

## **RSA Security Analytics**

Guide de configuration de RSA  
Analytics Warehouse S4 (basé  
sur MapR)

## Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to [www.emc.com/legal/emc-corporation-trademarks.htm](http://www.emc.com/legal/emc-corporation-trademarks.htm).

## License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by EMC.

## Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed in the [thirdpartylicenses.pdf](#) file.

## Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

## Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license. EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

# Guide de configuration de RSA Analytics Warehouse S4 (basé sur MapR)

- [Guide de configuration de RSA Analytics Warehouse S4 \(basé sur MapR\)](#) 4
  - [Description matérielle de Warehouse S4](#) 5
  - [Montage de l'appliance et configuration des paramètres réseau](#) 9
  - [Fin de la configuration de Warehouse dans Security Analytics](#) 15



# Guide de configuration de RSA Analytics Warehouse S4 (basé sur MapR)

---

## Présentation

Ce document est un guide étape par étape pour installer le RSA Analytics Warehouse (MapR) et le connecter à votre réseau. Cet entrepôt était précédemment appelé Security Analytics Warehouse (SAW).

---

## Contexte

Les instructions de configuration matérielle dans le présent document concernent uniquement le matériel. Elles ne s'appliquent pas à une version spécifique du logiciel Security Analytics. Une fois la configuration matérielle terminée, continuez l'installation et la configuration de Warehouse, comme décrit dans la documentation en ligne Security Analytics, qui est accessible via l'option **Aide** de Security Analytics et à l'adresse [sadoes.emc.com/fr-fr](http://sadoes.emc.com/fr-fr).

**Note:** Lors de l'affichage d'un guide imprimé, n'oubliez pas qu'une version plus récente peut être disponible en ligne sur le site [sadoes.emc.com/fr-fr](http://sadoes.emc.com/fr-fr). Ce guide est disponible dans l'aide en ligne de Security Analytics sous Guides de configuration matérielle.



# Description matérielle de Warehouse S4

---

## Présentation

Cette section présente le RSA Warehouse de la gamme 4 et fournit une description des contrôles et des connecteurs, ainsi que certaines caractéristiques.

---

## Introduction

Le RSA Warehouse de la gamme 4 est livré avec le logiciel installé. La configuration initiale du Warehouse sur votre réseau implique les étapes suivantes :

1. Vérifiez les exigences relatives au site et les informations de sécurité.
2. Montez le matériel du Warehouse.
3. Connectez le Warehouse à votre réseau et configurez les paramètres réseau du Warehouse.
4. Terminez la configuration du Warehouse dans Security Analytics.

Il existe plusieurs options pour la première connexion physique au Warehouse pour commencer la configuration des paramètres logiciels. Une fois connectée, la console de l'appliance Security Analytics est utilisée pour effectuer ces changements de configuration. Chaque étape est décrite en détail dans ce document.

---

## Contenu de l'emballage

Vérifiez le contenu de la boîte d'emballage afin de vous assurer que vous avez reçu tous les éléments nécessaires pour installer et configurer votre Warehouse.

- Appliance Warehouse de la gamme 4
  - Ensembles de glissières coulissantes (2)
  - Cordon d'alimentation (2)
- 

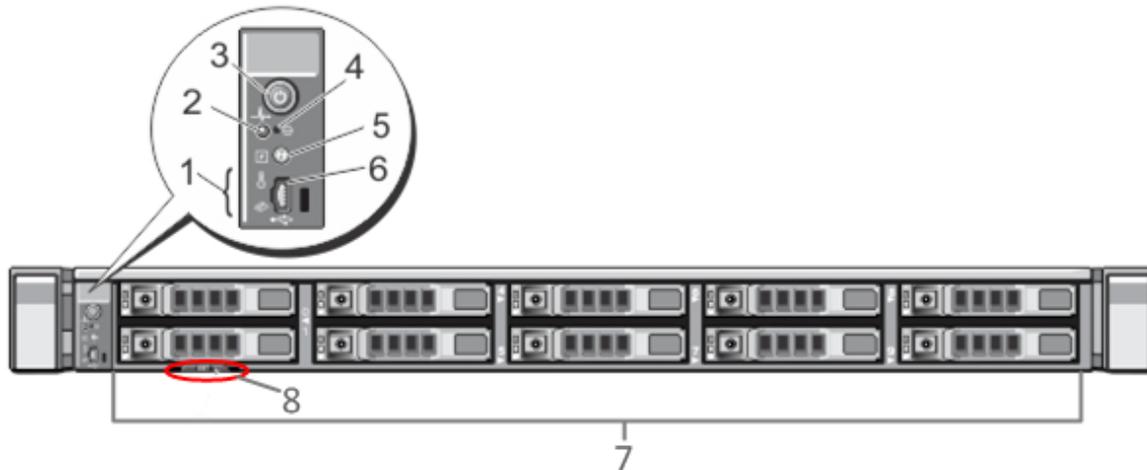
## Matériel fourni par le client

Pour terminer la procédure de configuration, vous aurez besoin des éléments suivants :

- Deux câbles de réseau Ethernet
-

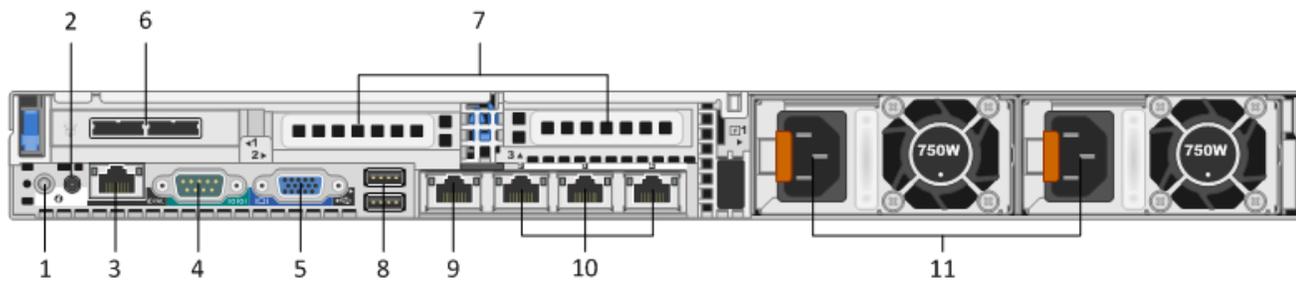
- Câbles pour la connexion d'un moniteur ou d'un adaptateur KVM au port VGA et d'un clavier ou d'un adaptateur KVM au port USB
- Outils standard d'installation et de montage du matériel informatique

## Vue avant du Warehouse



Clé	Description
1	Voyants de diagnostic
2	Voyant d'identification du système
3	Marche/Arrêt
4	Bouton d'interruption non masquable encastré
5	Bouton d'identification du système
6	Micro port USB
7	Dix baies de disque dur 2,5 pouces. Dix disques de 1 To sont installés sur le Warehouse. Un module de carte SD interne est également présent, où sont installées deux cartes de 32 Go et où le système d'exploitation est installé par défaut.
8	Détails du libellé du service

## Vue arrière du Warehouse



Clé	Description
1	Bouton d'identification du système
2	Voyant d'identification du système
3	Port iDRAC
4	Port série RS232 (connexion série pour les ordinateurs portables via DB9 ou serveur série)
5	Port vidéo VGA (moniteur)
6	Slot des cartes d'interface réseau : Contrôleur SAS installé avec deux ports d'interface DAC pour la connexion aux baies de stockage de disque.
7	Slots d'extension de la carte d'interface réseau pour les cartes supplémentaires. Les options possibles sont les suivantes : <ul style="list-style-type: none"> <li>• Carte de capture réseau 10 Gbit/s fibre/cuivre (RJ45)</li> <li>• Adaptateur de bus hôte Fibre channel (HBA) utilisé pour se connecter à un réseau SAN</li> </ul>
8	Ports USB (clavier)
9	Port Gigabit Ethernet 1 : em1 = port de gestion.
10	Ports Gigabit Ethernet (2-4) : em 2-4
11	Alimentation remplaçable à chaud 1 et 2

## Caractéristiques techniques du Warehouse

Encombrement	1U, profondeur complète
--------------	-------------------------

Poids	17,69 kg
Dimensions	48,23 cm (l) x 77,19 cm (p) x 4,26 cm (h)
Les alimentations	Remplaçables à chaud, redondant 750 W Autodétecteurs 100 à 240 V
Processeurs	Double six cœurs 2,66 GHz
RAM	96 Go



# Montage de l'appliance et configuration des paramètres réseau

---

## Présentation

Cette section fournit des instructions pour connecter une appliance RSA S4 à votre réseau et configurer des paramètres de gestion initiale sur l'appliance.

---

## Introduction

Avant de commencer la configuration réseau, montez ou placez l'appliance en toute sécurité, conformément aux exigences du site.

La configuration des paramètres réseau pour une appliance RSA S4 inclut la définition de l'adresse IP par défaut et le nom d'hôte, la configuration de vos serveurs DNS et du fichier **/etc/hosts**, ainsi que la définition de la source de l'horloge réseau. Pour définir ces paramètres, vous pouvez vous connecter à la console de l'appliance à l'aide d'un clavier et d'une souris ou de la connexion Ethernet. Dans les deux cas, connectez-vous à l'appliance en tant qu'utilisateur racine. Une fois que vous pouvez vous connecter à l'appliance, utilisez la ligne de commande du système d'exploitation pour modifier les paramètres de gestion de l'appliance et configurer les serveurs DNS.

Méthode	Username	Default Password
Console	racine	netwitness

Choisissez l'une des méthodes suivantes pour la connexion initiale :

- Console de l'appliance via une connexion VGA : Clavier (port USB) et moniteur (port VGA).
- Console de l'appliance via une connexion réseau : ordinateur utilisant un client SSH connecté à l'appliance via un câble Ethernet pour le port de gestion (em1), qui est configuré sur 192.168.1.1 par défaut.

---

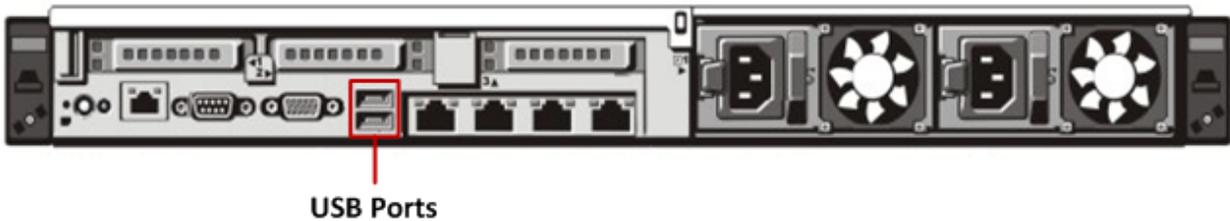
## Console de l'appliance via une connexion VGA

Pour utiliser la console de l'appliance via une connexion VGA :

1. Connectez un moniteur ou un adaptateur KVM au port VGA à l'arrière de l'appliance.



2. Connectez un clavier ou un adaptateur KVM à l'un des ports USB à l'arrière de l'appliance.



3. Connectez un câble d'alimentation à chacune des deux alimentations à l'arrière de l'appliance. Connectez les câbles d'alimentation à une source d'alimentation. Pour fournir une configuration plus robuste, connectez chaque alimentation à un circuit différent.

**⚠ Caution:** Une alimentation auxiliaire de 5 V est active chaque fois que le système est branché. Pour couper l'alimentation du système, vous devez débrancher les deux câbles d'alimentation CA de la source d'alimentation

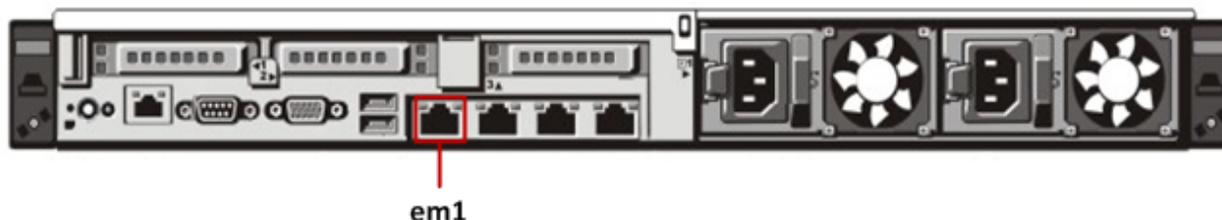
4. À l'invite de connexion, utilisez les informations d'identification (`root/netwitness`) par défaut pour accéder au système d'exploitation.
5. Passez à la section **Définir l'adresse IP** ci-dessous.

## Console de l'appliance via une connexion réseau

**⚠ Caution:** L'adresse IP par défaut de l'appliance est définie en usine sur 192.168.1.1. L'utilisation de 192.168.1.1 est assez courante et l'adresse IP est peut-être déjà dans le fichier de votre système SSH `known_hosts`. Il est possible que la ligne spécifique pour cette adresse doive être supprimée.

Pour utiliser la console de l'appliance via une connexion réseau :

1. Connectez un câble Ethernet entre un ordinateur et le port de gestion Ethernet à l'arrière de l'appliance.



2. Connectez les cordons d'alimentation aux connecteurs d'alimentation de l'appliance et du réceptacle d'alimentation.
3. L'adresse IP par défaut de l'appliance est définie en usine sur 192.168.1.1. Par conséquent, définissez l'adresse IP du système client sur le même sous-réseau. Par exemple, définissez votre ordinateur portable sur 192.168.1.15 avec la passerelle par défaut de 192.168.1.1, puis à l'aide d'un client secure shell (SSH) connectez-vous à l'appliance.

**Note:** Gardez à l'esprit que si vous modifiez les paramètres réseau tout en étant connecté via SSH, votre session SSH sera abandonnée et vous devrez vous reconnecter à la nouvelle adresse de l'appliance.

4. À l'invite de connexion, utilisez les informations d'identification (`root/netwitness`) par défaut pour accéder au système d'exploitation.
5. Passez à la section **Définir l'adresse IP** ci-dessous.

## Définir l'adresse IP

Vous devez configurer manuellement le réseau sur l'appliance Warehouse. Si vous envisagez d'avoir un cluster d'appiances Warehouse, veillez à effectuer les tâches suivantes sur toutes les appliances du cluster. Chaque appliance dans le cluster doit avoir des adresses IP configurées par le biais de la console de l'appliance ou via la console iDRAC (Dell Remote Access Console). Pour plus d'informations sur iDRAC, consultez la documentation Dell.

**Note:** L'adresse IP que vous définissez pour l'appliance doit être unique au sein de la plage d'IP privée dans votre environnement de réseau.

Les interfaces réseau à configurer en fonction de vos besoins sont les suivantes :

Interfaces	Objectif
em1	Public, se connecter au switch client
em2	Privé, se connecter au switch dédié de l'entrepôt
em3	Ouvrir, se connecter à n'importe quel réseau ou switch
em4	Ouvrir, se connecter à n'importe quel réseau ou switch

Pour configurer le réseau :

1. Connectez-vous à l'appliance en tant qu'utilisateur racine.

2. Pour configurer l'interface de réseau em1, modifiez le fichier `/etc/sysconfig/network-scripts/ifcfg-em1`. Saisissez la commande suivante :

```
vi /etc/sysconfig/network-scripts/ifcfg-em1
```

Définissez les valeurs appropriées pour les paramètres suivants dans le fichier :

Paramètre	Valeur
DEVICE	Type d'interface réseau. Par exemple, eth0.
BOOTPROTO	static
IPADDR	Adresse IP de l'interface réseau
NETMASK	Adresse du masque de sous-réseau
GATEWAY	Adresse de passerelle par défaut
HWADDR	Adresse Mac de l'appliance
ONBOOT	yes
TYPE	Type de réseau

3. Pour redémarrer le service réseau, entrez la commande suivante :  
`service network restart`
4. (Facultatif) Configurez l'interface de réseau em2, si l'interface interne utilisée par l'appliance d'entrepôt individuel pour communiquer avec les autres appliances d'entrepôt dans le cluster se fait via un switch. Le fichier de configuration respectif est `/etc/sysconfig/network-scripts/ifcfg-em2`.

## Définir le nom d'hôte

La création du nom d'hôte du système est une tâche relativement simple, mais il peut être profitable de la prendre en considération pour limiter les problèmes courants. Si vous recherchez des conseils pour choisir un nom d'hôte, reportez-vous à la RFC 1178. En termes de Security Analytics les bases de données sur les appliances sont associées au nom d'hôte. Si la collecte ou l'agrégation a commencé (c'est pour cette raison qu'elle n'est pas activée par défaut), alors la base de données est créée et si vous modifiez le nom d'hôte après que cela se produit correctement, cela crée une deuxième base de données. Le nom d'hôte doit uniquement comporter des caractères alphanumériques (pas de caractères spéciaux tels que #, \_, @, -) afin d'éliminer les problèmes de communication.

Pour définir le nom d'hôte :

1. Connectez-vous à l'appliance en tant qu'utilisateur racine.
2. Pour définir le nom d'hôte de l'appliance, modifiez le fichier `/etc/sysconfig/network` à l'aide de la commande suivante :  
`vi /etc/sysconfig/network`
3. Ajoutez la configuration, ou modifiez-la, comme suit :  
`NETWORKING=[yes|no]`  
`HOSTNAME=<sawnode_hostname>`  
où `<sawnode_hostname>` est le nom d'hôte de l'appliance Warehouse.  
`DOMAINNAME = <value>`

**Note:** Vous pouvez saisir une valeur pour `DOMAINNAME` si votre entreprise a besoin d'un nom de domaine pour les noms d'hôte de nœud d'entrepôt. Si vous choisissez de ne pas utiliser un nom de domaine, ne renseignez pas cette valeur.

4. Pour enregistrer les modifications et quitter l'éditeur vi, entrez la commande suivante :  
`:wq`
5. Pour redémarrer le réseau, entrez la commande suivante :  
`service network restart`
6. Pour vérifier si le nom d'hôte est défini correctement, entrez la commande suivante :  
`hostname`  
Le nom d'hôte que vous avez défini s'affiche.

## Configurer les serveurs DNS

Pour configurer les serveurs DNS :

1. Connectez-vous à l'appliance en tant qu'utilisateur racine.
2. Saisissez la commande suivante :  
`vi /etc/resolv.conf`
3. Ajoutez les lignes suivantes au fichier pour chaque serveur DNS :  
`nameserver <dns_server_ip_address>`  
`search <domain_name>`  
où `<DNS_server_ip_address>` est l'adresse IP de votre serveur DNS et `<domain_name>` est le nom de domaine.  
Par exemple :  
`nameserver 192.168.0.1`  
`search acmecorp.com`
4. Pour enregistrer les modifications et quitter l'éditeur vi, entrez la commande suivante :  
`:wq`

## Configurer le fichier /etc/hosts

Modifiez le fichier **hosts** de l'appliance afin d'inclure l'adresse IP et le nom d'hôte de chacun des nœuds de l'entrepôt dans le cluster.

**Caution:** Le nom d'hôte des nœuds de l'entrepôt ne doit pas s'afficher pas dans le cadre de la configuration de l'adresse loopback.

Pour configurer le fichier **/etc/hosts** :

1. Connectez-vous à l'appliance en tant qu'utilisateur racine.
2. Saisissez la commande suivante :  
`vi /etc/hosts`
3. Ajoutez la ligne suivante au fichier pour chacun des nœuds de l'entrepôt :  
`<node_private_ip_address> <node_fqdn> <node_hostname>`  
Où :  
`<node_private_ip_address>` est l'interface privée du nœud du cluster d'entrepôts.  
`<node_fqdn>` est le nom de domaine complet de n'importe quel nœud du cluster d'entrepôts.

`<node_hostname>` est le nom d'hôte du nœud du cluster d'entrepôts.

Ajoutez les détails de tous les nœuds dans le cluster d'entrepôts dans des lignes séparées dans le fichier **/etc/hosts**.

Voici un exemple du fichier **/etc/hosts** avec les détails de tous les nœuds du cluster d'entrepôts :

```
127.0.0.1 localhost.localdomain localhost
::1 localhost.localdomain localhost
192.168.1.10 sawnode1.domainname.com sawnode1
192.168.1.11 sawnode2.domainname.com sawnode2
192.168.1.12 sawnode3.domainname.com sawnode3
```

4. Pour enregistrer les modifications et quitter l'éditeur vi, entrez la commande suivante :  
:wq

---

## Spécifier la source de l'horloge réseau

Il est recommandé que tous les systèmes de la suite Security Analytics soient synchronisés à l'aide d'une source d'heure réseau afin que tous les services indiquent avec précision la même heure. Si cela n'est pas fait, alors l'heure sur les appliances peut ne pas être synchronisée, entraînant des requêtes pour une heure spécifique qui ne renvoient pas les résultats attendus. Vous devez mettre à jour manuellement les paramètres du protocole NTP (Network Time Protocol) fournis dans **/etc/NTP.conf** de l'appliance Warehouse.

Pour mettre à jour les paramètres NTP :

1. Connectez-vous à l'appliance en tant qu'utilisateur racine.
2. Pour modifier le fichier **/etc/ntp.conf**, entrez la commande suivante :  
`vi /etc/ntp.conf`
3. Faites défiler les lignes de serveur contenant les sites NTP et mettez à jour les serveurs répertoriés pour refléter les sites NTP appropriés.  
Exemple :  
Détails du serveur fournis en tant que nom de domaine complet :  
`server 0.centos.pool.ntp.org`  
Les détails du serveur ci-dessus peuvent également être fournis à l'aide de l'adresse IP en procédant comme suit :  
`server 91.121.92.90`
4. Pour enregistrer les modifications et quitter l'éditeur vi, entrez la commande suivante :  
:wq
5. Pour redémarrer le service, entrez la commande suivante :  
`service ntpd restart`



# Fin de la configuration de Warehouse dans Security Analytics

---

## Présentation

Cette section fournit des instructions pour terminer la configuration de RSA Analytics Warehouse (MapR).

---

## Introduction

Les dernières étapes de configuration de Warehouse peuvent inclure :

1. Générer et mettre à jour de la valeur par défaut UUID dans les appliances.
2. Mettre à jour de la version du serveur Hive dans l'appliance.
3. Mettre à jour le fichier de modèle de configuration de l'appliance Warehouse.
4. Installer le fichier de licence de Warehouse.
5. Générer l'adresse IP virtuelle pour l'appliance Warehouse.
6. Configurer le connecteur Warehouse pour écrire dans Warehouse.
7. Ajouter des sources de données Warehouse à Reporting Engine.

Pour obtenir des instructions détaillées, consultez le *Guide de configuration RSA Analytics Warehouse (MapR)* (Security Analytics 10.4) ou le *Guide de configuration de Security Analytics Warehouse* (Security Analytics 10.3 et versions antérieures) dans l'aide en ligne à l'adresse [sadoes.emc.com/fr-fr](http://sadoes.emc.com/fr-fr).