '/^server /d' /etc/chrony.conf

sed -i -- 's+# These servers were defined in the installation:+# These
servers were defined in the installation:\nserver 172.16.20.252
iburst\nserver 172.16.20.253 iburst+g' /etc/chrony.conf

systemctl restart chronyd
```

5.2.3.10. Configuration de la supervision

La supervision doit être activée sur les systèmes Linux par le biais de l'installation d'un agent et sa configuration.

- Installer le paquet
- Autoriser les communications sur le port d'écoute de l'agent Zabbix
- Créer le fichier de configuration Zabbix
- Activer Zabbix au démarrage du système
- Lancer l'agent Zabbix

```
dnf -y install zabbix-agent
firewall-cmd --add-port=10050/tcp --permanent
firewall-cmd --reload

echo -e "### Config file for Zabbix agent for CentOS 8 for Infra at Home
project

LogFile=/var/log/zabbix/zabbix_agentd.log

# Log rotation, from 1 to 1024M, 0 to disable log rotation
LogFileSize=0

# Debug Level
#  0 - basic information about starting and stopping of Zabbix processes
#  1 - critical information
#  2 - error information
#  3 - warnings
#  4 - for debugging (produces lots of information)
#  5 - extended debugging (produces even more information)
DebugLevel=3

Server=172.16.20.12,172.16.20.13
ServerActive=172.16.20.12,172.16.20.13
ListenPort=10050" >> /etc/zabbix/zabbix_agentd.d/zabbix_agentd_infra-at-
home.conf

systemctl enable zabbix-agent
systemctl start zabbix-agent
```