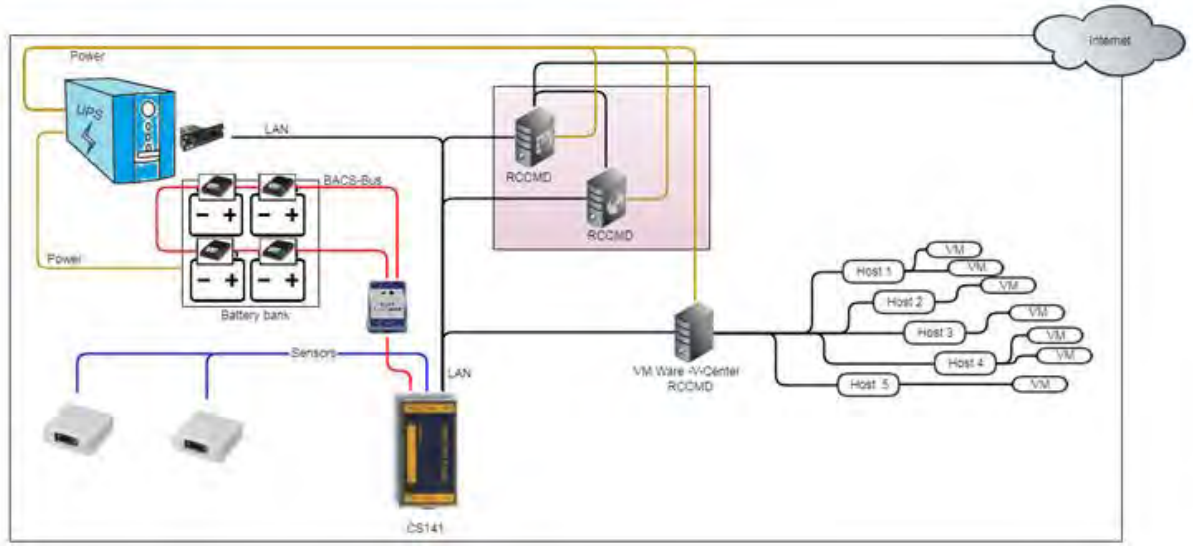
MANUEL UTILISATEUR

Logiciel Client RCCMD pour carte vmMiniSlot

Table des matières

INFOSEC UPS SYSTEM – 15, rue du Moulin – 44880 SAUTRON - FRANCE - www.infosec-ups.com
Hot Line – Tel + 33 (0)2 40 76 15 82 - Fax + 33 (0)2 40 94 29 51 - hotline@infosec.fr – 08 19 AA XX 202 09

1. Technologie RCCMD



RCCMD est utilisé pour éteindre le système en cas de panne. En effet, le serveur RCCMD (le plus souvent UPSMan ou la carte CS141/CS121) envoie des commandes d'extinction du système aux clients.

Plusieurs conditions sont à remplir :

1. Les clients RCCMD doivent avoir une adresse IP fixe.

Cette dernière doit être communiquée au serveur RCCMD pour qu'il leur envoie une commande d'extinction unique.

2. Le serveur RCCMD doit être autorisé à envoyer des requêtes.

Par défaut, RCCMD accepte toute diffusion émise par un serveur RCCMD. Si ces réceptions ne sont pas souhaitées, un émetteur autorisé peut être défini. Le client enregistrera toutes les autres commandes mais ne les exécutera plus.

3. Les ports suivants doivent être disponibles sur le réseau:

Port 8080 Est le port utilisé en local par l'interface web de RCCMD
Port 8443 Est le port utilisé pour l'accès à distance de l'interface web sur un autre ordinateur et/ou un serveur
Port 6003 Les clients RCCMD communique via ce port

2. Installation de l'appliance RCCMD avec Windows

Note : Le programme d'installation RCCMD utilise la version de Java Runtime Environment, qui est utilisée pour l'installation et la désinstallation. De plus, le configurateur Web RCCMD utilise un serveur Web Java. Vous pouvez désactiver le service RCCMD « RCCMDWebIf » dans l'administration des services et RCCMD s'exécutera sans Java.

2.1. Installation et configuration

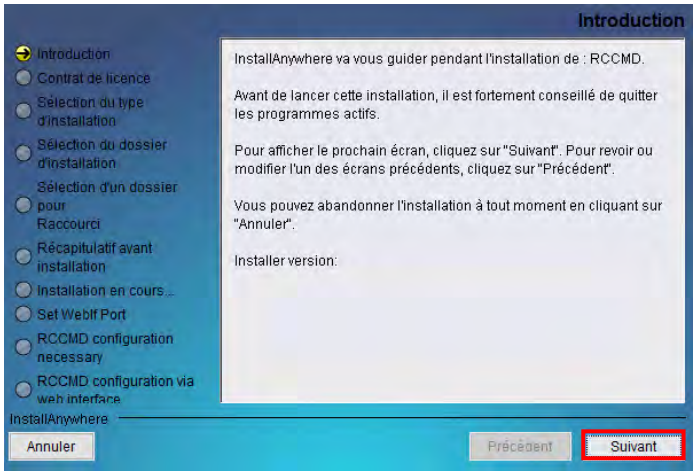
Avant de commencer l'installation, assurez-vous d'avoir tous les droits administrateurs. Sans avoir les droits, l'installation ne pourra pas aboutir.

Insérer le CD dans la machine ou télécharger RCCMD depuis https://www.infosec-ups.com/fr/accessoires-et-logiciels/logiciel-client-rccmd.html.

Menu « Introduction »

Dans le menu de démarrage vous pouvez voir les différentes étapes de l'installation.

Cliquer sur « Suivant ».



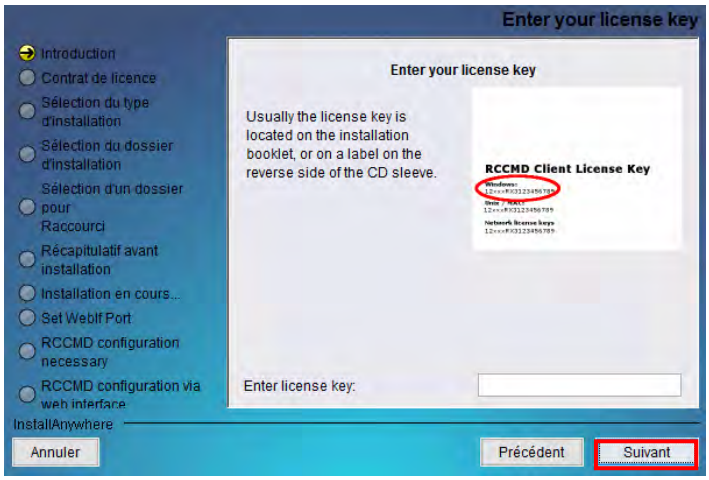
Menu « Contrat de licence »

Veuillez entrer votre clé de licence. La licence utilisée détermine quel module peut être installé.

Vous avez besoin d'une clé de licence spéciale pour votre logiciel RCCMD. Vous pouvez identifier la clé avec le « RX3 » dans la première partie de la clé de licence. La plupart du temps, vous devez commander la clé séparément.

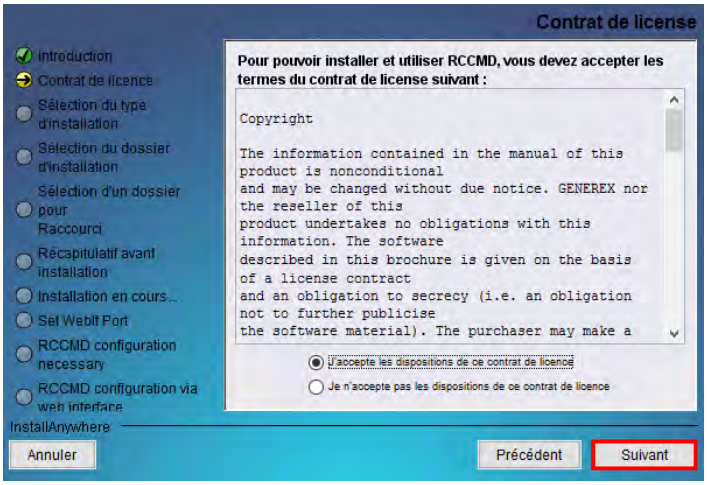
Cliquer sur « Suivant »

➔ Si vous n'entrez pas de clé de licence ou si vous l'avez mal saisie, RCCMD va automatiquement attribuer une licence d'évaluation de 30 jours.



Cocher « J'accepte les dispositions de ce contrat de licence ».

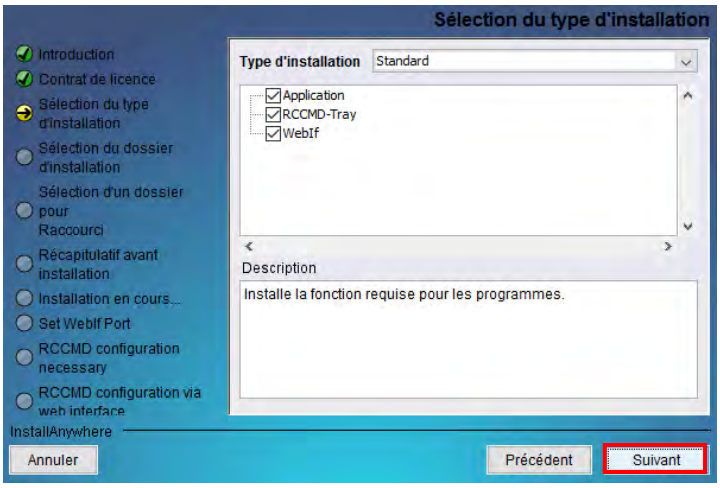
Cliquer sur « Suivant ».



Sélection du type d'installation

Sélectionner les élèments que vous souhaiter installer.

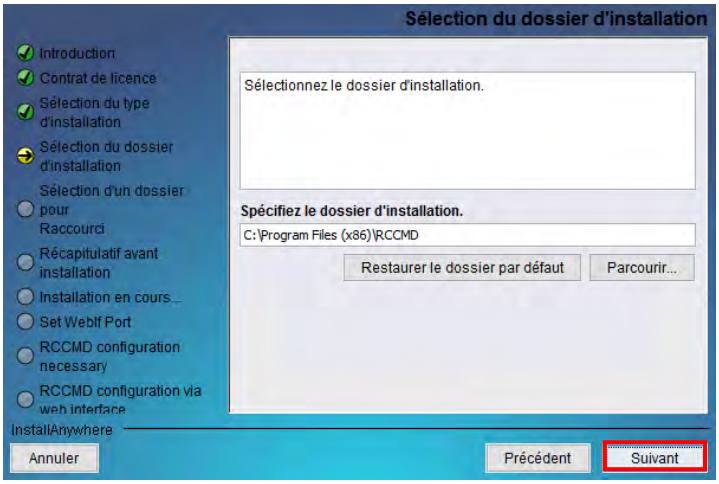
Cliquer sur « Suivant »



Sélection du dossier d'installation

Dans cet onglet, il est nécessaire de renseigner le chemin d'installation pour RCCMD. Par défaut, il se trouve dans « C\Program Files (x86) \RCCMD »

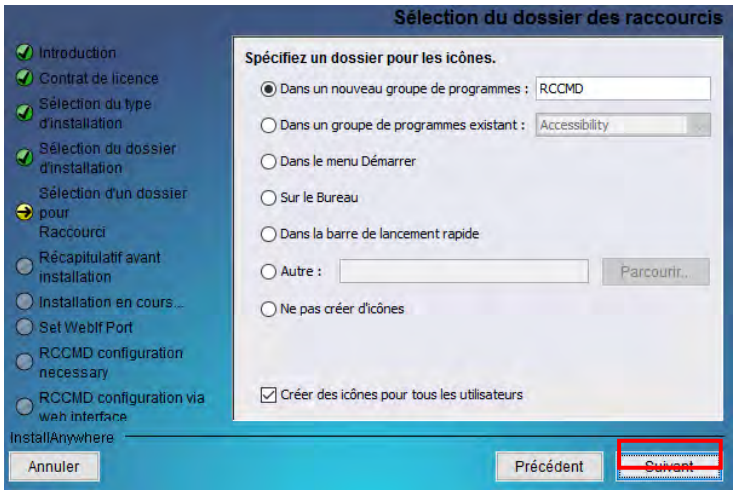
Cliquer sur « Suivant »



Sélection du dossier des raccourcis

Sélectionner l'endroit où sera stocké le raccourci pour accéder à RCCMD.

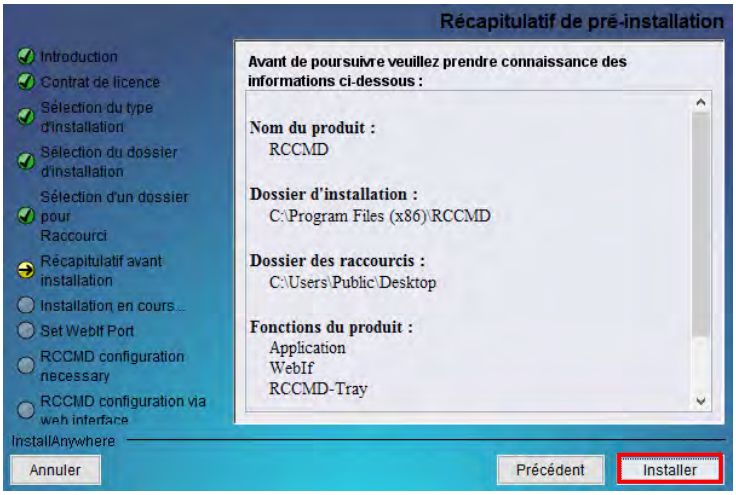
Cliquer sur « Suivant ».



Récapitulatif de pré-installation

Vérifier les informations que vous avez rentrées.

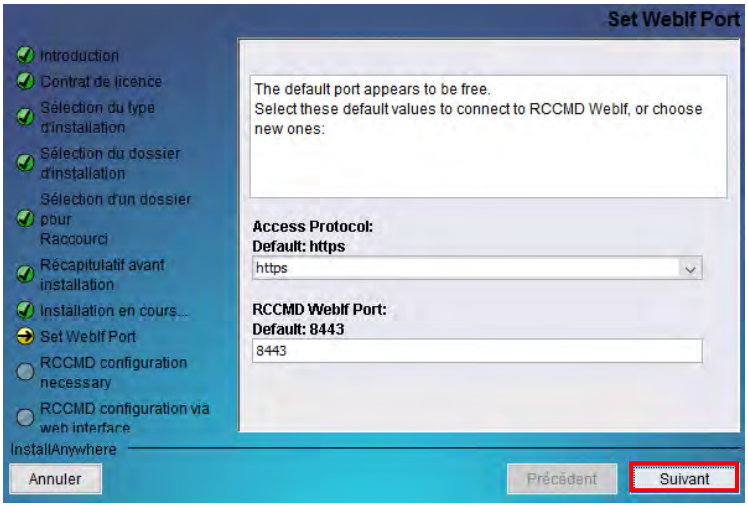
Une fois cela réalisé, cliquer sur « Installer ».



Menu « Set WebIf Port »

RCCMD utilise le protocole https ainsi que le port 8443 par défaut. Veuillez laisser ces valeurs par défaut pour éviter d'avoir des dysfonctionnements par la suite.

Cliquer sur « Suivant ».



Entrer le mot de passe par défaut qui est « RCCMD ».

Cliquer sur « Suivant ».

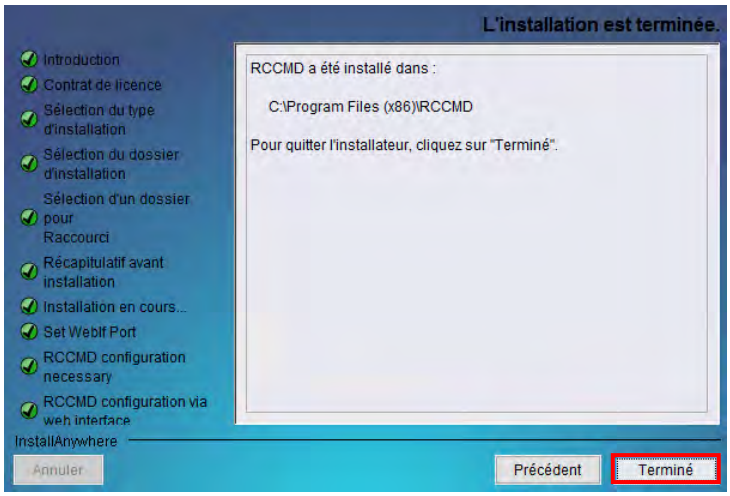
RCCMD configuration via web interface

Pour configurer RCCMD, utiliser le lien suivant :

https://localhost:8443.

Cliquer sur « Suivant »

Cliquer sur « Terminé » pour finaliser l'installation et accéder à RCCMD via l'interface web.



INFOSEC UPS SYSTEM – 15, rue du Moulin – 44880 SAUTRON - FRANCE - www.infosec-ups.com
Hot Line – Tel + 33 (0)2 40 76 15 82 - Fax + 33 (0)2 40 94 29 51 - hotline@infosec.fr – 08 19 AA XX 202 09

3. Installation de l'appliance RCCMD avec ESXi 6.0

Prérequis :

- VSphere Management Assistant (vMA) : Vous pouvez télécharger la version 6.0 sur le site de VMware. Cette appliance est nécessaire pour l'installation de RCCMD.
- Client FTP (WinSCP) : Cela va permettre de transférer les fichiers d'installation de RCCMD sur la machine vMA.
- Terminal client (PuttY) : Pour contrôler vMA pour l'installation de RCCMD de façon plus simple.

3.1 Installation et configuration de vMA

Cliquer sur « File », « Deploy OVF Template » et sélectionner le fichier OVF concernant vMA.

Accepter la licence et cliquer sur « Next »

Donner un nom à la VM. Le nom par défaut est « vMA ». Il est recommandé d'utiliser un nom court mais signifiant. (Par exemple : vMA_RCCMD)

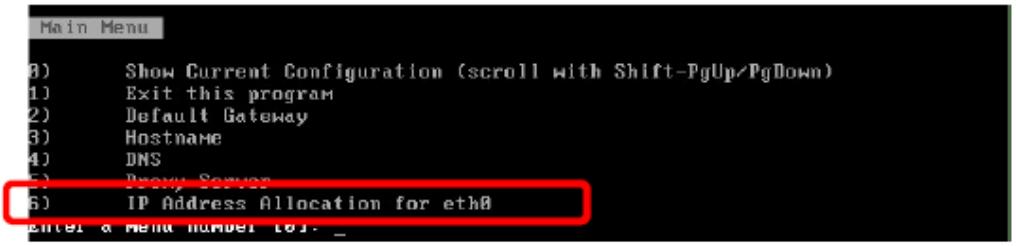
Après avoir choisi l'emplacement de stockage, l'installation va pouvoir débuter.

INFOSEC UPS SYSTEM – 15, rue du Moulin – 44880 SAUTRON - FRANCE - www.infosec-ups.com
Hot Line – Tel + 33 (0)2 40 76 15 82 - Fax + 33 (0)2 40 94 29 51 - hotline@infosec.fr – 08 19 AA XX 202 09

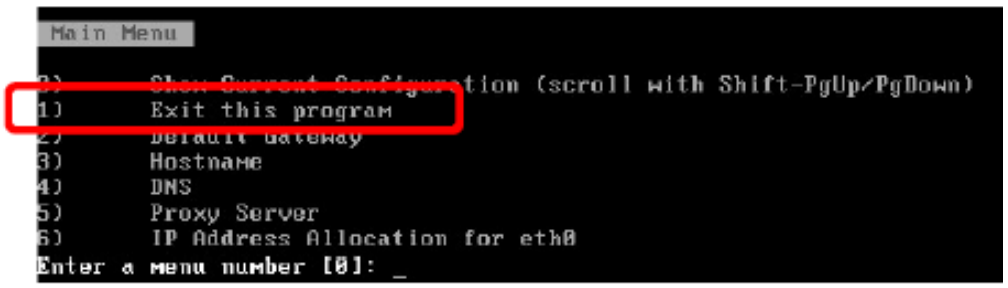
Démarrer la VM et ouvrer une console.

Une fois que la vm est bien démarré, vous arrivez sur le menu suivant.

Sélectionner le menu 6 pour configurer le réseau.



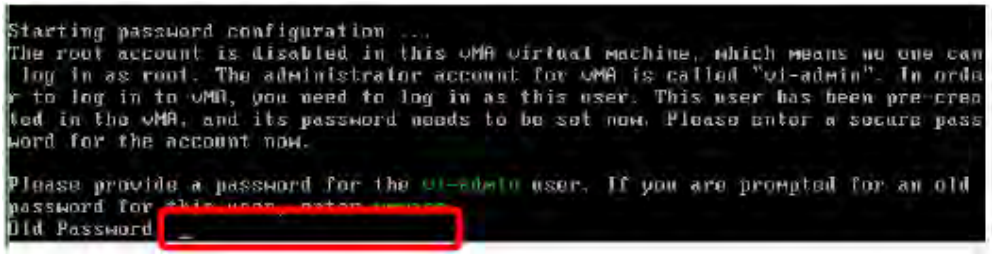
Pour quitter ce menu et rentrer en mode shell, sélectionner le menu 1



Entrer le mot de passe par défaut (« vmware »).

Ensuite, renseigner un nouveau mot de passe respectant les conditions suivantes :

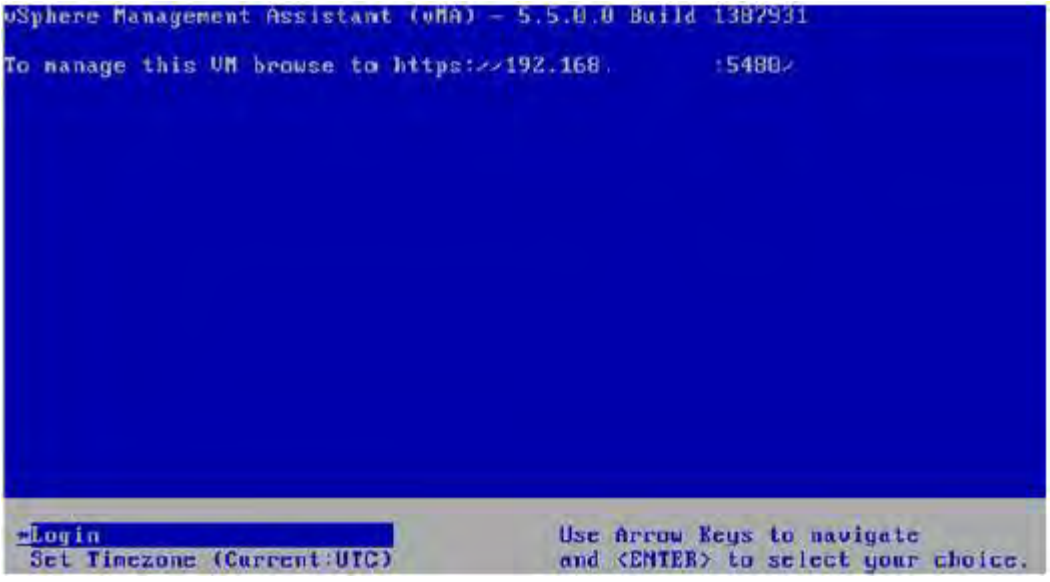
- Lettre minuscule
- Lettre majuscule
- Chiffre
- Caractère spécial



Une fois cela réalisé, vMA est prêt. Il vous reste à appuyer sur la touche Entrer et rentrer vos identifiants de connexion.

User : vi-admin

Password : *mot de passe renseigné auparavant*



3.2. Installation de RCCMD

Maintenant que l'appliance vMA est prête, il faut important l'archive comportant l'installation de RCCMD. (lien de téléchargement : https://www.infosec-ups.com/fr/accessoires-et-logiciels/logiciel-client-rccmd.html)

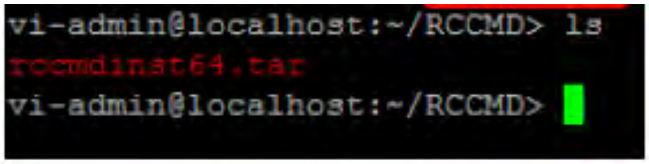
Pour l'importer dans la VM, il faut utiliser un client FTP (WINscp par exemple.) Ouvrez-le et connecté vous sur le port 22 (FTP) avec les identifiants vi-admin.

Ensuite, faite un copier glisser de votre poste vers la VM dans le dossier de votre choix (Il est conseillé de le placer dans /home/vi-admin/).

Connecté vous au terminal (PuttY par exemple). Renseigner l'adresse IP et appuyer sur « Open ». Renseigner les identifiants vi-admin.

Allez à l'emplacement où vous avez placé l'archive RCCMD à l'aide de la commande « cd /*chemin_du_dossier*/ ». (Par défaut : « cd /home/vi-admin »)

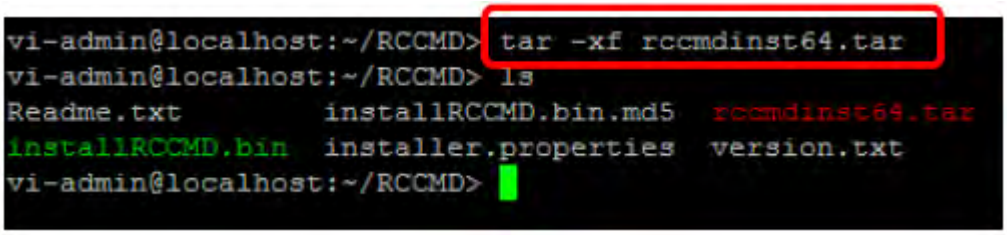
Taper la commande « ls » et vérifier que l'archive est bien présente comme ici.



Pour décompresser l'archive, utiliser la commande suivante :

« tar –xf *nom_de_l'archive* »

Vous pouvez vérifier à l'aide de la commande « ls » que l'archive a bien été décompressée.



INFOSEC UPS SYSTEM – 15, rue du Moulin – 44880 SAUTRON - FRANCE - www.infosec-ups.com
Hot Line – Tel + 33 (0)2 40 76 15 82 - Fax + 33 (0)2 40 94 29 51 - hotline@infosec.fr – 08 19 AA XX 202 09

Pour lancer l'installation de RCCMD, exécuter :
« sudo ./installRCCMD.bin »

```
vi-admin@localhost:~/RCCMD> sudo ./installRCCMD.bin

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

vi-admin's password:
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
```

Choix de langue. Sélectionner 4 pour français.

```
===============================
Choose Locale...
---------------

    1- Deutsch
  ->2- English
    3- Espa?ol
    4- Fran?ais
    5- Italiano
    6- Portugu?s

CHOOSE LOCALE BY NUMBER: 4
```

Entrer votre clé de licence fournit.

```
================================================================================
Enter your license key
----------------------

Enter your license key
Usually the license key is located on the installation booklet, or on a label
on the reverse side of the CD sleeve.
Enter license key:
```

Accepter le contrat de licence en écrivant « O » dans la console.

```
he operating systems, loss of data or interruption of work processes, other
PS problems or to other errors that may occur out of this combination.



cceptez-vous les dispositions de ce contrat de licence ? (O/N): O
```


INFOSEC UPS SYSTEM – 15, rue du Moulin – 44880 SAUTRON - FRANCE - www.infosec-ups.com
Hot Line – Tel + 33 (0)2 40 76 15 82 - Fax + 33 (0)2 40 94 29 51 - hotline@infosec.fr – 08 19 AA XX 202 09

Sélectionner les fonctions que vous souhaitez installer. Si vous ne savez pas, laisser par défaut et appuyer sur Entrée.

```
S?lection des fonctions
-----------------------

Entrez le num?ro des fonctions ? s?lectionner ou ? d?s?lectionner en les
s?parant par une virgule. Pour afficher la description d'une fonction, tapez
"?<num?ro>" et appuyez sur <Entr?e>. Lorsque vous avez termin?, appuyez sur
<Entr?e> :

    1- [X] Application
    2- [X] WebIf
    3- [X] XMessage

S?lectionnez les fonctions ? installer.:
```

Indiquer à présent le chemin dans lequel va s'installer RCCMD. Il est conseillé de laissé par défaut et appuyer sur Entrée.

```
Indiquez le dossier dans lequel installer le produit :

  Dossier d'installation par d?faut : /usr/rccmd

Entrez un chemin d'acc?s absolu, ou appuyez sur <Entr?e> pour accepter le
   chemin par d?faut
      :
```

Si vous disposez d'un vCenter et qu'il est accessible, laisser par défaut et appuyer sur Entrée.

Sinon, taper 2 puis Entrée.

```
Is a vCenter availabe for use?
------------------------------

If a vCenter is available, the credentials will be required. The vSpherePlugin
will be registered for use in the vSphere Client for Windows. RCCMD will then
be configured via that interface.

  ->1- Yes
    2- No

Tapez le num?ro de votre choix, ou appuyez sur <Entr?e> pour accepter la
   valeur par d?faut ::
```

Entrer ensuite les informations concernant un ESX que vous souhaitez manager. Il est possible d'en ajouter d'autre ensuite, à l'aide de l'interface WEB. Si vous ne voulez rien renseigner, taper Entrée.

```
What is your ESXi Host called?
------------------------------

Enter Name of one managed ESXi Host.
Additional Hosts may be configured in the Web interface after installation.

Name or IP-Address (Valeur par d?faut : ):
```


INFOSEC UPS SYSTEM – 15, rue du Moulin – 44880 SAUTRON - FRANCE - www.infosec-ups.com
Hot Line – Tel + 33 (0)2 40 76 15 82 - Fax + 33 (0)2 40 94 29 51 - hotline@infosec.fr – 08 19 AA XX 202 09

Sélectionner les options que vous souhaitez pour avoir les messages de RCCMD. Il est recommandé de laisser par défaut.

```
RCCMD Messages
--------------

By default rccmd will print the messages it receives from the network to
/dev/console.
Here you can choose additional output options.

  ->1- Display Messages on all terminals
  ->2- Log Messages
  ->3- Display Messages with Xmessage

Tapez le num?ro des fonctions requises en les s?parant par une virgule, ou
   appuyez sur <Entr?e> pour accepter la valeur par d?faut.:
```

Ensuite, le terminal affiche un récapitulatif de l'installation. Penser à vérifier toutes les informations.

Appuyer sur Entrée pour continuer.

```
Pour continuer, appuyez sur <Entr?e>.  Si les informations sont incorrectes,
tapez "Pr?c?dent" pour effectuer les modifications requises.


Nom du produit :
    RCCMD

Dossier d'installation :
    /usr/rccmd

Fonctions du produit :
    Application,
    WebIf,
    XMessage

Messaging Options
    "Display Messages on all terminals","Log Messages","Display Messages with Xm
essage"

Espace disque (pour la cible) :
    Requis :  229,869,744 octets
    Disponible : 520,146,944 octets

Pour continuer, appuyez sur <Entr?e>:
```

Sélectionner le protocole WEB de votre choix. Il est recommandé d'utiliser HTTPS (par défaut).

```
Set WebIf Protocol
------------------

This is the default protocol to access the RCCMD WebIf.
Select your preferred protocol here:

  ->1- https
    2- http

Tapez le num?ro de votre choix, ou appuyez sur <Entr?e> pour accepter la
   valeur par d?faut ::
```

Entrer un port pour l'accès WEB. Celui par défaut est 8443. Laisser par défaut également.

```
Set WebIf Port
--------------

The default port appears to be free.
Select these default values to connect to RCCMD WebIf, or choose new ones:

Port: (Valeur par d?faut : 8443):
```

L'installeur de RCCMD nous informe qu'il va créer 2 exceptions sur le firewall pour le port 8443 (WEB) et le port 6003/5769 (RCCMD).

```
Firewall Exceptions
--------------------

Firewall Exceptions (Iptables only) will be added for:
Ports 8443 (WebIf Server)
Ports 6003 & 5769 (RCCMD)

Pour continuer, appuyez sur <Entr?e>:
```

Entrer le mot de passe par défaut ainsi qu'une indication de mot de passe pour ne pas l'oublier.

```
Enter Password
--------------

Set a password for RCCMD Web Interface. If no password is set, the default
password "csl2l-snmp" will be used!

Please Enter the Password::



================================================================================
Enter Password Hint
-------------------

Enter a hint for the Password.

Password Hint (Valeur par d?faut : ): name_card
```

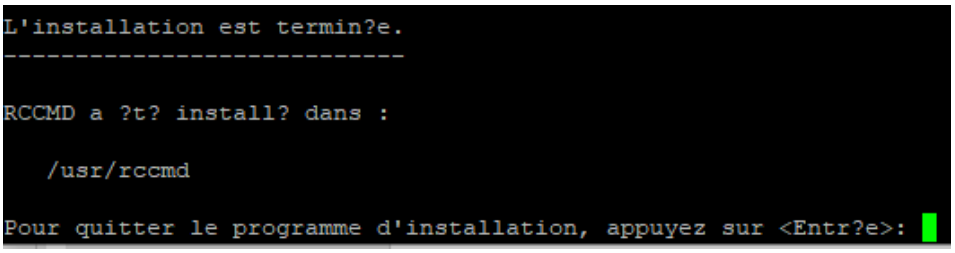
Information à propos de la connexion web sur RCCMD.

```
RCCMD configuration necessary
-----------------------------

It is necessary to configure RCCMD. Please use the web interface at
"https://172.20.50.148:8443".

Should you decide to run RCCMD with this default configuration RCCMD will
accept messages from any ip-address!
Please set one or more valid ip-addresses that are allowed to send (shutdown-)
messages to this RCCMD.

Pour continuer, appuyez sur <Entr?e>:
```

RCCMD demande si vous souhaitez le démarrer maintenant ou plus tard.

```
Start RCCMD now?
----------------

It is recommended to start RCCMD from WebIf after all necessary configuration.
If you want to start it manually, use "/usr/rccmd/rccmdctl start"

Do you want to start RCCMD now?

  ->1- Yes
    2- No

Tapez le num?ro de votre choix, ou appuyez sur <Entr?e> pour accepter la
   valeur par d?faut.:
```

L'installation est finie, appuyer sur Entrée pour quitter le menu d'installation.

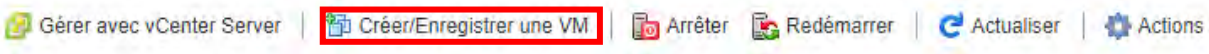


4. Installation de l'appliance RCCMD avec ESXi 6.5

4.1. Déploiement OVF/OVA

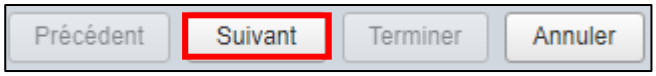
Ouvrer la page d'accueil de votre ESX et se connecter en tant que « root »

Après s'être connecté, vous pouvez créer une nouvelle VM (Sur la version ESXi 6.5, cela se trouve sur la barre du haut)

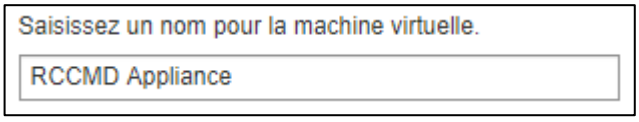


Sélectionner ensuite l'option suivante :

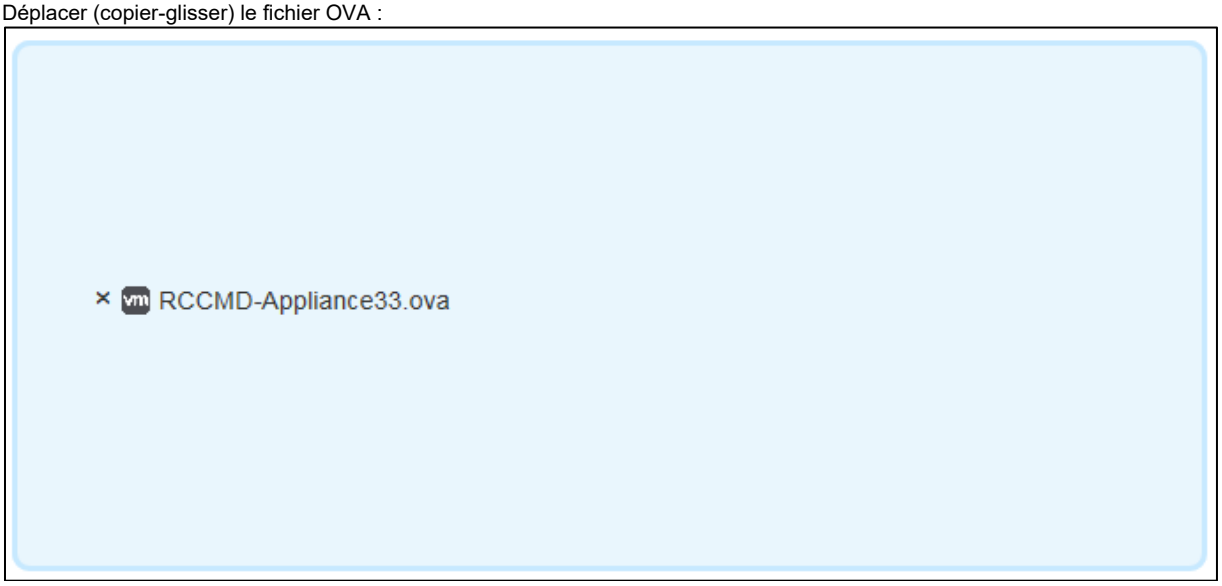
Cliquer sur Suivant pour continuer :



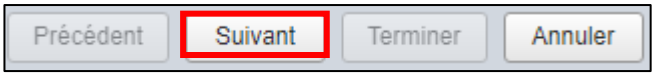
Donner un nom à la nouvelle VM :



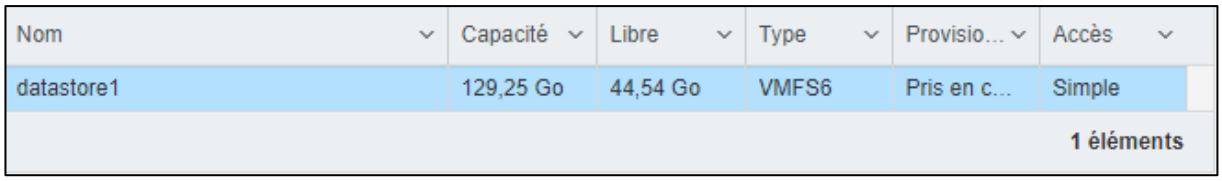
Déplacer (copier-glisser) le fichier OVA :



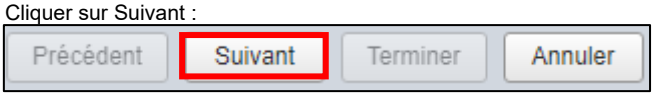
Puis cliquer sur Suivant :



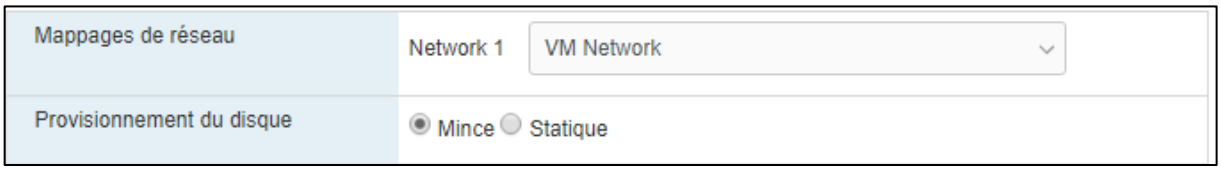
Le fichier OVA est déjà préconfiguré ; il n'y a pas besoin de rajouter d'autres paramètres :



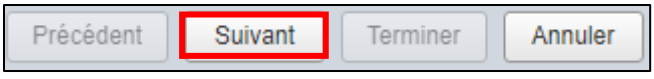
Cliquer sur Suivant :



Le client RCCMD sera géré par un serveur RCCMD correspondant. Ce serveur doit donc être capable d'atteindre votre client via le réseau local.
En général, vous pouvez accepter les paramètres préconfigurés.



Une fois que les paramètres sont correctes, cliquer sur Suivant :



INFOSEC UPS SYSTEM – 15, rue du Moulin – 44880 SAUTRON - FRANCE - www.infosec-ups.com
Hot Line – Tel + 33 (0)2 40 76 15 82 - Fax + 33 (0)2 40 94 29 51 - hotline@infosec.fr – 08 19 AA XX 202 09

C'est la dernière étape, vérifier tous les paramètres avant de cliquer sur « Terminer » :

Produit	RCCMD-Appliance
Nom de la VM	RCCMD Appiance
Disques	RCCMD-Appliance-disk1.vmdk
Banque de données	datastore1
Type de provisionnement	Mince
Mappages de réseau	bridged: VM Network
Nom du SE invité	Inconnu

Avertissement : Une notification apparait pour éviter de corrompre l'installation de RCCMD

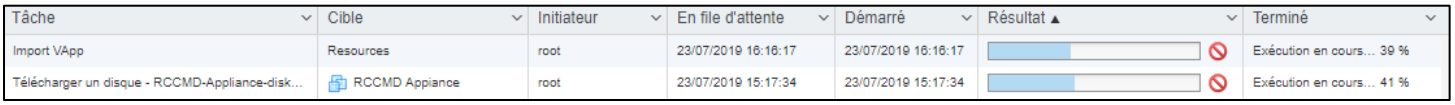
N'actualisez pas le navigateur lors du déploiement de cette VM.

VMware réagit de manière sensible aux mises à jour du navigateur pendant le processus d'installation. Si le navigateur est actualisé avant la fin de l'installation, le processus est interrompu, ce qui rend la machine virtuelle inutilisable.

Cliquer sur Terminer pour commencer l'installation :

Installation automatique

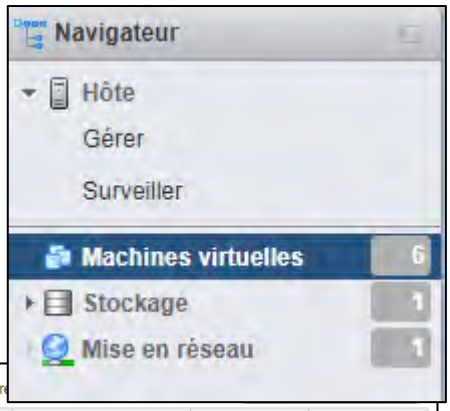
La colonne « Résultat » et « Terminé » permette de suivre le cours de l'installation :



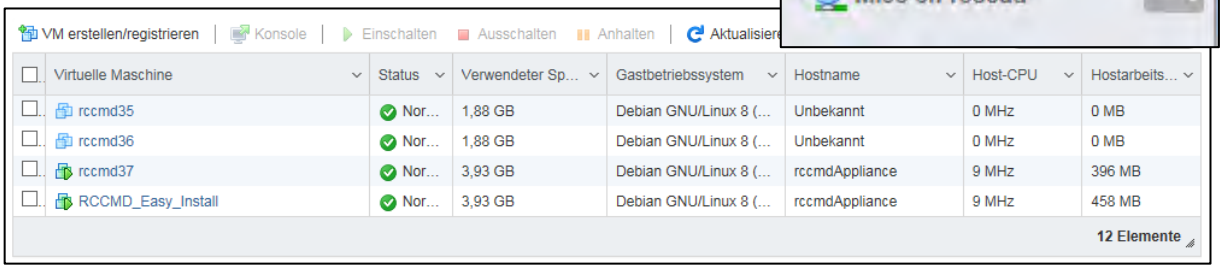
Tâche	Cible	Initiateur	En file d'attente	Démarré	Résultat ▲	Terminé
Import VApp	Resources	root	23/07/2019 16:16:17	23/07/2019 16:16:17		Exécution en cours... 39 %
Télécharger un disque - RCCMD-Appliance-disk...	RCCMD Appiance	root	23/07/2019 15:17:34	23/07/2019 15:17:34		Exécution en cours... 41 %

INFOSEC UPS SYSTEM – 15, rue du Moulin – 44880 SAUTRON - FRANCE - www.infosec-ups.com
Hot Line – Tel + 33 (0)2 40 76 15 82 - Fax + 33 (0)2 40 94 29 51 - hotline@infosec.fr – 08 19 AA XX 202 09

Sur le côté gauche on dispose du navigateur qui affiche une vue d'ensemble de toutes les machines virtuelles installées sur le système.



En cliquant sur la VM, vous aurez accès aux informations systèmes.



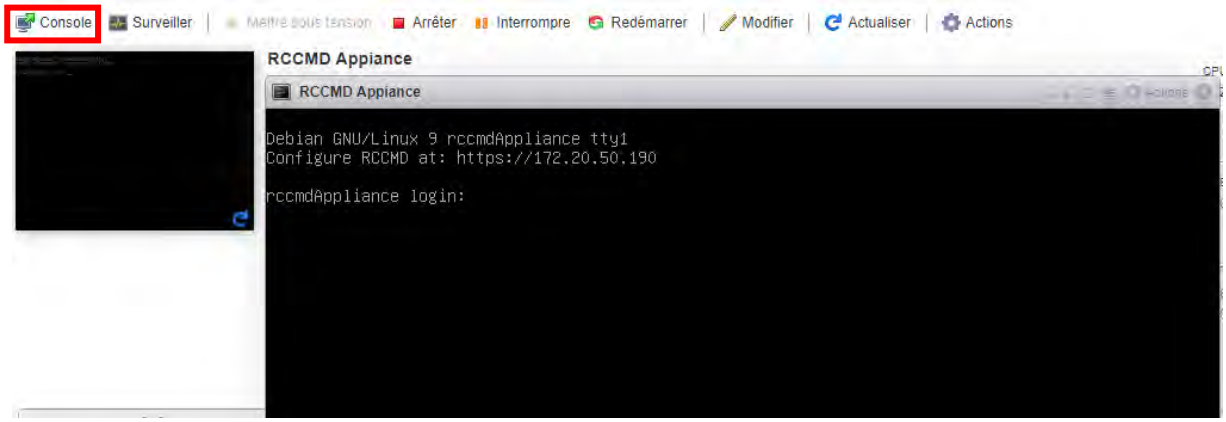
4.2. Configuration de la VM (réseau)

Assurez-vous que la VM soit allumée :

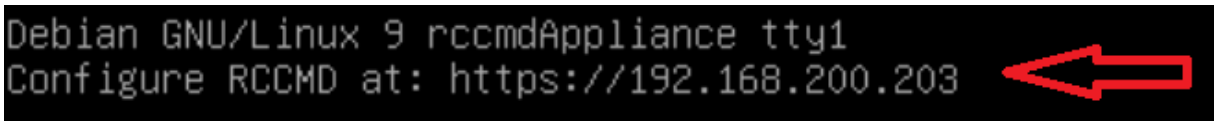
La VM est allumée

La VM est éteinte

Cliquer sur « Console » pour ouvrir la console de management :



Si vous avez un serveur DHCP sur votre réseau, la VM disposera automatiquement d'une adresse IP :



Si vous ne disposez pas de serveur DHCP, il faut mettre une adresse statique à la machine. Se référer à l'annexe Adressage IP statique ;pour suivre la procédure.

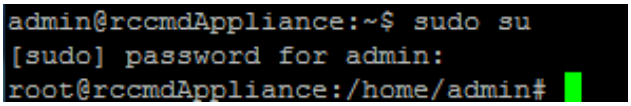
Il est possible de se connecter à l'appliance RCCMD avec :

User: admin

Password: RCCMD

Droit administrateur :

L'appliance VMware est basée sous Linux (Debian 9). Les privilèges root (administrateur) permettent l'installation manuelle des paquets officiels ainsi que la configuration avancée des interfaces réseau.



Commande : sudo su

Par défaut, l'administrateur n'a pas les privilèges pour faire des changements - vous devez attribuer des privilèges système en utilisant la commande Linux « sudo su ».

L'installation de l'appareil RCCMD est maintenant terminée. Pour plus de configuration, reportez-vous à l'interface Web. Un guide de configuration pour l'attribution manuelle d'une adresse IP se trouve dans l'annexe de ce manuel.

INFOSEC UPS SYSTEM – 15, rue du Moulin – 44880 SAUTRON - FRANCE - www.infosec-ups.com
Hot Line – Tel + 33 (0)2 40 76 15 82 - Fax + 33 (0)2 40 94 29 51 - hotline@infosec.fr – 08 19 AA XX 202 09

5. Installation de l'appliance RCCMD avec vCenter

5.1. Déploiement OVF/OVA

Dans le menu du vCenter, commencer par l'installation de RCCMD en choisissant « Déployer un modèle OVF »

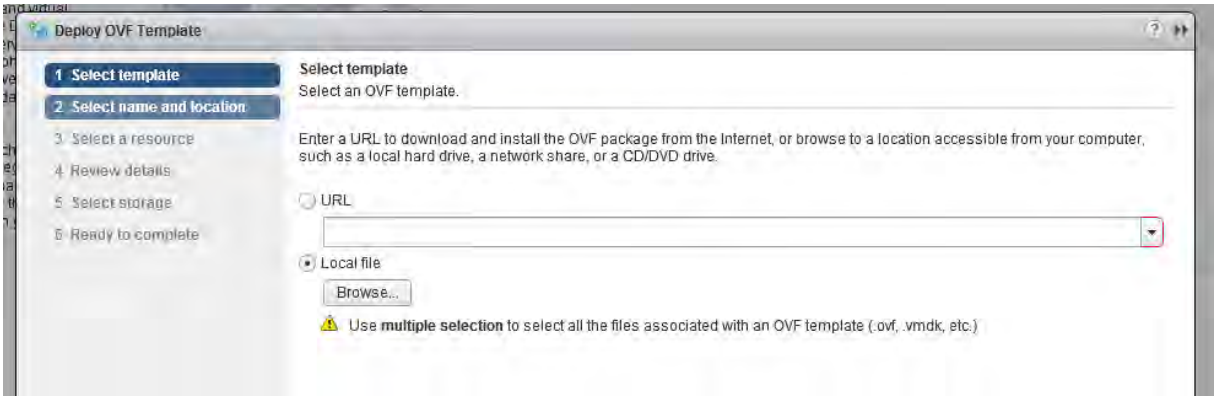
Premièrement, choisissez le fichier OVA/OVF. Le vCenter dispose de deux options :

URL:

Le fichier OVA/OVF provient d'une ressource distante, il faut spécifier le chemin d'accès.

Fichier local

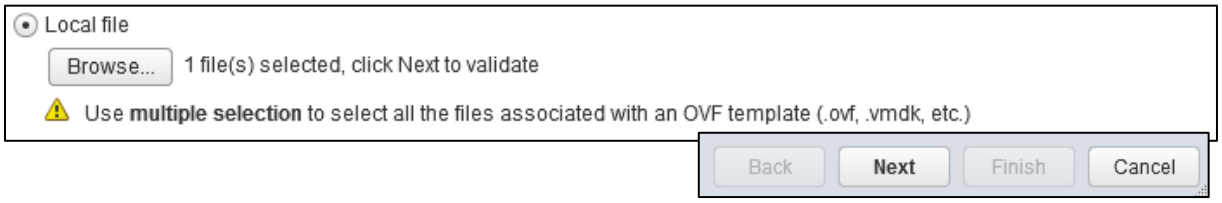
Le fichier OVA/OVF est enregistré en local, il faut sélectionner le fichier où il est enregistré :



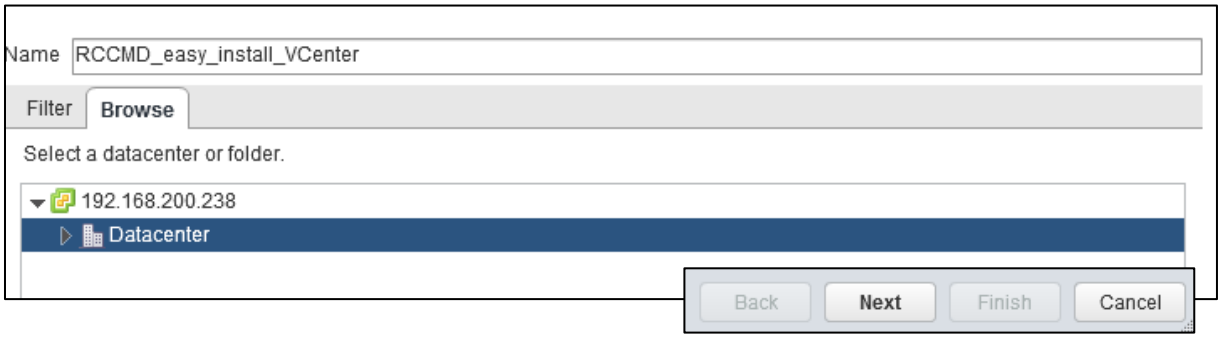
INFOSEC UPS SYSTEM – 15, rue du Moulin – 44880 SAUTRON - FRANCE - www.infosec-ups.com
Hot Line – Tel + 33 (0)2 40 76 15 82 - Fax + 33 (0)2 40 94 29 51 - hotline@infosec.fr – 08 19 AA XX 202 09

Dans cet exemple, le fichier OVA est enregistré en local.

Après avoir sélectionner le fichier, cliquer sur Suivant :

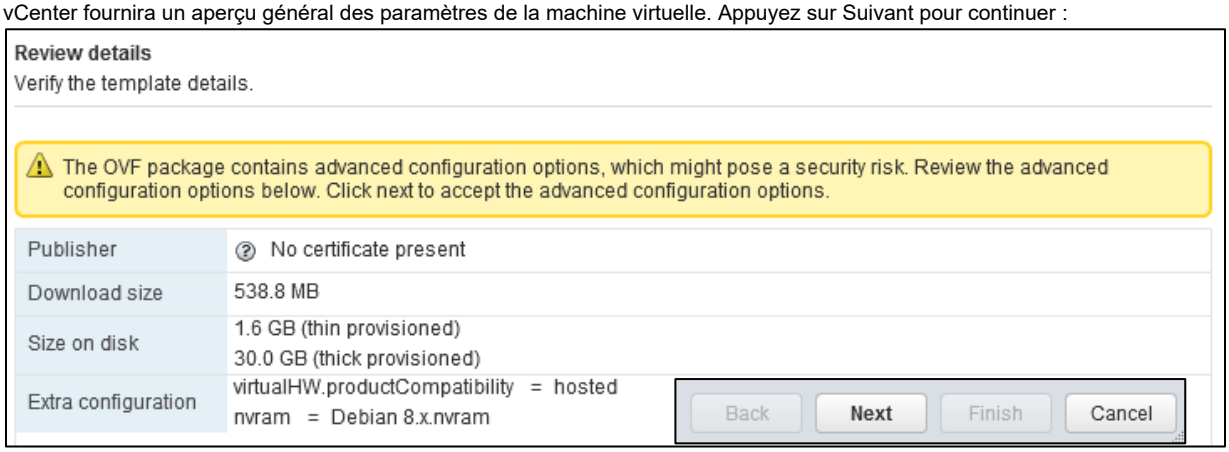


L'étape suivante consiste à donner un nom à la VM ; Cliquer sur Suivant pour continuer :

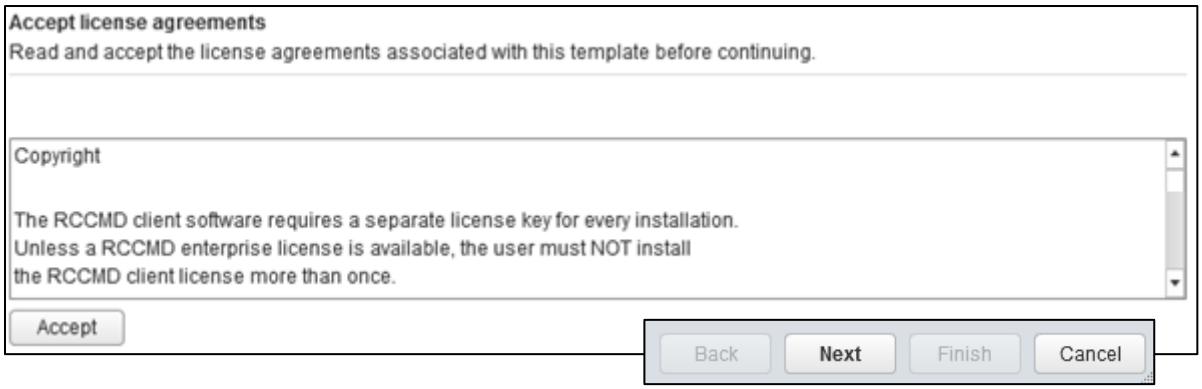


VCenter a besoin de connaitre l'hôte de destination de la VM pour effectuer l'installation :

vCenter fournira un aperçu général des paramètres de la machine virtuelle. Appuyez sur Suivant pour continuer :



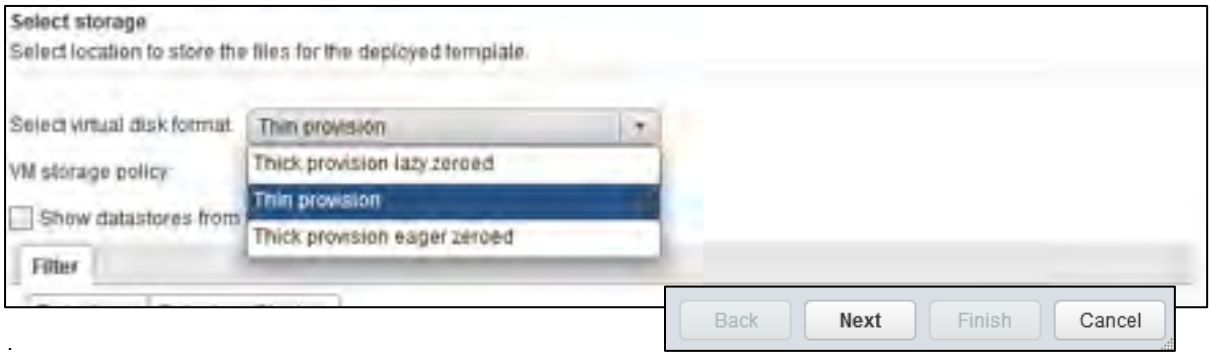
Accepter la licence avant de pouvoir continuer et procéder à l'installation.



L'utilisation du disque peut varier en fonction de la configuration de votre système :

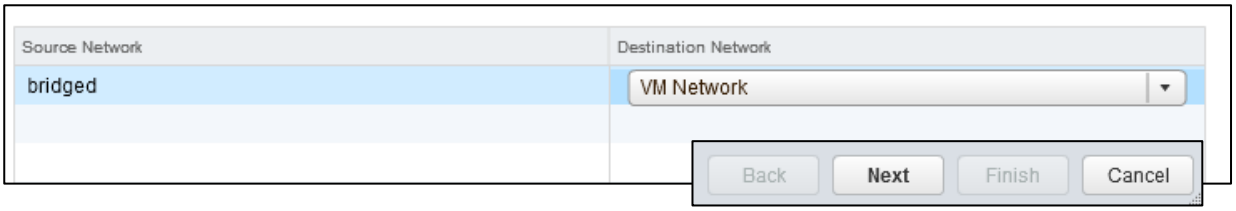
Référez-vous à votre administrateur pour obtenir les paramètres correspondants.

Si vous n'êtes pas sûr, sélectionnez « Thin provision » et comme VM storage policy « none ».

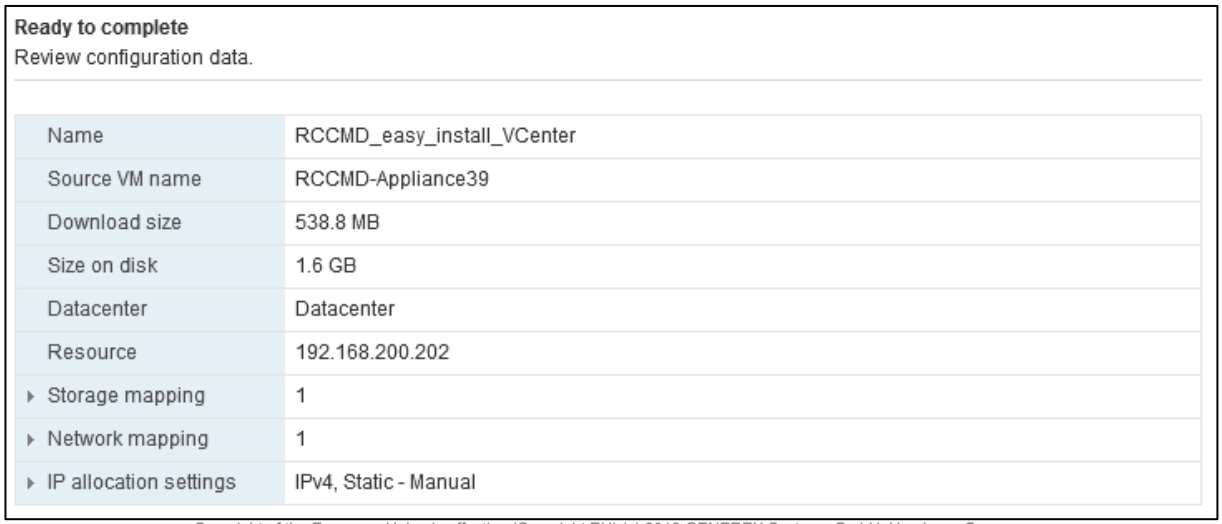


.

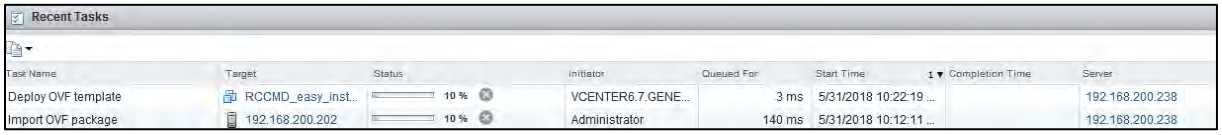
L'appareil a besoin d'un accès au réseau. Encore une fois, adressez-vous à votre administrateur. Si vous n'êtes pas sûr, sélectionnez d'abord « VM Network » en mode « bridged ». Dans cet exemple d'installation, nous utilisons VM Network pour connecter correctement la VM au réseau.



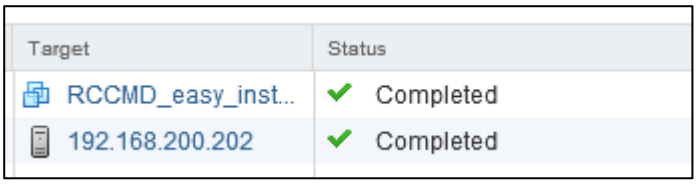
Vérifier vos paramètres : vous verrez un aperçu de votre configuration. Si les paramètres sont corrects, cliquez sur Terminer. Cette action quitte l'écran de configuration et déclenche l'installation automatique de RCCMD.



En dessous des tâches récentes, vous pouvez suivre le déroulement de l'installation :

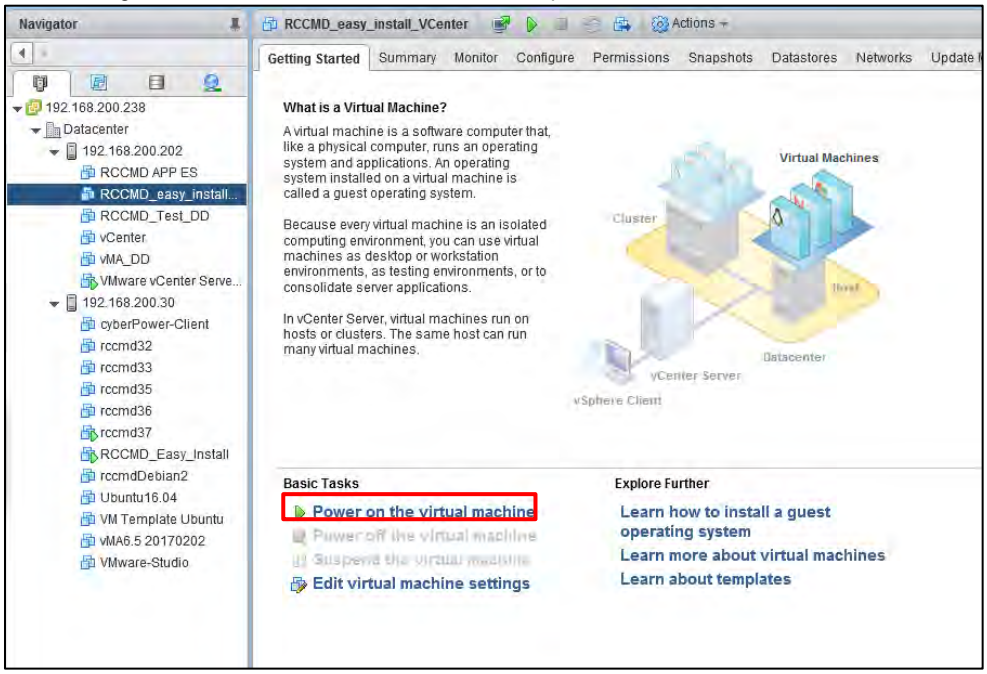


Veuillez patienter jusqu'à ce que le processus d'installation soit terminé et que le statut soit « Terminé » :



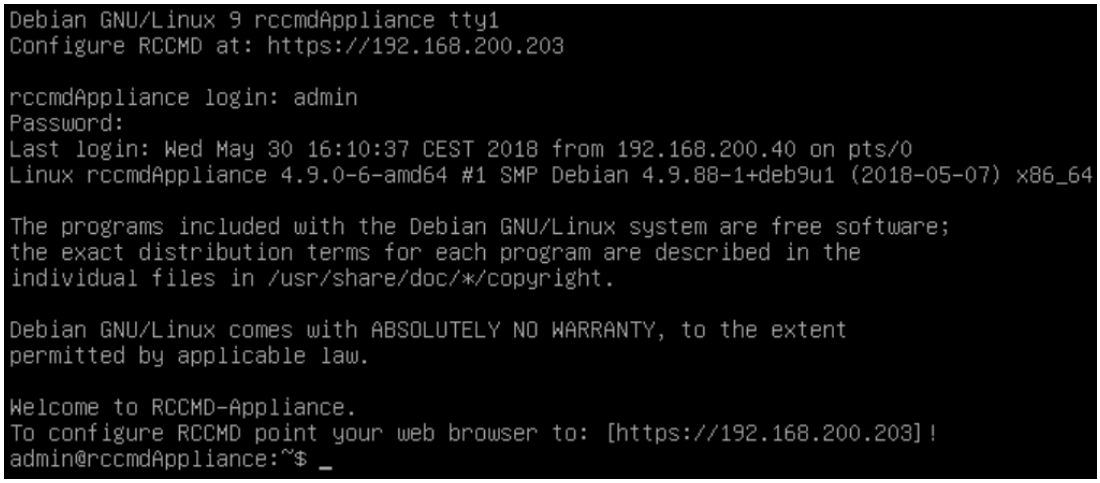
5.2. Configuration de la VM (réseau)

Dans le navigateur, recherchez la machine virtuelle correspondante et mettez-la sous tension.

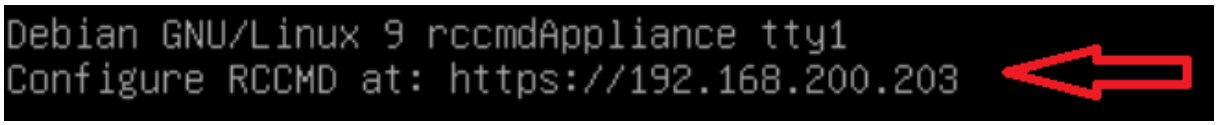


INFOSEC UPS SYSTEM – 15, rue du Moulin – 44880 SAUTRON - FRANCE - www.infosec-ups.com
Hot Line – Tel + 33 (0)2 40 76 15 82 - Fax + 33 (0)2 40 94 29 51 - hotline@infosec.fr – 08 19 AA XX 202 09

Après le démarrage de la VM, vous pouvez accéder à la console :



Si vous avez un serveur DHCP sur votre réseau, la VM disposera automatiquement d'une adresse IP :



Si vous ne disposez pas de serveur DHCP, il faut mettre une adresse statique à la machine. Se référer à l'annexe Adressage IP statique ;pour suivre la procédure.

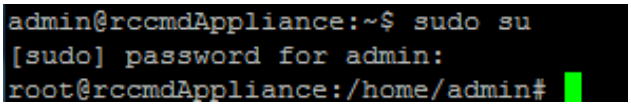
Il est possible de se connecter à l'appliance RCCMD avec :

User: admin

Password: RCCMD

Droit administrateur :

L'appliance VMware est basée sous Linux (Debian 9). Les privilèges root (administrateur) permettent l'installation manuelle des paquets officiels ainsi que la configuration avancée des interfaces réseau.



Commande : sudo su

Par défaut, l'administrateur n'a pas les privilèges pour faire des changements - vous devez attribuer des privilèges système en utilisant la commande Linux « sudo su ».

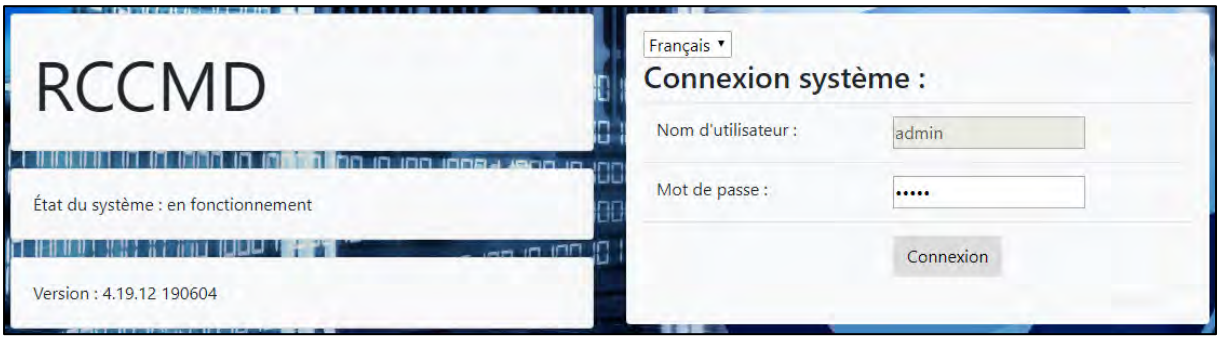
L'installation de l'appareil RCCMD est maintenant terminée. Pour plus de configuration, reportez-vous à l'interface Web. Un guide de configuration pour l'attribution manuelle d'une adresse IP se trouve dans l'annexe de ce manuel.

6. RCCMD : interface web

6.1. Page de connexion

Pour accéder à l'interface web de RCCMD, renseigner l'adresse IP inscrite lors de la configuration de la VM :

https:// <Adresse ip de l'appliance RCCMD>



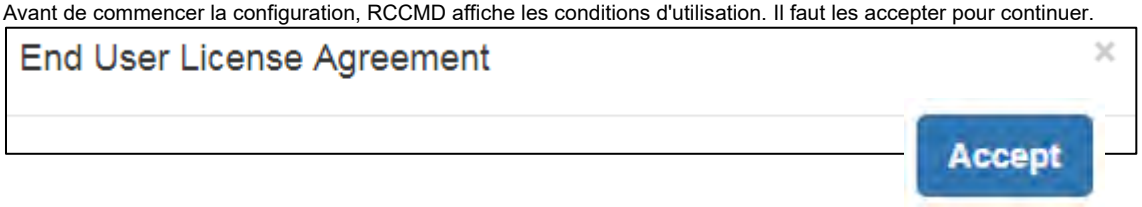
Se connecter avec les identifiants suivant :

User: *admin*
Password: *RCCMD*

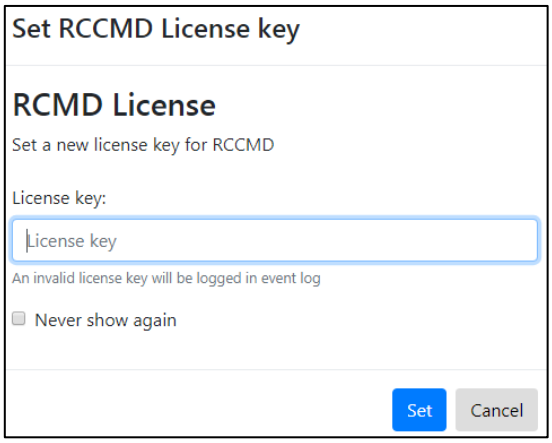
La page d'accueil montre l'état du système, la version de RCCMD et l'onglet de connexion.

6.2. Clé de licence

Avant de commencer la configuration, RCCMD affiche les conditions d'utilisation. Il faut les accepter pour continuer.



Vous pouvez lire les conditions d'utilisations et cliquer sur le bouton Accepter.
Ensuite, RCCMD vous demandera d'entrer une clé de licence valide :



La clé utilisée par l'installation de RCCMD fonctionnera avec les conditions :

1. ***une*** clé = ***une*** installation RCCMD

En général une clé est utilisée pour un client RCCMD. Si une clé est accidentellement assignée deux fois, le premier client RCCMD réclamera une licence. Les clients suivants de RCCMD qui démarrent reconnaîtront une licence revendiquée et afficheront une entrée de journal correspondante :

2018-05-30 09:17:51 rccmd[00490]: License fraud from IP address 192.168.200.144 detected. Functionality will deteriorate.

Veuillez noter que la clé de démonstration est une clé unique qui sera utilisée pour toute installation :
Vous ne pouvez pas utiliser plus d'une version d'essai du RCCMD dans votre réseau.

2. S'il n'y a pas de clé valide présente, RCCMD fonctionnera en version d'essai

Si vous n'avez pas la clé ou si vous souhaitez tester le produit, ne saisissez pas de clé. Ainsi, RCCMD comprendra qu'il s'agit d'une version d'essai et utilisera une clé d'évaluation intégrée de 30 jours. Il est possible de changer la clé à tout moment (Options → Paramètres avancés → Licence RCCMD).

6.3. Interface

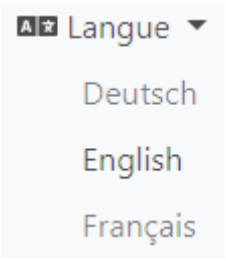
Après la connexion, voici l'écran affiché :

Sur la gauche de l'écran, plusieurs catégories sont disponibles :

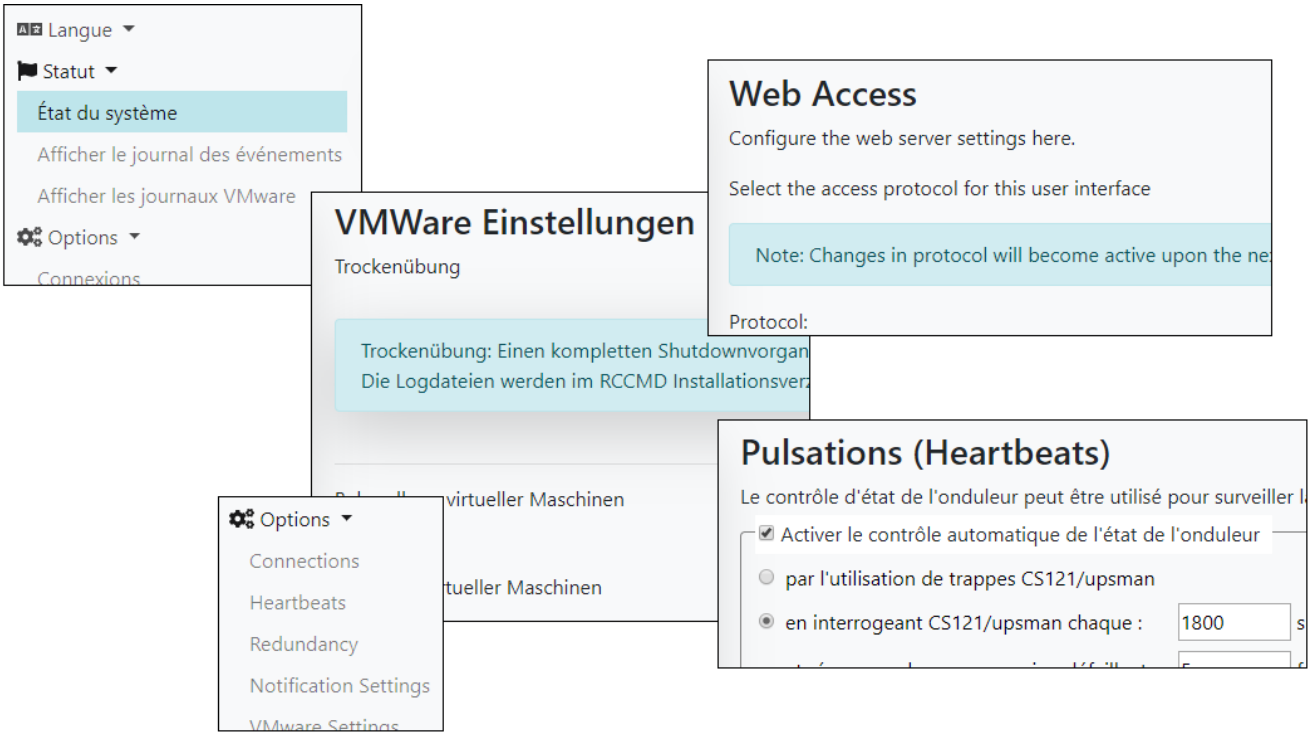
INFOSEC UPS SYSTEM – 15, rue du Moulin – 44880 SAUTRON - FRANCE - www.infosec-ups.com
Hot Line – Tel + 33 (0)2 40 76 15 82 - Fax + 33 (0)2 40 94 29 51 - hotline@infosec.fr – 08 19 AA XX 202 09

6.3.1. Langues

Pour sélectionner la langue désirée, allez dans le menu « Langue »



RCCMD est disponible en Allemand, Anglais et Français.



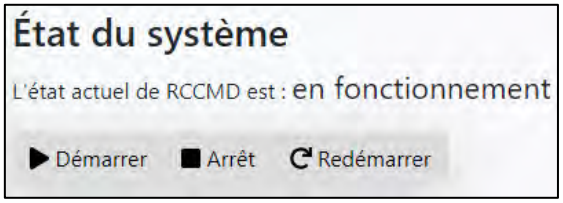
6.3.2. Statut du système

Menu: Statut → Statut système

Cliquer sur statut système et redémarrer.

Le message suivant nous informe sur le statut et la configuration actuelle de RCCMD

ne fonctionne pas	RCCMD est éteint
en fonctionnement	RCCMD est allumé



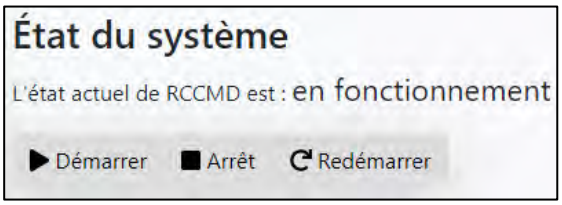
Le menu suivant contient les informations générales à propos de l'état de RCCMD ainsi que les fichiers de logs :

- ➔ Onglet système : Statut
- ➔ Afficher l'état de fonctionnement actuel de RCCMD, ainsi que les options de démarrage, d'arrêt et de redémarrage
- ➔ Afficher et télécharger les fichiers de logs
- ➔ Afficher et télécharger les fichiers de logs VMware

La page statut système permet d'avoir les informations immédiates sur l'état et la configuration de RCCMD.

Les boutons suivants entrainent les actions suivantes :

Démarrer	Allumé RCCMD quand il est éteint
Arrêt	Eteindre RCCMD quand il est allumé
Redémarrer	Eteint RCCMD puis le rallume



6.3.3. Journaux d'évènements

2019-06-13	13:41:12	rccmd[09099]: system: Operation now in progress
2019-06-13	14:10:42	rccmd[09099]: Trying to start program/job: /usr/rccmd/rccmd_notalive.sh 192.168.2.1 06/13/2019 14:10:42
2019-06-13	14:10:42	rccmd[09099]: error: check upsman failed, could not connect to 192.168.2.1
2019-06-13	14:10:42	rccmd[09099]: system: Operation now in progress
2019-06-13	14:10:57	rccmd[09099]: Trying to start program/job: /usr/rccmd/rccmd_notalive.sh 192.168.2.2 06/13/2019 14:10:57
2019-06-13	14:10:57	rccmd[09099]: error: check upsman failed, could not connect to 192.168.2.2
2019-06-13	14:10:57	rccmd[09099]: system: Operation now in progress
2019-06-13	14:11:12	rccmd[09099]: Trying to start program/job: /usr/rccmd/rccmd_notalive.sh 192.168.2.3 06/13/2019 14:11:12
2019-06-13	14:11:12	rccmd[09099]: error: check upsman failed, could not connect to 192.168.2.3

Les journaux d'évènements de RCCMD concernent le service RCCMD :

- Notifications
- Evènement système
- Actions
- Exécutions des scripts

Les logs de RCCMD disposent d'informations complémentaires :

- Date de l'évènement
- Heure où l'évènement s'est produit
- L'adresse IP de la machine concernée
- Succès/échec de l'exécution d'une action

Il est possible de savoir :

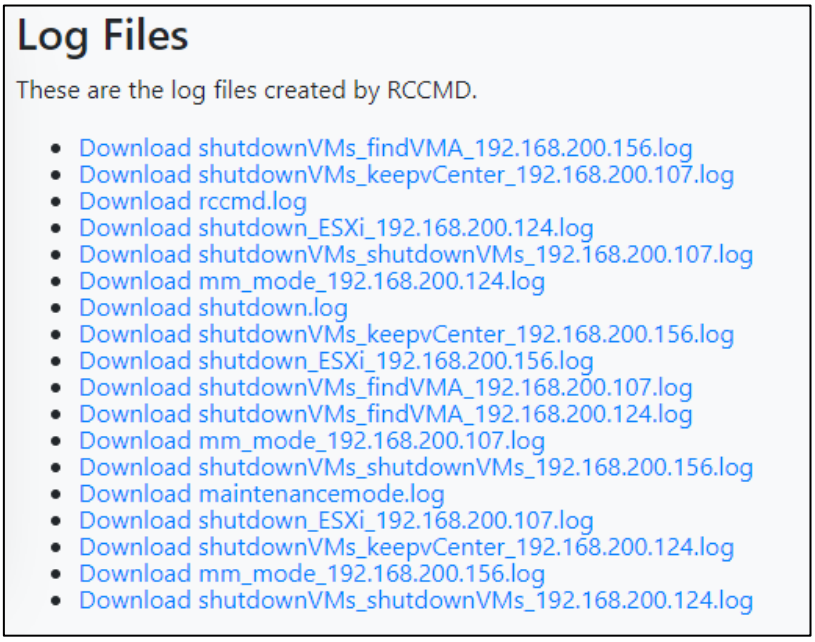
- Quand le serveur a été éteint
- Pourquoi il l'a été
- Qu'elle a été la rapidité du système à réagir face à l'incident.

Les journaux d'évènement permettent d'aider la résolution de problèmes complexes et de prévoir des problèmes futurs.

Télécharger un journal d'évènements

Vous trouverez le lien de téléchargement en dessous de la dernière ligne de logs:

6.3.4. Logs VMware



L'appliance RCCMD fournit d'autres journaux d'évènements pour permettre la résolution d'incidents.

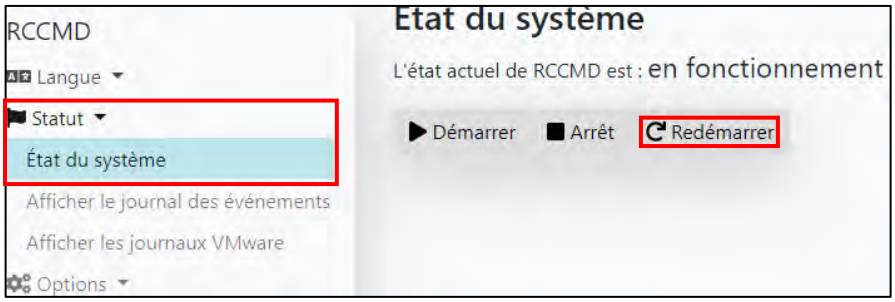
Les logs de RCCMD montrent les informations suivantes:

- ✓ Date
- ✓ Heure
- ✓ Signales reçu
- ✓ Communication en attente
- ✓ Exécution des scripts
- ✓ Résultats des tests

7. Configuration de RCCMD

Après un changement de configuration, il est nécessaire de redémarrer les services :

Si les services ne sont pas redémarrés, les données sont sauvegardées mais elles ne sont pas transférées dans la configuration active.



Sécurisée l'appliance RCCMD

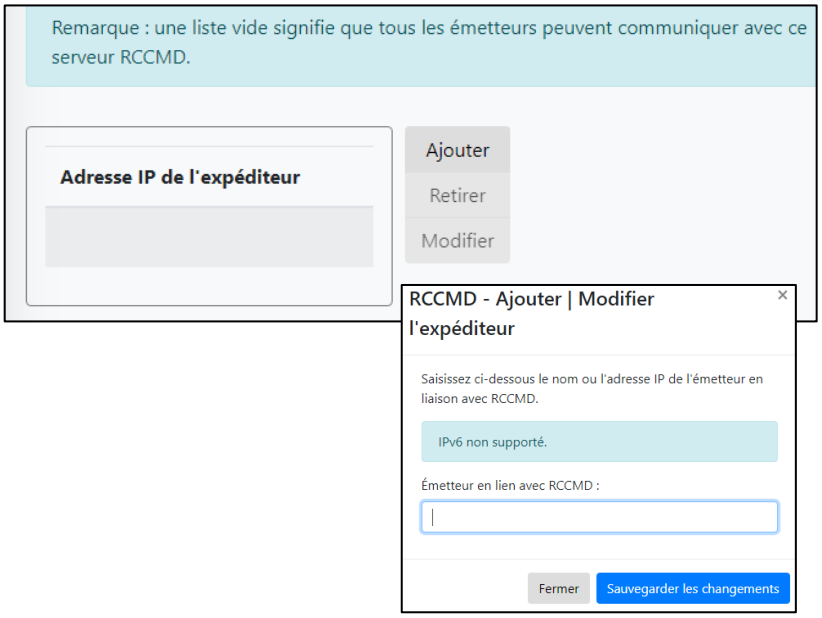
Menu: Connexions

Protection contre l'arrêt accidentelle du serveur

Actuellement, chaque émetteur RCCMD peut déclencher un arrêt qui ne peut être stopper. Le client RCCMD vous propose donc de limiter ces commandes à des postes spécifiques.

En dessous de « Options », cliquer sur Connexion. Cliquer sur insert pour ajouter une nouvelle adresse IP

Entrer l'adresse IP de la machine souhaitée.



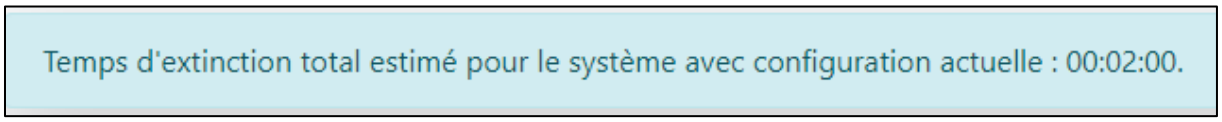
7.1. Connexions

En combien de temps se déroule un arrêt de serveur?

Arrêt basique

Après avoir entré toutes les données, il est possible d'estimer le temps nécessaire pour un arrêt complet.

Vous pouvez voir cela en dessous des options de l'hôte ESX (Paramètres VMware).



Note:

Chaque onduleur ne peut fournir qu'une alimentation de secours. Lorsque les batteries sont déchargées, l'onduleur s'arrête de lui-même pour éviter d'endommager ces dernières.

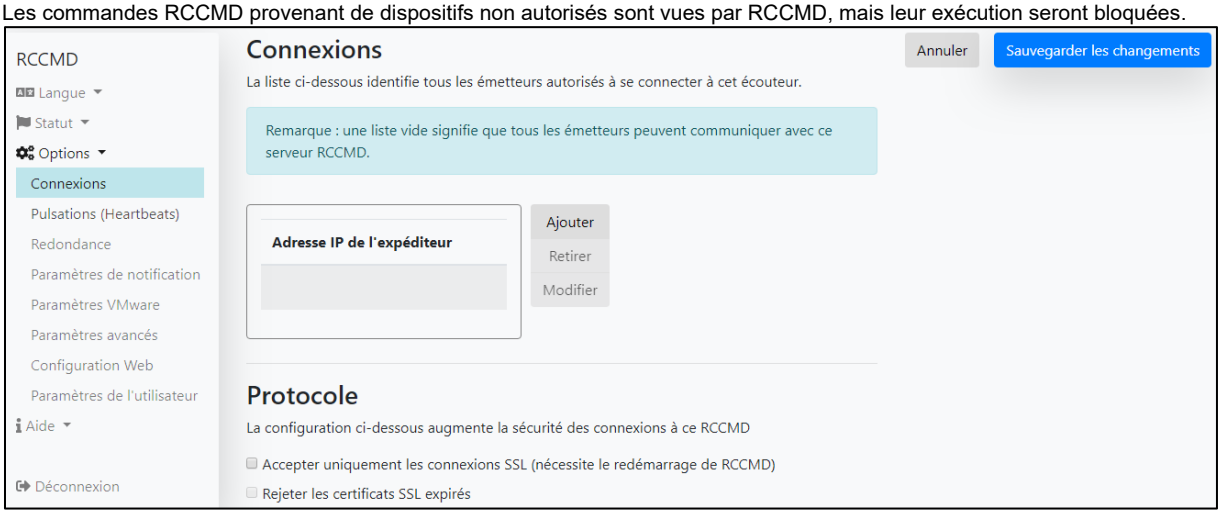
De plus, ces valeurs ne sont qu'un aperçu de votre système basé sur les données que vous avez saisies ! Vérifier régulièrement si les valeurs saisies correspondent à l'état d'arrêt réel en cas d'urgence.

N'oubliez pas qu'entre deux essais d'arrêt, les conditions peuvent changer. Lors du calcul et de l'adaptation du temps d'arrêt moyen, il est recommandé de prendre un peu plus de temps que le temps minimum requis.

Définir les connexions entrantes autorisées

Si vous laissez ce champ vide, tous les signaux d'arrêt RCCMD entrants peuvent déclencher un arrêt.
Cela n'est pas conseillé et doit être modifiée. En saisissant une adresse IP de l'expéditeur, vous limitez les périphériques qui sont autorisés à envoyer une commande d'arrêt à ce client RCCMD.

Les commandes RCCMD provenant de dispositifs non autorisés sont vues par RCCMD, mais leur exécution seront bloquées.



Configuration des connexions

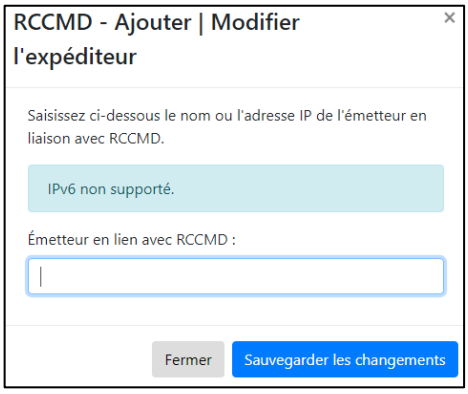
Insertion et modification

Ajouter : ajout d'une adresse IP.

Sauvegarder les changements quand vous avez ajouter l'adresse IP. Fermer la page de configuration et recommencer l'opération pour toutes les stations RCCMD autorisées.

Si il y a des modifications à apporter dans la configuration, cela peut être modifié :

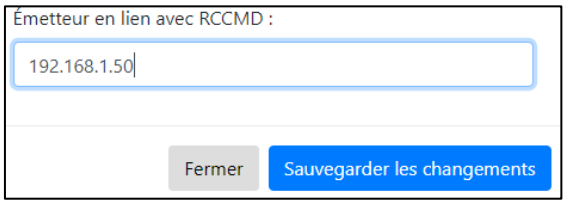
Sélectionner une adresse IP et cliquer sur « Modifier ». Une page de configuration s'affiche, vous pouvez ainsi modifier la configuration initiale. Sauvegarder les changements pour terminer.



Il est possible de mettre soit l'adresse IP de l'expéditeur ou son nom d'hôte.

Cela est plus difficile avec le nom d'hôte :

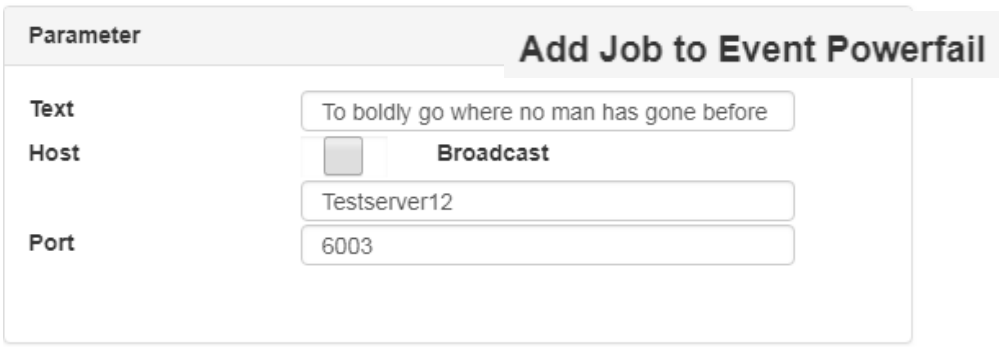
Vous avez besoin d'un serveur DNS pour la translation entre l'adresse IP et le nom de l'hôte. Si le serveur DNS n'est plus fonctionnel, ou que la communication avec le serveur est défaillante, RCCMD ne pourra pas contacter les hôtes et gérer les commandes d'arrêt.



RCCMD est fonctionnel ave les noms d'hôtes mais au vu des problèmes qui peuvent subvenir, il est fortement conseillé d'utilisé les adresses IP.

RCCMD attendra toujours un signal entrant ! Vous devez configurer un émetteur RCCMD comme le gestionnaire Web CS141 :

Lors de la gestion des événements UPS, sélectionnez la tâche « Arrêt» vous pouvez choisir entre l'adresse IP ou le nom d'hôte du client RCCMD.



Lors de la gestion de ressources critiques, il est recommandé de limiter autant que possible les interférences.

Par exemple, si vous avez besoin d'un serveur capable de résoudre les noms d'hôtes en adresses IP, la communication entre le client et l'expéditeur cessera de fonctionner dès que le serveur sera indisponible.

Par conséquent, il est recommandé d'utiliser une adresse IP manuelle : ainsi, tous les périphériques d'un segment de réseau peuvent communiquer entre eux sans serveur supplémentaire.

Note

Si vous configurez le CS141 et que vous voulez voir si les tâches que vous avez configurées sont correctement reçues par RCCMD, vous pouvez utiliser des connexions pour créer un journal entrant. Tant que l'expéditeur n'est pas explicitement inclus dans « Connexions », RCCMD enregistre l'exécution mais refusera de l'exécuter.

Toutefois, au moins une adresse IP doit être saisie pour activer cette fonction de filtrage.

Préparation pour la redondance de l'UPS

Certains réglages dépendent les uns des autres. Si plusieurs UPS fonctionnent simultanément afin de sécuriser l'infrastructure du serveur, il peut être nécessaire de spécifier plus d'un UPS pour déclencher une commande d'arrêt.

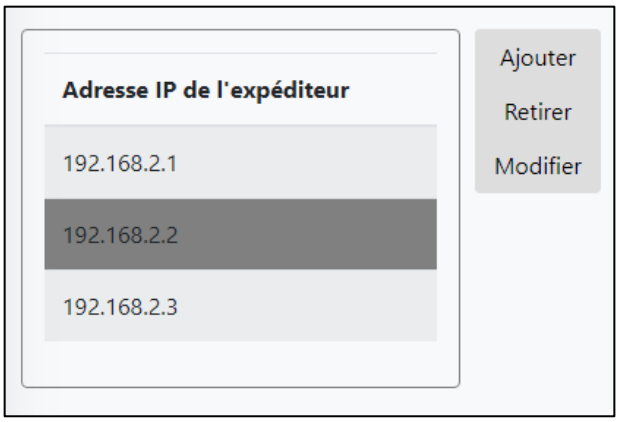
Si vous entrez deux ou plusieurs adresses IP valides pour un signal RCCMD valide, le menu « Redondance » est automatiquement activé et peut être utilisé.

RCCMD peut être configuré pour gérer les signaux d'arrêt RCCMD valides provenant de différentes sources. Pour plus de détails, reportez-vous au menu « Redondance ».

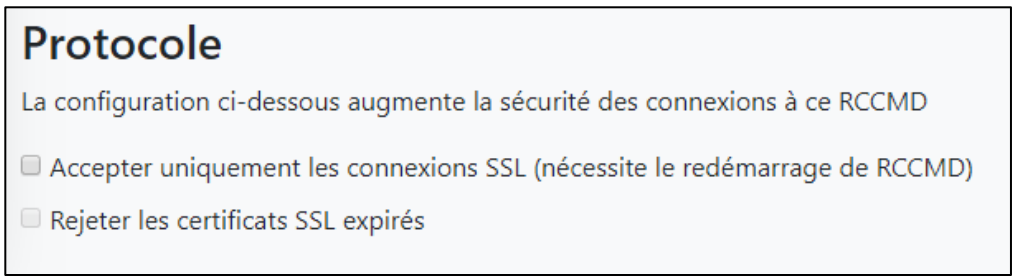
Comment supprimer une adresse IP

Cliquer sur l'adresse IP désiré et cliquer sur « Retirer ».

Ne pas oublier de cliquer sur « Sauvegarder ».



Augmenter la sécurité des connexions

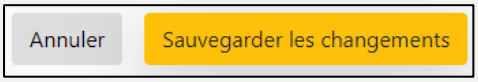


Cette partie permet d'ajouter une sécurité à votre réseau mais cela augmente le temps de gestion et d'administration.

Vous pouvez demander à RCCMD d'accepter les communications cryptées (SSL) avec un certificat valide.
Si un expéditeur ne dispose pas d'un certificat SSL pour s'identifier, la connexion est interrompue.

En plus de cette fonction, vous pouvez demander à RCCMD de vérifier que les certificats SSL sont à jour. Si le certificat est expiré, il est considéré comme non valide et la connexion est interrompue en conséquence.

Note



Si vous saisissez ou modifiez des données, ces dernières seront sauvegardées temporairement, mais sans aucun impact sur la configuration actuelle.
Si votre configuration est terminée, vous devez écrire vos paramètres locaux dans le fichier de configuration RCCMD.

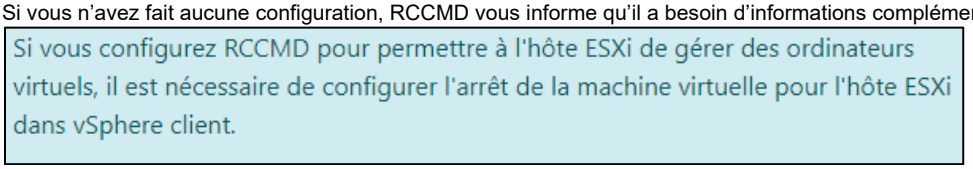
Pour activer la nouvelle configuration, RCCMD doit être redémarré. Il suffit d'appuyer sur la touche « Statut » puis « Arrêt » et « Démarrer » ou « Redémarrer ». RCCMD va voir les changements et prendra en charge la nouvelle configuration.

7.2. Contrôle de l'arrêt des machines

7.2.1. ESXi

Menu: Options → Paramètres VMware

Allez dans « Paramètres VMware »
Si vous n'avez fait aucune configuration, RCCMD vous informe qu'il a besoin d'informations complémentaires :



Bien que RCCMD soit installé en tant que machine virtuelle et qu'il soit déjà prêt à l'emploi, il ne peut pas encore remplir sa fonction réelle puisque les autorisations d'accès nécessaires n'ont pas encore été enregistrées. Confirmez ce message avec OK pour ouvrir les paramètres VMware.

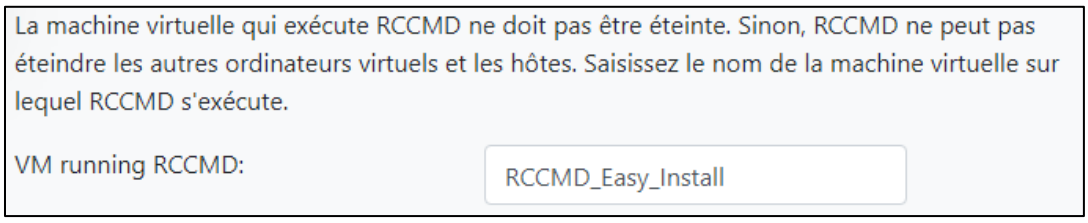
Lorsque vous utilisé un seul hôte, les machines virtuelles peuvent être mises hors tension avant que l'hôte ESXi lui-même ne s'éteigne.

Note

L'arrêt d'urgence entraine l'arrêt des machines virtuelles et l'arrêt de l'hôte lui-même. Le délai d'attente du mode maintenance définit le temps que RCCMD accorde à vMotion avant que l'arrêt des hôtes n'entre en vigueur. Le mode de maintenance dans le comportement d'arrêt peut donc également être utilisé pour déclencher un arrêt pour différents hôtes, y compris une temporisation.

Pour « Gestion de la machine virtuelle » sélectionner « Par RCCMD ». Et pour le « Comportement de la machine virtuelle » sélectionner « Arrêter les machines ».

Pour éviter que RCCMD ne s'arrête de lui-même, l'hôte VMware doit connaître la machine sur laquelle tourne le client RCCMD :

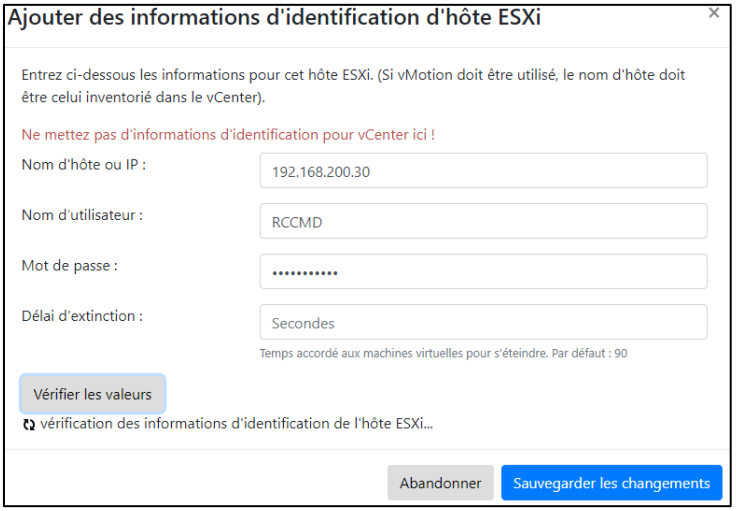


RCCMD a besoin des informations suivante :

<u>Nom d'hôte/ Adresse IP</u>
Il est recommandé d'utilisé une adresse IP mais un nom d'hôte fonctionne.

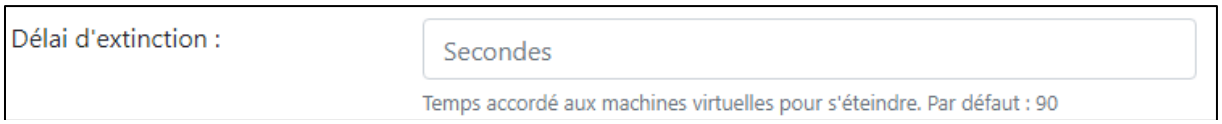
<u>Nom d'utilisateur</u>
L'utilisateur doit avoir les privilèges pour éteindre l'environnement VMware.

<u>Mot de passe</u>
Mot de passe correspondant à l'utilisateur pour authentifier la session.



INFOSEC UPS SYSTEM – 15, rue du Moulin – 44880 SAUTRON - FRANCE - www.infosec-ups.com
Hot Line – Tel + 33 (0)2 40 76 15 82 - Fax + 33 (0)2 40 94 29 51 - hotline@infosec.fr – 08 19 AA XX 202 09

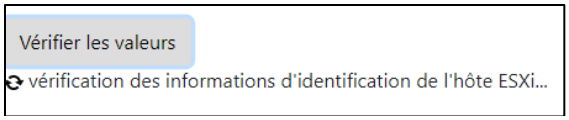
La prochaine étape consiste à déterminer le nombre de secondes pour éteindre les VM :



Chaque machine virtuelle a un temps d'arrêt différent d'une autre pour s'éteindre correctement. Ainsi, le temps dont une machine a besoin varie beaucoup et dépend fortement des tâches et de la taille de la VM. Pour éviter la perte de données ou l'endommagement de la machine virtuelle, l'hôte peut donner aux machines virtuelles un temps appropriée pour s'éteindre. Le délai d'arrêt indique le temps en secondes pendant lequel l'hôte attend avant d'être éteint.

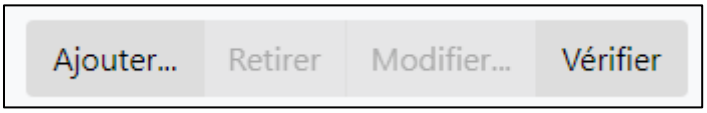
Le réglage par défaut est de 90 secondes - les machines virtuelles qui prennent plus de temps seront alors éteintes du fait que l'hôte ESXi s'éteint.

Vous pouvez vérifier les informations renseignées à l'aide du bouton « Vérifier les valeurs » :



Si les tests sont bons, cliquer sur « Sauvegarder les changements » pour quitter la page de configuration.

Cliquer sur « Vérifier » pour confirmer les informations de l'ESX :



Vous pouvez remarquer sur le bouton « Sauvegarder les changements » a changé de couleur :

Vous avez donc effectué une modification qui nécessite le redémarrage du RCCMD pour enregistrer la nouvelle configuration et ainsi l'appliqué à la configuration active. Cela est indiqué par le bouton vert

7.2.2. vCenter

Menu: Options → Paramètres VMware

Le vCenter diffère par ses modes de fonctionnement d'un hôte autonome. Tandis qu'un l'hôte unique travaille seul et arrête les machines virtuelles selon les besoins, vCenter fournit la Haute Disponibilité ; avec vMotion, qui permet de déplacer les machines virtuelles d'un hôte à l'autre en cas de problème/maintenance d'un hôte.

A noter :

Avant de pouvoir utiliser RCCMD avec vMotion, le Distributed Resources Scheduler (DRS) doit être configuré en mode entièrement automatique.

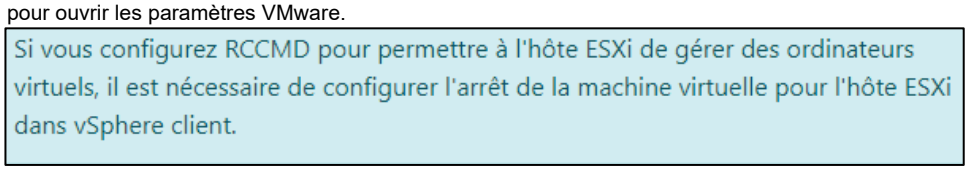
Note

Avant de pouvoir utiliser RCCMD et vMotion, il est nécessaire de vérifier que chaque machine virtuelle s'exécutant sur l'hôte a été testée en mode maintenance. Si le mode de maintenance échoue, les machines virtuelles non migrées seront désactivées lorsque l'hôte est hors tension.

Ouvrer les « Paramètres VMware »:

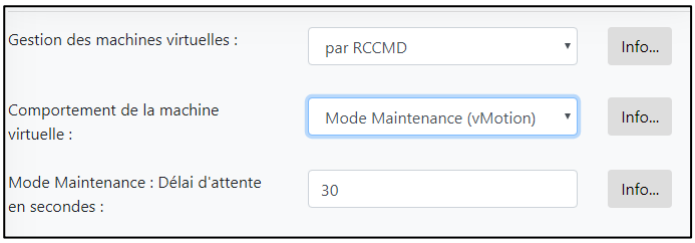
Si vous n'avez fait aucune configuration, RCCMD vous informe qu'il a besoin d'informations complémentaires :

Bien que RCCMD soit installé en tant que machine virtuelle et qu'il soit déjà prêt à l'emploi, il ne peut pas encore remplir sa fonction réelle puisque les autorisations d'accès nécessaires n'ont pas encore été enregistrées. Confirmez ce message avec OK pour ouvrir les paramètres VMware.



Lors de l'utilisation d'un vCenter, les machines virtuelles peuvent d'un hôte à un autre. Les machines virtuelles continueront à fonctionner de manière transparente. Veuillez noter les différentes données :

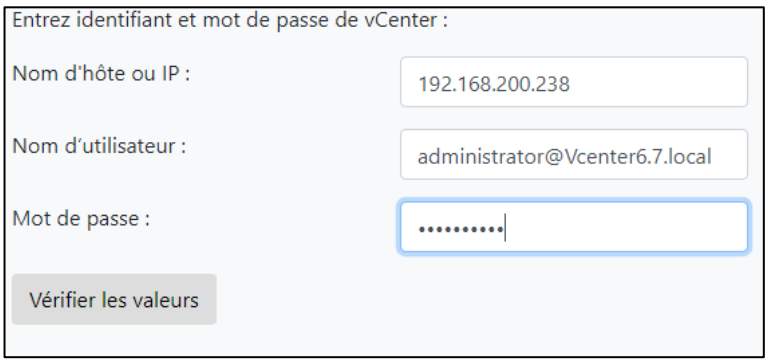
Sous « Comportement de la machine virtuelle », sélectionnez Mode de maintenance (vMotion).



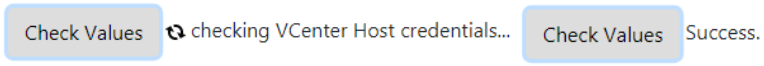
Le délai d'attente du mode Maintenance en secondes définit le temps donné à vCenter pour déplacer une machine virtuelle vers un autre hôte. Le comportement de vMotion est configuré dans la haute disponibilité (HA) du vCenter. Dès que le temps est écoulé, la procédure d'arrêt standard est lancée :

Les machines virtuelles n'ayant pas eu le temps de s'éteindre s'arrêteront en même temps que l'hôte.

Contrairement à un hôte unique, RCCMD a besoin des données utilisateur avec les autorisations correspondantes du vCenter :

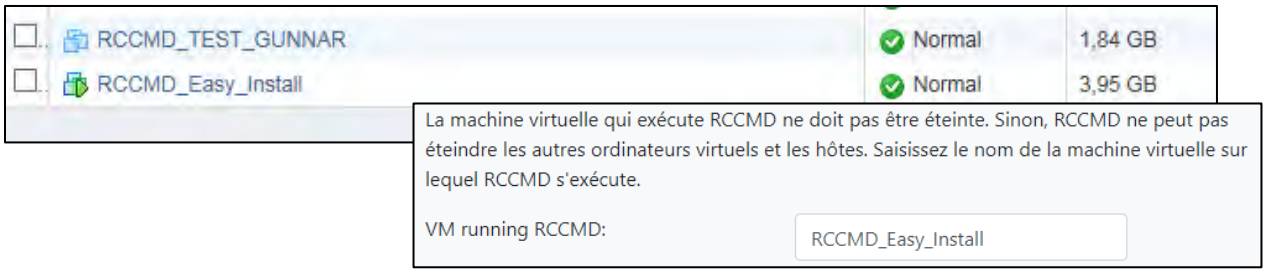


Cliquer sur « Vérifier les valeurs » pour valider les identifiants de vCenter. Les valeurs de contrôle indiquent si le vCenter est joignable et si les données d'accès ont été saisies correctement :

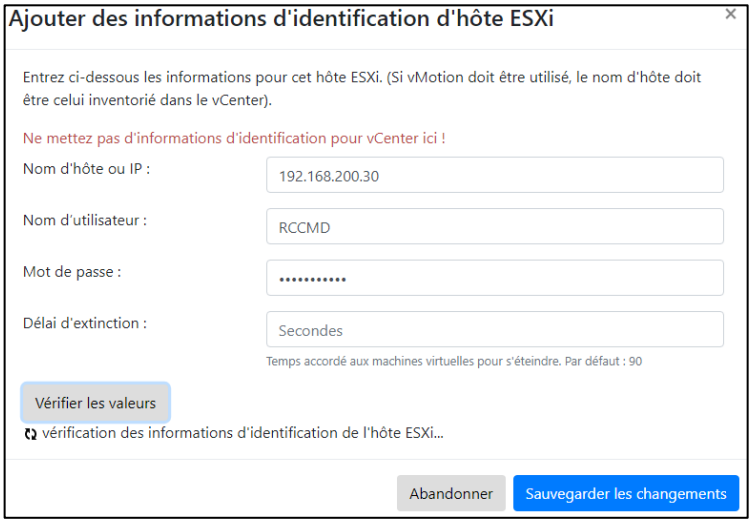


Si RCCMD n'arrive pas à joindre le vCenter, un message d'erreur apparaitra.

Pour éviter que RCCMD ne s'arrête de lui-même, l'hôte VMware doit connaître la machine sur laquelle tourne le client RCCMD :



RCCMD a besoin des informations suivante :



Nom d'hôte/ Adresse IP
Il est recommandé d'utilisé une adresse IP mais un nom d'hôte fonctionne.

Utilisateur
L'utilisateur doit avoir les privilèges pour éteindre l'environnement VMware.

Mot de passe
Mot de passe correspondant à l'utilisateur pour authentifier la session

La prochaine étape consiste à déterminer le nombre de secondes pour éteindre les VM :

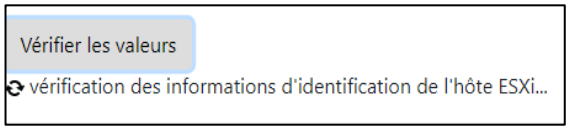
Chaque machine virtuelle a un temps d'arrêt différent d'une autre pour s'éteindre correctement.

Ainsi, le temps dont une machine a besoin varie beaucoup et dépend fortement des tâches et de la taille de la VM. Pour éviter la perte de données ou l'endommagement de la machine virtuelle, l'hôte peut donner aux machines virtuelles un temps appropriée pour s'éteindre.

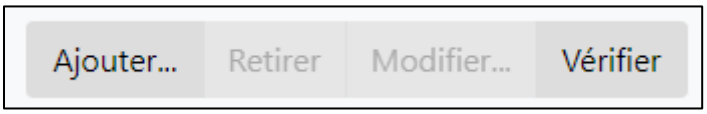
Le délai d'arrêt indique le temps en secondes pendant lequel l'hôte attend avant d'être éteint.

Le réglage par défaut est de 90 secondes - les machines virtuelles qui prennent plus de temps seront alors éteintes du fait que l'hôte ESXi s'éteint.

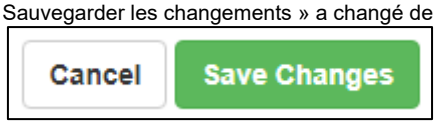
Vous pouvez vérifier l'accès aux données en cliquant sur « Vérifier les valeurs »



Si les tests sont corrects, cliquer sur « Sauvegarder les changements » pour quitter la page de configuration.
Cliquer sur « Vérifier » pour vérifier les informations de l'ESX :



Vous pouvez remarquer que le bouton « Sauvegarder les changements » a changé de couleur :



Vous avez donc effectué une modification qui nécessite le redémarrage du RCCMD pour enregistrer la nouvelle configuration et ainsi l'appliquer à la configuration active. Cela est indiqué par le bouton vert.

7.2.3. vSAN

Avant de commencer, il est important de lire la configuration suivante pour éviter les problèmes causés par une mauvaise configuration de RCCMD.

RCCMD fonctionne avec un environnement vSAN.

En raison du fait qu'un vSAN est très complexe et que les conditions de fonctionnement d'un vSAN diffèrent par rapport à un seul hôte ou à un cluster standard, certaines conditions préalables doivent être remplies avant que le RCCMD puisse arrêter un vSAN :

En raison du fait que chaque hôte d'un vSAN doit être mis en mode maintenance avant de pouvoir être éteint, tant qu'une machine virtuelle fonctionne, il n'est pas possible d'éteindre les hôtes.

Le vCenter qui gère le vSAN est la première machine virtuelle qui démarre et la dernière machine virtuelle qui s'arrête.

Le vCenter est l'unité de commande d'un vSAN. Il est permis d'installer le vCenter à l'intérieur du vSAN ainsi que de l'exécuter sur un seul hôte qui ne fait pas partie du cluster. La fonction essentielle du vCenter est de gérer la synchronisation de toutes les données dans vSAN après que toutes les autres machines virtuelles soient hors service. Vous devez vous assurer que le vCenter peut terminer cette opération.

Si vous utilisez un Witness-Server (témoin) comme machine virtuelle dans un vSAN :

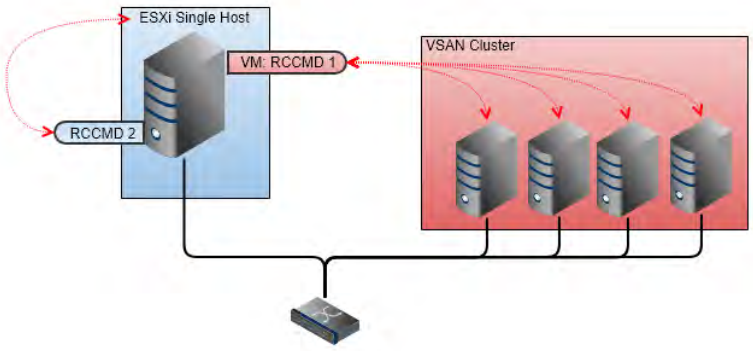
Le serveur témoin à une tâche spéciale Si deux hôtes ne correspondent pas à l'hôte qui contient les données les plus récentes, ils demandent au serveur témoin. Le serveur témoin agit comme un hôte complet, mais ne peut pas maintenir les machines virtuelles.

De ce fait, le serveur témoin peut également être virtualisé dans le vSAN et fonctionne comme un hôte autonome. Dans ce cas, vous devez différentier l'adresse IP du serveur témoin et la machine virtuelle de l'hôte où se trouve la machine virtuelle du serveur témoin :

Le serveur témoin est régulièrement arrêté dans le cluster vSAN.

L'hôte qui maintient la machine virtuelle qui contient le serveur témoin a besoin d'un deuxième client RCCMD pour activer le mode de maintenance après que le serveur témoin soit éteint.

Techniquement, un client RCCMD ne peut gérer que le vSAN ou l'hôte sur lequel il fonctionne.



Par conséquent, si vous avez des hôtes uniques ET un cluster VSAN, vous aurez besoin d'au moins 2 clients RCCMD : RCCMD 1 gère l'arrêt du cluster VSAN et RCCMD 2 gère l'arrêt de l'hôte unique. La routine d'arrêt est ensuite divisée en 2 commandes différentes pour le CS141 :

- o Arrêter le cluster VSAN
- o Arrêt de l'hôte unique

Puisque les deux clients RCCMD fonctionnent côte à côte :

Lors du choix du temps correcte pour les tâches d'arrêt, assurez-vous que le VSAN a complètement éteint tous les hôtes avant d'éteindre le dernier hôte unique restant ;sinon le client RCCMD qui gère l'arrêt du VSAN pourrait ne pas être en mesure de terminer la routine d'arrêt car le second client RCCMD effectue un arrêt de machine virtuelle local.

Note

Qu'est-ce que la machine virtuelle et qu'est-ce que le « client RCCMD » ?

Fondamentalement, les deux appareils ne diffèrent pas l'un de l'autre : Les deux sont des machines virtuelles. Cependant, comme vous utilisez deux appliances, le nom de la machine virtuelle sur laquelle elles s'exécutent sera différent. En entrant le nom de la machine virtuelle, vous éviterez qu'un client RCCMD s'éteigne d'abord lui-même. Ainsi, si vous indiquez à RCCMD 2 le nom de sa propre machine virtuelle, il considérera que RCCMD 1 n'est qu'une autre VM et l'arrêtera. Lors de l'utilisation d'un vSAN, les commandes d'arrêt du CS141 permettent d'harmoniser le comportement d'arrêt des deux appareils.

Si vous utilisez un vSAN, faites attention au temps requis pour la séquence d'arrêt.

La raison d'utiliser un vSAN est de combiner une redondance maximale des données avec une disponibilité maximale des serveurs :
Fondamentalement, il n'y a aucune raison pour qu'un cluster vSAN s'arrête régulièrement.
Un arrêt complet est un problème d'urgence et doit être traité en conséquence :
Il est difficile de prédire combien de temps le vCenter prendra dans vSAN pour amener les hôtes en mode maintenance.
En principe, l'arrêt du vSAN s'effectue en trois étapes :

Extinction des machines virtuelles

A cette étape, l'ensemble des VM sont éteintes.

Phase de postsynchronisation

Ici, tous les hôtes synchronisent les données.

Passage en mode maintenance

Toutes les machines virtuelles sont éteintes et les données sont à jour. Les hôtes peuvent passer en mode maintenance.

La partie la plus critique est celle de la postsynchronisation. C'est un processus difficile qu'il faut évaluer :

Le mode maintenance peut être possible seulement si les données des hôtes sont à jour. Or, ce processus est dynamique et le temps nécessaire à sa réalisation dépend du niveau de matériel utilisé, du nombre de machines virtuelles ainsi que de la quantité et le type de données qui existent dans les machines virtuelles.

Pour compliquer les choses, ce processus se déroule dans le VSAN sans aucune information sur l'état actuel de synchronisation des données. Lorsque les hôtes sont en mode maintenance, cela signifie que le processus est terminé.

Cependant, le temps disponible est déterminé par le temps de fonctionnement maximum de l'onduleur :

RCCMD a besoin de paramètres de minuterie valides qui non seulement utilisent les temps calculés pour un arrêt, mais qui respectent également le temps de fonctionnement accordé de l'onduleur :

Assurez-vous que ce temps :

- Permet d'éteindre le vSAN quand il est fonctionnel.
- Contient un peu plus de temps si la phase de postsynchronisation a besoin de plus de temps que prévu.
- Permettre à l'onduleur d'assurer son temps de fonctionnement.
- Assure également la fermeture des autres hôtes et clusters.

Note :
Avant de commencer la configuration pour l'extinction de vSAN, plusieurs informations sont nécessaires :

1. Un aperçu du temps qu'un UPS peut accorder pour un arrêt ordonné
2. Combien de temps faut-il pour un arrêt manuel ?

Note :

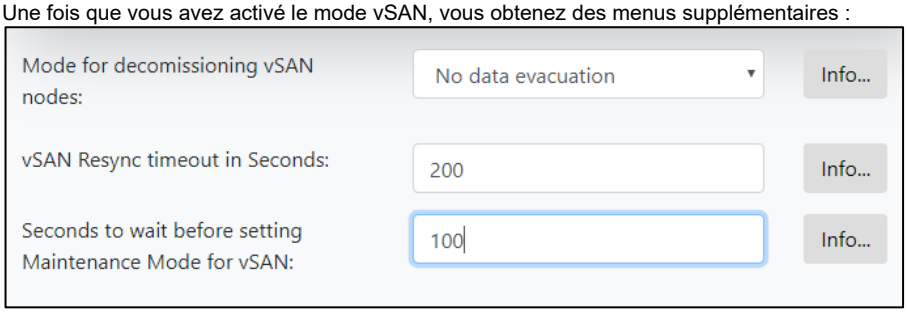
En raison du fait qu'un vSAN est sensible aux défaillances d'arrêt, il est techniquement un processus critique qui nécessite votre attention.

Préparation de RCCMD pour vSAN

Dans « Paramètres VMware », activer « Hosts are also vSAN nodes»

Pour gérer la tâche d'arrêt, assurez-vous que l'appareil RCCMD est situé à l'extérieur du cluster vSAN.

Une fois que vous avez activé le mode vSAN, vous obtenez des menus supplémentaires :



Mode de mise hors service des nœuds vSAN

Laissez le mode de mise hors service en mode « No data evacuation ». Ce mode est la méthode la plus rapide pour éteindre un cluster vSAN :
Les machines virtuelles sont arrêtées de manière structurée et toutes les données sont synchronisées sur tous les hôtes affectés.

Définition du délai d'attente de la fonction vSAN Resync

Contrairement à la procédure par défaut, le vCenter devient actif après l'arrêt de la machine virtuelle et commence à synchroniser tous les enregistrements du cluster.

Cette phase de post synchronisation définit la phase critique de la procédure d'arrêt :

L'ensemble des données des machines virtuelles doivent être synchronisés avec les données en miroir stockées sur d'autres hôtes.
Tant que cet état système synchrone n'est pas atteint, le mode maintenance ne peut aboutir sur aucun hôte.

Note:

Ce processus est très dynamique et dépends du type de données que vous avez besoin de synchroniser. Si vous avez créé des nouvelles machines virtuelles, le temps de synchronisation ne changera que marginalement. Cependant, il peut aussi arriver que vous créiez une machine virtuelle et que vous augmentiez ainsi le temps de post-sync. Dans d'autres scénarios, les données dans la machine virtuelle peuvent croître organiquement à cause de l'utilisation, ce qui à son tour affecte le temps requis :

Cette valeur ne peut pas être déterminée lors de la première installation en tant que valeur fixe, elle doit être vérifiée régulièrement pour vérifier son actualité et être ajustée si nécessaire.

Le vCenter prend tout le temps nécessaire pour ce processus. Ce laps de de temps est en lien avec le temps défini qui peut être fournie par l'onduleur pendant une opération d'alimentation de secours. Vous devez calculer le temps pour donner au vCenter une réserve au cas où la période calculée serait insuffisante.

Définition du mode de maintenance du vCenter.

Ce paramètre définit le temps dont dispose le vCenter pour s'éteindre après la synchronisation des données. Si le vCenter fonctionne comme une machine virtuelle dans le vSAN, ce moment devient intéressant : Après ce temps, les hôtes sont mis en mode maintenance et le vCenter est éteint par son hôte.

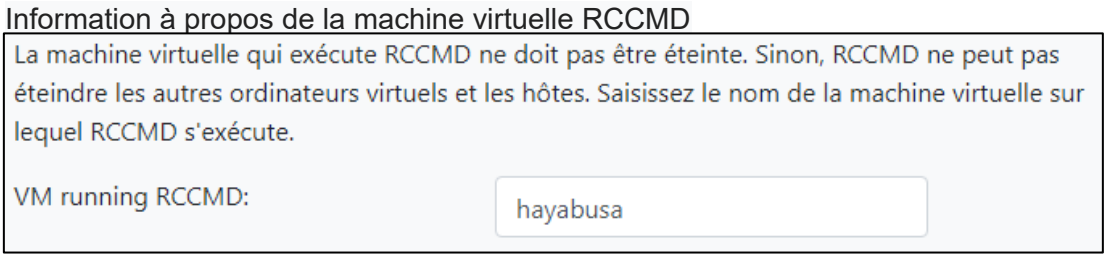
Entrer les données pour vSAN gérant vCenter

Étant donné que RCCMD doit coordonner l'ensemble du processus avec le vCenter, les données d'accès du vCenter, qui gère vSAN, sont nécessaires.

Sur cette page de configuration, ne saisissez pas d'informations d'identification pour chaque hôte.

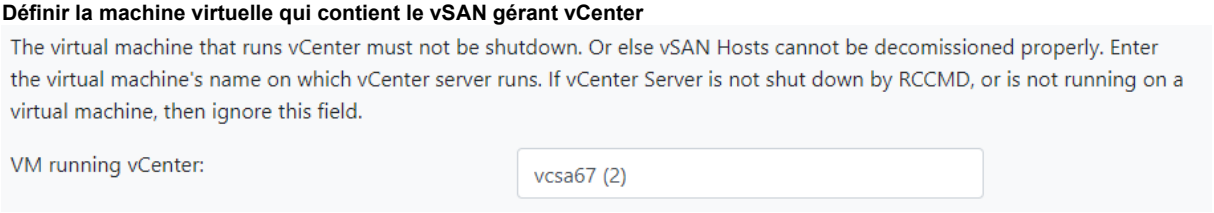
Définir le client vSAN gérant RCCMD :

RCCMD a pour tâche d'éteindre toutes les machines virtuelles et d'éteindre les hôtes à la fin. Puisque dans un vCenter, non seulement un vSAN mais aussi d'autres hôtes peuvent être mappés, RCCMD peut aussi les arrêter. Il y a deux exceptions qui nécessitent plus d'attention :



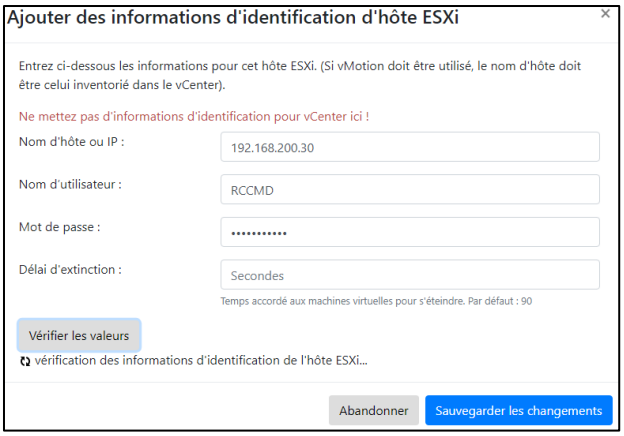
Bien que RCCMD lui-même ne puisse pas s'exécuter dans vSAN, le vCenter qui gère le vSAN peut inclure des hôtes supplémentaires dans sa liste. L'appliance RCCMD est une machine virtuelle qui doit respecter les commandes de contrôle de l'hôte sur lequel elle s'exécute - si l'hôte signale un arrêt, l'appliance le fera. Pour éviter que RCCMD ne se donne par inadvertance une commande d'arrêt, entrez le nom de la machine virtuelle que vous avez choisie pour RCCMD. Une fois saisie, la machine virtuelle qui porte ce nom sera exclue du processus d'arrêt.

Définir la machine virtuelle qui contient le vSAN gérant vCenter



Dans le système vSAN, le vCenter effectue des tâches administratives spéciales, mais est également une machine virtuelle. Pendant l'arrêt, RCCMD obtient d'abord une vue d'ensemble des machines virtuelles actives, puis les éteint, les migre, etc. Avec ce paramètre, RCCMD saura laquelle des machines virtuelles est le vCenter et l'éteindra exclusivement comme la dernière machine dans la procédure d'arrêt du vSAN.

Définition des nœuds hôtes vSAN ESXi



Définir les hôtes que RCCMD doit fermer. Les machines virtuelles peuvent être déplacées vers d'autres hôtes via le vCenter. Pour éteindre un hôte, RCCMD a besoin des informations suivantes :

Nom d'hôte / adresse IP

Nous recommandons d'utiliser l'adresse IP de l'hôte pour éviter les problèmes lorsque des parties de l'infrastructure (DNS) sont hors service.

Étant donné que RCCMD prend en charge les noms d'hôtes, vous pouvez également entrer un nom d'hôte.

Utilisateur

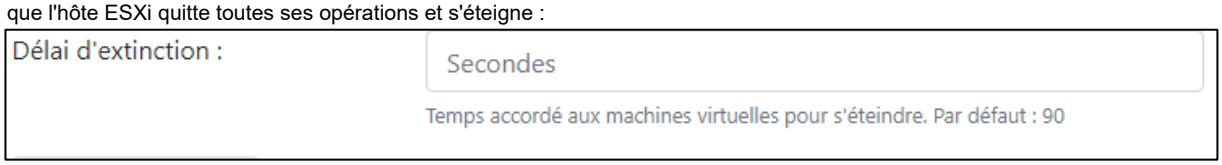
Un utilisateur disposant des droits systèmes appropriés pour fermer l'environnement VMware en conséquence. Normalement, c'est l'administrateur local de l'hôte.

Mot de passe

Le mot de passe attribué à l'utilisateur qui permet à RCCMD de s'authentifier comme autorisé.

Délai d'arrêt

L'étape suivante consiste à déterminer combien de temps RCCMD devrait permettre aux machines virtuelles de s'arrêter avant que l'hôte ESXi quitte toutes ses opérations et s'éteigne :



vSAN présente une particularité par rapport aux autres modes de fonctionnement :

La durée d'arrêt définit généralement la fenêtre de temps qu'un hôte accorde aux systèmes d'exploitation des machines virtuelles avant que la machine virtuelle ne soit simplement mise hors tension. Cela n'a pas d'importance si un vCenter a déjà essayé de migrer des machines ou non.

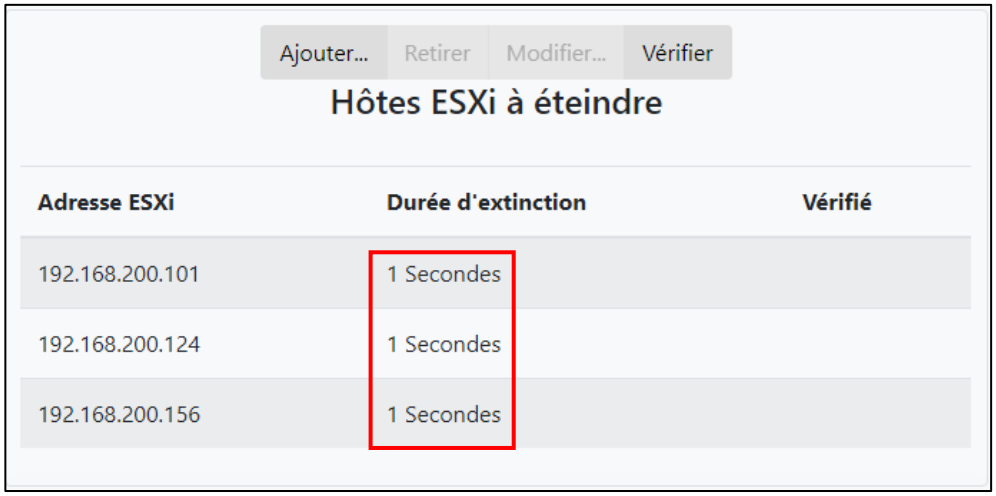
Lorsque cette commande est émise aux hôtes exécutant vSAN, plus aucune machine virtuelle a besoin d'être éteinte car :

- Tous les hôtes doivent être en mode maintenance

- Un hôte ne peut être en maintenance que si toutes les machines virtuelles sont déplacées ou éteintes.

Pour les hôtes vSAN, cela signifie que le temps d'arrêt des machines virtuelles peut être fixé à 1 seconde :

La routine d'arrêt d'un vSAN a déjà mis tous les hôtes en mode de maintenance. Par conséquent, aucun laps de temps n'est nécessaire pour accorder aux systèmes d'exploitation d'une machine virtuelle la possibilité de s'arrêter.



INFOSEC UPS SYSTEM – 15, rue du Moulin – 44880 SAUTRON - FRANCE - www.infosec-ups.com
Hot Line – Tel + 33 (0)2 40 76 15 82 - Fax + 33 (0)2 40 94 29 51 - hotline@infosec.fr – 08 19 AA XX 202 09

Rôle spécial : Le serveur des témoins

Les petits systèmes vSAN ne disposent pas des ressources nécessaires pour pouvoir ajuster indépendamment toutes les données.

Pour éviter les problèmes de synchronisation des données dans les systèmes vSAN minimalistes, un serveur témoin est utilisé :

Ce serveur témoin agit en tant qu'hôte autonome dans vSAN, mais n'est pas responsable de l'hébergement et de la gestion des machines virtuelles. Dès que les hôtes sont incapables de s'accorder sur l'ensembles de données, le serveur témoin décide quel hôte doit synchroniser les données.

Le serveur témoin peut être à la fois une machine physique réelle avec son propre matériel ou une machine virtuelle agissant comme un hôte physique mais fonctionnant virtuellement. Les nœuds vSAN ne peuvent pas voir la différence entre les différentes stratégies de configuration d'un serveur témoin.

Mais cette différence affecte la configuration du RCCMD :

Si vous utilisez un vrai serveur témoin en tant que machine autonome :

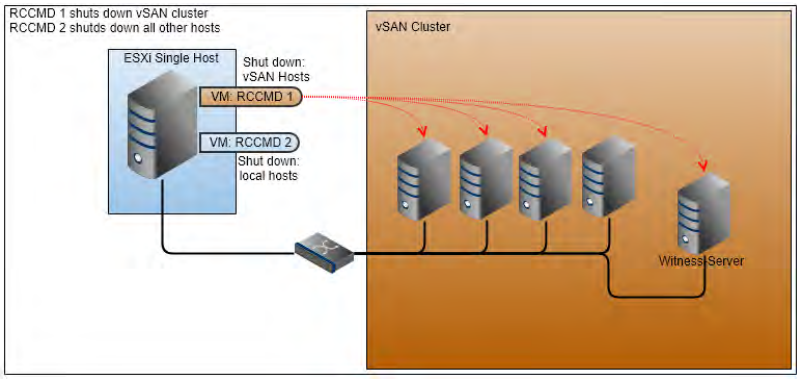
Dans ce cas, inscrivez le serveur témoin et tous les hôtes que vous voulez arrêter. Les hôtes passeront en mode maintenance et en conséquence :

- Arrêter les machines virtuelles

- Le vCenter effectuera la reSynchro.

- Les hôtes passent en mode maintenance

- Le matériel peut être éteint.



Lorsque vous utilisez une machine virtuelle pour exécuter un serveur témoin

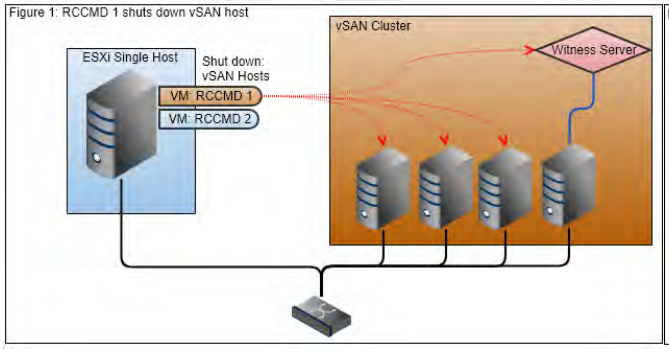
Si vous exécutez le serveur témoin en tant que machine virtuelle dans vSAN, vous devez différencier l'hôte sur lequel le serveur témoin est stocké et le serveur témoin comme hôte autonome. Puisque le serveur témoin agit comme un hôte dans le vSAN, il est perçu et traité en conséquence - Le type d'installation n'a pas d'importance :

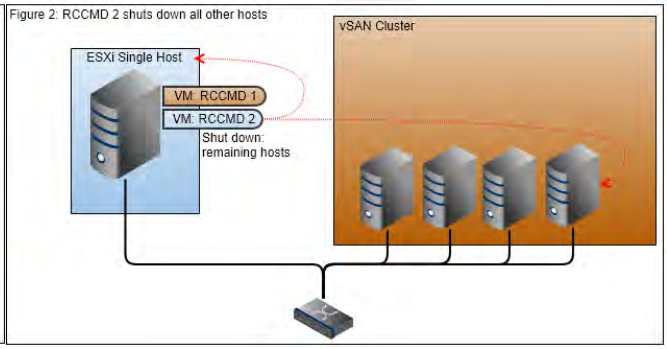
Alors que l'hôte qui maintient la machine virtuelle du témoin en interne ne perçoit qu'une seule machine virtuelle exécutant un système, il accepte le serveur témoin comme un hôte autonome et un nœud sur le réseau. Si la mauvaise adresse IP a été spécifiée, l'hôte responsable de la machine virtuelle répondra correctement :

- L'hôte arrêtera l'exécution de la machine virtuelle

- L'hôte passe en mode Maintenance

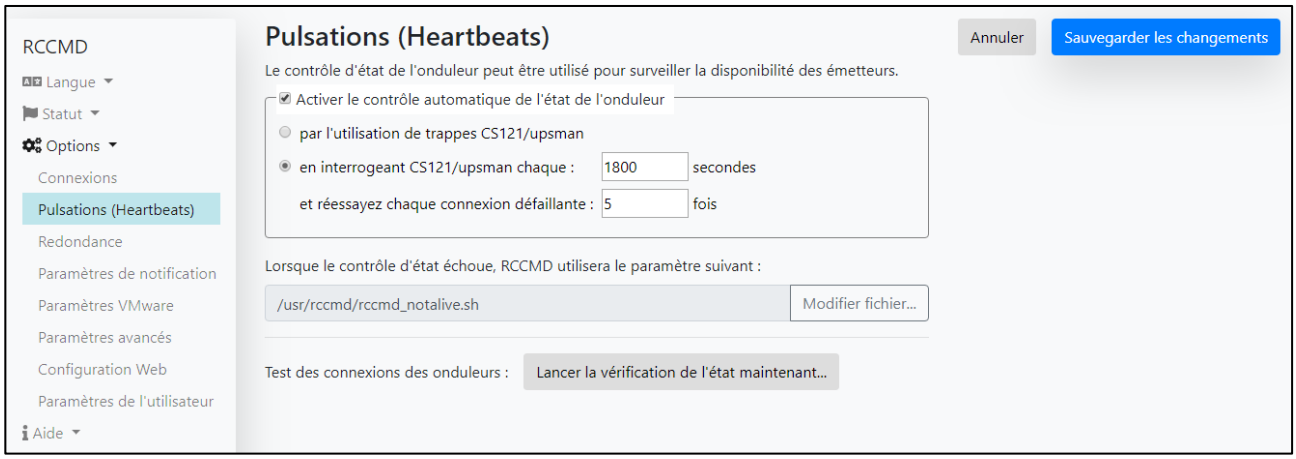
Cependant, étant donné que le serveur témoin (bien que virtualisé) représente un nœud d'hôte et de réseau à part entière, il doit donc être traité comme un hôte réel et mis en mode maintenance avant d'être désactivé. Officiellement, vous avez besoin de deux appareils RCCMD pour éteindre un vSAN. Si vous utilisez un serveur témoin virtualisé, vous pouvez utiliser le deuxième RCCMD pour éteindre régulièrement l'hôte qui gère le serveur témoin virtuel.





7.3. Signaux de présence (Heartbeat)

La fonction de signaux de présence fournit une recherche de disponibilité. La communication entre le client RCCMD et le serveur associé peut être surveillée et enregistrée :



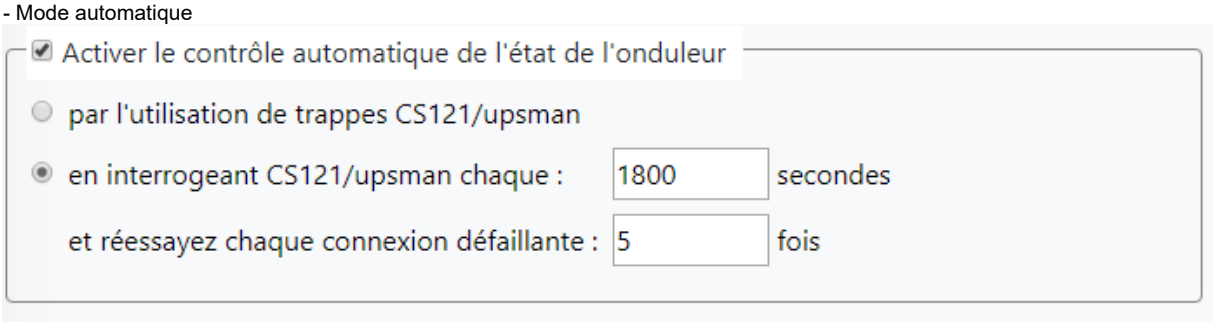
En principe, deux sources sont vérifiées :

1. L'accessibilité générale du réseau
2. Le service UPSMan du CS141

Ce test n'est pas conçu pour exécuter des diagnostics réseau complexes. RCCMD peut utiliser ce test pour savoir si le dispositif d'envoi de signal RCCMD est disponible et s'il fonctionne correctement.

Le client RCCMD offre deux options de base :

- Mode automatique



.

Vous pouvez choisir entre deux options :

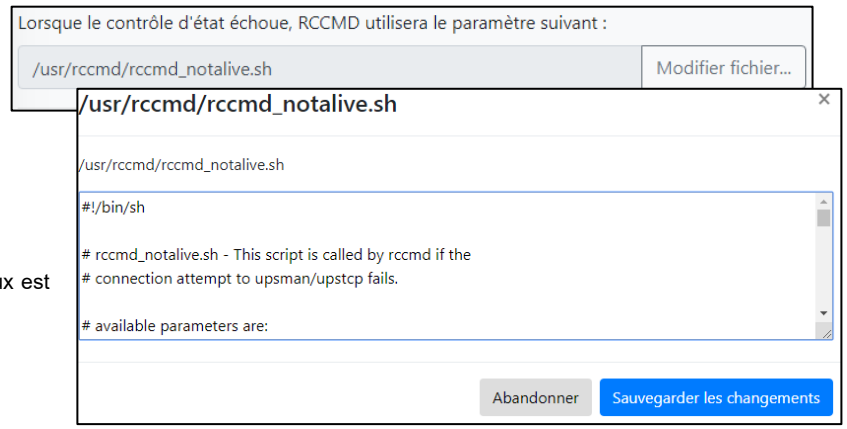
Traps UPSMAN

Le serveur RCCMD envoie un message au client RCCMD. La réception de ce message est enregistrée en conséquence.

Par Polling

Le client RCCMD demande cycliquement un message du serveur RCCMD et enregistre l'accessibilité de la station distante. En cas de perte de connexion, les requêtes peuvent être répétées aussi souvent qu'elles ont été configurées. Si l'interrogation échoue, un script automatique peut être lancé.

Ce script peut être personnalisé librement selon vos besoins. Avec « Edit File » pouvez éditer et adapter directement le fichier dans le navigateur Web.



Pour éditer ce fichier, la connaissance des scripts Linux est nécessaire.

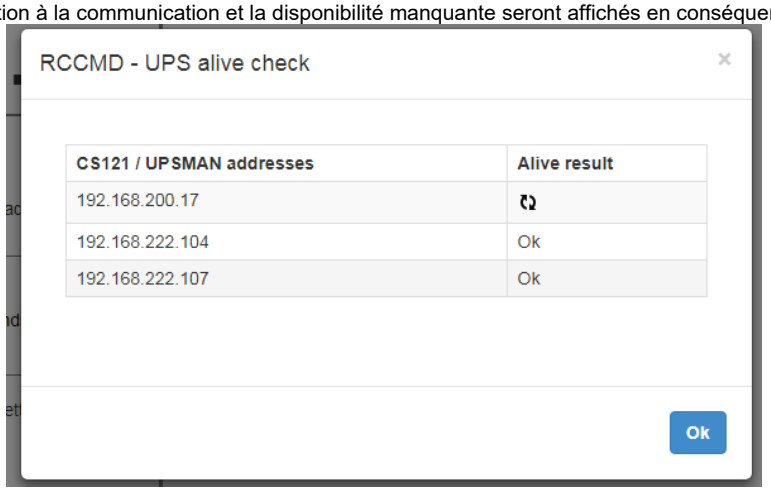
Mode manuel

Avec les connexions test UPS, RCCMD fournit un outil qui permet une consultation rapide des tests d'accessibilité.

Exécutez le contrôle de test en vie de l'hôte

Ouvre une fenêtre supplémentaire. Tous les dispositifs RCCMD entrés à « Connexions » sont listés et seront interrogés.

Le manque de préparation à la communication et la disponibilité manquante seront affichés en conséquence :



… Test en cours

Ok … Test finit, l'appareil est prêt et le service UPSMan est démarré

Not Ok … Test finit, l'appareil n'est pas trouvé

Note: RCCMD affichera le résultat à des fins d'information et de dépannage.

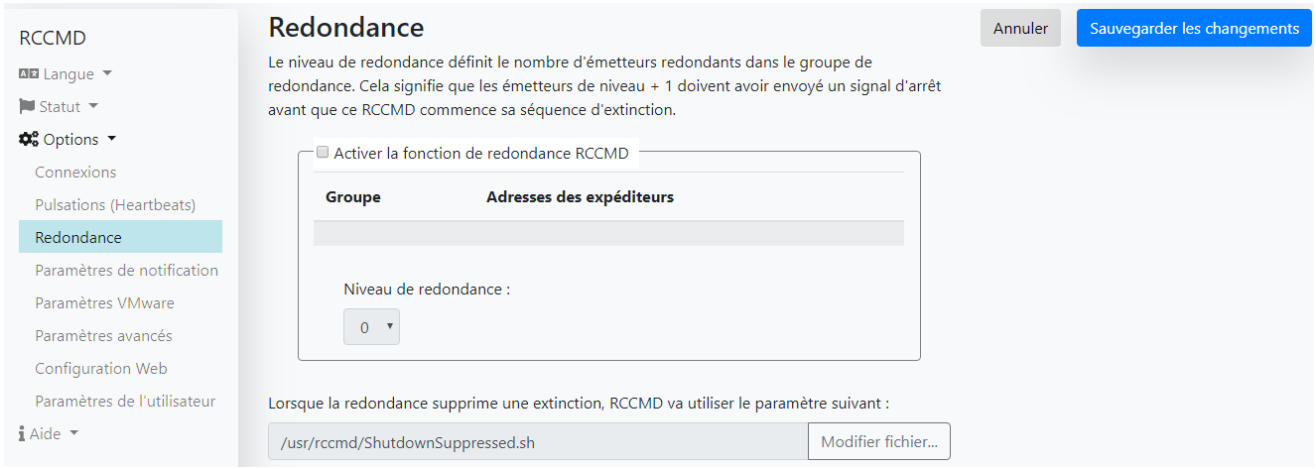
Un contrôle de test de vie de l'hôte peut échouer dans les conditions suivantes :

- Panne de réseau ou panne d'infrastructure
- L'appareil cible est éteint
- Ports verrouillés ou mal configurés
- Acheminement incorrect
- Le service UPSMan ne répond pas

Contrairement à l'interrogation automatique, aucun script automatique n'est exécuté en cas d'échec, car RCCMD suppose qu'un administrateur autorisé surveille ce processus de consultation manuelle.

Veuillez noter que la configuration ne prendra effet qu'après que vous aurez appuyé sur le bouton vert Enregistrer les modifications, car le client RCCMD doit être redémarré pour cette fonction.

7.4. Redondance



La redondance dépend des réglages des connexions et des signaux de présence :

Pour que la redondance fonctionne correctement, deux conditions préalables :

1. deux adresses IP valides doivent être spécifiées sous « Connexions ».

Au moins deux adresses IP doivent être stockées et permettre les commandes RCCMD entrantes.
La redondance signifie que RCCMD ne doit pas arrêter le serveur tant qu'au moins deux émetteurs n'ont pas donné l'ordre de mettre l'hôte hors tension.

2. Les signaux de présence doivent être réglés « contrôle automatique de l'état de l'onduleur en interrogeant CS121 (Polling) ».

RCCMD est chargé, par les signaux de présence, de vérifier automatiquement la disponibilité des adresses IP enregistrées :
Si un onduleur enregistré devient injoignable et que le système de redondance s'arrête, le RCCMD supposera qu'il y a un problème grave et arrêtera le système en ignorant le paramètre de redondance.

Note:
Gardez à l'esprit que les intervalles peuvent être cruciaux pour un arrêt.

Note : Le comportement de redondance se réfère exclusivement à l'arrêt de la commande RCCMD.

Les autres commandes sont traitées individuellement et enregistrées en conséquence. Avec la possibilité d'exécuter vos propres scripts, RCCMD offre des options pour contourner les procédures standard en cas d'urgence.

Définition des niveaux de redondance

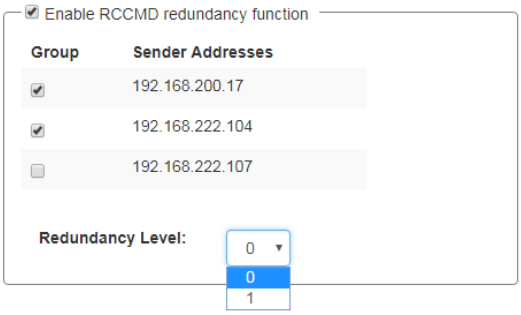
Activez d'abord la fonction de redondance de RCCMD.

Sélectionnez ensuite les adresses IP qui sont autorisées à envoyer un signal d'arrêt.

Le niveau de redondance dépend du nombre d'appareils sélectionnés :

Nombre d'unités sélectionnées X -1

En utilisant deux dispositifs, les deux doivent envoyer un signal d'arrêt RCCMD.



Étant donné que deux systèmes seulement ont été sélectionnés, seul un système supplémentaire au maximum peut envoyer cette commande. Il n'est donc pas important de savoir quel appareil est le premier expéditeur - ceci peut changer dynamiquement.

Pour 3 systèmes sélectionnés, la valeur maximale est 2 :

Si 1 unité + 2 autres unités instruisent l'arrêt, celui-ci sera exécuté.

Avec 3 systèmes, vous pouvez également modifier le niveau de redondance à 1 :

Par conséquent, deux systèmes sur trois sont nécessaires pour que RCCMD arrête le serveur. La combinaison peut changer dynamiquement. Si vous souhaitez simplement avoir 2 onduleurs sur 3, il est recommandé de les sélectionner et de régler le niveau de redondance à 1, ce qui signifie que l'arrêt ne sera effectué que si les deux onduleurs sélectionnés envoient une commande de mise hors tension.

Ne pas oublier :

Avec la redondance, vous combinez plusieurs appareils. Sous les connexions, vous autorisez les signaux d'arrêt généraux entrants. Par conséquent, il est possible de configurer un arrêt redondant ainsi que plusieurs émetteurs d'arrêt unique.

Note
N'oubliez pas qu'une instruction d'arrêt reste active jusqu'à ce que le système qui a donné l'instruction d'arrêt la retire explicitement. Ceci est contrôlé via la commande personnalisée RCCMD.

Arrêt avec deux systèmes UP

En cas de signal d'arrêt, la redondance vérifiera la connectivité et la disponibilité du deuxième système UPS. S'il répond correctement, le signal d'arrêt sera supprimé avec réserve jusqu'à nouvel ordre :

Dès que le deuxième système ordonne l'arrêt, cette commande est exécutée et le système s'arrête. Si un signal d'arrêt est envoyé par le premier système et que le deuxième système n'est pas joignable, RCCMD arrête le système - dans ce cas, RCCMD suppose que le deuxième système n'est pas disponible..

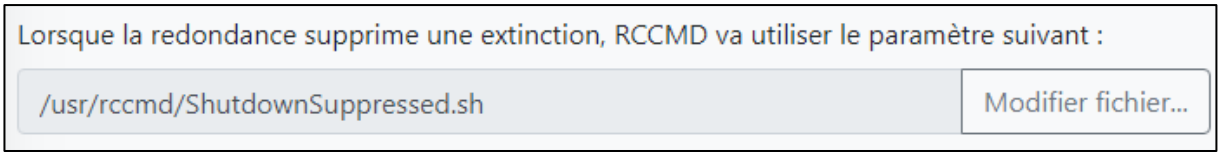
Arrêt avec 3 systèmes valides

A partir de trois appareils, le comportement de redondance peut être adapté individuellement aux conditions nécessaires :

1. si l'un des trois systèmes envoie un arrêt d'urgence
2. lorsque deux systèmes sur trois envoient un arrêt d'urgence
3. les trois systèmes doivent décider ensemble de l'arrêt

Chaque système peut donner des instructions individuelles et retirer son arrêt via la commande personnalisée RCCMD. En général, RCCMD n'exécutera pas l'arrêt tant que la condition d'arrêt exacte n'est pas remplie.
Scripts liés à la redondance

Si vous utilisez la redondance, le client RCCMD attend pour exécuter l'arrêt jusqu'à ce que le nombre approprié de dispositifs donne également des instructions d'arrêt.

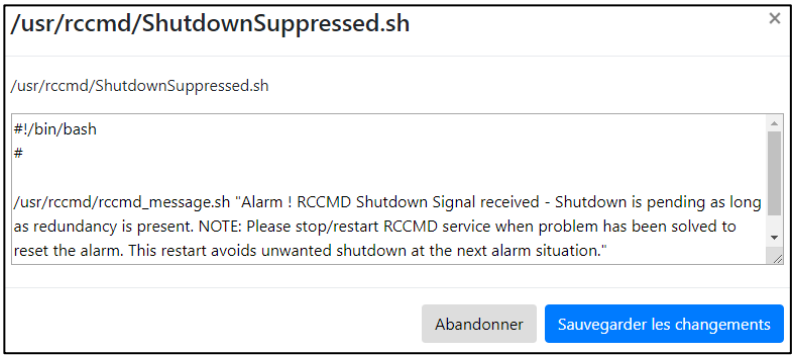


Comme ce processus a un impact direct sur le fonctionnement des serveurs surveillés par RCCMD, un script sera lancé pour indiquer un incident.

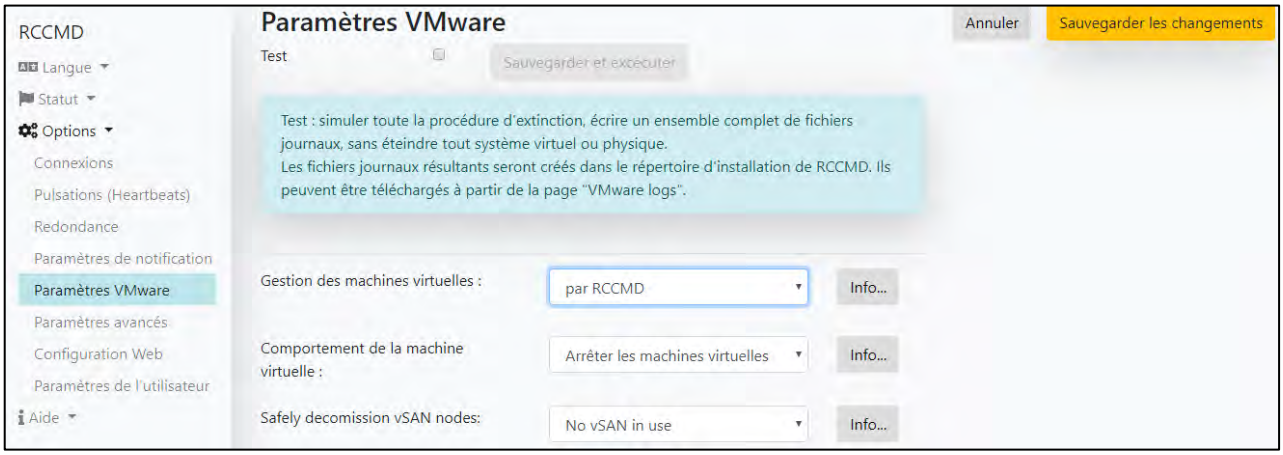
Utilisez « Edit File » pour personnaliser et adapter ce script à vos besoins individuels.

Abandonner fermera l'éditeur et retirera toutes les modifications que vous avez apportées.

Par défaut, une notification texte est prédéfinie pour indiquer un comportement d'arrêt basé sur la redondance.



7.5. Paramètres VMware



Les paramètres VMWare contrôlent le comportement général d'arrêt des serveurs et des hôtes dans VMware. Selon le niveau de configuration et le type de configuration, différents types de configuration sont nécessaires pour gérer une infrastructure VMware. En plus des données de base obligatoires telles que les informations d'identification des utilisateurs, 'adresses IP, vous pouvez avoir besoin, entre autres, de connaissances plus spécifiques sur le comportement d'arrêt de votre environnement informatique.

Veuillez noter que certaines données ne sont pas statiques. Les valeurs peuvent changer et doivent être ajustées lors des contrôles réguliers du système.

➔ RCCMD évalue et affiche les temps d'arrêt estimés en fonction des données saisies.

Part 1: Installation basique

Les paramètres de base supposent que vous utilisez des hôtes sans vCenter. Vous pouvez éteindre autant d'hôtes que vous le souhaitez avec un seul appareil RCCMD.

Gestion des machines virtuelles

Ce menu définit si vous voulez que les hôtes et les machines virtuelles soient gérés par RCCMD ou par un vCenter. Si vous utilisez les hôtes en mode verrouillage, par exemple, les commandes de contrôle sont approuvées exclusivement par un vCenter. Même si vous saisissez correctement les informations d'identification, l'hôte refusera l'exécution de la commande.

Dans le réglage par défaut, « par RCCMD »; est préréglé.

Comportement de la machine virtuelle

Utilisez ce paramètre pour définir si vous voulez utiliser vMotion ou simplement éteindre vos machines. L'arrêt d'une machine virtuelle sera contrôlé directement par l'hôte : les machines virtuelles sont arrêtées normalement, puis l'hôte est éteint.

Si vous activez vMotion, l'arrêt local des machines virtuelles est le protocole secondaire. Tout d'abord, le vCenter va essayer de déplacer les machines virtuelles vers un autre hôte.

Le réglage par défaut est « Arrêter les machines virtuelles ».

➔ Si le mode maintenance est sélectionné, des informations supplémentaires sont requises comme les informations d'identification du vCenter ainsi qu'un nombre de secondes qui devrait être disponible pour que le vCenter puisse déplacer les machines virtuelles vers un autre hôte.

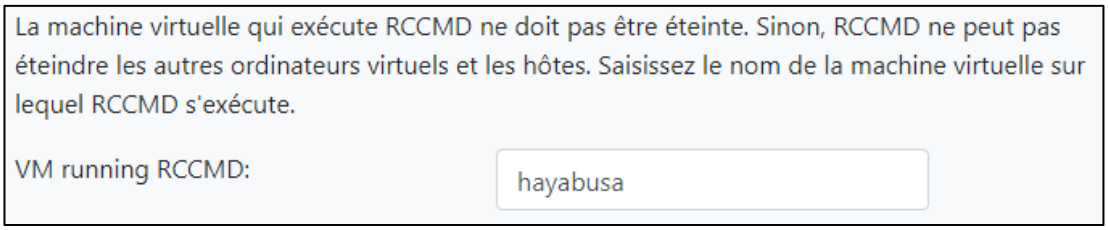
Mise hors service en toute sécurité des nœuds vSAN en cas d'utilisation non autorisée

Ce paramètre définit le comportement d'arrêt en cas d'utilisation d'un vSAN. Le vCenter fournit différents paramètres de base, à sélectionner à ce point de configuration. Si vous souhaitez utiliser un vSAN géré par RCCMD, reportez-vous aux exigences de base qui doivent être remplies.

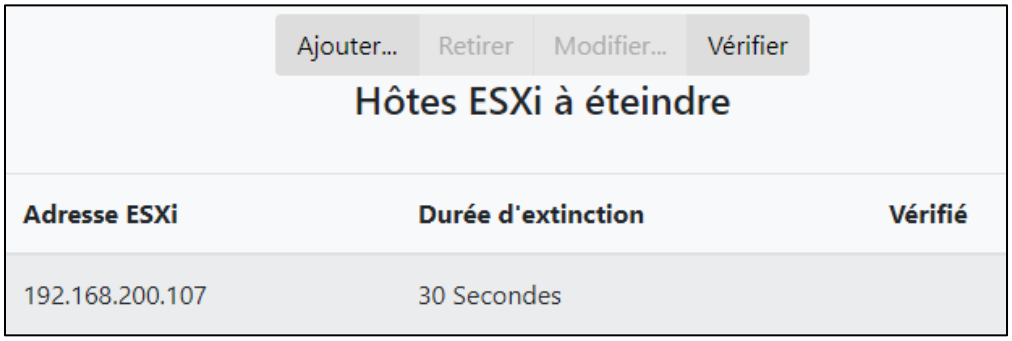
Le paramètre par défaut est « No vSAN in use ».

VM exécutant RCCMD

RCCMD a besoin de connaître le nom de la machine virtuelle qui contient l'appliance RCCMD. Cette option permet de prévenir contre l'extinction accidentel du client RCCMD.



Tous les ESX sont éteins par RCCMD



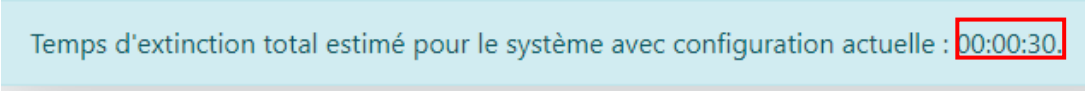
Avec cette boîte de dialogue de configuration, déclarez quels hôtes ESXi doivent être fermés par RCCMD :

La barre de menu offre plusieurs fonctions :

- Ajouter : Ajouter un autre hôte.
- Retirer : Sélectionnez un hôte et cliquez sur Supprimer pour le supprimer de la liste actuelle.
- Modifier : Sélectionnez un hôte. Avec Editer, vous pouvez éditer les données d'accès.
- Vérifier : Si vous appuyez sur ce bouton, la configuration actuelle sera sauvegardée et les données de connexion seront validées. Une fois vérifié, RCCMD affiche la tentative de connexion.

Estimé la durée d'extinction

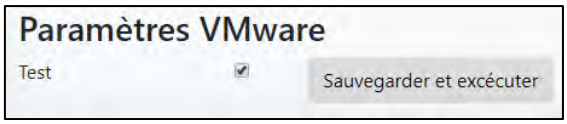
Une fois que la configuration est faite, RCCMD affiche une estimation du temps d'arrêt :



Il s'agit du temps d'arrêt moyen actuel de votre infrastructure. Veuillez noter que ce temps d'arrêt est calculé et peut être utilisé pour le comparer avec le temps d'alimentation de secours accordé par l'onduleur.

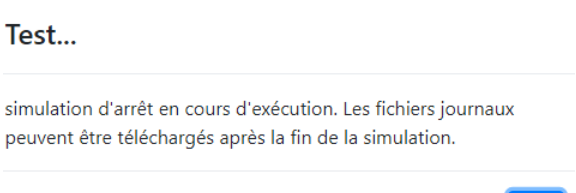
En raison du fait qu'il s'agit d'une valeur calculée : Veuillez tester votre réglage d'arrêt avant de l'activer !

Dry run (tests):



Avec le Dry Run, RCCMD offre une fonction unique dans les paramètres VMware :

Le Dry Run est un mode de simulation, dans lequel votre installation RCCMD simule le comportement, mais ne l'exécute pas physiquement.



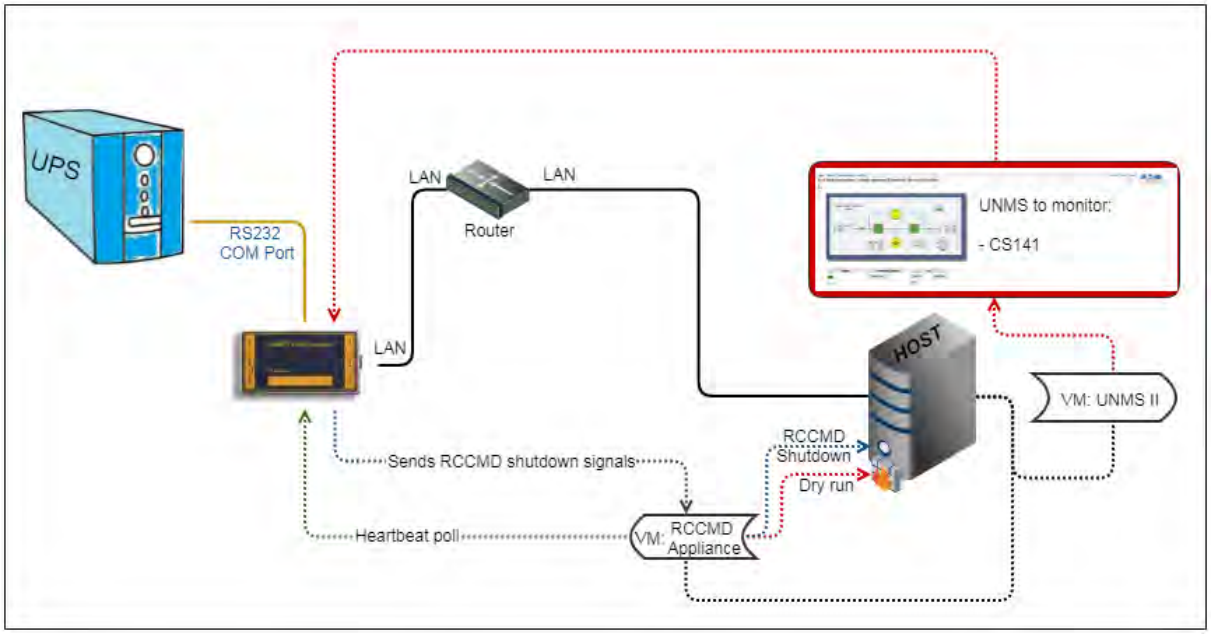
Cette fonction est utile lors de l'installation d'une installation RCCMD sur un serveur de production :

L'arrêt accidentel est ainsi évité. Avec « Enregistrer » et « Exécuter », cette fonction est activée, protégeant ainsi votre configuration future d'un arrêt accidentel.

Note

Certains menus de configuration sont verrouillés pendant le test et ne peuvent pas être ajustés.

Qu'est-ce que fait le Dry Run ?



Normalement, un CS141 est le serveur RCCMD qui envoie une commande RCCMD valide à un client RCCMD - le logiciel RCCMD. Vous pouvez utiliser la gestion des événements du CS141 pour envoyer des commandes individuelles afin de démarrer des scripts très délicats et complexes, il est possible d'automatiser un serveur via des scripts et donc vous n'avez pas nécessairement besoin d'éteindre un serveur avec RCCMD.

Avec VMware, l'appliance RCCMD diffère de l'installation client normale :

Il est conçu pour assurer une séquence d'arrêt structurée pour tous les hôtes dans un environnement VMware.

Pour s'acquitter de cette tâche, RCMMD a besoin de données d'accès accompagnées de droits d'accès au système pour permettre l'arrêt du système. Le problème est que RCCMD ne peut pas différentier une situation d'urgence réelle et un utilisateur qui appuie sur le bouton de test de la tâche. Pendant les essais, cela pourrait poser un problème. Dès que RCCMD accepte un signal valide, il lance la procédure d'arrêt.

Bien sûr, vous ne pouvez pas simplement éteindre tous les serveurs; pendant le fonctionnement parce que vous voulez tester votre configuration - éteindre un système en temps réel avec une disponibilité de 100% n'est utile que pour de vrais problèmes d'urgence.

Le Dry Run est un mode de simulation automatique intégré.

1. Tous les hôtes configurés seront contactés
2. Les identifiants des hôtes seront testés.
3. Un journal de protocole sera écrit pour afficher les problèmes de configuration ainsi que les tests de connexion réussis.
4. Le signal d'arrêt RCCMD standard est supprimé tant que le mode simulation est actif.

Tant que le Dry Run est actif, aucun arrêt d'urgence n'est possible via un serveur RCCMD valide.

Note:

Si vous modifiez ou ajustez les scripts standard fournis avec l'installation par défaut ou ajoutez de nouveaux scripts, ils seront exécutés en conséquence. Le Dry Run ne supprime que sa propre séquence d'arrêt standard - elle ne vérifie pas les modifications que vous avez ajoutées manuellement.

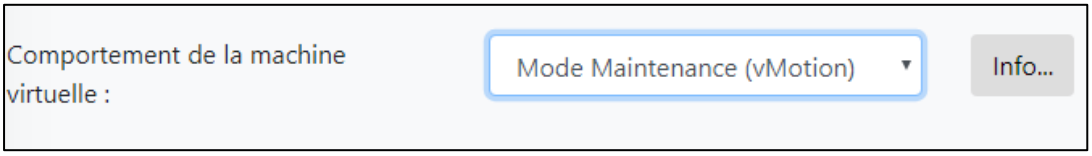
Ce comportement comporte des avantages et des inconvénients

1. Etant donné que vos scripts sont exécutés avec force, le Dry Run doit avoir lieu au préalable !

2. En ajoutant vos propres scripts qui déclenchent des actions inoffensives, vous pouvez vérifier si vos scripts fonctionnent et si tous les partages administratifs sur le système cible sont respectés.

Part 2: Paramètres avancés

Si le mode maintenance (vMotion) est sélectionné



RCCMD présente deux menus supplémentaires :

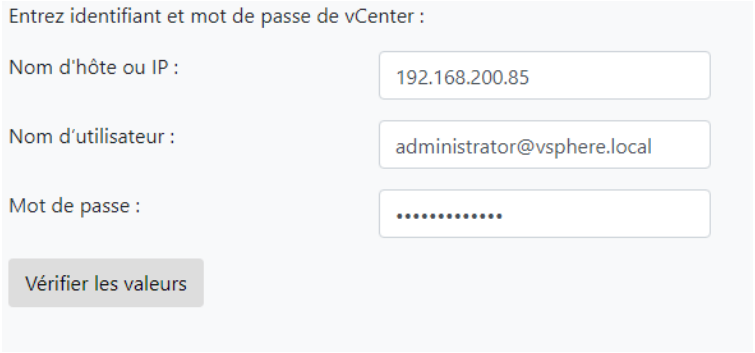
Délai d'attente du mode de maintenance en secondes

Cette valeur définit le temps que RCCMD accorde au vCenter pour déplacer les machines virtuelles vers l'hôte qui ne passent pas en mode maintenance.

Les machines virtuelles qui n'ont pas été migrées durant cette période seront arrêtées par l'hôte ESXi.

Informations d'identification vCenter

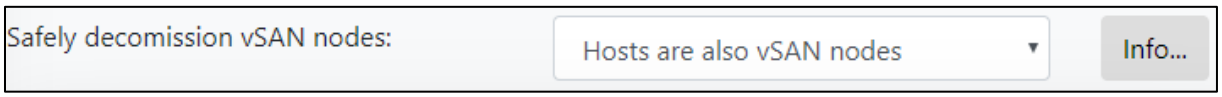
Pour utiliser vMotion, RCCMD a besoin des identifiants vCenter valides. Veuillez noter qu'un client RCCMD peut éteindre de nombreux hôtes, mais ne peut techniquement maintenir qu'un seul vCenter. Si vous avez besoin de configurer plusieurs types de configuration différents, il peut être nécessaire d'utiliser 2 appareils RCCMD qui fonctionnent ensemble.



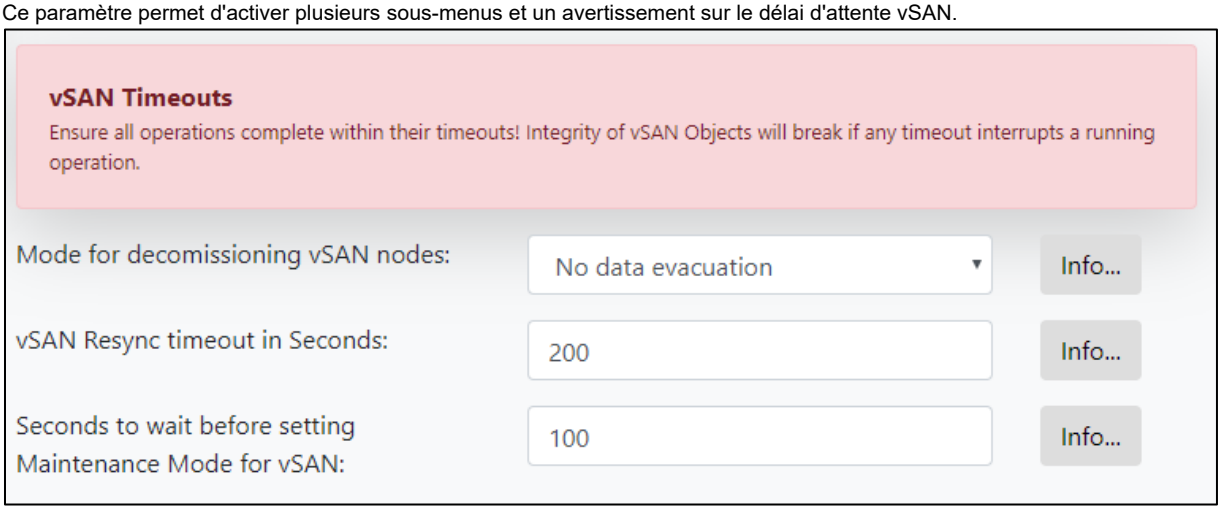
Check values

Test des identifiants du vCenter. RCCMD va essayer de se connecter au vCenter et donner un retour, y compris une raison pour laquelle la tentative de connexion a échoué.

Part 3: Sélectionner « Host are also vSAN nodes »



Ce paramètre permet d'activer plusieurs sous-menus et un avertissement sur le délai d'attente vSAN.



Gardé un œil sur le message d'avertissement !

vSAN est un peu délicat lorsqu'on exécute un arrêt. Il est même possible qu'un d'arrêt mal configurée entraîne une corruption des données ou même une perte totale de données.

Options d'arrêt du vSAN

Aucun déplacement des données

C'est le moyen le plus rapide d'assurer l'arrêt du système. RCCMD arrête les machines virtuelles, puis le vCenter synchronise tous les hôtes qui se trouvent dans le vSAN. Il n'y aura pas de migration de données ou de machines virtuelles à déplacer vers d'autres hôtes.

Déplacement de toutes les données vers d'autres hôtes

En principe, c'est la même fonction qui déclenche vMotion. Un vSAN peut également être réparti sur différents sites, de sorte que vous pouvez également déplacer des machines virtuelles vers des hôtes externes qui ne se trouvent pas dans le cluster vSAN que vous allez éteindre. Si vous utilisez vMotion, il sera exécuté en premier. De ce fait, il est possible que votre hôte vSAN ne possède aucune machine virtuelle nécessitant une migration. Mais vous pouvez l'utiliser comme deuxième possibilité pour déplacer les machines de votre vSAN.

Assurer l'accessibilité des données

Si vous disposez d'un vSAN de plus grande taille fournissant suffisamment de capacités pour des redondances, aucune donnée ne sera déplacée. La migration des données ne se fera que pour les données sans redondance.

Note

Avec les extensions vSAN, RCCMD introduit une solution pour vous permettre d'effectuer un arrêt d'urgence de l'ensemble du système vSAN aussi rapidement que possible. Les machines virtuelles qui ont déjà été migrées vers un autre emplacement via vMotion ne sont pas affectées.

Si vous voulez arrêter et fermer le vSAN parce qu'il y a une urgence, sélectionner « Pas d'évacuation des données » ; c'est le meilleur choix.

Délai d'attente de la resynchronisation vSAN en secondes

Ce paramètre est le temps de base que RCCMD accorde au vCenter pour synchroniser les bases de données entre les hôtes avant de la séquence d'arrêt. Cette valeur de temps est complexe, car le temps de resynchronisation est une valeur très relative ; en principe, vous pouvez dire qu'il dure aussi longtemps qu'il le faut. Le vCenter ne vous indique pas le temps de resynchronisation estimé, vous devez le tester pendant un arrêt manuel. Si votre vCenter annonce que le travail est terminé, vous disposez d'un délai minimum pour votre arrêt d'urgence. Veuillez calculer du temps supplémentaire car le temps mesuré lors d'un arrêt manuel n'est qu'un instantané et non une valeur générale.

Secondes d'attente avant de régler le mode de maintenance du vSAN

Une fois la resynchronisation terminée, le vCenter est la dernière machine virtuelle qui doit être arrêtée. Avec ce paramètre, vous définissez combien de temps le vCenter a de temps de s'éteindre avant que RCCMD commence la prochaine étape de la séquence d'arrêt.

Déterminer sur qu'elle VM fonctionne vCenter

A l'intérieur d'un vSAN, le vCenter :

Gère le transfert complet des données à l'intérieur d'un vSAN et gère la phase complète de postsynchronisation pendant l'arrêt du vSAN. Cela signifie :

Si le vCenter fonctionne à l'intérieur d'un vSAN ou sur un hôte qui sera éteint trop rapidement, le vSAN complet sera inutilisable. Si le vCenter est situé en tant que machine virtuelle dans le vSAN, RCCMD doit connaître le nom de la machine virtuelle afin de l'exclure de l'arrêt de la machine virtuelle.

Note:

Le vCenter qui gère un vSAN n'est pas toujours à l'intérieur de ce cluster - il peut être installé quelque part et géré séparément. Si la machine virtuelle avec le vCenter n'est pas dans la liste des hôtes à fermer, vous n'avez pas besoin de l'entrer à ce stade. Mais vous devez y jeter un coup d'œil si vous utilisez différents appareils RCCMD - Sans son vCenter, un vSAN ne peut pas s'éteindre comme prévu.

7.6. Paramètres de notification

Selon la commande reçue par un émetteur RCCMD valide, trois scripts de base sont exécutés automatiquement. Chaque script déclenche une fonction RCCMD. Les scripts RCCMD sont préconfigurées et il n'est normalement pas nécessaire de les modifier.

Cependant, si vous voulez exécuter vos propres scripts par RCCMD, vous pouvez soit écrire ces scripts directement dans le script. sh approprié et les exécuter comme une commande personnalisée, soit éditer ces fichiers de base.

Attention :

Si vous modifiez, personnalisez ou étendez ces scripts, vous modifiez le comportement global de RCCMD dans votre système. Assurez-vous d'effectuer une sauvegarde avant de modifier les scripts pour retrouver l'état d'origine du système. Toute modification de la configuration d'origine peut entraîner un comportement imprévisible du RCCMD et peut causer des problèmes à l'échelle du système.

Editez ces scripts sont à vos risques et périls !

Quand ces scripts seront-ils exécutés ?

RCCMD dispose de 3 scripts différents :

Notification par Email

Le CS141 s'appuie normalement sur son propre client de messagerie. C'est la méthode recommandée. Cependant, dans certains réseaux hautement sécurisés, il peut ne pas être souhaitable que le gestionnaire Web puisse envoyer ses propres mails. Le client RCCMD peut être utilisé comme interface pour transférer des messages courts.

Vous pouvez également utiliser ce script pour déclencher des scripts supplémentaires :

Envoyez un email ET exécutez le script suivant :

Pour cette fonction, l'outil gratuit Linux send mail est installé, ce qui permet à RCCMD d'envoyer des e-mails. Vous pouvez configurer l'outil à tout moment en vous connectant via une console sur l'interface Linux du client RCCMD.

Pour transférer un courriel à partir d'un CS141, utilisez les commandes personnalisées et entrez la commande suivante en entrant l'adresse IP :

Mail targetmailaddress@targetmailserver.com <Text message>

Sur la CS141, vous pouvez entrer :

Mail Kirk@enterprise.de Jean-Luc Picard était ici

RCCMD prendrait la relève et écrirait un mail à kirk@enterprise.de avec comme objet « Jean-Luc Picard était ici »

La seule fonction de ce script est-elle le déclencheur d'un email ?

Non, ce script peut être édité pour tout faire.

- ➔ Changer le script complet entraînera un changement de comportement et peut entraîner une exécution inattendue de RCCMD.
- ➔ Vous le modifiez à vos risques et périls.

Notification de message

Ce script contrôle la réception des messages et est responsable de leur affichage sur le moniteur. Parce que l'appliance RCCMD est un programme serveur non graphique qui s'exécute sans surveillance permanente, vous devriez laisser ce script simple il est :

Puisqu'il est déclenché par chaque signal de notification RCCMD entrant, un contenu supplémentaire serait également exécuté à chaque fois.

En raison du fait que c'est la plupart du temps sans fonction (pas d'interface graphique), vous pouvez l'utiliser pour les scripts.

- ➔ Changer le script complet entraînera un changement de comportement et peut entraîner une exécution inattendue du RCCMD.
- ➔ Vous le modifiez à vos risques et périls.

Notification d'exécution

Ce script est intéressant :

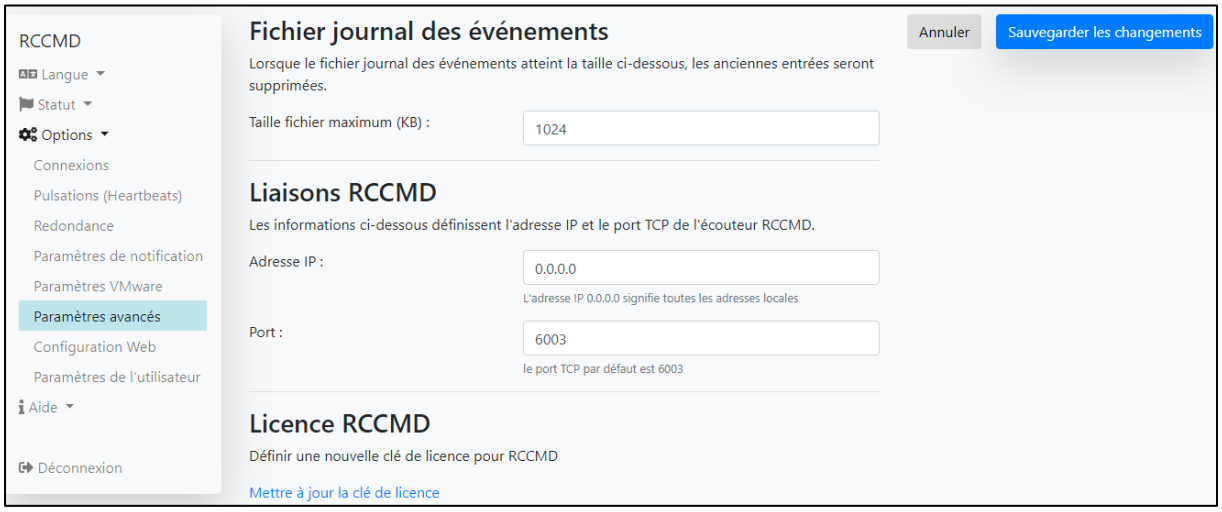
Il exécute toutes les commandes entrantes valides qu'un CS141 peut envoyer. Ce script déclenche l'arrêt d'urgence complète que RCCMD fournit.

Avec ce script, RCCMD vous fournira l'option unique d'ajouter et de déclencher votre propre solution de script d'arrêt personnalisée et même de programmer une routine non standard supplémentaire qui correspond exactement à votre réseau.

Ce script est une option très puissante et dangereuse parce que les changements interfèrent directement avec toutes les fonctions du RCCMD. Toute modification ou amélioration que vous apporterez aura une incidence directe sur le comportement de l'arrêt.

Des compétences avancées en scripts sous Linux sont essentielles pour modifier ce script !

7.7. Paramètres avancés

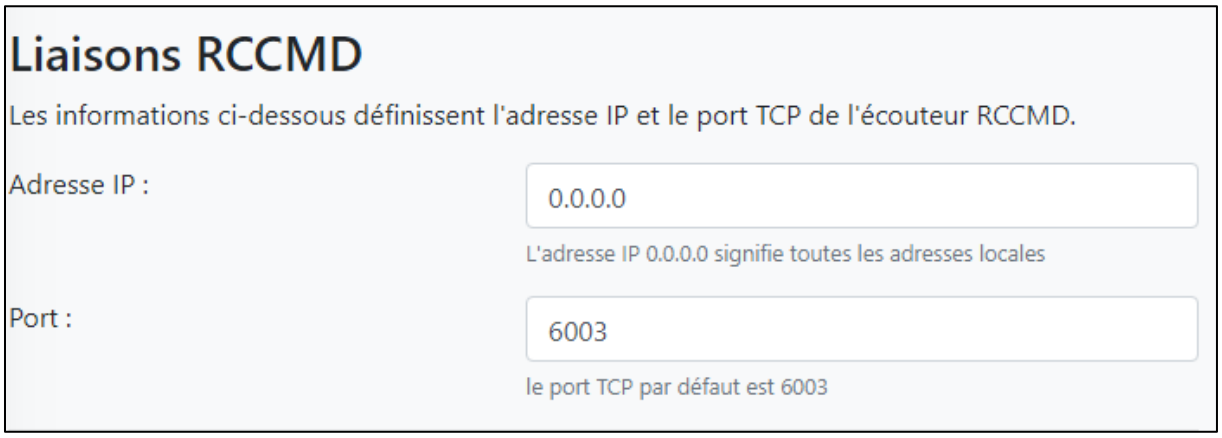


Utilisé l'onglet « Paramètres avancés » pour avoir davantage de paramètres pour configurer RCCMD. Le menu est divisé en 3 parties :

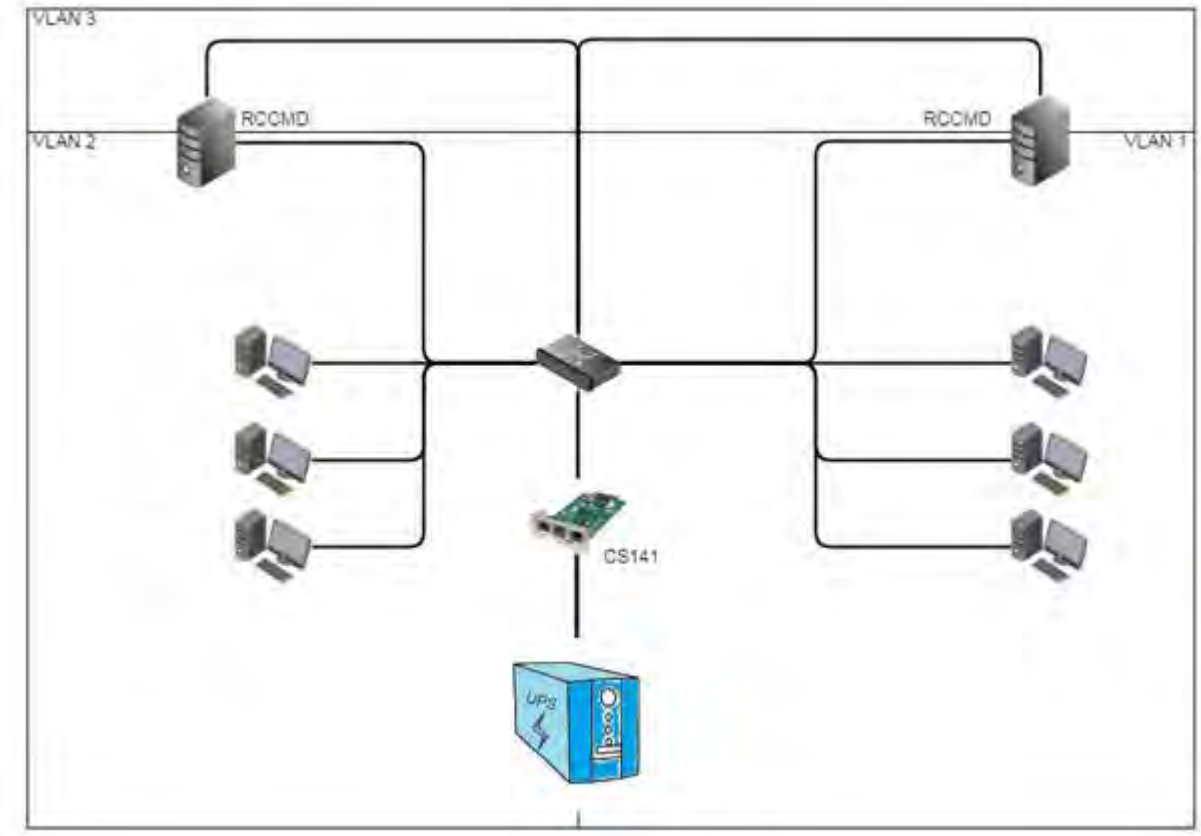
Fichier, journal des évènements

En général, tout signal RCCMD affectant le client sera enregistré. En raison du fait que les systèmes serveurs peuvent fournir des ressources mémoire limitées pour les fichiers journaux, il peut être nécessaire de limiter la taille du fichier journal à une taille maximale à consommer. Si la taille maximale du fichier est atteinte, l'entrée la plus ancienne est remplacée par une nouvelle entrée.

Liaisons RCCMD

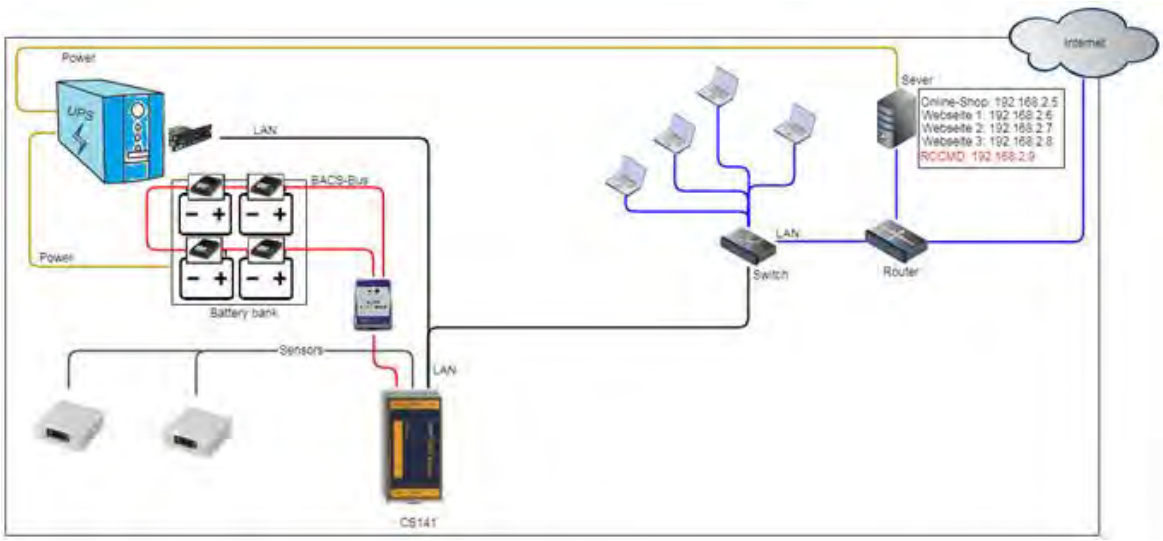


RCCMD Bindings est un outil sophistiqué qui vous aide à limiter le trafic. Étant donné que ce paramètre affecte profondément votre configuration réseau, il doit être utilisé avec prudence. Les liaisons permettent de forcer RCCMD à écouter sur une carte réseau spécifique. En cas d'utilisation du multi hébergement, l'écoute peut être configurée sur une adresse IP spécifique dans une carte réseau. A titre d'exemple, il sera utilisé s'il est nécessaire de diviser logiquement le réseau en un réseau de production et un réseau d'infrastructure via les VLAN :



Dans cet exemple de scénario, deux ou plusieurs adaptateurs réseau peuvent être installés. Le fait de lier RCCMD à une carte réseau spécifique empêchera les utilisateurs d'accéder au client RCCMD et d'arrêter accidentellement un serveur - ceci n'est possible que via des périphériques situés dans le VLAN 3 ou qui ont été correctement activés via un routeur.

Un autre scénario est ce qu'on appelle le multi hébergement :

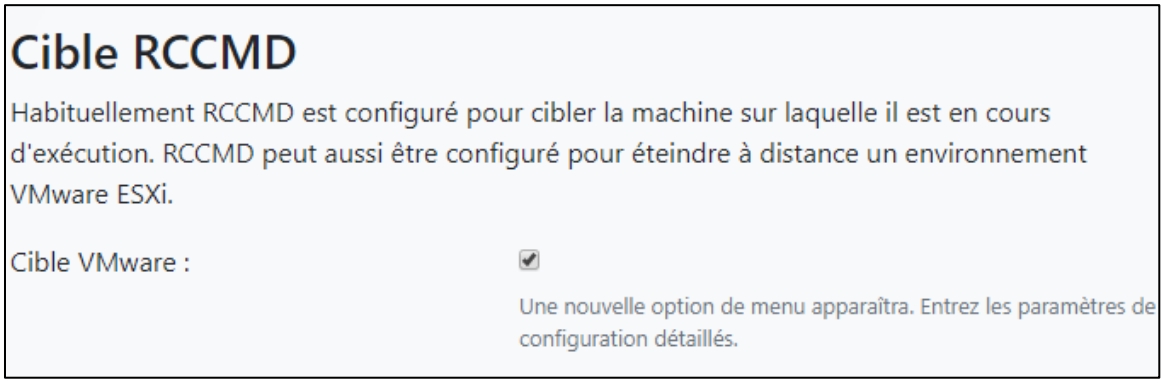


Il n'est pas nécessaire pour les périphériques réseau modernes qu'une adresse IP soit fermement liée à une interface réseau. En fait, plusieurs adresses IP peuvent être connectées via une interface réseau - elles partagent du matériel, mais forment par ailleurs des instances autonomes. Par exemple, il peut s'agir d'un serveur web qui gère différents sites web avec une adresse IP unique : le serveur est connecté par un routeur qui détermine entre les signaux entrants et les signaux fournis par le réseau local. Bindings demandera à RCCMD d'écouter les signaux RCCMD entrants uniquement à une adresse IP spécifique qui est attribuée au réseau local uniquement.

Note

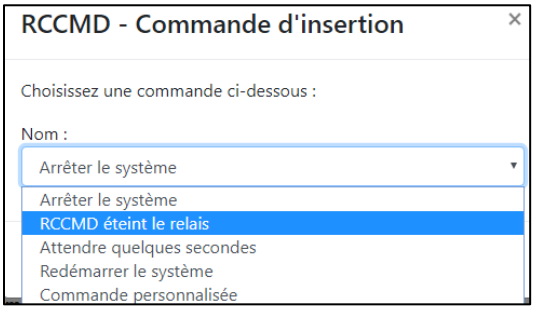
Ces configurations sont utilisées dans des scénarios spéciaux. Normalement, vous pouvez quitter le paramètre 127. 0. 0. 0. 1 localhostl, port 6003. Dans ce cas, le RCCMD écoutera toutes les adresses IP disponibles pour trouver un signal d'entrée valide. Puisque vous avez défini l'adresse d'expéditeur valide dans le menu « Connexions », RCCMD remarquera le signal mais refusera l'exécution et enregistrera ce fait comme une commande RCCMD invalide.

Changer la cible RCCMD



L'appliance RCCMD est bien plus qu'un petit outil pour gérer uniquement les hôtes VMware. En décochant la case et en appuyant sur « Sauvegarder les changements », RCCMD passe en mode local :

Tous les menus VMware sont désactivés et les paramètres d'arrêt passent en options locales



En raison du fait que RCCMD ne peut pas seulement recevoir, mais aussi envoyer des signaux d'arrêt RCCMD, il est possible d'utiliser un appareil RCCMD comme un relais RCCMD central qui fonctionne avec un scripting supplémentaire personnalisé complet.

Lorsque le mode local est actif, RCCMD fournit les séquences de commandes suivantes :

Arrêter le système

RCCMD éteindra le serveur sur lequel il fonctionne

RCCMD éteint le relais

Avec cette option, RCCMD transmettra un arrêt du RCCMD à :

- Une seule adresse IP
- Une plage d'adresse IP

Avec cette option, il est possible d'obtenir des options de redondance avancées. Par exemple, vous pouvez combiner un CS141 et un deuxième client RCCMD. Si les deux conseillent un arrêt, le système RCCMD cible exécute la commande.

Attendre quelques secondes

RCCMD attendra un créneau horaire personnalisable jusqu'à ce que la prochaine commande de la liste soit exécutée.

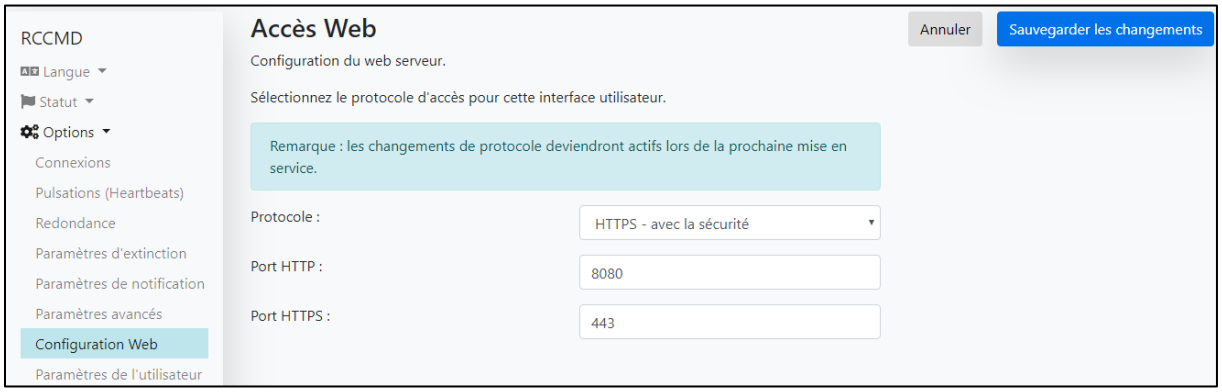
Redémarrer le système

RCCMD redémarrera l'intégralité du serveur RCCMD exécuté sur une machine virtuelle.

Commande personnalisée

Lancez des programmes, lancez des commandes kill, lancez vos propres scripts, entrez simplement la commande et les extensions obligatoires etRCCMD fera le reste.

7.8. Configuration WEB



Définir la disponibilité de la console Web RCCMD.

L'accès web par défaut est :

http: port 8080

https: port 8443

Veuillez noter que la modification des valeurs par défaut entraînera l'accès de la console Web de RCCMD uniquement via les ports que vous avez définis manuellement.

7.9. Paramètres utilisateur

Personnalisez le mot de passe administrateur en fonction de vos idées et des politiques de sécurité de l'entreprise. Veuillez noter que ce mot de passe s'applique également à l'administrateur de la console. L'annexe contient des instructions sur la configuration d'un utilisateur d'urgence pour la récupération de mot de passe.

Utilisateur Administrator : admin
Ce nom d'utilisateur est codé en dur et ne peut pas être modifié.

Mot de passe administrateur actuel :
Ceci est le mot de passe actuellement attribuer.

Nouveau mot de passe administrateur
Mettre le nouveau mot de passe

Confirmer le nouveau mot de passe
Répétez le mot de passe que vous avez attribué. Veuillez noter que le copier-coller répète les erreurs de frappe et peut verrouiller votre client RCCMD.

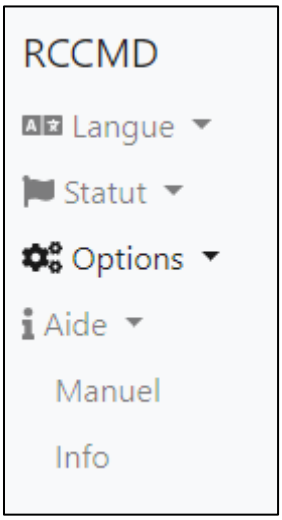
Note

Selon la version du programme, deux mots de passe par défaut peuvent être attribués.

Versions du programme jusqu'au 5/2018: cs121-snmp
Versions du programme du 5/2018: RCCMD

Étant donné que RCCMD est fourni avec une autorisation de mise à jour de deux ans, il est possible que vous ayez besoin de ces deux mots de passe par défaut.

7.10. Aide



➔ Onglet : Aide

➔ Documentation et liens de téléchargement pour RCCMD

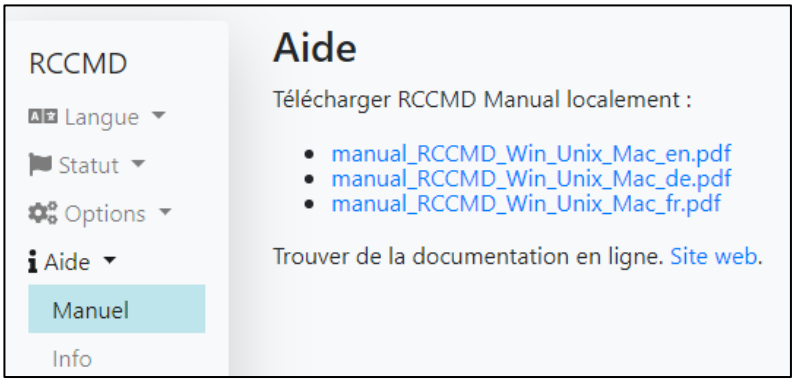
➔ Version actuelle de RCCMD

Manuel

Besoin d'aide?

Les manuels sont disponibles dans RCCMD - vous n'avez besoin d'aucune connexion réseau supplémentaire.

Étant donné que le manuel est un fichier pdf, des outils logiciels supplémentaires peuvent être nécessaires pour ouvrir le fichier correspondant.

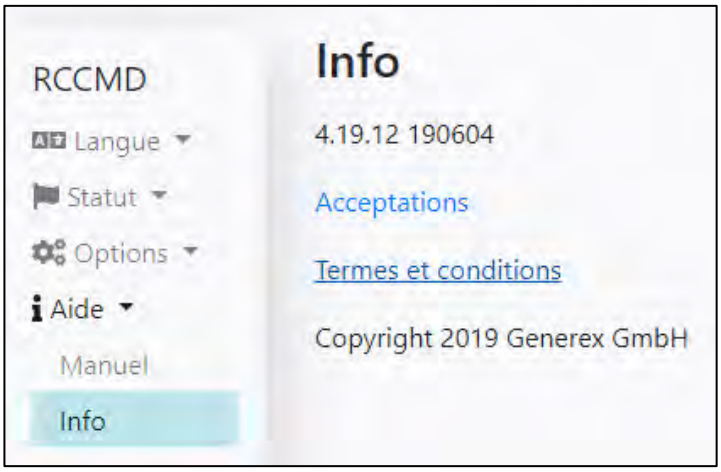


Info

Besoin d'informations supplémentaires sur votre RCCMD?

L'onglet information montrera :

- Remerciements
- Termes et conditions
- Copyright



8. Annexes

RCCMD FAQ's

8.1. Adressage IP statique

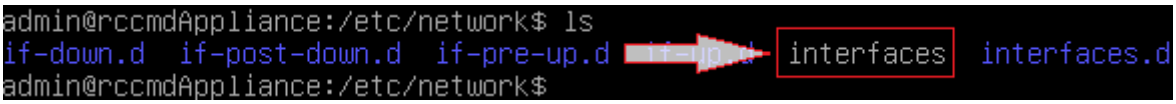
Dans certains cas, une conception de réseau peut ne pas fournir de serveur DHCP:

Le système de transporteur démarre mais ne reçoit pas d'adresse IP valide que RCCMD peut utiliser. Étant donné que la disponibilité à 100% d'un serveur DHCP ne peut jamais être donnée, il est conseillé d'attribuer une adresse IP statique ici. Rechercher les interfaces de fichiers - ce fichier est responsable de la gestion des entrées d'adresses IP dynamiques ou statiques.

Vous avez besoin de deux commandes pour trouver les fichiers requis:

Commande: cd /etc/network

Commande: ls



L'appliance RCCMD utilise nano, un petit éditeur destiné à faciliter la visualisation et la modification de fichiers.

Commande: nano interfaces

L'éditeur s'ouvre et affiche le contenu du fichier Interfaces:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet dhcp
# iface ens33 inet static
#       address 192.168.200.223/24
#       gateway 192.168.200.1
#       # dns-* options are implemented by the resolvconf package, if installed
#       dns-nameservers 192.168.200.3 192.168.200.5 192.168.200.1
#       dns-search local
```

8.2. Paramètres réseaux RCCMD

Recherchez cette entrée :

- ➔ iface ens33 inet dhcp
- ➔ iface ens33inet static

Fondamentalement, ces deux lignes de configuration décident d'utiliser une adresse IP statique ou que l'appliance demande un serveur DHCP.

```
Source /etc/network/interfaces.d/*

# The loopback network interface
Auto lo
Iface lo inet loopback
#The primary network interface
alllow-hotplug ens33

#Iface ens33 inet dhcp                          <- use # to disable DHCP
iface ens33 inet static                         <- Remove # to enable manual IP address settings
address 192.168.200.99                          <- Enter static IP-address
subnet 255.255.255.0                            <- Enter subnet mask
gateway 192.168.200.1                           <- Enter IP address of the gateway

# dns-* options are implemented by the resolvconf package, if installed

dns-namservers 192.168.200.3 192.168.200.5 168.168.200.1    <- Enter DNS Server Ip address data
# dns-search local
```

Après le redémarrage (utilisé la commande « init 6 » pour redémarrer), l'appliance doit utiliser et afficher une adresse IP statique.

Note

Si vous choisissez d'entrer l'adresse IP attribuée par le serveur DHCP lors du démarrage sous forme d'adresse IP statique, assurez-vous que cette adresse IP sera supprimée du groupe d'adresses IP attribuables de manière dynamique. Vous pouvez également affecter une adresse IP fixe via un serveur DHCP et la saisir de manière statique dans l'appliance. Ce faisant, RCCMD se verra attribuer une adresse IP accessible, ce qui augmentera considérablement la résilience.

8.3. Paramétrage d'un utilisateur de secours (VMware)

Mise en place d'un utilisateur d'urgence

Note

Il est possible que les mots de passe peuvent être perdus - malheureusement toujours accompagné de gros ennuis:

Pour les systèmes complexes, la perte d'un mot de passe peut s'avérer très lourde et coûteuse. L'utilisateur d'urgence n'est pas une solution tout-en-un pour ces problèmes, mais il peut s'avérer très utile en cas d'imprévu. Vous pouvez configurer l'utilisateur d'urgence à tout moment. Il n'est pas nécessaire de le faire avant la configuration initiale de RCCMD.

Vous pouvez ignorer cette partie si vous n'utilisez pas un utilisateur d'urgence ou si vous souhaitez le configurer ultérieurement.

Il arrive souvent que des mots de passe soient perdus en raison de circonstances défavorables:

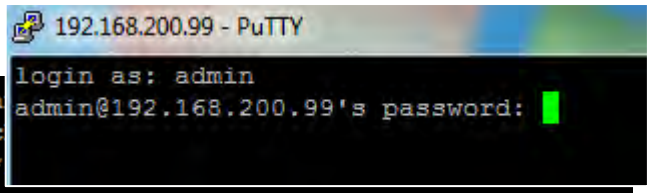
- par exemple : pas de documentation appropriée sur les systèmes installés
- les systèmes et les mots de passe ont été oubliés
- les systèmes sont hérités d'autres sociétés

Pour des raisons de sécurité, aucune porte arrière n'est installée par défaut dans RCCMD.

Si vous attribuez un nouveau mot de passe à l'utilisateur admin, assurez-vous qu'il sera documenté!

Sinon, vous devrez à nouveau configurer l'appliance RCCMD complète et réassembler tous les scripts d'arrêt. Pour éviter cet incident, il est recommandé de configurer un utilisateur de sauvegarde pour assurer la réinitialisation des mots de passe.

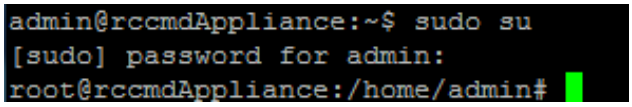
Après avoir installé l'appliance, il est possible d'accéder à la console avec un outil gratuit comme Putty:
User: admin
Password: RCCMD



Les privilèges root sont requis

Command: sudo su

Remarque: l'utilisateur "admin" n'a pas encore obtenu les droits nécessaires pour configurer un utilisateur d'urgence correspondant. Cette commande activera le super utilisateur pour les droits avancés



Création d'un utilisateur et un mot de passe

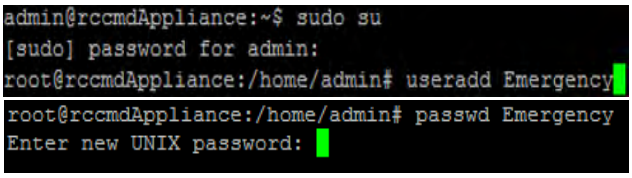
Cette étape requiert 2 commandes

Commande 1: useradd <Username>

Cette commande créer un nouvel utilisateur.

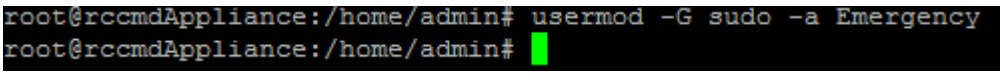
Commande 2: passwd <Username>

Cette commande affecte un mot de passe.



Ajout à un groupe d'utilisateur

Commande: usermod – G sudo -a Emergency



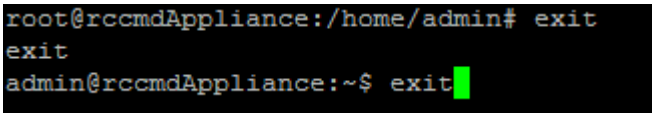
Pour que les droits nécessaires soient accordés à l'utilisateur nouvellement créé, il doit être attribué au groupe d'utilisateurs approprié.

Se déconnecter

Command: exit

Note: Entrer exit deux fois:

La première sortie fermera le « SuperUser », la seconde quittera la connexion à RCCMD et fermera la console..



Effectuer une réinitialisation d'urgence du mot de passe

Démarrez la session en utilisant les informations d'identification de l'utilisateur d'urgence.

Demande de droits système étendus

Commande: sudo su

```
Welcome to RCCMD-Appliance.
To configure RCCMD point your web browser to: [https://192.168.200.99]!
$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for Emergency:
root@rccmdAppliance:/#
```

L'utilisateur d'urgence n'a fondamentalement aucune autorisation pour administrer l'appliance RCCMD. Puisque cet utilisateur est répertorié dans le groupe des super-utilisateurs, sudo su permet d'étendre les droits systèmes.

Navigation dans le répertoire requis

Commande: cd /usr/rccmd/webconfig/resources

Ce répertoire contient les scripts de configuration dont vous avez besoin pour modifier le mot de passe de l'utilisateur admin.

```
root@rccmdAppliance:/# cd /usr/rccmd
root@rccmdAppliance:/usr/rccmd# cd webconfig/resources/
root@rccmdAppliance:/usr/rccmd/webconfig/resources#
```

Utiliser un éditeur de texte pour changer les mots de passe

Commande: nano realm.properties

Nano est un éditeur très pratique et très bien conçu pour visualiser et éditer des fichiers et des scripts dans le système d'exploitation RCCMD. Le fichier « realm.properties » contient le mot de passe chiffré pour l'interface Web de RCCMD.

```
#RCCMD realm.properties
# username: password [,rolename ...]
admin: CRYPT:adg.Dq8TXmNZI, admin
```

Les modifications suivantes doivent être apportées:

```
#RCCMD realm.properties
# username: password [,rolename ...]
#admin: CRYPT:adg.Dq8TXmNZI, admin          -> Utiliser  # Pour désactiver cette ligne
admin: Notfall, admin                       -> Ajouter cette ligne
```

Dans cet exemple, l'utilisateur admin aurait maintenant le mot de passe «Notfall»:

Sauvegarder les paramètres

Commande: CTRL X

Enregistrez le fichier et quittez l'éditeur de texte. Veillez à écraser le fichier d'origine. Changer le nom du fichier ne fonctionnera pas.

Redémarrer l'interface Web RCCMD

Commande: /etc/init.d/rccmdConfig restart

```
root@rccmdAppliance:/usr/rccmd/webconfig/resources# /etc/init.d/rccmdConfig restart
stopping RCCMD-Configurator...
RCCMDConf has been stopped.
Starting RCCMD-Configurator...
RCCMDConf has been started.
```

Cette commande redémarre l'interface Web et définit le nouveau mot de passe.

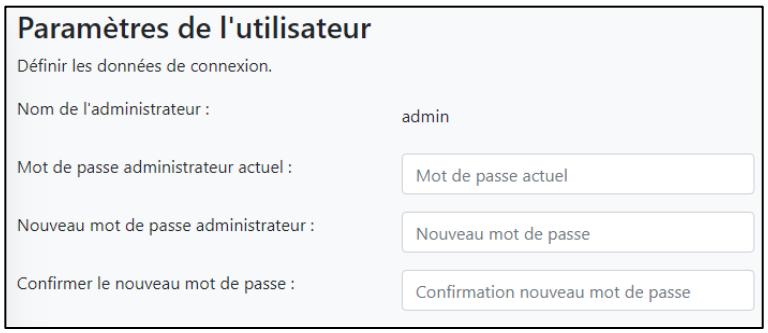
Synchroniser les mots de passe

Pour le moment, l'utilisateur admin utilise deux mots de passe différents:

- L'ancien mot de passe est valide à l'intérieur de la console de l'appliance RCCMD.

- Le nouveau mot de passe est valide pour l'interface Web de RCCMD

De plus, vos modifications de mot de passe ne sont pas cryptées.



Pour synchroniser et chiffrer les informations d'identification de l'utilisateur admin, ouvrez un navigateur Web et entrez l'adresse IP de vottre RCCMD. Après la connexion, accédez aux paramètres utilisateur et changez le mot de passe.

Appuyez sur Enregistrer les modifications pour synchroniser et chiffrer le mot de passe.

9. Copyright et licences

Les droits d'auteur de Generex et des autres fournisseurs de logiciels concernés doivent être respectés. Generex et ses fournisseurs se réservent les droits sur les composants logiciels.
Sont notamment interdits:

- *la copie et la distribution,*
- *modifications et dérivations,*
- *décompilation, ingénierie inverse,*

Les composants relevant de la licence publique générale GNU et d'autres licences Open Source sont intégrés au logiciel. Vous trouverez un aperçu des composants Open Source intégrés et une copie de la licence actuelle à l'adresse www.generex.de/legal/sla.

Generex fournira le code source de tous les composants de logiciels sous licence GNU General Public License et de licences Open Source comparables.

Pour les demandes de code source, veuillez envoyer un courrier électronique à info@generex.de