

Principales fonctionnalités de sécurisation VMware

1. Le chiffrement et les certificats

a. Autorité de certification

Généralité

Le rôle d’une autorité de certification est de fournir des certificats et de maintenir leurs cycles de vie (création, révocation, renouvellement).

Clé de chiffrement symétrique

Dans un système de chiffrement à clé symétrique ou à secret partagé, une seule et même clé est utilisée pour chiffrer et déchiffrer le message. Cette clé est donc partagée par l’émetteur et par le receveur du message. Le système à clé de chiffrement symétrique le plus populaire est le Data Encryption Standard (DES). La famille DES compte plusieurs versions comme les 3DES (triple DES). Dans le tableau ci-dessous, nous parlons de TDEA. Le TDEA est l’acronyme de Triple Data Encryption Algorithm.

Voici la liste des systèmes à clé symétrique utilisés pour le chiffrement et le déchiffrement encore valides (http://csrc.nist.gov/publications/drafts/800-131A/sp800-131a_r1_draft.pdf)

Algorithme	Utilisation
TDEA à 2 clés pour le chiffrement	Restreint en 2015, non autorisé après 2015
TDEA à 2 clés pour le déchiffrement	Utilisation liée aux anciens systèmes (rétrocompatibilité)
TDEA à 3 clés pour le chiffrement et le déchiffrement	Valide
SKIPJACK chiffrement	Non autorisé
SKIPJACK déchiffrement	Utilisation liée aux anciens systèmes (rétrocompatibilité)
AES-128 pour le chiffrement et le déchiffrement	Valide
AES-192 pour le chiffrement et le déchiffrement	Valide
AES-256 pour le chiffrement et le déchiffrement	Valide

Le 3DES utilise un système de clé de 168 bits. La donnée passe par trois phases successives de chiffrement.

La première phase consiste à l’application de la première clé. Elle s’applique au message à chiffrer, ce qui produit C1.

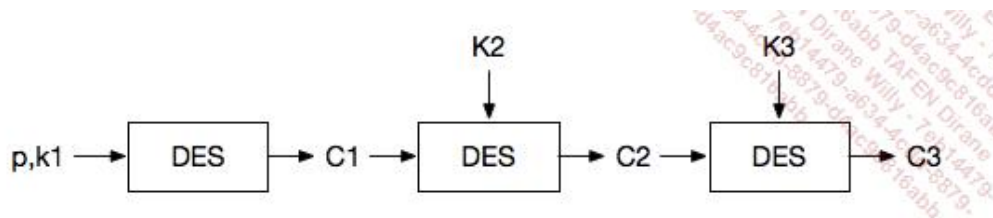
Nous répétons ce schéma encore deux fois, en utilisant une seconde clé pour produire C2, et enfin une troisième clé afin de produire C3 le message chiffré final (<https://msdn.microsoft.com/en-us/library/cc767123.aspx>).

$$E(p,k_1)=C_1$$

$$E(C_1,k_2)=C_2$$

$$E(C_2,k_3)=C_3$$

Où E est la fonction de chiffrement, p le message en clair, k représente une clé, k1, k2 et k3 sont différentes, et C le texte :



Public Key Cryptographic Standards (PKCS)

Le PKCS (<https://en.wikipedia.org/wiki/PKCS>) ou Public Key Cryptographic Standard est une norme publiée et révisée par la société RSA Security. Il définit le principe d'utilisation de l'algorithme RSA (clé publique, clé privée, échange de clé via la méthode DH - Diffie-Hellman, etc.).

Système à clé asymétrique ou infrastructure à clé publique

Un système à clé asymétrique est composé de deux clés différentes. L'une est une clé publique, l'autre est une clé privée. La clé privée est généralement stockée sur la machine, la localisation exacte dépend de votre système et de votre outil de génération de certificat SSL, il est recommandé d'en faire une copie de sauvegarde. Un utilisateur va utiliser la clé publique pour chiffrer le message et nous l'envoyer, tandis que nous allons utiliser, notre clé privée, pour le déchiffrer. C'est une communication à sens unique.

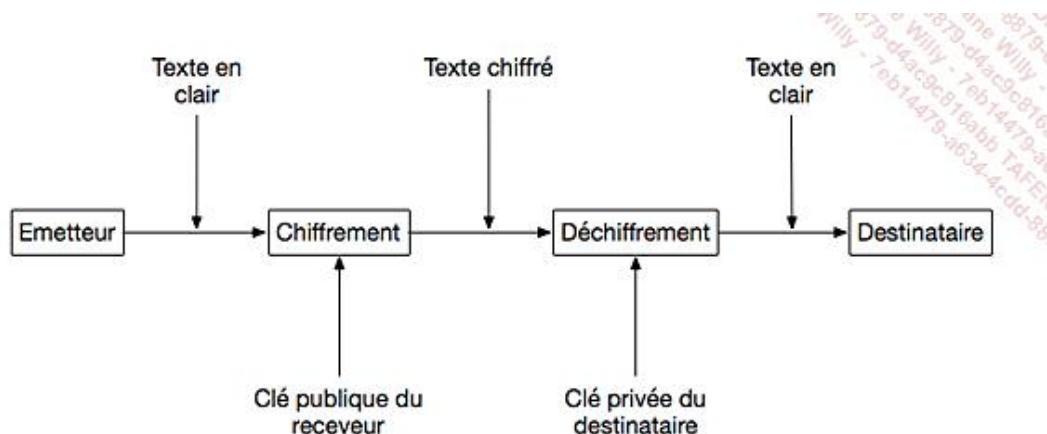
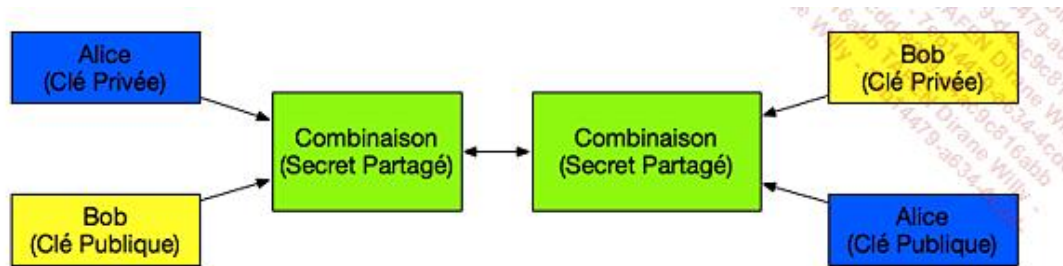


Schéma de fonctionnement

Le système de clé asymétrique le plus utilisé est le RSA (de Rivest - Shamir - Adelman). Il se base sur l'utilisation des nombres premiers. La taille de la clé doit être d'au moins 2048 bits. Il existe plusieurs versions de ce système de chiffrement, une des versions les plus communes est le RC5 créé par Ron Rivest (RC signifiant Ron ou Rivert's Cipher). Le RC6 participa à la finale du concours permettant de définir le nouveau Standard AES (*Advanced Encryption System*) (http://www.encryptionanddecryption.com/algorithms/asymmetric_algorithms.html). Le gagnant du concours définissant l'AES fut l'algorithme de chiffrement Rijndael (<http://searchsecurity.techtarget.com/definition/Rijndael> et <https://www.lri.fr/~fmartignon/documenti/systemesecurite/5-AES.pdf>) qui est une combinaison de permutation et de substitution.

Distribution des clés et secret Key Distribution and Secrecy

Pour avoir une communication à deux sens, il est nécessaire de générer une clé symétrique. Cette clé symétrique est constituée de l'association de ma clé privée et la clé publique de mon partenaire pour mon côté de la communication, et de la clé prive de mon partenaire et de ma clé publique pour le côté de la communication que mon partenaire gère. L'échange se fait via l'algorithme DH (Diffie-Hellman).



Composant et rôle au sein d'une PKI

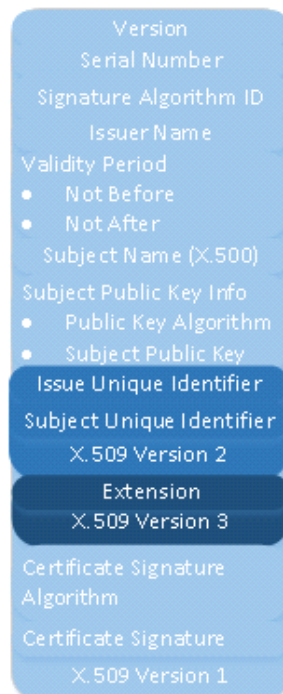
Autorité de certification et rôle hiérarchique

Une autorité de certification est une entité qui émet et signe des certificats. Elle est responsable de leur cycle de vie. Dans une infrastructure de clé publique, nous avons l'autorité de certification racine, qui en général ne sert qu'à valider les autorités de certification subordonnées. Les autorités de certification subordonnées émettent les certificats pour les utilisateurs, services et périphériques. L'autorité racine délègue donc son droit aux autorités subordonnées.

Certificat (Digital Certificate)

Les certificats sont des représentations électroniques des utilisateurs, services, ou de périphériques, générés par une autorité de certification. Il s'agit de l'association d'une clé publique et d'une clé privée. Un certificat peut être exporté en suivant le standard PKCS. Par exemple le PKCS7 représente le standard de syntaxe de message cryptographique), ou encore le PKCS12 représente le standard de syntaxe d'échange d'informations personnelles).

Le certificat est basé sur le standard x509 :



La demande de génération de certificat est nommée CSR ou *Certificate Signing Request*.

Autorité de Certification Racine (Root CA)

Une autorité de certification racine est le sommet hiérarchique dans une infrastructure de gestion de certificat. Dans une infrastructure à clé publique (*Public Key Infrastructure*), l'autorité de certification racine agit comme un point de confiance pour l'ensemble des certificats générés par ladite infrastructure. En règle générale, une autorité de certification racine est utilisée pour générer d'autres certificats pour les autorités de certification intermédiaires, ou qui génèrent les certificats pour les utilisateurs, services ou périphériques. Pour créer une autorité de certification racine, il faut créer un certificat racine, qui est auto généré. Pour que ce certificat racine soit automatiquement reconnu comme valide (*trusted*), il doit être inclus dans le magasin de certificats racines.

Autorité de certification intermédiaire

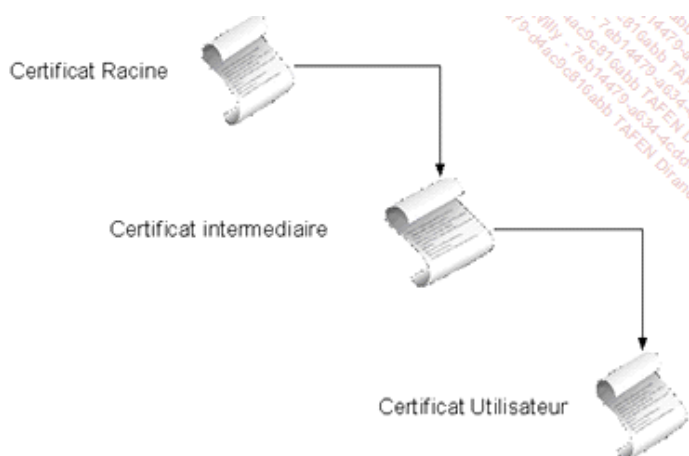
Une autorité de certification intermédiaire est une autorité de certification qui est subordonnée à une autorité de certification racine. Elle génère des certificats pour d'autres dans une hiérarchie d'autorité de certification. Nous trouvons des autorités de certification intermédiaire à tous les niveaux à l'exception du premier niveau (autorité de certification racine).

Autorité de certification délivrant des certificats

Une autorité de certification délivrant des certificats est l'échelon le plus bas dans une hiérarchie d'autorité de certification. Elle délivre des certificats aux utilisateurs, services et périphériques.

Chaîne de certificat ou Certificate of trust

Une chaîne de certificat (<https://technet.microsoft.com/en-us/library/cc778623%28v=ws.10%29.aspx>) est représentée par l'ensemble des certificats de l'infrastructure allant du certificat racine au certificat qui est délivré aux utilisateurs, services et périphériques.



Nous vous recommandons de lire les guides suivants concernant l'implémentation d'une infrastructure de clés publiques :

<https://www.sans.org/reading-room/whitepapers/certificates/implementing-public-key-infrastructure-pki-microsoft-windows-server-2012-certificate-servic-35427>.

La série de Derek Seaman sur la PKI de Windows 2012 : <https://www.derekseaman.com/2014/01/windows-server-2012-r2-two-tier-pki-ca-pt-1.html>.

La virtual Academy de Microsoft : <https://channel9.msdn.com/Events/TechEd/Europe/2014/EM-H301>.

L'autorité de certificats VMware

Par défaut, VMware utilise des certificats auto générés. Ces dernières années, les prérequis en matière de sécurité (SOX, PCI DSS, HIPASS et autres normes de sécurité et de traçabilité) ainsi que le déploiement intensif des infrastructures de clé publiques, pour répondre à ces besoins, ont rendu les infrastructures de clés publiques courantes.

Dans une infrastructure VMware, les ESXi et le vCenter, communiquent de manière sécurisée via le SSL afin d'assurer la confidentialité, l'authentification et l'intégrité des échanges. Les certificats produits sont au format x509 v3.

Les certificats

Dans les versions inférieures à vSphere 6.0, la gestion des certificats était (soyons honnêtes) plus que pénible. Depuis la version 6.0 avec l'introduction du PSC, VMware a repensé la gestion des certificats et a fourni le VMCA ou *VMware Certificate Authority*. Nous retrouvons des certificats aux niveaux suivants :

Certificate	Provisioned by	Stored
ESXi certificates	VMCA (default)	Installé localement sur l'ESXi
Machine SSL certificates	VMCA (default)	VMware Certificate Endpoint Store (VECS)
Solution user certificates	VMCA (default)	VECS
Center Single Sign-On SSL signing certificate	Créé lors de l'installation	Gérer ce certificat depuis le vSphere Web Client. Note: Ne pas changer ce certificat au niveau du système de fichier, sous peine de comportement erratique.
VMware Directory Service (vmdir) SSL certificate	Créé lors de l'installation	

<https://pubs.vmware.com/vsphere-65/index.jsp#com.vmware.psc.doc/GUID-3AF7757E-A30E-4EEC-8A41-28DA72102520.html>

Le certificat pour un serveur ESXi est un certificat auto généré lors de son installation. Dès qu'un ESXi intègre ou réintègre l'inventaire d'un serveur vCenter, le certificat ESXi est fourni par la VMCA. Le certificat d'un serveur ESXi se trouve dans /etc/vmware/ssl. Dans le cas de l'ajout d'un ESXi dans le vCenter, le vCenter envoie un CSR pour le serveur ESXi à la VMCA. Il est possible de modifier certains paramètres de configuration du vCenter en fonction de nos besoins comme nous le voyons dans le tableau ci-dessous :

Paramètre	Valeur par défaut	Option avancée du vCenter
Taille de la clé	2048	N.A.
Algorithme de la clé	RSA	N.A.
Algorithme de la clé de signature du certificat	sha256WithRSAEncryption	N.A.
Nom Commun	Nom de l'hôte, si l'hôte a été ajouté au vCenter par son nom d'hôte. Adresse IP si l'hôte a été ajouté au vCenter par son adresse IP.	N.A.
Pays	USA	vpzd.certmgmt. certs.cn.country
Adresse email	vmca@vmware.com	vpzd.certmgmt. certs.cn.email
Localisation (ville)	Palo Alto	vpzd.certmgmt.certs.cn. localityName
Nom du service	VMware Engineering	vpzd.certmgmt.certs.cn. organizational UnitName

Nom de l'organisation	VMware	vpzd.certmgmt.certs.cn. organizationName
Pays ou province	California	vpzd.certmgmt.certs. cn.state
Nombre de jours où le certificat sera valide	1825	vpzd.certmgmt.certs.cn. daysValid
Seuil de génération d'une alerte critique par le vCenter dans le cadre du renouvellement de certificat.	30 jours	vpzd.certmgmt.certs.cn. hardThreshold
Intervalle de vérification de la validité du certificat par le vCenter	5 jours	vpzd.certmgmt.certs.cn. pollIntervalDays
Seuil de génération d'une alerte par le vCenter dans le cadre du renouvellement de certificat.	240 jours	vpzd.certmgmt.certs.cn. softThreshold
Mode de fonctionnement du vCenter lors de la génération de nouveaux certificats.	La valeur par défaut est vmca. Nous pouvons aussi spécifier thumbprint ou custom.	vpzd.certmgmt.mode

Le VECS (*VMware Certificat Endpoint Store*)

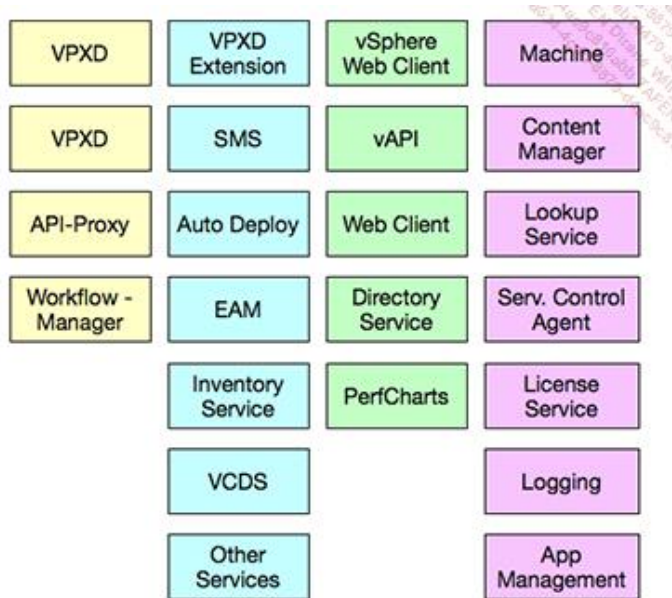
Le VECS sert de magasin pour les certificats du côté client. Il est dépendant pour son exécution de VMAFD (*VMware Authentication Framework*). Le VMAFD est présent sur chaque nœud exécutant le PSC. Le VECS interroge régulièrement le VMDir (*VMware Directory Service*) afin de savoir s'il y a des mises à jour des TRUSTED_ROOT (magasin des certificats approuvés).

Il existe plusieurs magasins dans un VECS que l'on peut classer en trois catégories :

- Magasin de certificats machine :
 - Machine_SSL_CERT : il est utilisé par le reverse proxy, et le VMware Directory Service. Depuis la version vSphere 6, l'ensemble des services utilise le Machine_SSL_CERT via le reverse proxy. Il crée un socket SSL du côté serveur auquel les clients se connectent. Le certificat est utilisé pour vérifier et sécuriser les communications. Chaque nœud (vCenter et/ou PSC) a son propre Machine_SSL_CERT, chaque service présent sur le nœud utilise ce certificat machine pour s'exposer.
- Les certificats racines :
 - Trusted_Roots : liste les certificats racines approuvés.
 - Trusted_Roots_CRL : liste de révocation des certificats racines approuvés.
- Solution Users
 - vpzd : magasin de démon du service vCenter (vpzd) sur les nœuds de gestion et les déploiements intégrés. vpzd utilise le certificat d'utilisateur de solution qui est stocké dans ce magasin pour s'authentifier auprès de vCenter Single Sign-On.
 - Vpzd-extensions : magasin d'extensions vCenter. Incluant le service Auto Deploy, Inventory Service, VUM, Dump Collector...
 - vsphere-webclient : magasin vSphere Web Client. Inclut également certains services supplémentaires tels que le service de graphiques de performance.
 - Machine : il est utilisé par le service de logging, de licences et le gestionnaire des composants ainsi que lors des authentications via SAML. À ne pas confondre avec le certificat ssl de la machine. (tiré de <https://pubs.vmware.com/vsphere-65/index.jsp?topic=%2Fcom.vmware.psc.doc%2FGUID-EB2D4685-D9B1-4F87-B02D-934FDEECE3F2.html>)

Le certificat Solution User

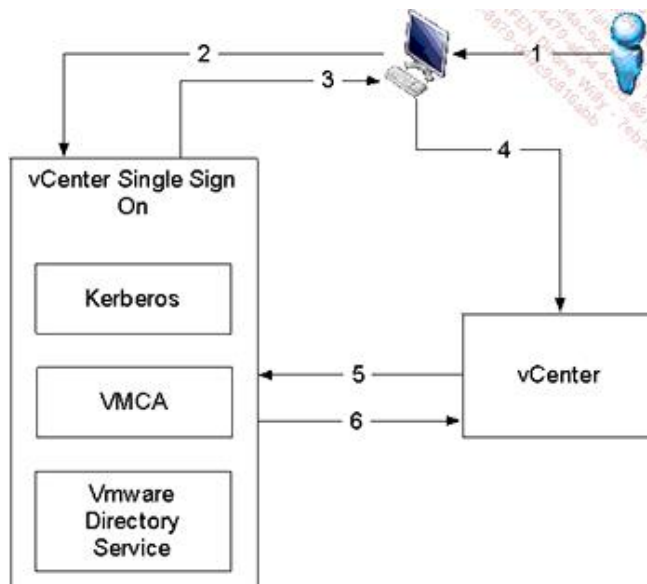
Les Solutions Users représentent un ou plusieurs services du vCenter. Le Solution User utilise les certificats pour s'authentifier auprès du vCenter Single Sign On via un jeton SAML. Un Solution User présente son certificat au vCenter SSO, lors d'une première authentification (suite à un reboot) ou après expiration de l'authentification. La durée de vie (*Holder of Key Timeout*) par défaut est de 2 592 000 secondes (30 jours), il est configurable via le client web vSphere. Les certificats Solutions User étant embarqués dans le VECS, ils sont présents sur chaque PSC.



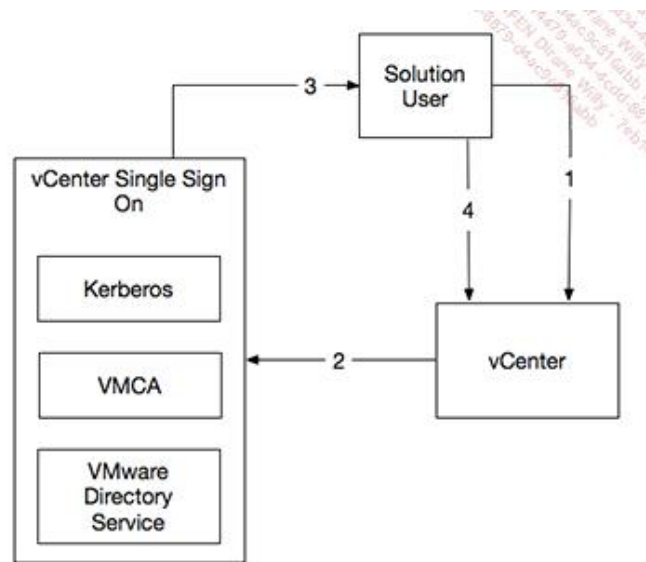
Le vCenter Single Sign On

Le vCenter SSO est un courtier d'authentification et d'échange de jetons de sécurité (SAML). À partir de vSphere 6.0, le vCenter SSO est intégré dans le PSC. Le vCenter SSO fonctionne de deux manières différentes en fonction de si la source de l'authentification est humaine ou un service.

- Authentification pour un utilisateur :



1. Connexion de l'utilisateur (login/mot de passe ou authentification Windows).
 2. Le Web Client transfère les informations de connexion au vCenter SSO. Le vCenter SSO vérifie le jeton de connexion (SAML). Si le jeton est valide, le vCenter SSO vérifie que l'utilisateur existe dans les sources d'identités (vsphere.local, Active Directory...).
 3. L'utilisateur s'authentifie auprès de la source d'identité, le vCenter SSO renvoie un jeton.
 4. Le Web Client transmet le jeton au vCenter.
 5. Le vCenter fait vérifier par le vCenter SSO que le jeton est valide et n'a pas expiré.
 6. Le vCenter SSO renvoie le jeton au vCenter en s'appuyant sur les rôles et permissions de l'utilisateur.
- Authentification pour un service :



2. Le Solution User est redirigé vers le vCenter SSO. Si le Solution User est nouveau dans le vCenter, il doit présenter un certificat valide.
3. Si le certificat est valide, le vCenter SSO donne un jeton signé au Solution User.
4. Le Solution User est redirigé vers le vCenter, il effectue ses tâches en fonctions des autorisations qui lui sont attribuées.
5. À la prochaine authentification, le Solution User pourra utiliser le SAML pour se connecter au vCenter.

Le vCenter SSO se compose de quatre composants :

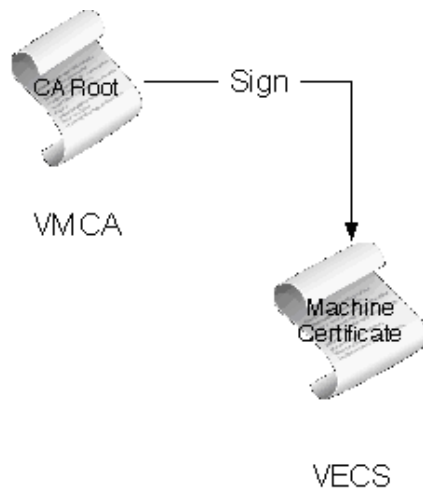
- Le Security Token Service (STS) : le STS authentifie (via les sources d'identité), crée et signe un jeton SAML (Security Assertion Markup Language), contenant les attributs de l'utilisateur. Une fois correctement authentifié auprès du vCenter SSO afin d'accéder aux services du vCenter, l'utilisateur n'a pas besoin de se réauthentifier.
- Le Server d'administration : il permet de configurer et d'administrer le vCenter SSO. Par défaut seul le compte administrator@vsphere.local a les accès. Il permet aussi de définir les droits au niveau du vCenter SSO. Il permet de configurer la gestion des mots de passe pour les comptes du domaine (vsphere.local par défaut).

Il est accessible via le PSC ou via l'interface web du client vSphere

- Le VMware Directory Service (vmdir) : ce service d'annuaire LDAP est associé au domaine lors de l'installation. Il est présent dans chaque instance PSC. Depuis vSphere 6.0, il contient aussi les informations liées au certificat (VECS).
- Identity Management Service : il gère les demandes aux sources d'identité et l'authentification au STS.

VMCA en tant que Root CA

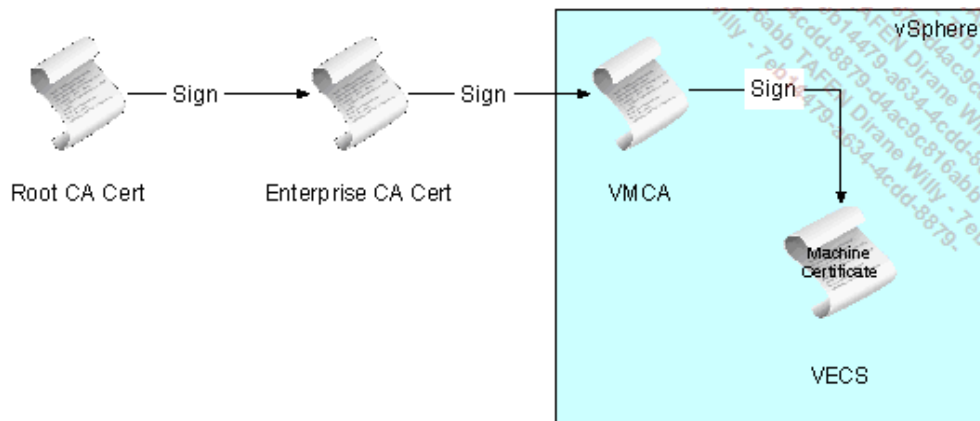
La génération du certificat de l'ESXi se fait au moment de l'ajout dans le vCenter que ce soit fait manuellement ou automatiquement. L'ensemble des certificats d'un ESXi sont stockés localement dans le magasin de certificat. Le certificat racine du VMCA a une durée de validité de 10 ans. Après cela, l'ensemble des certificats sont périmés, et nous devons les régénérer. C'est le mode de fonctionnement par défaut.



VMCA en tant qu'autorité subordonnée

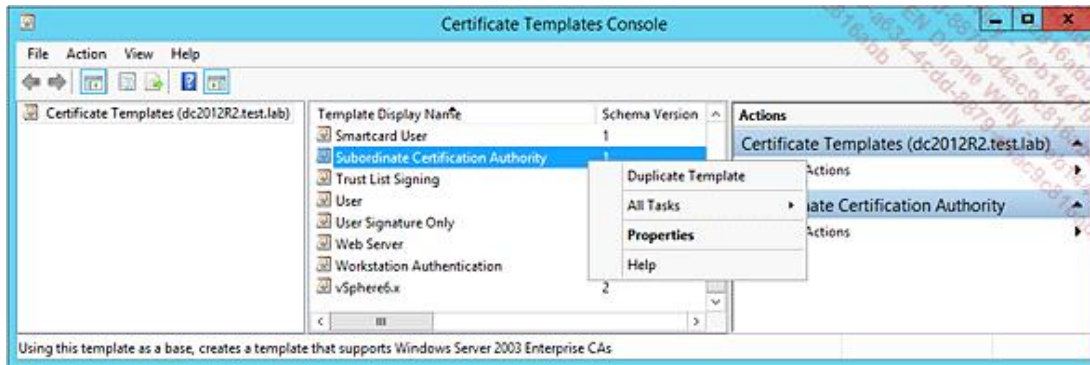
Lorsque l'on utilise la VMCA en tant qu'autorité subordonnée, il est nécessaire de remplacer le certificat par défaut, par un certificat signé par la PKI de la société. Attention, nous ne parlons pas d'un certificat utilisateur, mais du certificat pour une autorité de certification. À partir de ce moment, la VMCA peut signer des certificats qui sont reconnus et donc valides dans l'infrastructure PKI.

Attention cependant, dans le cas où l'on part d'une infrastructure vierge, l'opération est facile. On installe le PSC, puis on remplace le certificat racine dans la VMCA avant l'intégration des ESXi. L'intérêt est que nous aurons ainsi la chaîne complète de certification et le renouvellement se fera automatiquement.

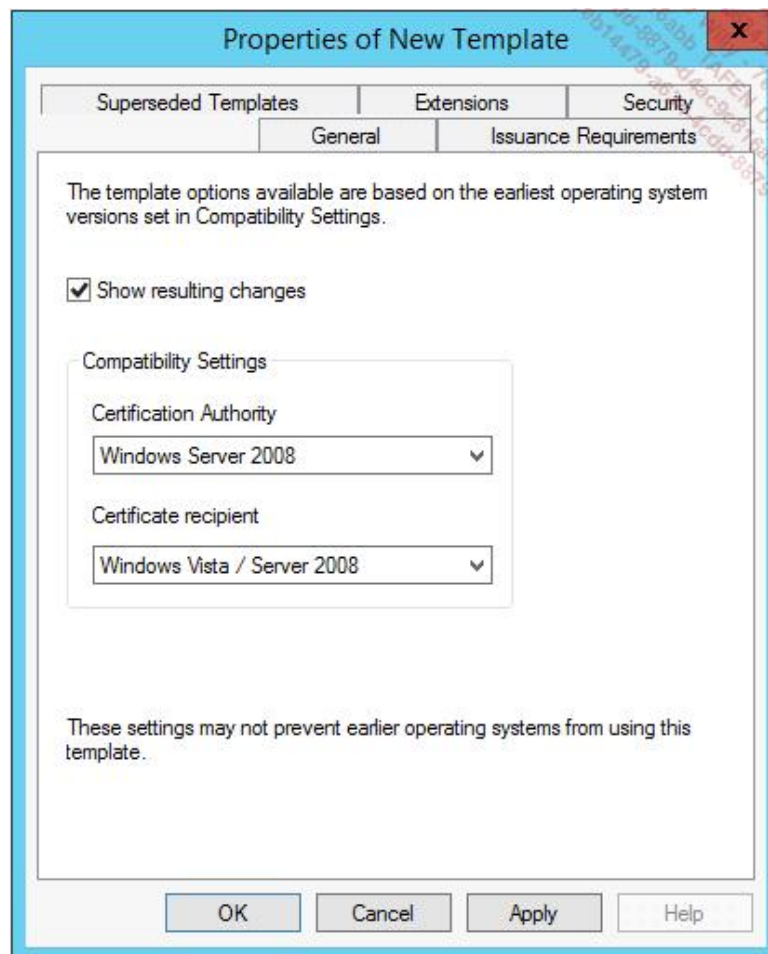


- Création du template de certificat

La première étape dans l'utilisation du VMCA en tant que qu'autorité de certification subordonnée est une duplication du template Subordinate Certificate Authority à partir de la console Windows : certtmpl.msc



En cas d'utilisation d'un chiffrement d'une version supérieure au SHA1, il faut une compatibilité liée à Windows 2008.



L'étape suivante consiste à nommer le template et à configurer la période de validité ainsi que son renouvellement.

Properties of New Template

Superseded Templates Extensions Security

Compatibility General Issuance Requirements

Template display name:
VMCA 6.x

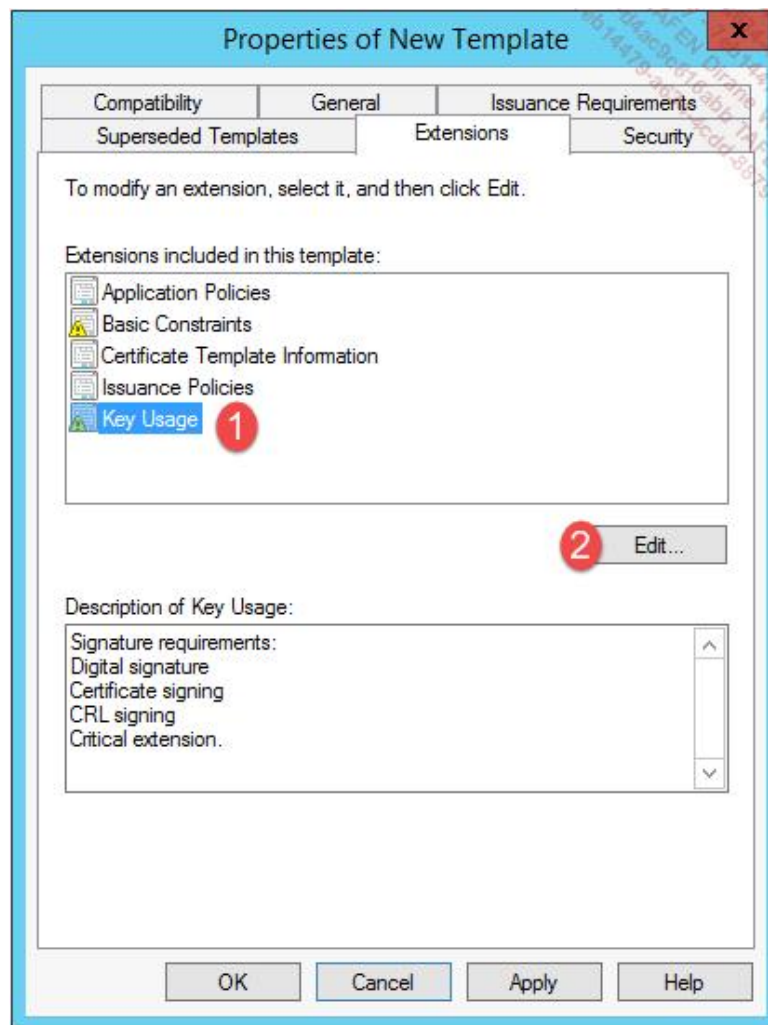
Template name:
VMCA6.x

Validity period: 5 years Renewal period: 6 weeks

☐ Publish certificate in Active Directory
☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

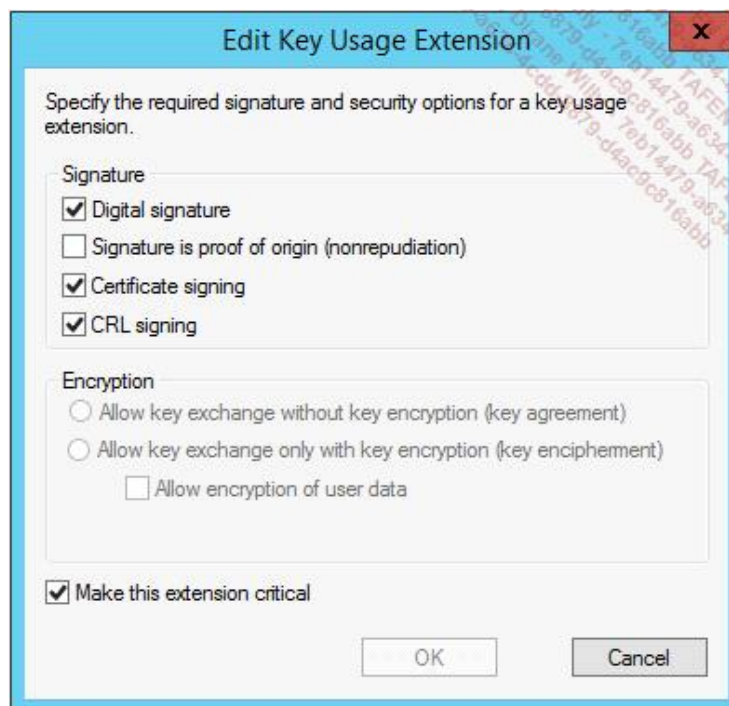
OK Cancel Apply Help

Ensuite, allez dans l'onglet **Extensions**, sélectionnez **Key Usage** (1).

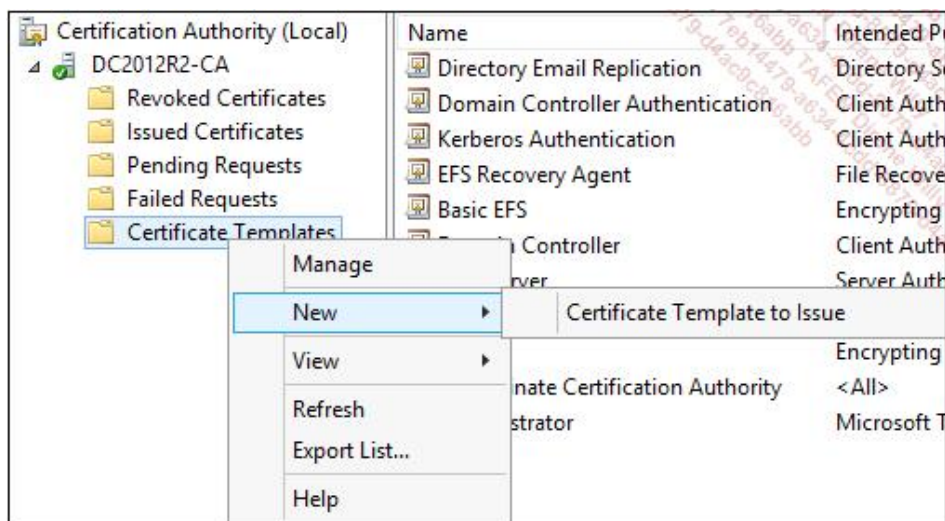


Cliquez sur **Edit** (2).

→ Vérifiez que les options **Digital signature**, **Certificate signing** et **CRL signing** sont cochées.



Validez le template. Pour publier un template de certificat, allez dans la console de gestion de l'autorité de certification : Certmgr.msc. Parcourez l'arborescence jusqu'à parvenir à **Certificate Templates**. Un clic droit donne accès au menu contextuel. Allez dans New, puis **Certificate Template to Issue**.



Sélectionnez le template (ici VMCA 6.x) puis cliquez sur **OK**.

- Génération de la requête de certificat pour la VMCA

Connectez-vous via putty, puis activez le shell. La première commande à taper est la suivante :

```
root@vcsa [ ~ ]# chsh -s /bin/bash root
```

Elle sera utile lorsque vous aurez besoin de faire des transferts de fichiers via WinSCP.

Créez le répertoire qui servira à recevoir la clé et la demande de certificat (CSR).

```
root@vcsa [ ~ ]# mkdir /certs
```

Ces préparatifs effectués, nous allons entamer la partie génération du CSR. Pour cela, lancez le certificate-manager, puis sélectionnez l'option 2 : **Replace VMCA Root certificate with Custom Signing Certificate and replace all Certificates**.

```
root@vcsa [ ~ ]# /usr/lib/vmware-vmca/bin/certificate-manager

*** Welcome to the vSphere 6.0 Certificate Manager ***

-- Select Operation --

1. Replace Machine SSL certificate with Custom Certificate
2. Replace VMCA Root certificate with Custom Signing Certificate and replace all Certificates
3. Replace Machine SSL certificate with VMCA Certificate
4. Regenerate a new VMCA Root Certificate and replace all certificates
5. Replace Solution user certificates with Custom Certificate
6. Replace Solution user certificates with VMCA certificates
7. Revert last performed operation by re-publishing old certificates
8. Reset all Certificates

Note : Use Ctrl-D to exit.
Option[1 to 8]: 2
```

Comme il s'agit de la première fois que vous lancez le certificate-manager, il propose de générer l'ensemble des certificats à partir du fichier de configuration.

Utilisez le compte administrator@vsphere.local (compte par défaut). Renseignez son mot de passe.

```
Do you wish to generate all certificates using configuration file : Option[Y/N] ? : y

Please provide valid SSO and VC privileged user credential to perform certificate operations.
Enter username [Administrator@vsphere.local]:
Enter password:
```

Les étapes suivantes reprennent les paramètres que nous fournissons afin de créer l'ensemble des certificats nécessaires. Attention, comme pour tous certificats, il faut faire attention au fait que le nom de chacun d'entre eux doit être unique. Vous pouvez mettre un nom [Name] différent pour chacun d'entre eux et utiliser par exemple une valeur unique pour chaque [OrgUnit].

- Configuration du fichier Machine_ssl_cert.cfg

```
Please configure MACHINE_SSL_CERT.cfg with proper values before proceeding to next step.
Press Enter key to skip optional parameters or use Default value.
Enter proper value for 'Country' [Default value : US] : FR
Enter proper value for 'Name' [Default value : CA] : vcsa.test.lab
Enter proper value for 'Organization' [Default value : VMware] : lab
Enter proper value for 'OrgUnit' [Default value : VMware Engineering] : test
Enter proper value for 'State' [Default value : California] : France
Enter proper value for 'Locality' [Default value : Palo Alto] : Paris
Enter proper value for 'IPAddress' [optional] :
Enter proper value for 'Email' [Default value : email@acme.com] :
Enter proper value for 'Hostname' [Enter valid Fully Qualified Domain Name(FQDN), For Example : example.domain.com] :
vcsa.test.lab
```

- Configuration du fichier machine.cfg


```

Please configure machine.cfg with proper values before proceeding to next step.
Press Enter key to skip optional parameters or use Default value.
Enter proper value for 'Country' [Default value : US] : FR
Enter proper value for 'Name' [Default value : CA] : machine-vcsa.test.lab
Enter proper value for 'Organization' [Default value : VMware] : lab
Enter proper value for 'OrgUnit' [Default value : VMware Engineering] : test
Enter proper value for 'State' [Default value : California] : France
Enter proper value for 'Locality' [Default value : Palo Alto] : Paris
Enter proper value for 'IPAddress' [optional] :
Enter proper value for 'Email' [Default value : email@acme.com] :
Enter proper value for 'Hostname' [Enter valid Fully Qualified Domain Name(FQDN), For Example : example.domain.com] :
vcsa.test.lab

```

- Configuration du fichier vsphere-webclient.cfg

```

Please configure vsphere-webclient.cfg with proper values before proceeding to next step.
Press Enter key to skip optional parameters or use Default value.
Enter proper value for 'Country' [Default value : US] : FR
Enter proper value for 'Name' [Default value : CA] : webclient.vcsa.test.lab
Enter proper value for 'Organization' [Default value : VMware] : lab
Enter proper value for 'OrgUnit' [Default value : VMware Engineering] : test
Enter proper value for 'State' [Default value : California] : France
Enter proper value for 'Locality' [Default value : Palo Alto] : Paris
Enter proper value for 'IPAddress' [optional] :
Enter proper value for 'Email' [Default value : email@acme.com] :
Enter proper value for 'Hostname' [Enter valid Fully Qualified Domain Name(FQDN), For Example : example.domain.com] :
vcsa.test.lab

```

- Configuration du fichier vpxd.cfg

```

Please configure vpxd.cfg with proper values before proceeding to next step.
Press Enter key to skip optional parameters or use Default value.
Enter proper value for 'Country' [Default value : US] : FR
Enter proper value for 'Name' [Default value : CA] : vpxd-vcsa.test.lab
Enter proper value for 'Organization' [Default value : VMware] : lab
Enter proper value for 'OrgUnit' [Default value : VMware Engineering] : test
Enter proper value for 'State' [Default value : California] : France
Enter proper value for 'Locality' [Default value : Palo Alto] : Paris
Enter proper value for 'IPAddress' [optional] :
Enter proper value for 'Email' [Default value : email@acme.com] :
Enter proper value for 'Hostname' [Enter valid Fully Qualified Domain Name(FQDN), For Example : example.domain.com] :
vcsa.test.lab

```

- Configuration du fichier vpxd-extension.cfg

```

Please configure vpxd-extension.cfg with proper values before proceeding to next step.
Press Enter key to skip optional parameters or use Default value.
Enter proper value for 'Country' [Default value : US] : FR
Enter proper value for 'Name' [Default value : CA] : vpxd-ext-vcsa.test.lab
Enter proper value for 'Organization' [Default value : VMware] : lab
Enter proper value for 'OrgUnit' [Default value : VMware Engineering] : test
Enter proper value for 'State' [Default value : California] : France
Enter proper value for 'Locality' [Default value : Palo Alto] : Paris
Enter proper value for 'IPAddress' [optional] :
Enter proper value for 'Email' [Default value : email@acme.com] :
Enter proper value for 'Hostname' [Enter valid Fully Qualified Domain Name(FQDN), For Example : example.domain.com] :
vcsa.test.lab

```

Sélectionnez l'option 1 afin de générer le CSR et la clé qui va avec, puis donnez le chemin où seront générés les fichiers.

```

1. Generate Certificate Signing Request(s) and Key(s) for VMCA Root Signing certificate
2. Import custom certificate(s) and key(s) to replace existing VMCA Root Signing certificate

Option [1 or 2]: 1

Please provide a directory location to write the CSR(s) and PrivateKey(s) to:
Output directory path: /certs

```

Sous le nom barbare de certtool.cfg se cache le fichier de configuration qui sera utilisé dans le cadre de la génération du CSR du certificat racine du VMCA.

```

Please configure certtool.cfg with proper values before proceeding to next step.
Press Enter key to skip optional parameters or use Default value.
Enter proper value for 'Country' [Default value : US] : FR
Enter proper value for 'Name' [Default value : CA] : vmca-vcsa.test.lab
Enter proper value for 'Organization' [Default value : VMware] : test
Enter proper value for 'OrgUnit' [Default value : VMware Engineering] : test
Enter proper value for 'State' [Default value : California] : France
Enter proper value for 'Locality' [Default value : Palo Alto] : Paris
Enter proper value for 'IPAddress' [optional] :
Enter proper value for 'Email' [Default value : email@acme.com] :
Enter proper value for 'Hostname' [Enter valid Fully Qualified Domain Name(FQDN), For Example : example.domain.com] :
vcsa.test.lab

```

- Le processus de génération du CSR et de la clé privée et de la clé publique.

```

2017-02-03T07:43:31.078Z Running command: ['/usr/lib/vmware-vmca/bin/certool', '--genkey', '--privkey', '/certs/
vmca_issued_key.key', '--pubkey', '/tmp/pubkey.pub']
2017-02-03T07:43:31.151Z Done running command
2017-02-03T07:43:31.151Z Running command: ['/usr/lib/vmware-vmca/bin/certool', '--gencsr', '--privkey', '/certs/
vmca_issued_key.key', '--pubkey', '/tmp/pubkey.pub', '--config', '/var/tmp/vmware/certool.cfg', '--csrfile', '/certs/
vmca_issued_csr.csr']
2017-02-03T07:43:31.196Z Done running command

CSR generated at: /certs/vmca_issued_csr.csr
1. Continue to importing Custom certificate(s) and key(s) for VMCA Root Signing certificate
2. Exit certificate-manager
Option [1 or 2]: 2

```

- Mise en place du certificat de subordination pour le VMCA
Éditez le fichier vmca_issued_csr.csr via WinSCP afin d'en copier le contenu dans Saved request. Sélectionnez le template de certificat créé (VMCA6.x) et soumettez-le.

Microsoft Active Directory Certificate Services -- DC2012R2-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```

1+Z5CzvB38xD016B4RYn/RnGVEfk36w9Bp9tetWW.
S4jlNcbSK4wyR4vPhcbZzzn70d9n9GO2MNOETq9E!
9bTk8g2x2zD4ECflniy5ml1w7hIUoUWVq9eYBPD8!
YWQwz4vZGLnofLSCfQUF0efRSI6b2w7wNndBaXpN
PHNAf0Bvmru5pBOCJq5g
-----END CERTIFICATE REQUEST-----

```

Certificate Template:

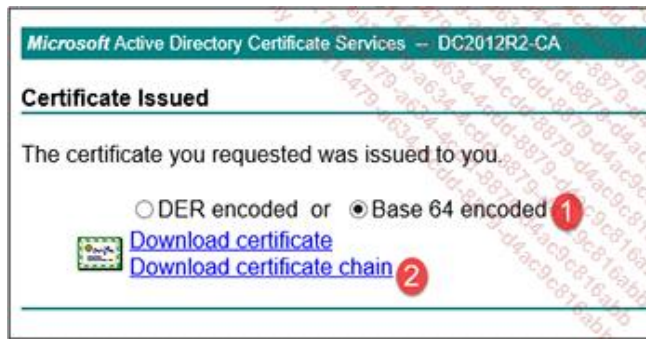
VMCA 6.x

Additional Attributes:

Attributes:

Submit >

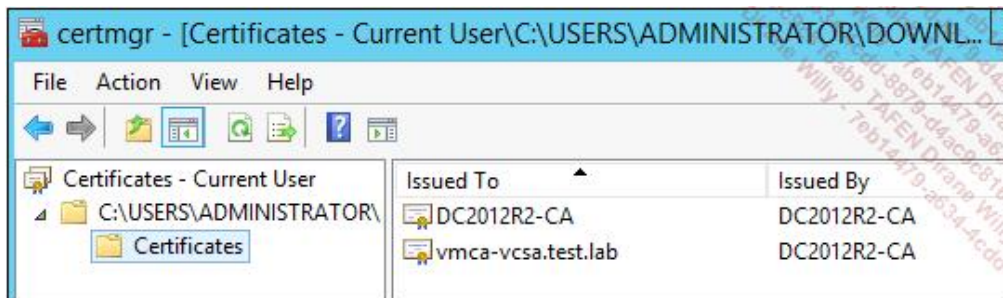
Une fois le certificat généré, exportez la chaîne de certificats encodée en base 64.



Par défaut, le certificat se nomme certnew.

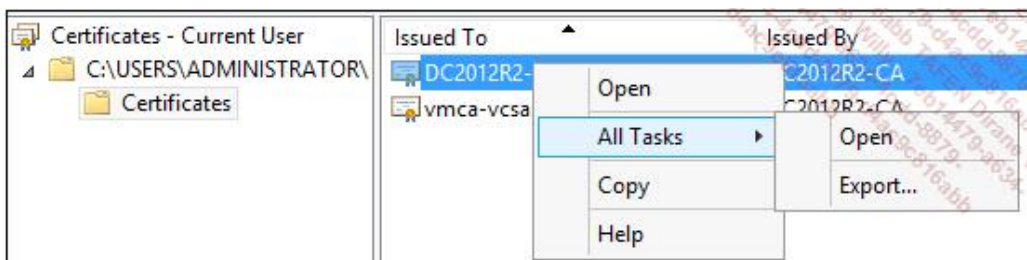


Double cliquez dessus afin de l'ouvrir.



Exportez les deux certificats (racine et subordonné) sous la forme d'un fichier CER x509 encodé en base 64. L'exemple ci-dessous concerne le certificat racine, mais vous auriez pu prendre le certificat subordonné.

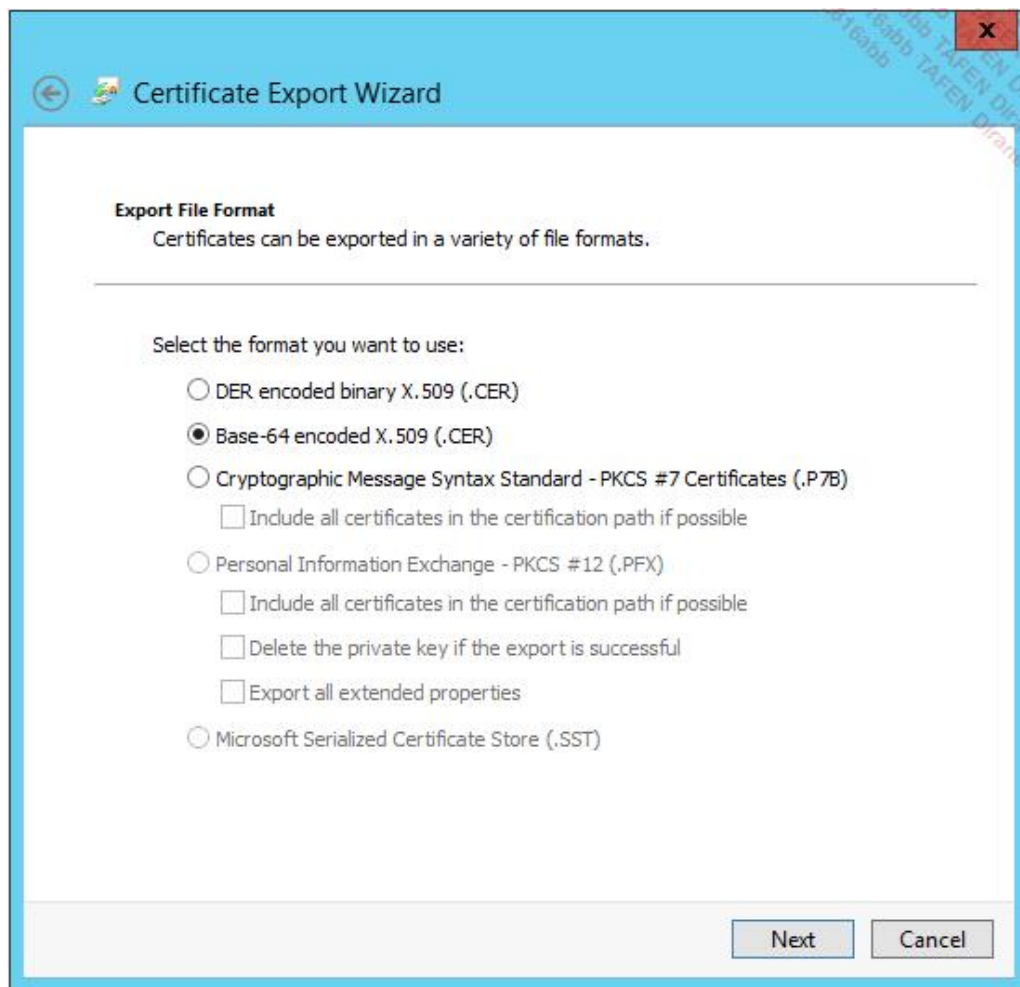
Faites un clic droit sur le certificat que vous voulez exporter, puis allez dans **All tasks** pour avoir accès à l'option **Export**.



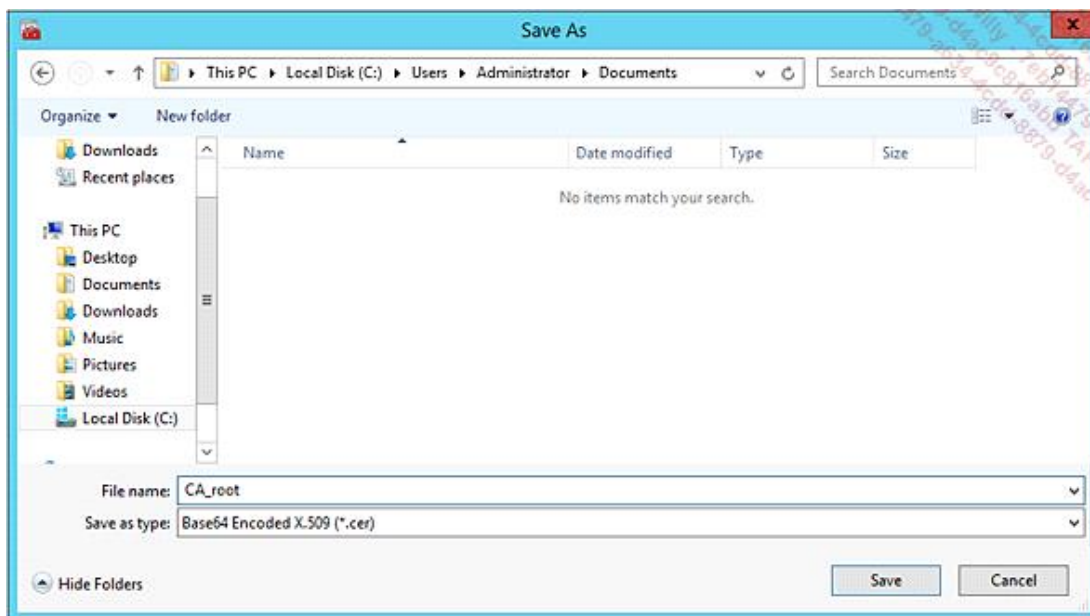
L'assistant s'ouvre.



Sélectionnez le type d'export souhaité : **Base-64 encoded X.509 (.CER)**.



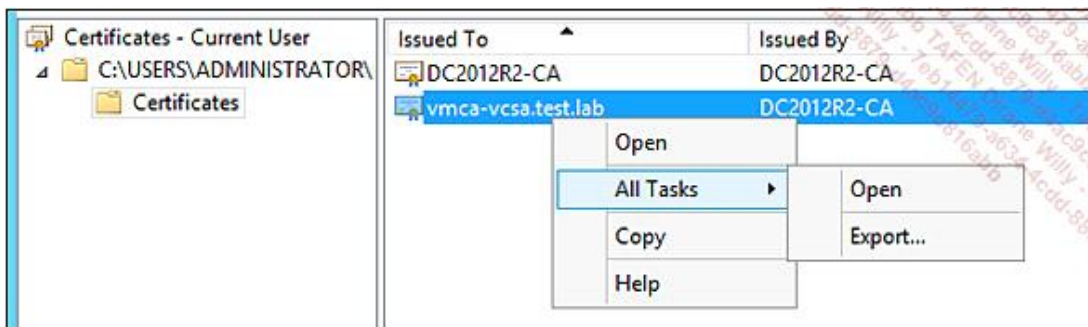
Choisissez l'emplacement de l'export.



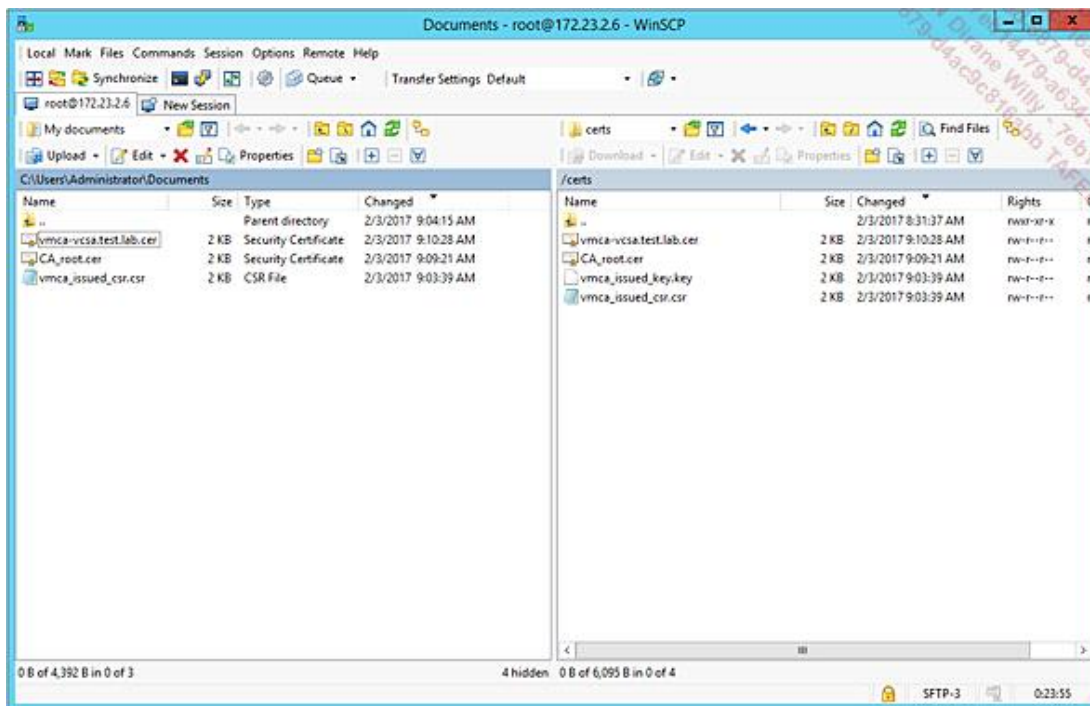
L'opération est terminée.



Répétez l'export avec le second certificat.



Transférez les deux fichiers sur le VCSA.



Concaténez ces deux certificats. Attention à l'enchaînement lors de la concaténation. Il faut que la structure respecte la norme suivante :

- Certificat subordonné
- Certificat racine

```
root@vcsa [ ~ ]# more /certs/vmca-vcsa.test.lab.cer >>/certs/vmca_issued_cer.cer
root@vcsa [ ~ ]# more /certs/CA_root.cer >>/certs/vmca_issued_cer.cer
root@vcsa [ ~ ]#
root@vcsa [ ~ ]# mv /certs/vmca_issued_cer.cer /tmp
root@vcsa [ ~ ]# mv /certs/vmca_issued_key.key /tmp
```

Relancez le certificate manager, toujours avec l'option 2, mais cette fois ne générez aucun certificat.


```
root@vcsa [ ~ ]# /usr/lib/vmware-vmca/bin/certificate-manager

*** Welcome to the vSphere 6.0 Certificate Manager ***

-- Select Operation --

1. Replace Machine SSL certificate with Custom Certificate
2. Replace VMCA Root certificate with Custom Signing Certificate and replace all Certificates
3. Replace Machine SSL certificate with VMCA Certificate
4. Regenerate a new VMCA Root Certificate and replace all certificates
5. Replace Solution user certificates with Custom Certificate
6. Replace Solution user certificates with VMCA certificates
7. Revert last performed operation by re-publishing old certificates
8. Reset all Certificates

Note : Use Ctrl-D to exit.
Option[1 to 8]: 2
Do you wish to generate all certificates using configuration file : Option[Y/N] ? : n
```

Reconnectez-vous, puis importez le certificat (CER) et la clé publique.

```
Please provide valid SSO and VC privileged user credential to perform certificate operations.
Enter username [Administrator@vsphere.local]:
Enter password:
MACHINE_SSL_CERT.cfg file exists, Do you wish to reconfigure : Option[Y/N] ? : n
1. Generate Certificate Signing Request(s) and Key(s) for VMCA Root Signing certificate
2. Import custom certificate(s) and key(s) to replace existing VMCA Root Signing certificate
Option [1 or 2]: 2
```

Donnez le chemin d'accès à la clé et au certificat. Dans notre cas, le répertoire /tmp contient la clé privée (vmca_issued_key.key) et le fichier CER copié.

```
Please provide valid custom certificate for Root.
File : /tmp/vmca_issued_cer.cer

Please provide valid custom key for Root.
File : /tmp/vmca_issued_key.key
```

Confirmez votre volonté de remplacer le certificat racine par votre certificat et de régénérer les certificats dépendants.

```

You are going to replace Root Certificate with custom certificate and regenerate all other certificates
Continue operation : Option[Y/N] ? : y
Get site nameCompleted [Replacing Machine SSL Cert...]
lab
Lookup all services
Get service lab:5d2f0b9b-90b7-4901-8846-fc9993733ed7
Update service lab:5d2f0b9b-90b7-4901-8846-fc9993733ed7; spec: /tmp/svcspec_X06bVL
Get service lab:c29c590d-7cd2-4d30-a7fb-5508128e1d3a
Update service lab:c29c590d-7cd2-4d30-a7fb-5508128e1d3a; spec: /tmp/svcspec_Oiw38d
Get service lab:a458b308-51a6-460a-ba10-d1cac87eb2ed
Update service lab:a458b308-51a6-460a-ba10-d1cac87eb2ed; spec: /tmp/svcspec_LNJmj0
Get service 4e551344-23b0-4983-ba87-adac57c878b
Update service 4e551344-23b0-4983-ba87-adac57c878b; spec: /tmp/svcspec_Cn2EVQ
Get service 0bba6929-fc86-48d1-b4c5-c6b63f2987c2
Update service 0bba6929-fc86-48d1-b4c5-c6b63f2987c2; spec: /tmp/svcspec_9UcyV_
Get service 5423e362-e615-4d76-a23e-75b6e9c6aa02
Update service 5423e362-e615-4d76-a23e-75b6e9c6aa02; spec: /tmp/svcspec_w588lB
Get service 69b1365d-4ac6-48c7-9445-365cd3a38d62
Update service 69b1365d-4ac6-48c7-9445-365cd3a38d62; spec: /tmp/svcspec_RGhZej
Get service 03d673a3-745f-4ef9-b826-e33cee0c6fe2
Update service 03d673a3-745f-4ef9-b826-e33cee0c6fe2; spec: /tmp/svcspec_Z9fKWt
Get service c54935e2-ef91-47c3-9dc5-fcab0ba81812
Update service c54935e2-ef91-47c3-9dc5-fcab0ba81812; spec: /tmp/svcspec_NqiFcB
Get service b8afbe72-facf-4275-ad36-513b335774d4
Update service b8afbe72-facf-4275-ad36-513b335774d4; spec: /tmp/svcspec_53f9cW
Get service 2eb4bd60-5002-443a-97e0-c3805f13e170_authz
Update service 2eb4bd60-5002-443a-97e0-c3805f13e170_authz; spec: /tmp/svcspec_h3m6BY
Get service 80aaff57-9b3e-450f-b6a2-36c25175efde
Update service 80aaff57-9b3e-450f-b6a2-36c25175efde; spec: /tmp/svcspec_U9q3sd
Get service 16d04ebd-c92d-4430-8c02-8ef2ff03f64c
Update service 16d04ebd-c92d-4430-8c02-8ef2ff03f64c; spec: /tmp/svcspec_1vbcUu
Get service 4bae16be-8e57-452e-bea5-7d17c0276095
Update service 4bae16be-8e57-452e-bea5-7d17c0276095; spec: /tmp/svcspec_JfM1X8
Get service 4ee8fcb3-dfaf-4ee1-8099-dee482558206
Update service 4ee8fcb3-dfaf-4ee1-8099-dee482558206; spec: /tmp/svcspec_QapkF2
Get service f84688e3-bff7-47de-bf04-8aad254d717
Update service f84688e3-bff7-47de-bf04-8aad254d717; spec: /tmp/svcspec_Yp_s0L
Get service cab44dd8-8751-4038-a93d-919927baaaff
Update service cab44dd8-8751-4038-a93d-919927baaaff; spec: /tmp/svcspec_vIZqul
Get service 7f3ff78c-3082-42dd-9c3b-de7530ef5144
Update service 7f3ff78c-3082-42dd-9c3b-de7530ef5144; spec: /tmp/svcspec_1BNFn1
Get service 5698aea6-301e-4722-b6e9-c1f0966fffca
Update service 5698aea6-301e-4722-b6e9-c1f0966fffca; spec: /tmp/svcspec_HjJRZl
Get service b06ea56b-3102-454d-b729-873cc9abc8a9
Update service b06ea56b-3102-454d-b729-873cc9abc8a9; spec: /tmp/svcspec_MXlFvr
Get service c2ca9820-1492-46ba-b08a-dcd9bb2ff02e
Update service c2ca9820-1492-46ba-b08a-dcd9bb2ff02e; spec: /tmp/svcspec_0e0ruo
Get service bd35e33b-e7c5-4ffd-b8ce-2f929fc68f73
Update service bd35e33b-e7c5-4ffd-b8ce-2f929fc68f73; spec: /tmp/svcspec_k86yMP
Get service 39d7bbbb-1aff-42b8-ae6-3cd85b0b6271
Update service 39d7bbbb-1aff-42b8-ae6-3cd85b0b6271; spec: /tmp/svcspec_Vw_F0s
Get service 8e6e46f5-61dd-45f9-ad7d-82fe61d4a535
Update service 8e6e46f5-61dd-45f9-ad7d-82fe61d4a535; spec: /tmp/svcspec_mMEndS
Get service 47311da6-727c-4fe8-babc-36df8fd99a
Update service 47311da6-727c-4fe8-babc-36df8fd99a; spec: /tmp/svcspec_VxbfKR
Get service 2eb4bd60-5002-443a-97e0-c3805f13e170

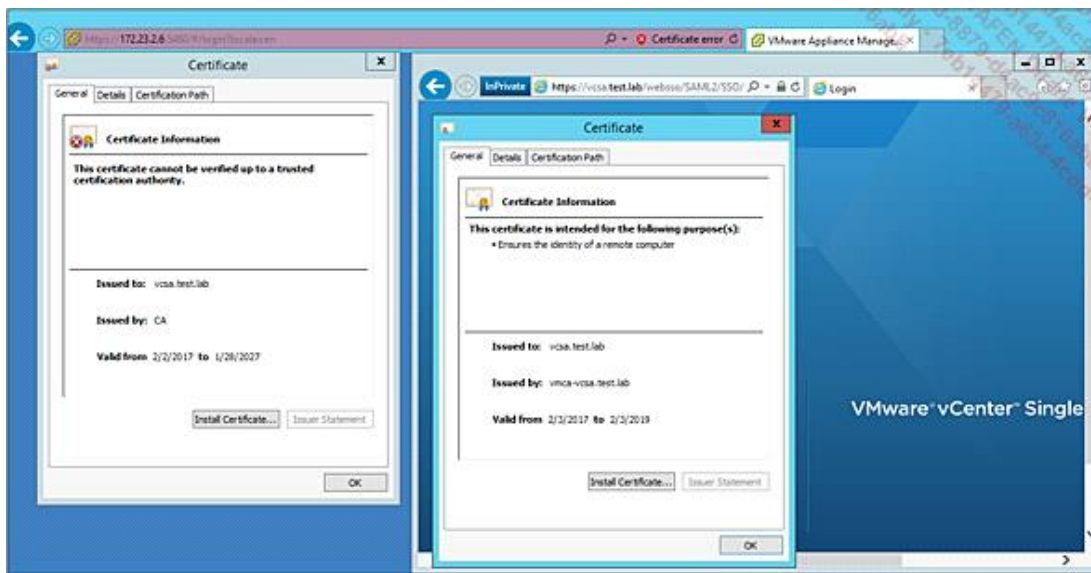
```

```

Get service 2eb4bd60-5002-443a-97e0-c3805f13e170
Update service 2eb4bd60-5002-443a-97e0-c3805f13e170; spec: /tmp/svcspec_tQUdpH
Get service 5ac86833-b15c-4c8a-80a1-da55e95d40db
Update service 5ac86833-b15c-4c8a-80a1-da55e95d40db; spec: /tmp/svcspec_R3mCvW
Get service 2eb4bd60-5002-443a-97e0-c3805f13e170_kv
Update service 2eb4bd60-5002-443a-97e0-c3805f13e170_kv; spec: /tmp/svcspec_XdZ_JW
Get service 9b8baa7e-6503-4c38-b121-f90ab9253af7
Update service 9b8baa7e-6503-4c38-b121-f90ab9253af7; spec: /tmp/svcspec_aYJT4A
Updated 29 service(s)
Status : 100% Completed [All tasks completed successfully]

```

Une fois que l'ensemble des services est mis à jour, vous pouvez vérifier que le lien du vCenter est mis à jour.



Par contre, comme nous pouvons le voir sur la capture d'écran, il nous reste la partie VAMI à mettre à jour.

```
root@vcsa [ ~ ]# service vami-lighttpd restart
```

Attention, lorsque l'on utilise le VMCA en tant qu'autorité de subordination, les certificats des hyperviseurs ESXi sont générés avec une date antérieure de 24h. Il est possible de modifier cela via le paramètre avancé : `vpxd.certmgmt.certs.minutesBefore` (<https://kb.vmware.com/kb/2123386>).

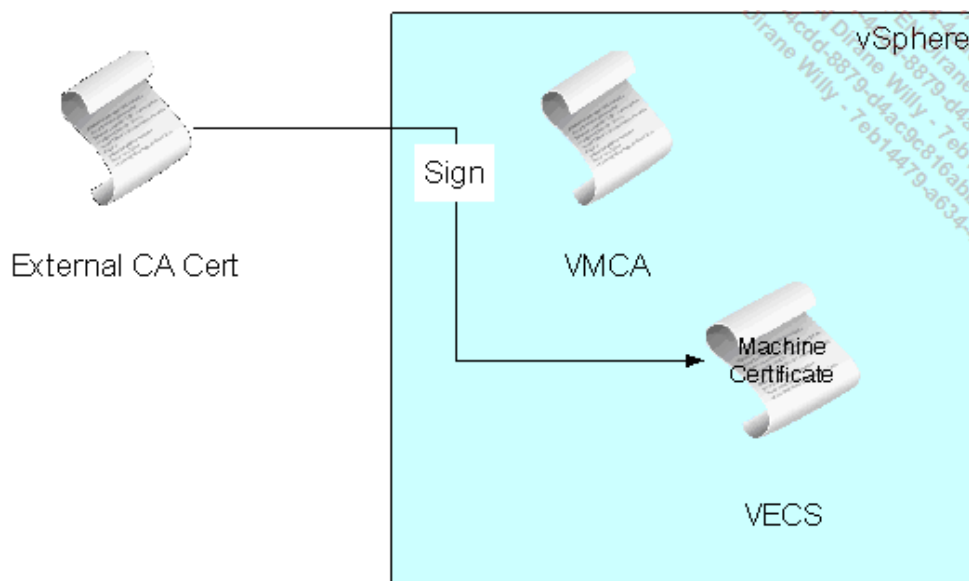
Attention aux certificats avec l'option SAN (*Subject Alternate Name*) (<https://kb.vmware.com/kb/2145544>) !

Autorité de certification Externe

Nous pouvons encore simplement passer outre la VMCA, en utilisant une autorité de certification externe. Dans cette approche, nous devons manuellement surveiller et générer les certificats pour l'infrastructure. Nous sommes dans le mode de fonctionnement comme il existe sous vSphere 5.5.

Nous devons quand même respecter quelques exigences au niveau de la configuration :

- Taille de la clé : 2048 bits et plus (Encodage PEM)
- VMware prend en charge les formats PKCS8 et PKCS1 (clés RSA). Lorsque des clés sont ajoutées à VECS, elles sont converties en PKCS8.
- x509 version 3
- Pour le certificat racine, l'option CA extension doit être configurée sur True et contenir la signature numérique.
- L'option SubjectAltName (SAN) doit contenir le nom DNS (Fully Qualified Domain Name)
- Être au format CRT
- Il doit contenir les informations suivantes sur :
 - La signature numérique
 - Les clés de chiffrement (attention certaines suites de chiffrement sont considérées comme faibles et à ne pas utiliser (md2WithRSAEncryption, md5WithRSAEncryption, sha1WithRSAEncryption)).



Pour plus d'informations sur la gestion des certificats dans une infrastructure VMware consultez l'article suivant : <https://kb.vmware.com/kb/2111219>.

b. Chiffrement des machines virtuelles

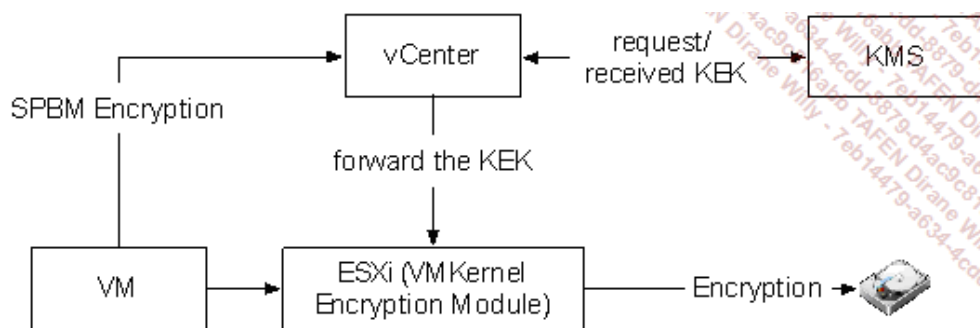
En tant que mesure de sécurité supplémentaire, nous trouvons le chiffrement de machines virtuelles, et pour être plus précis des fichiers VMDK. Le chiffrement des VMDK s'appuie sur VAIO (Filtre I/O). Il s'intègre dans les politiques de gestion, d'ailleurs lorsque nous regardons les politiques par défaut, nous voyons la politique de gestion du chiffrement : VM Encryption. Le chiffrement de machines virtuelles est complètement agnostique à tout stockage, système d'exploitation invité.

Il faut bien prendre en compte que nous travaillons avec des clés de chiffrement. Il existe deux types de clés de chiffrement dans le cadre du chiffrement des machines virtuelles :

- La première est générée par l'ESXi et est utilisée dans le chiffrement des machines virtuelles et des disques (VMDK). Ce sont les DEK (*Data Encryption Key*). Leurs générations utilisent l'algorithme de chiffrement XTS-AES-256 (la taille de la clé est de 512 bits). Le chiffrement et le déchiffrement sont pris en charge par le CPU (via les instructions AES-NI). Attention, cela est à prendre en compte tant au niveau de la latence de lecture/écriture que de la charge CPU (<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vm-encryption-vsphere65-perf.pdf>).
- La seconde est générée par le KMS (*Key Management Server*) et est transmise au vCenter lorsque celui-ci la demande. Cette clé est la KEK (*Key Encryption Key*). Le vCenter ne stocke que l'ID des KEK et non les KEK elles-mêmes. Dans le cas d'un cluster HA, l'ensemble des KEK pour les machines virtuelles du cluster sont mises à disposition sur les ESXi du cluster.

La KEK est utilisée par l'ESXi pour chiffrer la DEK, qui est stockée dans le fichier VMX de la machine virtuelle (TechPreview INF8856).

En cas de changement de KMS, il est nécessaire de chiffrer à nouveau la DEK avec la nouvelle KEK. Celle correspond au Shallow Recrypt (<https://blogs.vmware.com/vsphere/2016/12/powercli-for-vm-encryption.html>). Dans le cas, où l'on souhaite aussi chiffrer à nouveau les VMDK (nouvelle KEK et nouvelle DEK), cette technique se nomme Deep Recrypt. Attention, autant le Shallow Recrypt est fait à chaud, autant le Deep Recrypt est fait machine éteinte. Pendant ces opérations il est nécessaire d'avoir les deux KMS.



Les fichiers chiffrés sont les suivants :

- Les VMDK.
- Les fichiers de configuration de la machine virtuelle (NVRAM, VSWP, VMSN, etc.).
- Les vidages mémoire du composant core de l'ESXi.

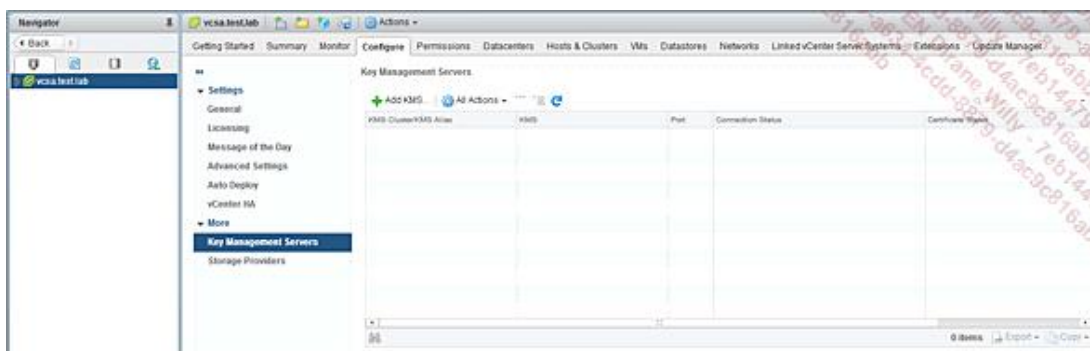
Attention cependant, certains fichiers peuvent n'être que partiellement chiffrés ou non chiffrés :

- Les fichiers de configuration de la machine virtuelle (NVRAM, VSWP, VMSN, etc.).
- Les fichiers de log.
- Les fichiers de description des disques virtuels.

Qui dit nouvelle fonctionnalité, dit aussi nouveaux rôle et privilège. Le nouveau rôle No Cryptography Administrator Role, correspond au même privilège que le rôle d'Administrator à l'exception des privilèges liés au chiffrement.

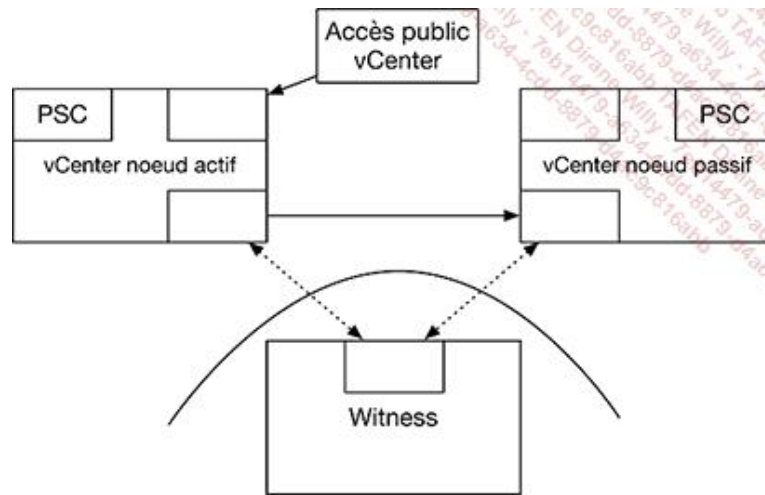
Le chiffrement des machines virtuelles nécessite un composant que VMware ne fournit pas : le *Key Management Server* ou KMS. Nous avons tenté d'avoir accès à une version d'essai d'un KMS que l'on pourrait rencontrer dans le monde professionnel. Malheureusement nous n'avons pas réussi. Un éditeur, dont le KMS n'est pas encore validé par VMware au moment de l'écriture de cet ouvrage, a proposé de nous fournir son logiciel une fois la validation effectuée. Cela fera certainement l'objet d'un article sur <http://www.vexperience.net>. Dans le cadre de ce livre afin de vous fournir les différentes étapes, nous nous sommes basés sur l'article de William LAM (<http://www.virtuallyghetto.com/2016/12/kmip-server-docker-container-for-evaluating-vm-encryption-in-vsphere-6-5.html>) afin d'intégrer le KMS sur la VCSA.

Le chiffrement des machines virtuelles est une option que l'on trouve au niveau du vCenter. Afin de pouvoir la configurer, il est nécessaire d'aller dans l'onglet **Configure** lorsque l'on est au niveau du vCenter dans l'inventaire. Allez dans **Key Management Servers** et cliquez sur **Add KMS**.



La boîte de discussion de configuration du serveur KMS s'ouvre.

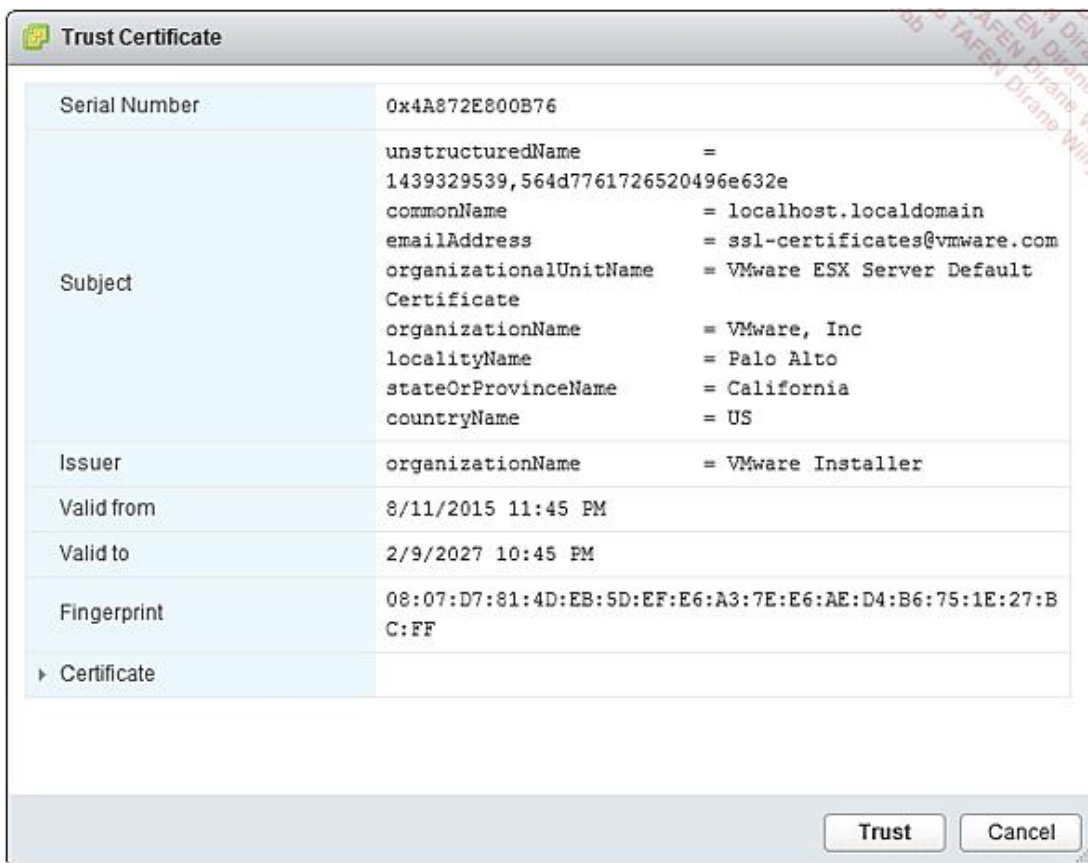
- KMS Cluster permet de créer un nouveau cluster KMS ou d'ajouter un serveur KMS à un cluster existant.
- Cluster name correspond au nom du cluster que l'on crée.
- Server Alias correspond à l'alias du serveur KMS, cela permet de pallier une défaillance du vCenter.
- Server IP correspond à l'adresse IP du serveur KMS, cela permet de pallier à une défaillance du vCenter.



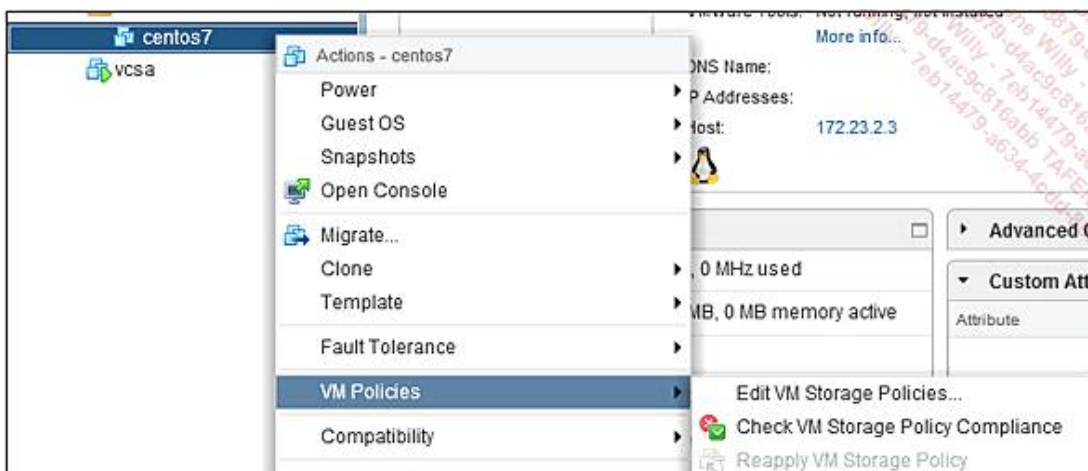
Un message avertit que si des machines virtuelles sont déjà chiffrées via un autre serveur KMS, elles continueront à utiliser les KEK de leur serveur KMS. Pour en changer, il faudra faire un Shallow ou un Deep Reencrypt. Ces notions seront expliquées plus loin.



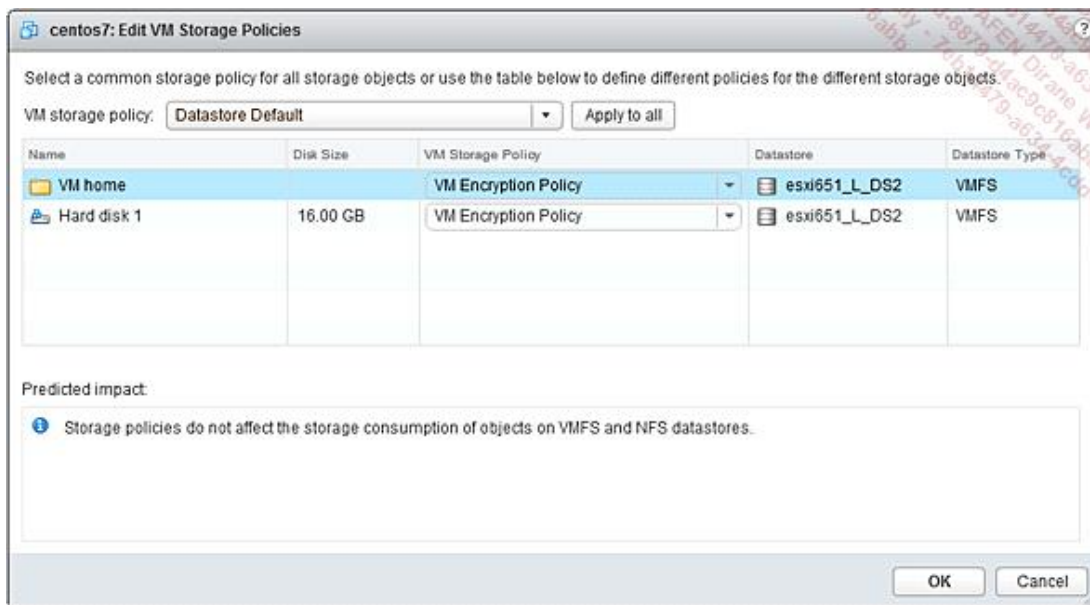
Acceptez l'empreinte du certificat du KMS.



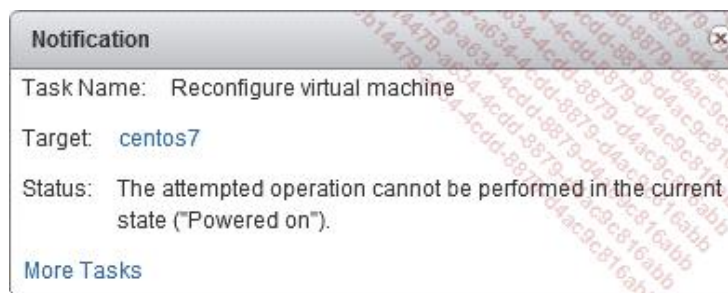
Les étapes suivantes se font au niveau des machines virtuelles. Sélectionnez la machine virtuelle éteinte, faites un clic droit pour avoir accès au menu **VM Policies**. Cliquez sur **Edit VM Storage Policies**.



Au niveau de votre machine virtuelle, vous pouvez sélectionner la politique de chiffrement. Attention, si vous ne souhaitez chiffrer que le VMDK, un message apparaîtra disant qu'il est nécessaire de chiffrer le VM home aussi.



En cas de tentative de chiffrement sur une machine allumée, vous obtenez l'erreur suivante :



Une fois le chiffrement terminé, vous pouvez voir dans le fichier VMX de la machine virtuelle que les clés KEK et DEK ont été ajoutées.

Limitations

Actuellement, il existe un certain nombre de limitations avec le chiffrement de machines virtuelles :

- La majorité des opérations liées au chiffrement des machines virtuelles se fait à l'arrêt : le clonage d'une machine virtuelle déjà chiffrée, tout comme changer la KEK (Shallow Recrypt).
- Il n'est pas possible de mettre en pause et de relancer la machine virtuelle chiffrée.
- Il n'est pas possible de capturer la mémoire lors de la création d'un snapshot.
- Il n'est pas possible de chiffrer une machine virtuelle qui possède des snapshots.

En plus de ces limitations, certaines fonctionnalités ne sont tout simplement pas compatibles :

- La tolérance de panne (Fault Tolerance) n'est pas supportée.
- vSphere ESXi Dump Collector n'est pas supporté.
- La migration intervCenter
- vSphere Replication
- Content Library

- L'accès au KMS via IPv6 n'est pas supporté.
- Toutes les solutions de sauvegarde s'appuyant sur VMware vSphere Storage API Data Protection (VADP).

De même certaines configurations de disques ne sont pas supportées avec le chiffrement des machines virtuelles :

- vFRC
- RDM
- L'accès multiple (MSCS/WSFC/ Oracle RAC)

L'ensemble de ces limitations est disponible sur le site de VMware (<https://pubs.vmware.com/vsphere-65/index.jsp#com.vmware.vsphere.security.doc/GUID-C0AF1F3A-67B4-41A6-A933-7E52A3603D9D.html>).

Il existe sur les ESXi dans le profil de sécurité une option concernant le chiffrement des machines virtuelles :

- Le Host Encryption Mode.

Dans la plupart des cas, il est activé automatiquement lors des actions liées au chiffrement. Il existe certains cas où ce doit être configuré explicitement comme par exemple pour chiffrer les vidages mémoire (dumps).



Après activation de ce mode, le retour en arrière est contraignant car il nécessite de faire une migration des machines virtuelles, de désenregistrer le serveur ESXi du vCenter, de rebooter l'ESXi et de l'enregistrer de nouveau dans l'inventaire vCenter.

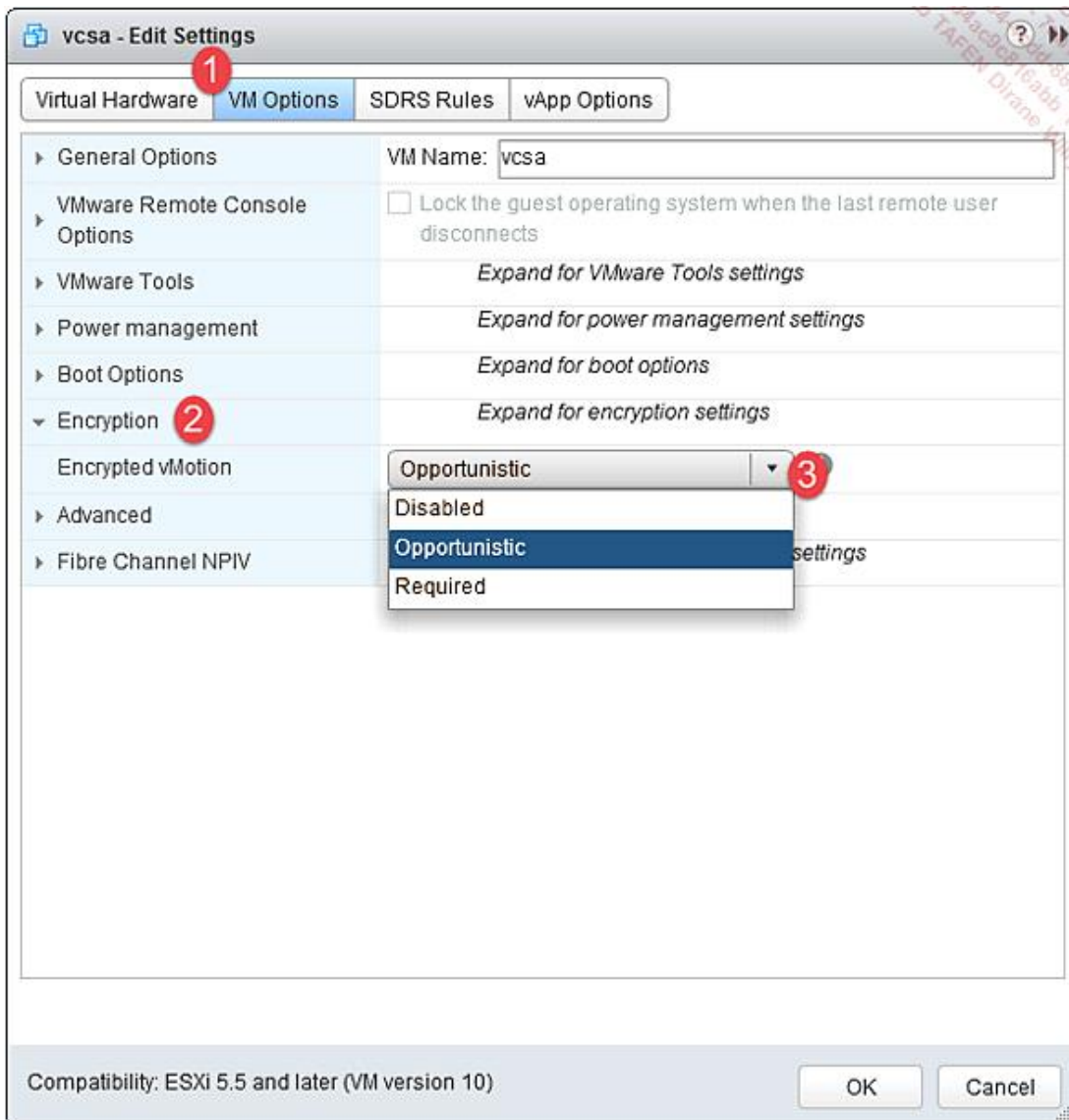
Le chiffrement du vMotion

À partir de vSphere 6.5, le vMotion utilise par défaut une nouvelle fonctionnalité (attendue depuis un certain temps), le chiffrement pour la migration des machines virtuelles. Le vMotion chiffré s'intègre dans l'ensemble des migrations à quelques points près :

- Pour les machines virtuelles dont les disques (VMDK) ne sont pas chiffrés, le Storage vMotion chiffré n'est pas supporté.
- Pour les machines virtuelles chiffrées, le vMotion utilise toujours le mode chiffré et il ne peut pas être désactivé.
- Pour les machines virtuelles non chiffrées, il est possible d'activer le vMotion chiffré. Il existe trois configurations pour l'activation du vMotion chiffré :
 - Désactivé (**Disabled**) : le vMotion ne sera jamais chiffré.
 - Opportuniste (**Opportunistic**) (configuration par défaut) : si la source et la cible le supportent, ce qui implique d'être en version 6.5 minimum.
 - Requis (**Required**) (autorise uniquement le vMotion chiffré) : si la source ou la cible ne supportent pas le vMotion chiffré, le vMotion n'est pas autorisé.

Attention, l'activation du chiffrement d'une machine virtuelle, laisse des traces dans les paramètres de ladite machine au niveau du vMotion chiffré. Lorsque l'on désactive le chiffrement de la machine virtuelle, le paramètre du

vMotion chiffré reste sur Requis. Il est nécessaire de le changer manuellement.



2. Le Secure Boot

Pour utiliser le Secure Boot, la machine (serveur ou PC) doit être configurée pour démarrer via le UEFI et non via le BIOS. Il est préférable de faire la mise à jour des Firmwares et BIOS/UEFI afin d'avoir accès aux dernières fonctionnalités et derniers correctifs (cela inclus aussi les dernières mises à jour des signatures pour le secure boot). Le but du Secure Boot, est comme son nom l'indique de sécuriser le démarrage de la machine, en bloquant le démarrage de pilotes ou de systèmes d'exploitation qui ne sont pas signés avec le bon certificat (<http://www.digitaltrends.com/computing/microsoft-secure-boot-tool-policy-patched/> et <http://www.zdnet.com/article/microsoft-secure-boot-key-debacle-causes-security-panic/>). Le fonctionnement interne du Secure boot est disponible ici : <http://blog.fpmurphy.com/2012/11/list-secure-boot-certificates.html#sthash.017GU8ky.dpbs>

Attention dans le cas d'une mise à jour de vSphere 5.5 ou 6.0 vers 6.5, il est nécessaire de lancer le script : `/usr/lib/vmware/secureboot/bin/secureBoot.py` (<https://kb.vmware.com/kb/2147606>).

La mise en place du Secure Boot au niveau de l'ESXi est liée à la configuration de l'UEFI de la machine physique. Il force l'utilisation de VIB certifiée par VMware.

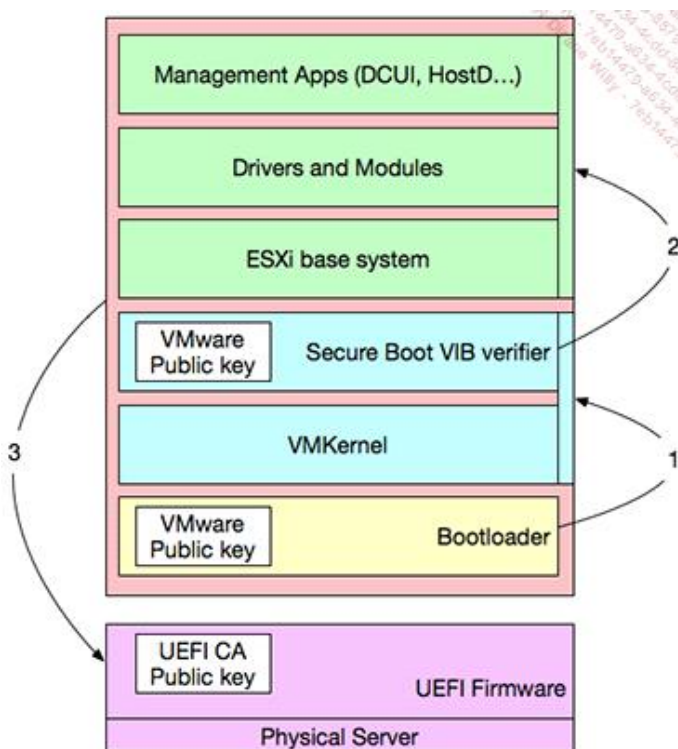
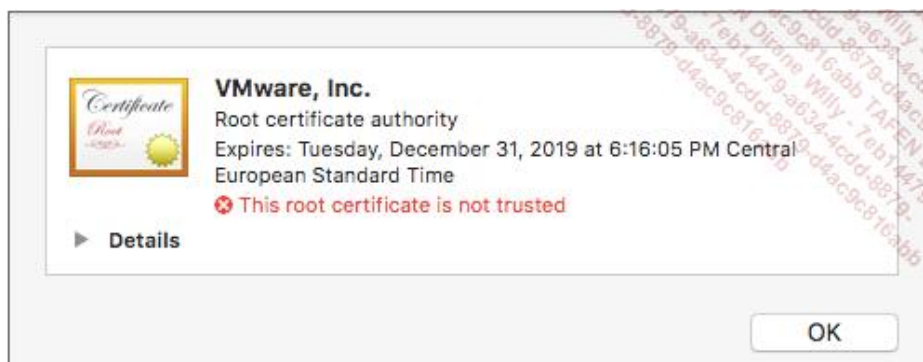
1. Lors du démarrage de l'ESXi le bootloader contient une clé publique de VMware. Le bootloader utilise cette clé

pour vérifier chaque composant depuis la signature de kernel aux sous-systèmes tel que le Secure Boot VIB Verifier.

2. Le VIB Verifier vérifie la signature de chacune des VIBs qui sont installés dans le système.

3. Le système démarre avec la chaîne de certificat validée de l'UEFI.

Attention, si après la mise à jour du microcode UEFI, il n'est toujours pas possible d'utiliser le Secure Boot avec vSphere 6.5, il est nécessaire de contacter le constructeur, afin qu'il vous donne la marche à suivre pour intégrer le certificat de VMware. Dell supporte vSphere 6.5 avec UEFI depuis la génération 13 des serveurs de la gamme Power Edge (en.community.dell.com/techcenter/extras/m/white_papers/20443328/download). Nous aurons le même problème avec AutoDeploy (<https://kb.vmware.com/kb/2148532>) (le certificat, fourni au moment de l'écriture de ce livre, est valide jusqu'au 31 décembre 2019).

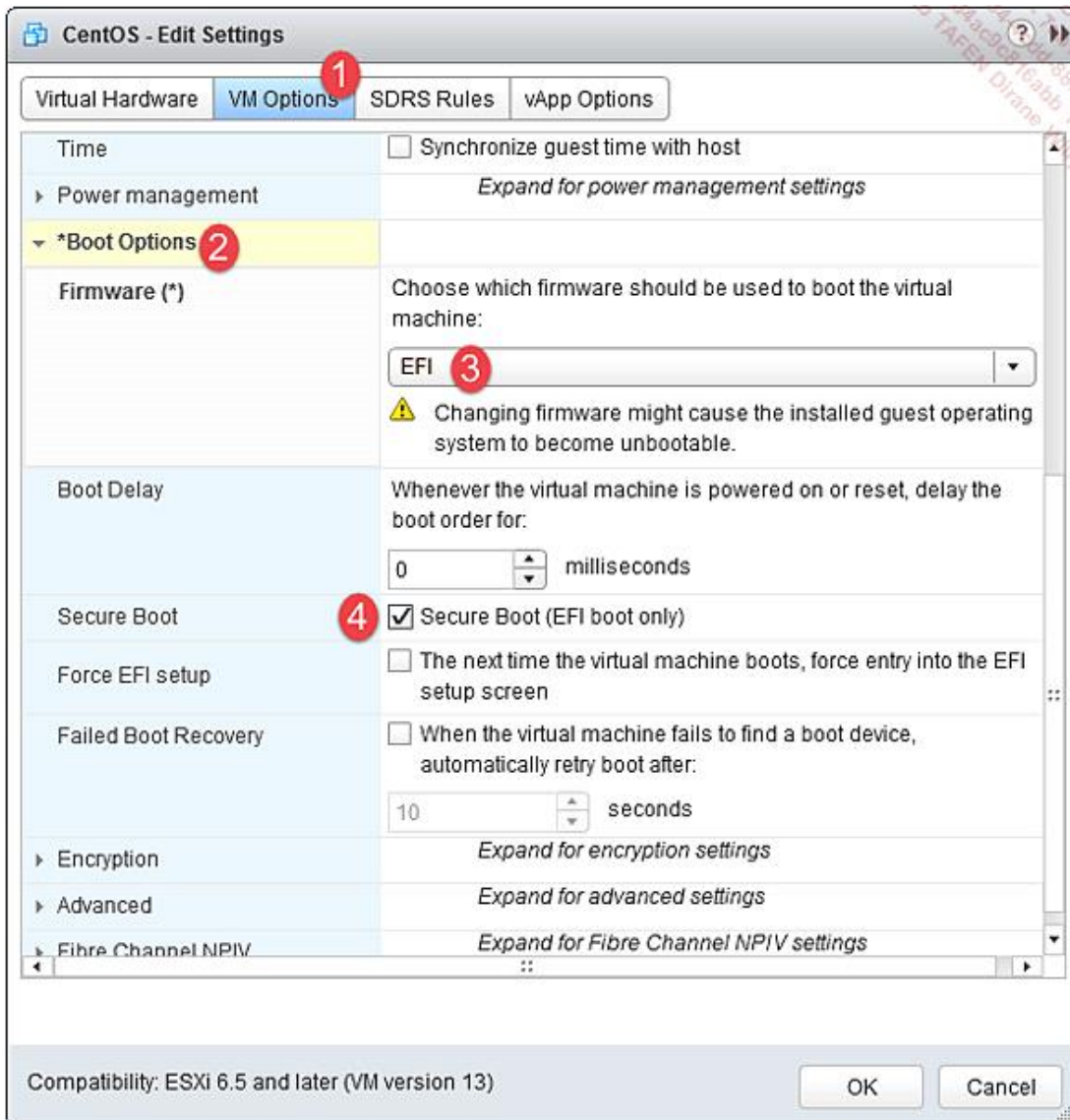


a. Le SecureBoot pour les machines virtuelles

Tout comme pour un serveur ESXi, le Secure Boot force l'utilisation de pilotes signés pour démarrer le système d'opération. L'activation du Secure Boot sur une machine virtuelle est facile. Attention cependant, le fait de faire évoluer la configuration de la machine virtuelle du BIOS, vers l'UEFI peut avoir un impact sur le système d'exploitation (instabilité, problème de démarrage...).

Il est nécessaire d'avoir installé les VMware Tools en version 10.1 minimum et le matériel virtuel en version 13. De plus, il faut retirer le composant VMware Host-Guest Filesystem pour les machines virtuelles Linux avant de pouvoir utiliser le Secure Boot.

Pour activer le Secure Boot, il faut aller dans les paramètres de la VM, puis dans les options de VM (**VM Options**) (1), puis les options de boot (**Secure Boot**) (2), afin d'activer l'EFI (3) et sans oublier de cocher l'activation du **Secure Boot** (4).



Dans le cas où l'on désire remplacer le certificat utilisé lors du Secure Boot au sein d'une VM, il est nécessaire de modifier la configuration du fichier VMX de la VM (<https://communities.vmware.com/thread/554062?start=0&tstart=0>).

3. Gestion des droits

Il existe une relation entre la vue sur la partie PSC (certificats, SSO) et le Web Client vSphere. Une partie des informations disponibles au niveau du PSC est renvoyée au Web Client.

a. Interaction avec l'Active Directory

L'intégration des composants d'une infrastructure de virtualisation dans un Active Directory simplifie la gestion des

accès par rôles (*Role Based Access Control* - RBAC), en se basant sur la gestion des groupes Active Directory. Dans le cas contraire, nous devons gérer au niveau du vCenter la création des groupes et utilisateurs. Quelle que soit la manière dont nous gérons les accès utilisateurs, une règle de base en matière de sécurité est leur fournir le minimum de droits nécessaires tout en leur permettant de faire les tâches quotidiennes.

L'intégration de la VCSA dans l'Active Directory est assez simple, via une simple ligne de commande :

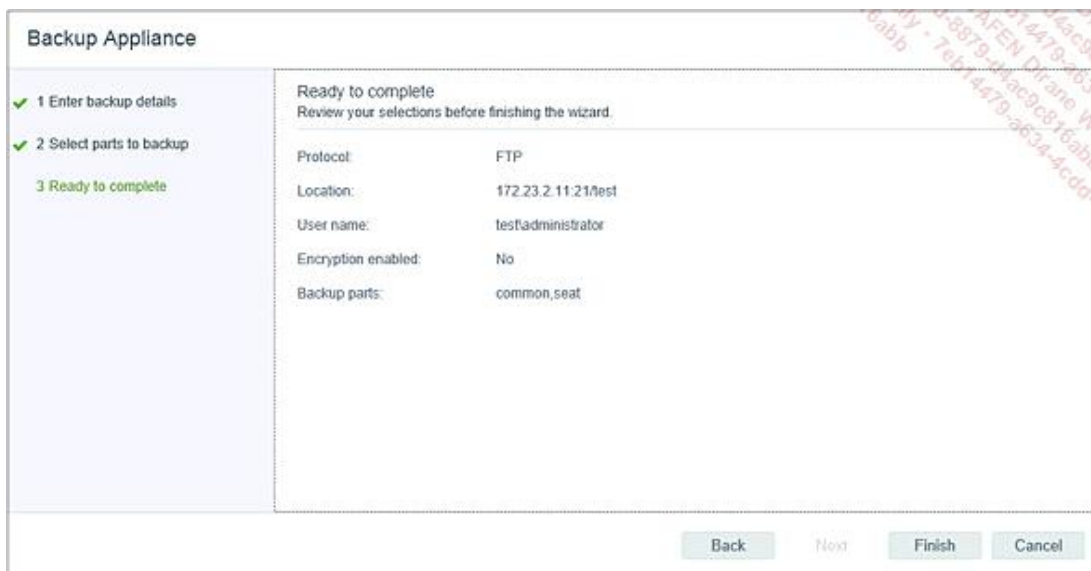
```
root@vcsa [ /opt/likewise/bin ]# /opt/likewise/bin/domainjoin-cli join test.lab administrator
Joining to AD Domain: test.lab
With Computer DNS Name: vcsa.test.lab

administrator@TEST.LAB's password:

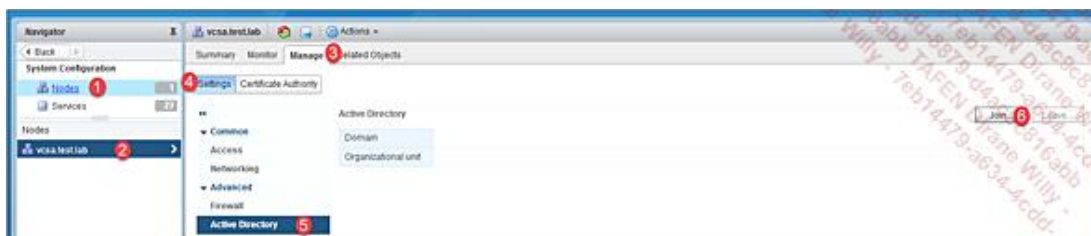
SUCCESS
```

Il est possible de choisir l'Unité d'Organisation (OU) en détaillant le chemin complet de OU sous sa forme distinguished name « ou=ESXi,ou=Infrastructures,ou=Servers,dc=test,dc=lab ».

En mode graphique, il faut se rendre dans le menu **Général**, puis dans **System Configuration** (1).

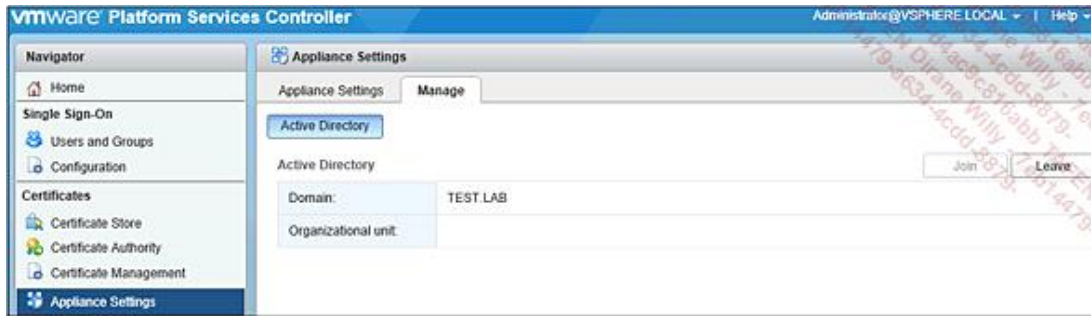


Dans **System Configuration**, allez dans **Nodes** (1), puis sélectionnez le VCSA (2). Dans **Manage** (3), allez dans **Settings** (4), puis **Active Directory** (5) afin d'avoir accès à la fonctionnalité d'intégration au domaine (6). Mettez le domaine, le nom de l'OU où le vCenter devra être créé et renseignez le compte ayant le droit de créer l'objet Active Directory.

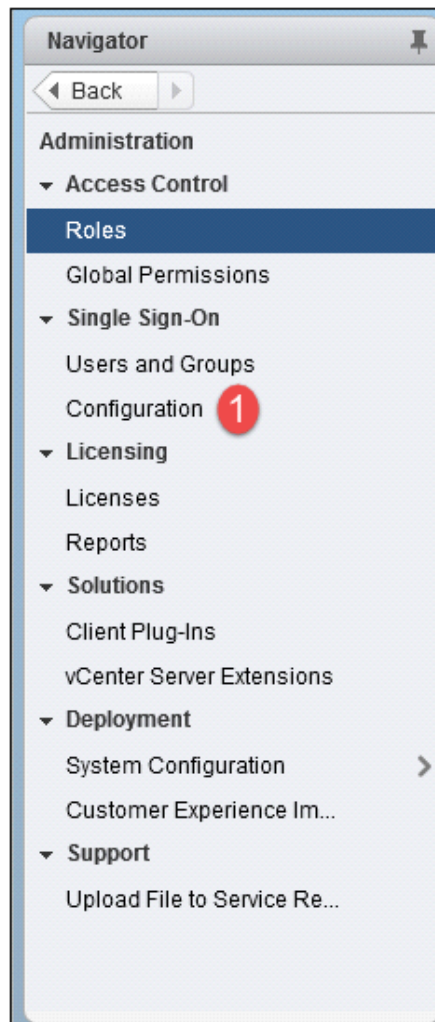


Après le redémarrage, allez dans la partie SSO.

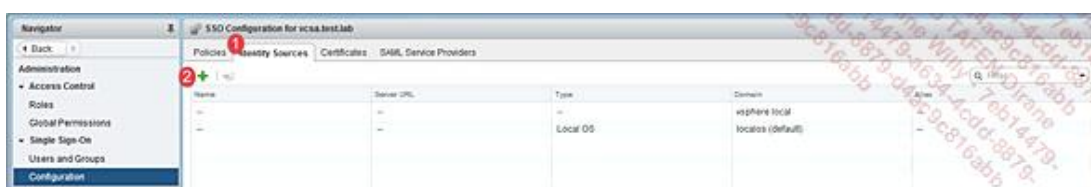
Il est possible d'arriver au même écran beaucoup plus simplement en se connectant sur le PSC ([https://\[vcenter FQDN\]/psc](https://[vcenter FQDN]/psc)).



Puis occupez-vous de l'ajout de l'Active Directory en tant que source d'identité via le menu **Configuration** (1).

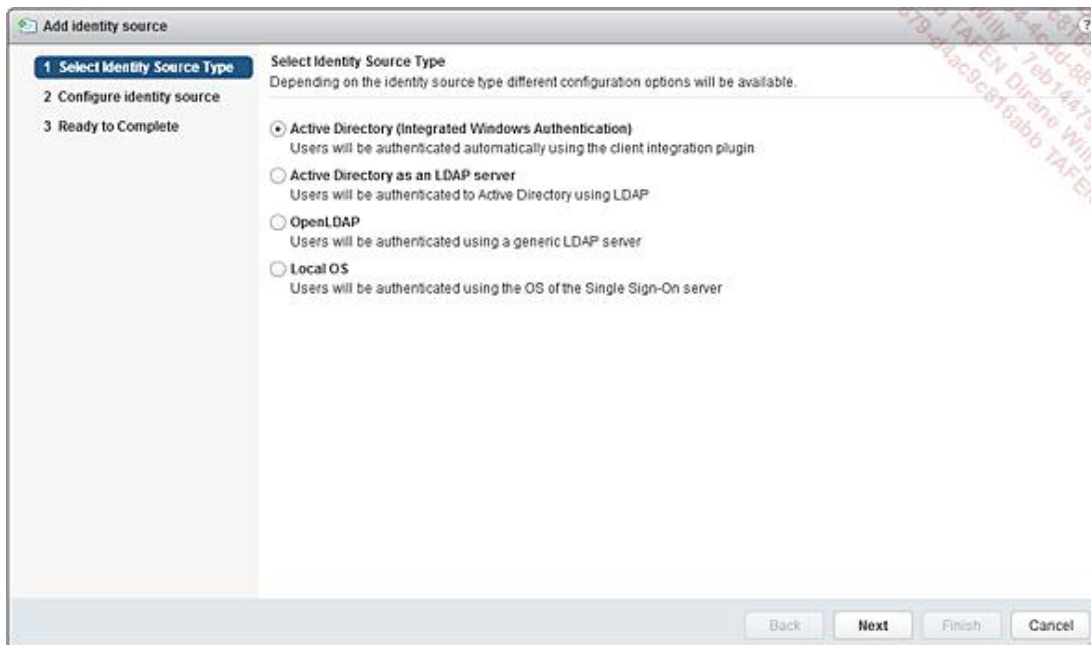


Allez dans l'onglet **Identity Sources** (1) et cliquez sur le + (2).

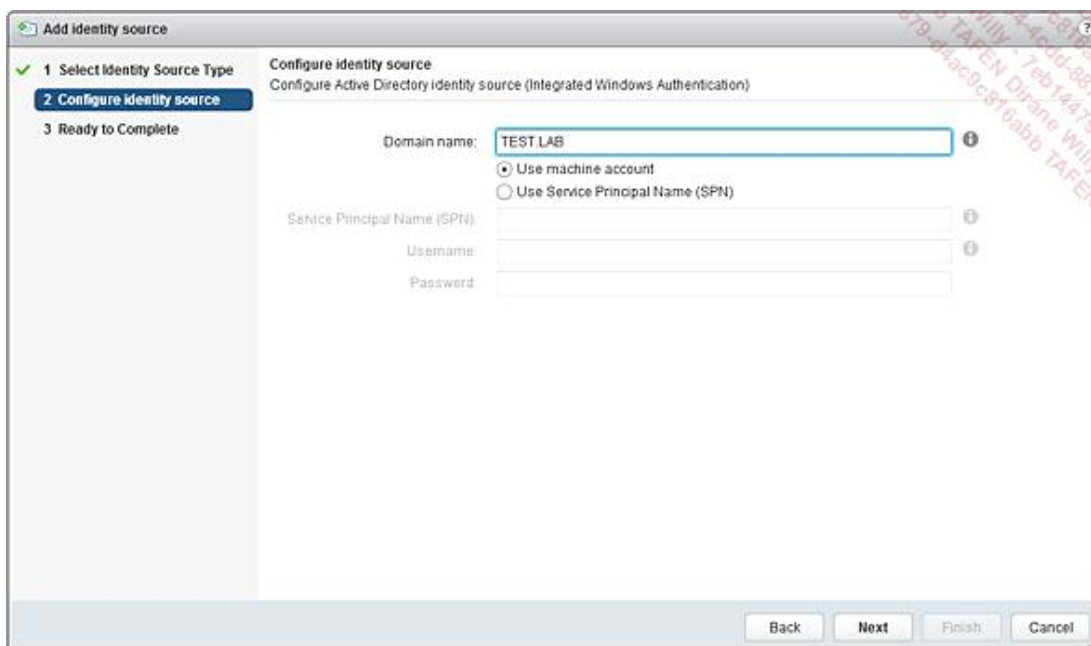


Vous avez le choix entre :

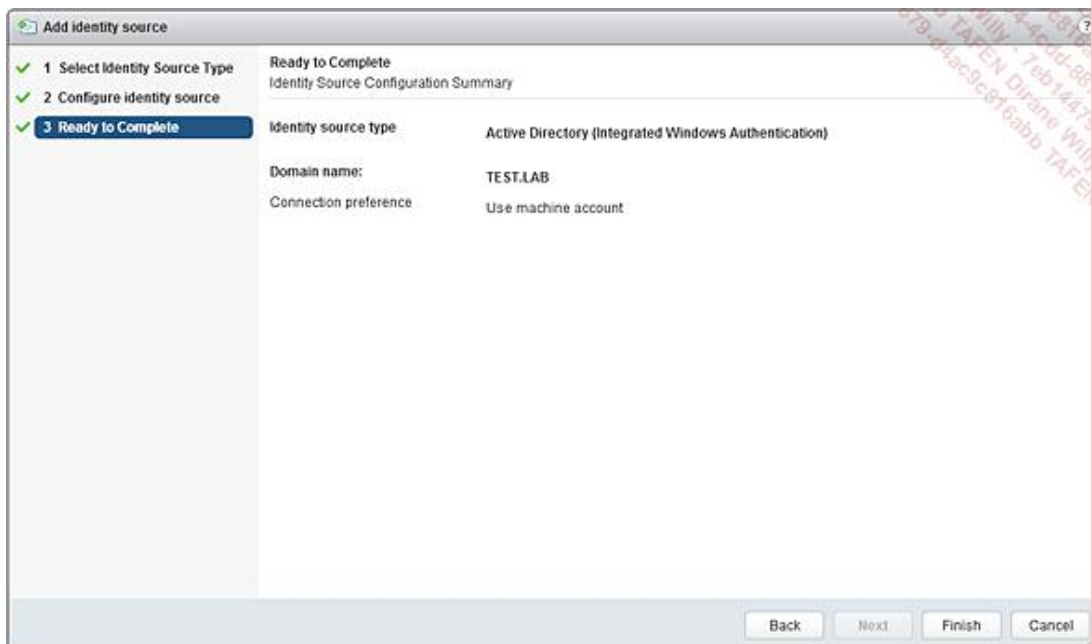
- l'authentification intégrée de Windows via l'Active Directory,
- l'Active Directory en tant qu'annuaire LDAP,
- l'Open LDAP,
- le vCenter SSO (Local OS).



Ici, il s'agit d'utiliser l'Active Directory (c'est cette option que l'on préférera si le serveur vCenter fait partie du domaine à utiliser comme source d'identité. Pour les domaines « suivants », utilisez l'option **Active Directory as an LDAP Server**).



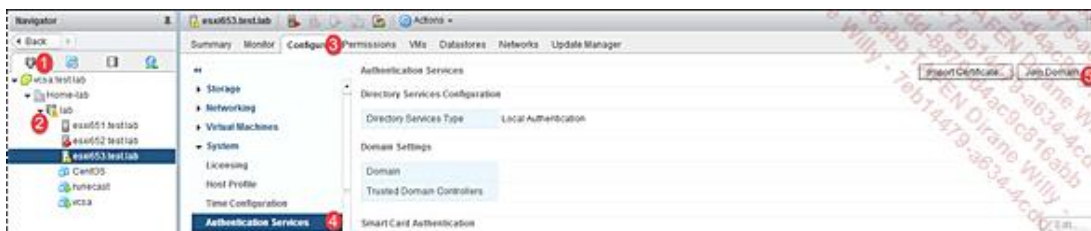
Validez.



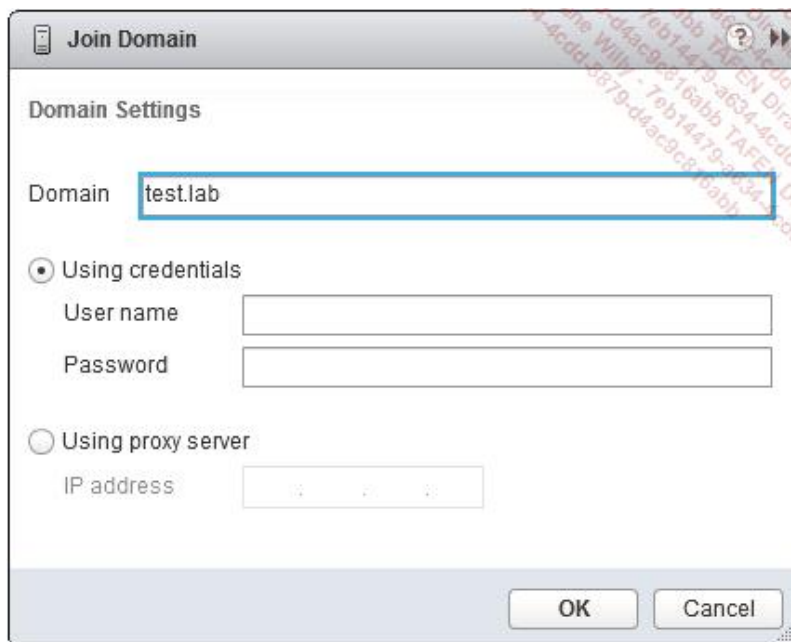
Dans le cas des ESXi, et selon votre infrastructure et vos droits, vous devrez précréer le compte d'ordinateur et le groupe d'administration par défaut : ESX Admins dans l'Active Directory (<https://kb.vmware.com/kb/1025569>). Ce groupe est lié aux options avancées de l'ESXi (Config.HostAgent.plugins.hostsvc.esxAdminsGroup et ses options associées esxAdminsGroupAutoAdd, esxAdminsGroupUpdateInterval) et permet un contrôle total sur l'ESXi.

Les opérations dans ce cas se compliquent légèrement, nous avons la possibilité d'utiliser :

- Soit une connexion directe à l'Active Directory sous la forme Domaine/Ou1/Ou2



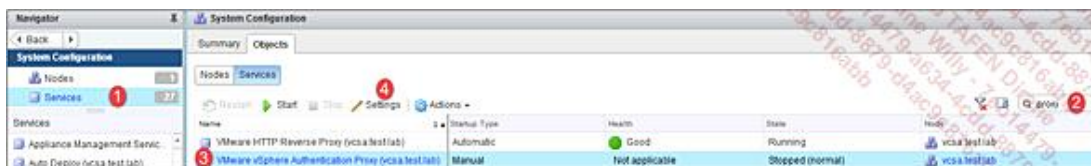
Les points 1 à 4 correspondent au chemin permettant d'avoir accès à l'option **Join domain**, où l'on va rentrer le nom de notre domaine Active Directory et le compte ayant les droits de faire l'ajout au domaine.



- Soit via un proxy.

L'intérêt de la connexion via un proxy est de limiter la diffusion du compte Active Directory qui permet d'ajouter un serveur ESXi à l'Active Directory sans avoir d'authentification à faire lors de l'utilisation la fonction Auto Deploy.

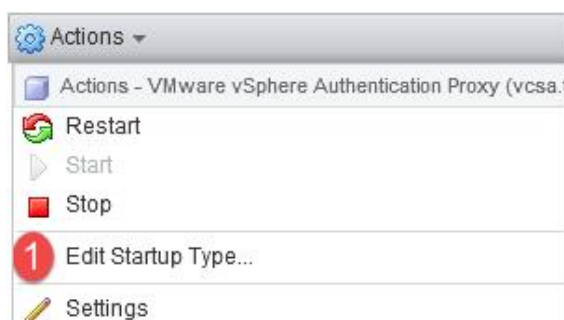
Vous devez démarrer le service VMware vSphere Authentication Proxy.



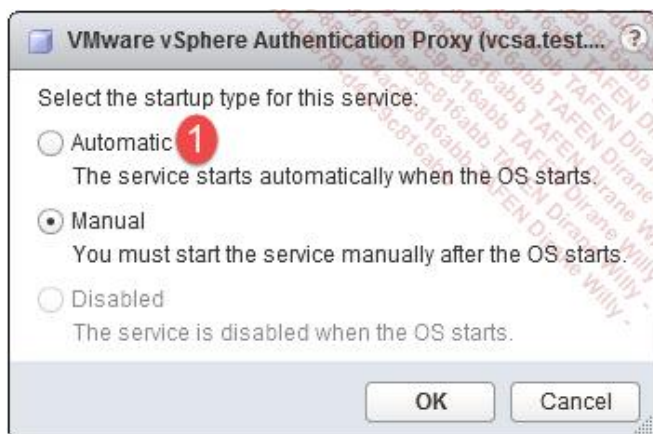
Les points 1 à 4 montre comment rechercher le service proxy.



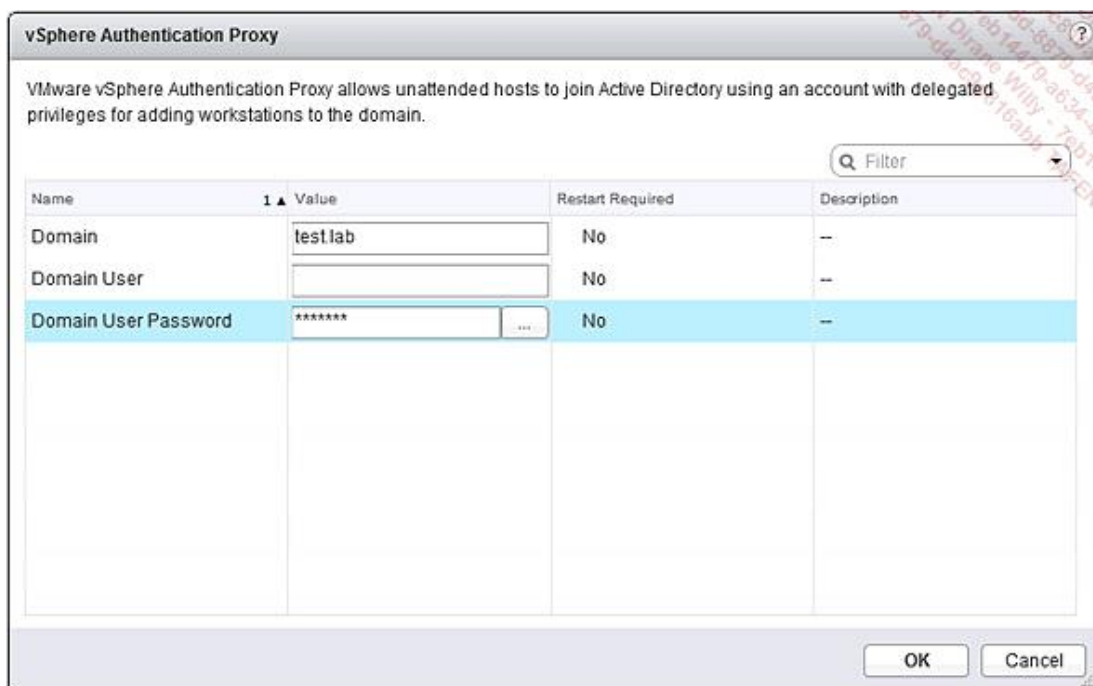
Une fois activé (1), modifiez les paramètres de démarrage du service (2) qui est en mode manuel.



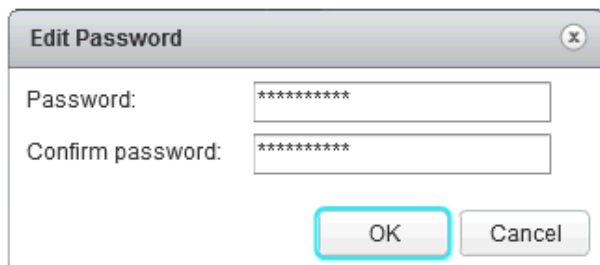
Passez-le en mode automatique.



Puis configurez le compte qui sera utilisé pour ajouter les serveurs ESXi dans le domaine. Si le compte n'a pas les droits de création d'objet de type ordinateur, il faudra les précréer manuellement (3).



Confirmez le mot de passe.



En ligne de commande, la même opération se fait en une ligne.

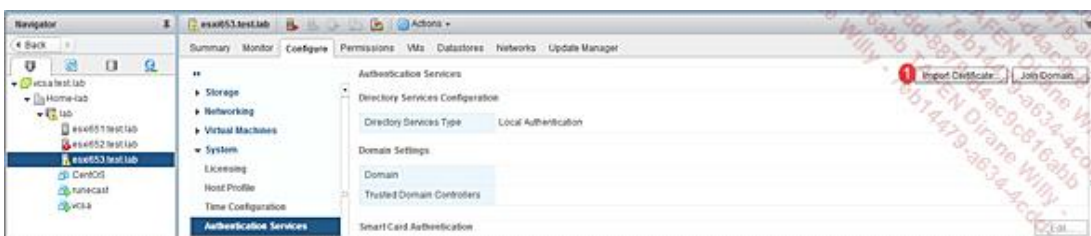
```
root@vcsa [ ~ ]# /usr/lib/vmware-vmcam/bin/camconfig add-domain -d test.lab -u administrator
Enter password for administrator:
Domain added successfully.
```

Vous pouvez renforcer la sécurité en forçant la vérification des certificats du client.

```
root@vcsa [ /usr/lib/vmware-vmcam/bin ]# /usr/lib/vmware-vmcam/bin/camconfig ssl-cliAuth -e
Flag set successfully. Webserver restarted.
root@vcsa [ /usr/lib/vmware-vmcam/bin ]#
```

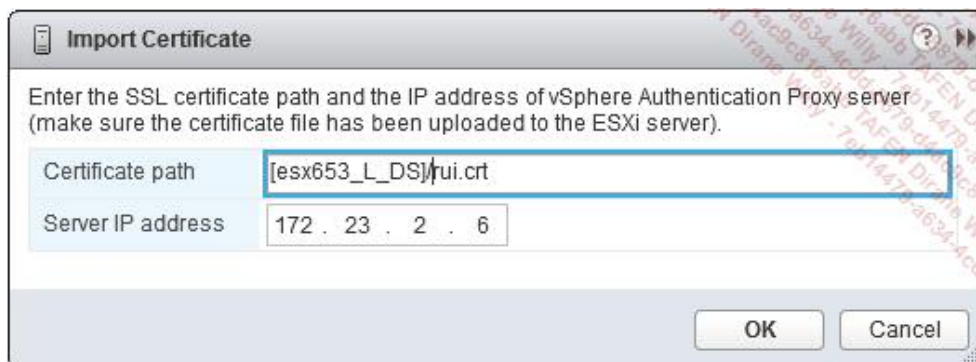
Il reste à faire la configuration au niveau de l'ESXi.

Importez le certificat du vSphere Authentication Proxy server. Il se trouve au sein du vcenter (/var/lib/vmware/vmcam/ssl/rui.crt pour l'appliance ou C:\ProgramData\VMware\VCenterServer\data\vmcamd\ssl\rui.crt pour la version Windows).



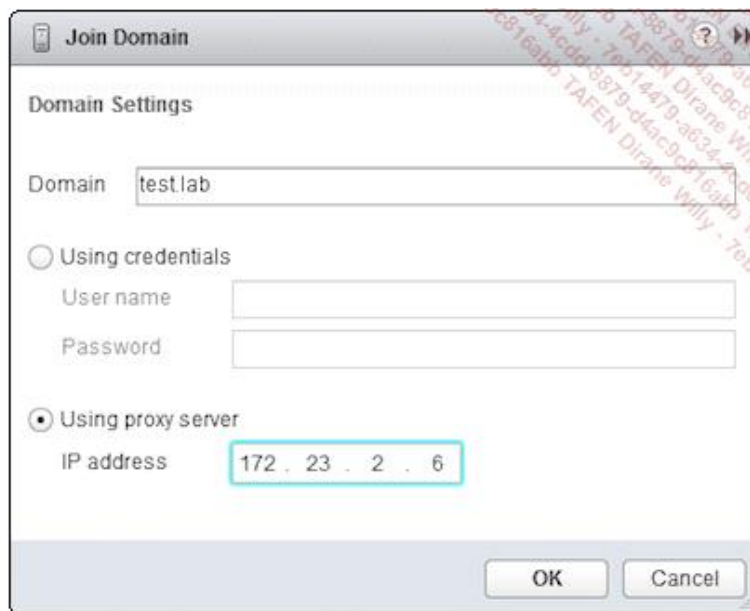
Attention, vous n'avez pas de moyen de chercher le certificat sur le bureau Windows. Le plus simple restant de le déposer dans un datastore.

Puis spécifiez l'adresse IP du serveur Proxy.



Il est possible d'utiliser la VMCA afin de générer le certificat, VMware fournit les commandes nécessaires dans le guide d'exploitation du proxy (<https://pubs.vmware.com/vsphere-65/index.jsp?topic=%2Fcom.vmware.vsphere.security.doc%2FGUID-AEA12D51-3959-4B51-9306-E74BC50643DB.html>).

Il reste à intégrer l'hyperviseur à l'active directory via le proxy que vous venez de configurer.



b. L'authentification forte ou à deux facteurs

La nouveauté au niveau de l'authentification dans une infrastructure vSphere est la mise en place d'authentification forte.

On l'active à deux niveaux :

- Le premier niveau est l'ESXi. Via le vCenter, il est possible d'activer l'utilisation des cartes à puces (ce qui nécessite un lecteur USB). Lorsque l'on se connecte sur la console de l'ESXi (DCUI), il demandera le code secret à la place de la traditionnelle boîte de discussion utilisateur et mot de passe. Il est possible de revenir à la connexion traditionnelle en appuyant sur F3. Juste sous l'ajout de l'ESXi dans le domaine se trouve l'option qui active la gestion des cartes à puce.

Pour activer les cartes à puces, il suffit de trois actions :

- 1 Cliquez sur **Edit**.
- 2 Cochez l'activation.
- 3 Ajoutez les certificats de l'infrastructure de clés publiques qui authentifiera les cartes à puces.

- Le second niveau est celui du vCenter. Dans le cas du vCenter, il est possible de se connecter via une carte à puce ou via une authentification RSA.

Dans le cas de l'authentification RSA, VMware recommande la lecture de deux articles (<https://blogs.vmware.com/vsphere/2016/04/two-factor-authentication-for-vsphere-rsa-secrid.html> et <https://blogs.vmware.com/vsphere/2016/04/two-factor-authentication-for-vsphere-rsa-secrid-part-2.html>) de Mike Foley.

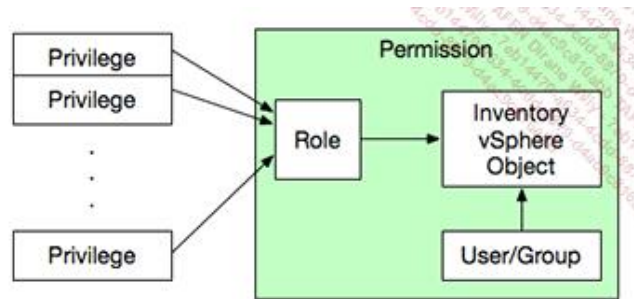
Dans le cas de la carte à puce, il y a des prérequis à mettre en place au niveau du PSC. Dans la version 6.0U2, il faut configurer le serveur Tomcat, et dans la version 6.5, il faut configurer le reverse proxy, puis activer et configurer l'authentification par carte à puce.

c. La gestion des privilèges, rôles, permissions d'accès

La gestion des accès à une infrastructure vSphere, est identique à la gestion des accès dans une infrastructure LDAP (Active Directory ou non). Nous créons un utilisateur, à qui nous donnons des droits ou permissions (*Access Control List* - ACL) en lecture et/ou écriture (ou autres) sur une ressource via un groupe d'accès.

Dans une infrastructure vSphere, nous avons les privilèges qui sont associés pour former un rôle. Nous avons les utilisateurs que nous regroupons dans des groupes. Nous faisons l'association d'utilisateur/groupe (vSphere

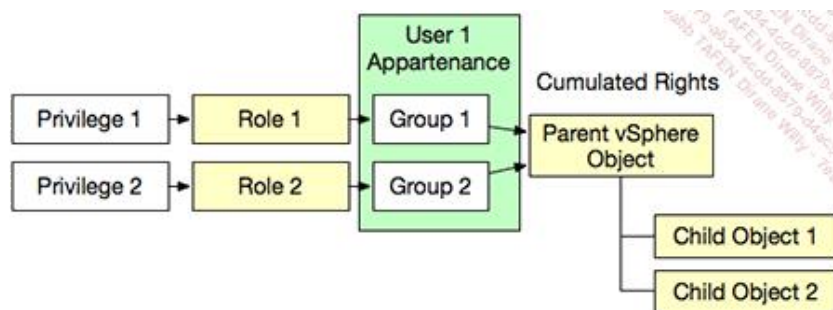
Single Sign One - SSO, Active Directory...) avec un rôle sur un objet de l'inventaire vSphere (machine virtuelle, serveur ESXi, cluster...) que ce soit au niveau du vCenter ou du serveur ESXi, ce qui donne une permission.



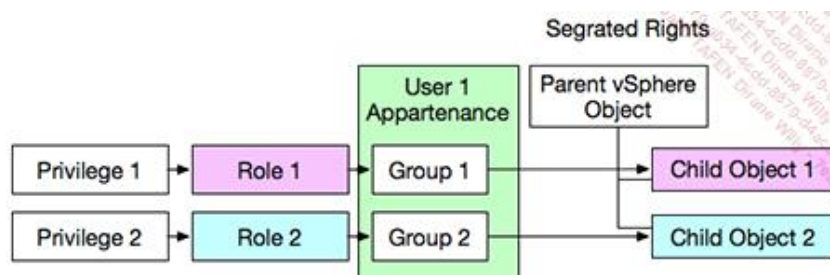
Il est possible de propager cette nouvelle permission sur l'ensemble de l'inventaire sous-jacent (les sous-dossiers et objets vSphere).

Attention aux imbrications de groupes. Si nous avons deux types de droits différents tels qu'un droit étendu et un droit restrictif à un même niveau sur les objets de l'inventaire, nous serons limités par le droit le plus restrictif.

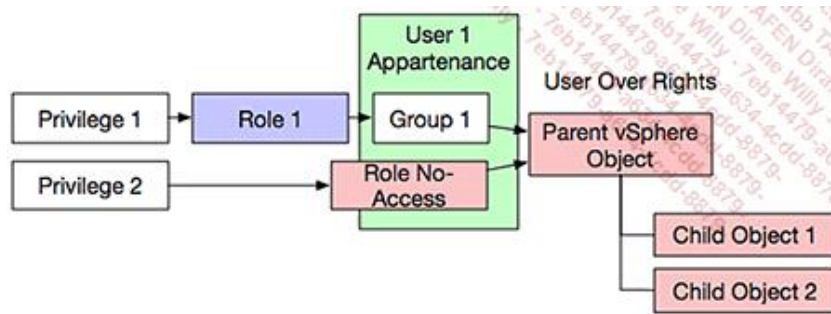
Nous pouvons résumer cela par les trois schémas suivants :



Les droits cumulés



Les droits ségrégés



Les droits restreints

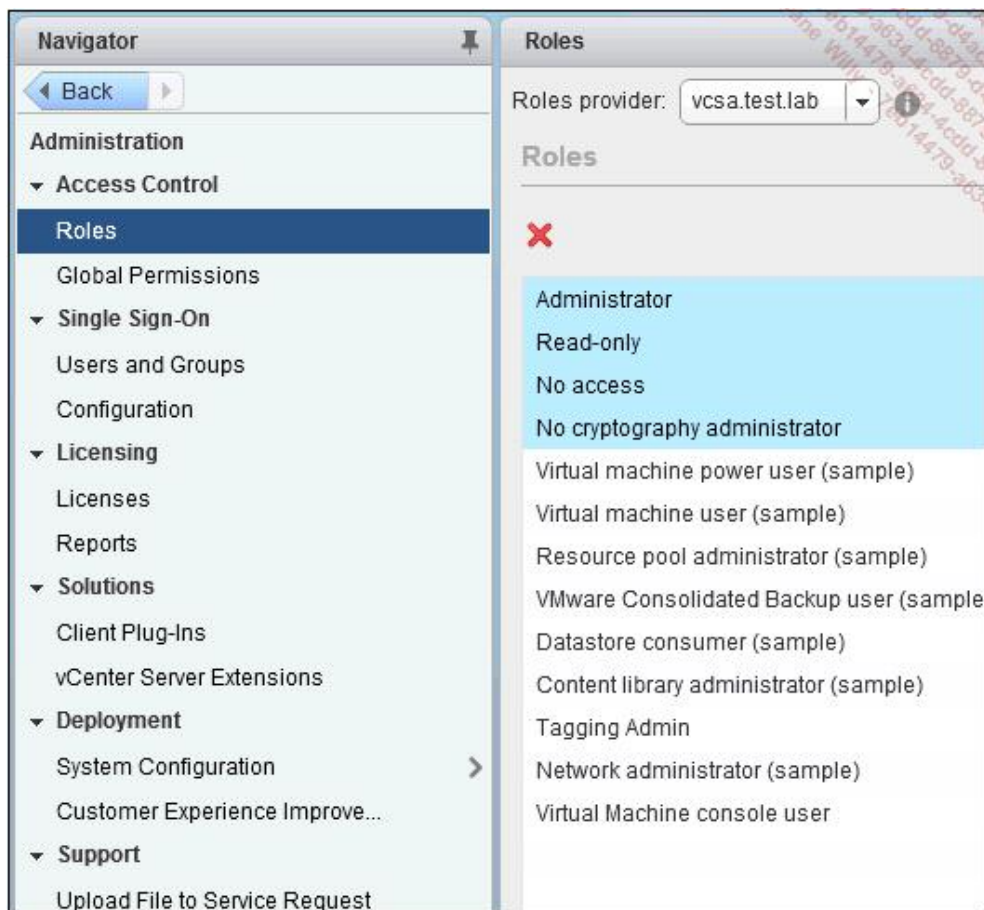
Il existe deux types de permissions au sein d'une infrastructure de virtualisation VMware :

La première donne des droits sur l'arborescence d'objets vCenter (inventaire). On donne des droits et accès permettant d'exécuter les tâches quotidiennes.

La seconde donne des droits sur les objets globaux (vCenter, VMware Orchestrator...) et permet de voir l'ensemble des objets de l'inventaire. Dans le cas du vCenter, les objets globaux sont les licences, les tags, les rôles et sessions.

VMware fournit un organigramme (<https://pubs.vmware.com/vsphere-65/index.jsp#com.vmware.vsphere.security.doc/GUID-03B36057-B38C-479C-BD78-341CD83A0584.html>) montrant l'arborescence des objets vSphere.

Il existe plusieurs types de rôles au sein d'une infrastructure vSphere chacun ayant des privilèges spécifiques.

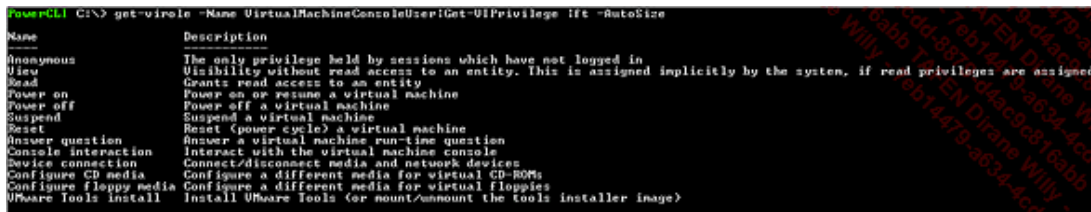


Le premier type de rôles correspond aux rôles dits système, ils ne sont pas modifiables :

- L'administrateur possède l'ensemble des droits, par défaut il s'agit du compte administrator@vsphere.local. Lors de la création du domaine SSO, l'administrateur SSO reçoit automatiquement le rôle administrateur vSphere.
- L'administrateur n'ayant pas de droits de chiffrement, ce rôle donne les mêmes privilèges que le rôle administrateur à l'exception des privilèges de chiffrements des machines virtuelles.
- Aucun accès : c'est le rôle par défaut de tout utilisateur ou groupe à l'exception des comptes administrator@vsphere.local, vpxuser.
- Lecture seule, comme son nom l'indique, ce rôle permet d'avoir accès aux informations (configuration et détails) en tant que lecteur uniquement. Aucune action de configuration ou modification n'est possible.

Le second type de rôles est les rôles exemples. VMware nous fournit des exemples de rôles permettant déjà de faire les tâches quotidiennes en fonction du principe de sécurité du droit minimal. Il est possible de les modifier. Il est cependant conseillé d'en faire des copies et de modifier les copies de ces rôles afin de pouvoir réutiliser les rôles génériques au besoin.

Exemple des permissions pour le rôle Virtual machine console user : `Get-Virole -name virtualmachineconsoleuser | get-viprivilege`



Name	Description
Anonymous	The only privilege held by sessions which have not logged in
View	Visibility without read access to an entity. This is assigned implicitly by the system, if read privileges are assigned
Read	Grant read access to an entity
Power on	Power on or resume a virtual machine
Power off	Power off a virtual machine
Suspend	Suspend a virtual machine
Reset	Reset (power cycle) a virtual machine
Answer question	Answer a virtual machine run-time question
Console interaction	Interact with the virtual machine console
Device connection	Connect/disconnect media and network devices
Configure CD media	Configure a different media for virtual CD-ROMs
Configure floppy media	Configure a different media for virtual floppies
VMware Tools install	Install VMware Tools (or mount/unmount the tools installer image)

L'explication de l'ensemble des privilèges est disponible sur le site de vmware : <https://pubs.vmware.com/vsphere-65/index.jsp#com.vmware.vsphere.security.doc/GUID-ED56F3C4-77D0-49E3-88B6-B99B8B437B62.html>

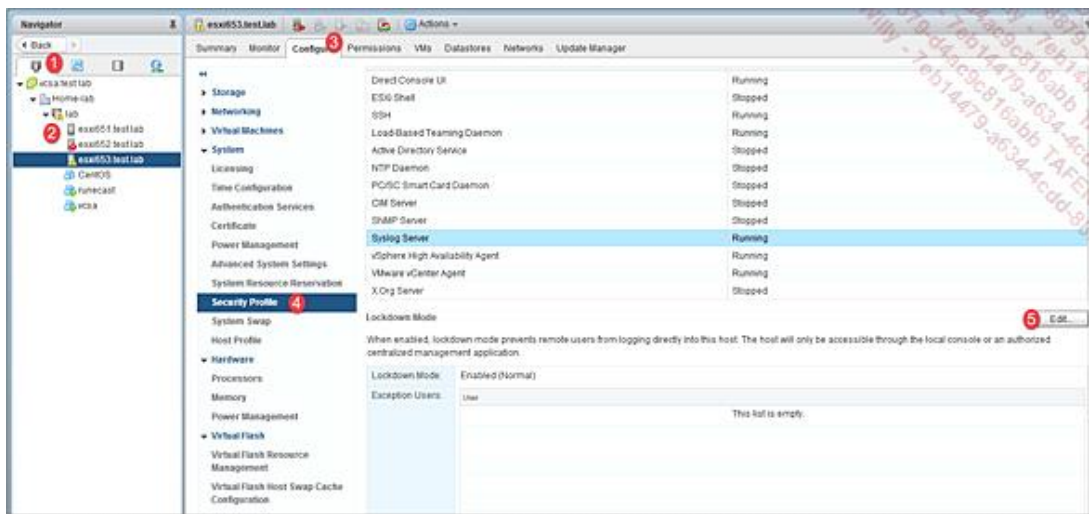
4. Verrouillage

Le verrouillage ou le lockdown en anglais est une option qui permet de désactiver l'accès direct à la console ESXi. Depuis la version 6.0 de vSphere.

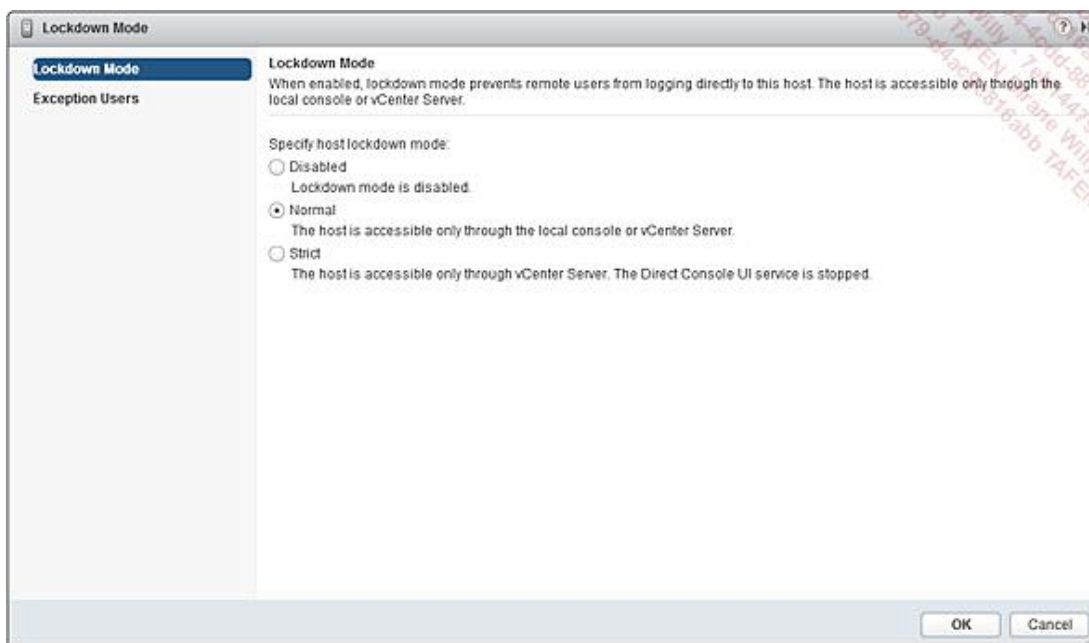
Il existe deux manières de le mettre en place :

- Depuis le client web, il permet de forcer les changements de configuration uniquement depuis le vCenter, l'accès en direct via le client web n'étant plus possible. Les deux modes de fonctionnement possibles sont :
 - Normal qui autorise tout compte ayant des droits d'administrateur à se connecter à l'ESXi, s'il fait partie de la liste d'exception ou de la liste définie dans l'option DCUI.access. Attention, la connexion doit se faire via le vCenter ou en local sur la console ESXi.
 - Strict qui désactive le service DCUI du serveur ESXi, cela rend l'ESXi accessible uniquement depuis le vCenter. L'accès au serveur ESXi est toujours possible pour les comptes d'administrateurs étant déclarés dans la liste d'exception et dans l'option avancée dcui.access via le SSH et le shell. En cas d'activation de l'option alors que des utilisateurs non présents dans ces listes sont connectés, ils sont déconnectés depuis vSphere 6.0.

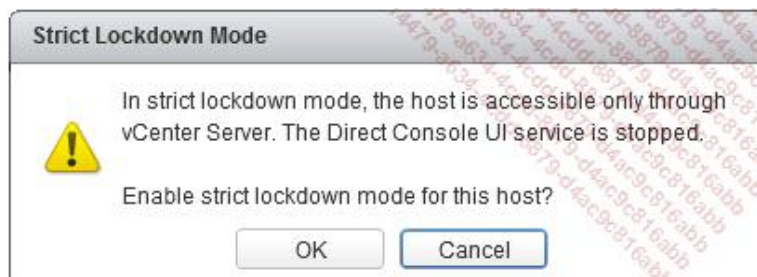
Pour configurer le verrouillage, il faut aller au niveau de l'hyperviseur (2), dans son profil de sécurité (4), puis cliquez sur **Edit** (5).



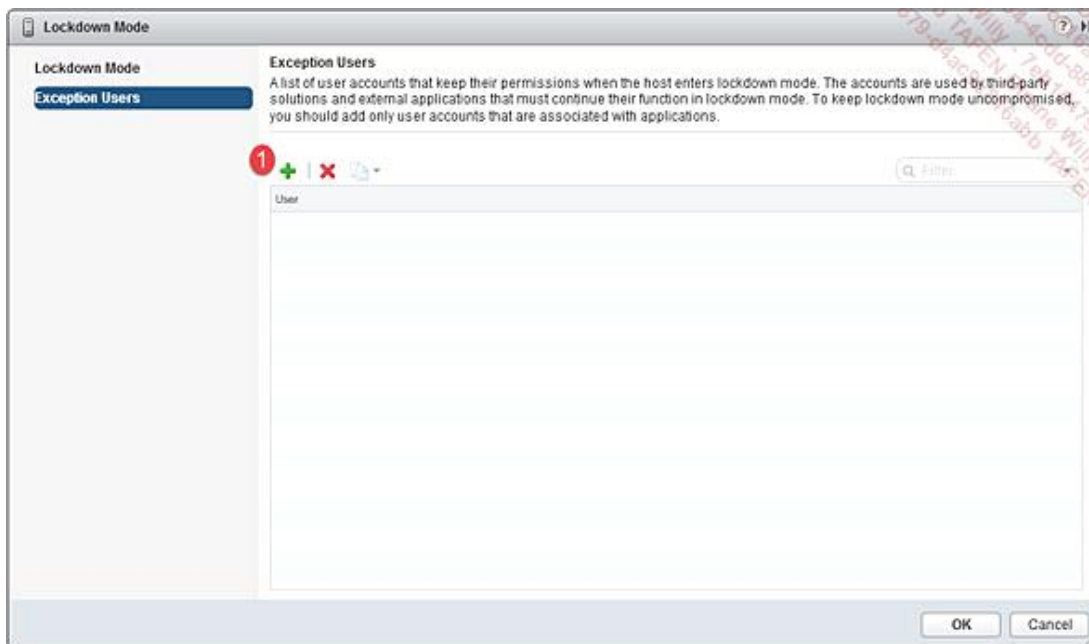
Sélectionnez le mode de verrouillage que vous désirez utiliser.



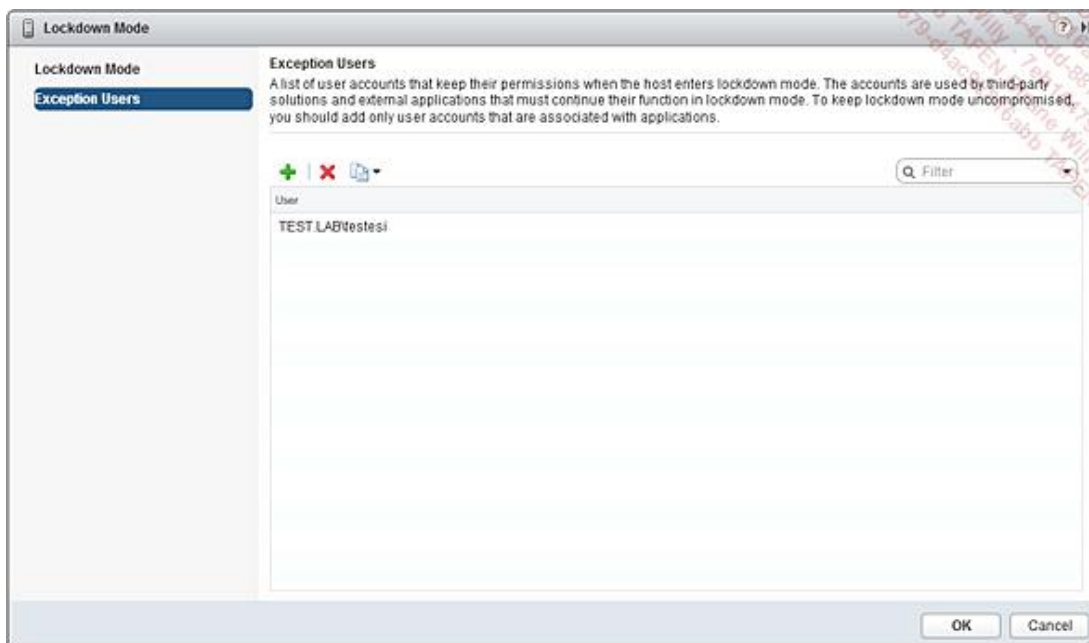
Dans le cas du mode strict, un message avertit que le service DCUI sera arrêté.



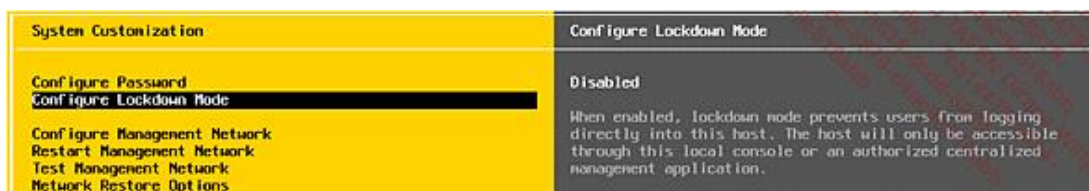
Vous devez ensuite gérer les exceptions (les comptes qui auront le droit de se connecter). Cliquez sur le bouton plus (en vert).



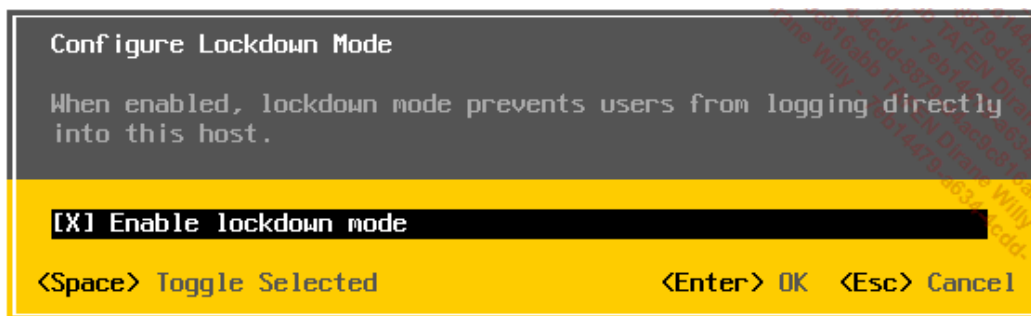
Cherchez le(s) compte(s) approprié(s).



Depuis le DCUI (*Direct Console User Interface*), vous avez uniquement accès au mode Normal. Il faut aller dans **Configure lockdown mode**.



Activez le lockdown.



La liste des exceptions est définie par le paramètre avancé DCUI.Access. Attention, nous parlons ici de comptes locaux sur l'ESXi, qu'il est possible de créer soit via les commandes PowerShell :

```
New-vmhostaccount -password $password -useraccount $useraccount_name
```

```
PowerCLI C:\> New-VMHostAccount -password qwe4r!! -Description "Test account" -useraccount testuser4
```

Name	Domain	Description	Server
testuser4		Test account	esxi652

Soit via les commandes propres à ESXi : `esxcli -server %server_esxi% -u root -p %password_root% system account add -id %login% -password %password% -password-confirmation %password%`

Un point d'attention sur le mot de passe car il doit répondre aux caractéristiques suivantes :

« Retry 3 min=disable, disable,disable,7,7 » définit par l'option avancée Security.PasszordQualityControl. L'explication de ses caractéristiques est disponible dans l'aide du module PAM_Passwdqc. La structure des informations passée au module est la suivante :

Name	Value
Security.PasswordQualityControl	retry=3 min=disabled,disabled,disabled,7,7

min=N0,N1,N2,N3,N4.

N0 : utilisation d'un mot de passe avec une classe de caractère.

N1 : utilisation d'un mot de passe avec deux classes de caractère.

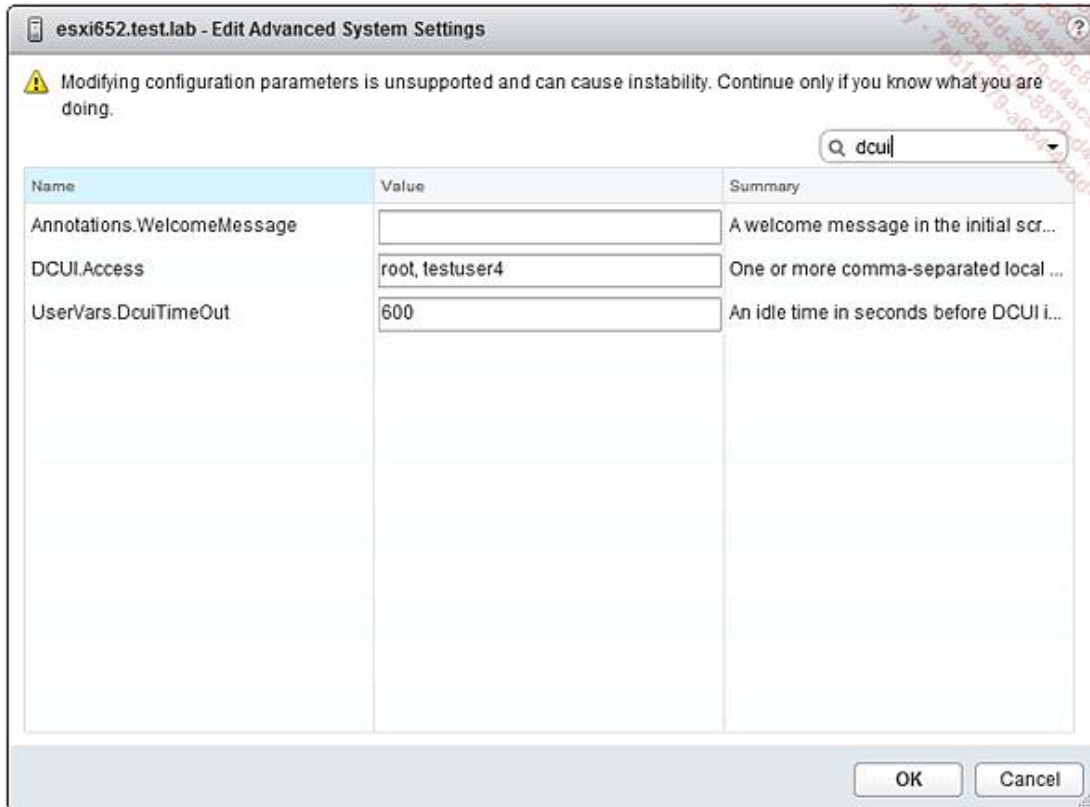
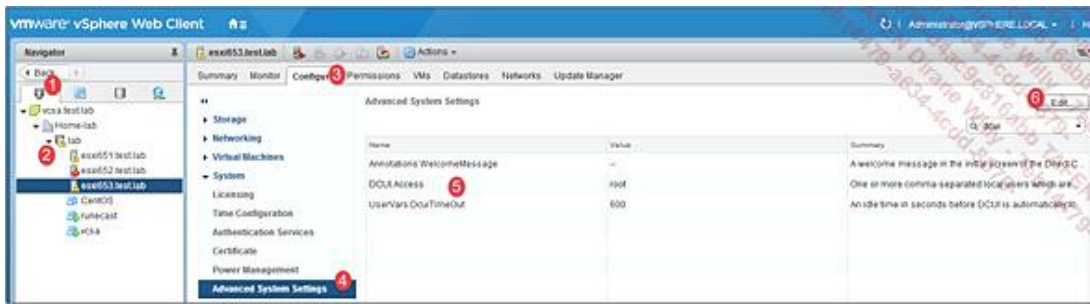
N2 : utilisation d'une passphrase.

N3 et N4 utilisation de 3 et 4 classes de caractères.

Disable signifiant que l'option est désactivée et 7 est la longueur minimale du mot de passe.

Attention, si une majuscule est utilisée en tant que premier caractère et un chiffre en dernier caractère, ils ne sont pas pris en compte.

Il reste à ajouter le compte créé dans la gestion des exceptions locales de l'hyperviseur. Pour cela il faut aller dans les paramètres avancés de l'hyperviseur (**Advanced System Settings**) (4), faire une recherche sur «dcui» puis sélectionner **DCUI.Access** (5) et l'éditer (6).



La fonctionnalité de lockdown peut se résumer par ce tableau.

Configuration à partir de	Lockdown Mode	Gestion des Accés d'exception	Changement de configuration
Web Client	Normal	dcui.access + user list	N/A
	Strict		DCUI Service disable
DCUI	Normal		N/A

5. VMware Update Manager

Nous avons vu dans le second chapitre que nous pouvions utiliser VUM afin de faire la mise à jour de l'hyperviseur d'une version à une autre comme de la 6.0 à la 6.5. Mais VUM ne sert pas seulement à cela et permet aussi de faire des mises à jour de sécurité et/ou de fonctionnalités. En d'autres termes, VUM fait de la gestion et du déploiement de correctifs (patch).