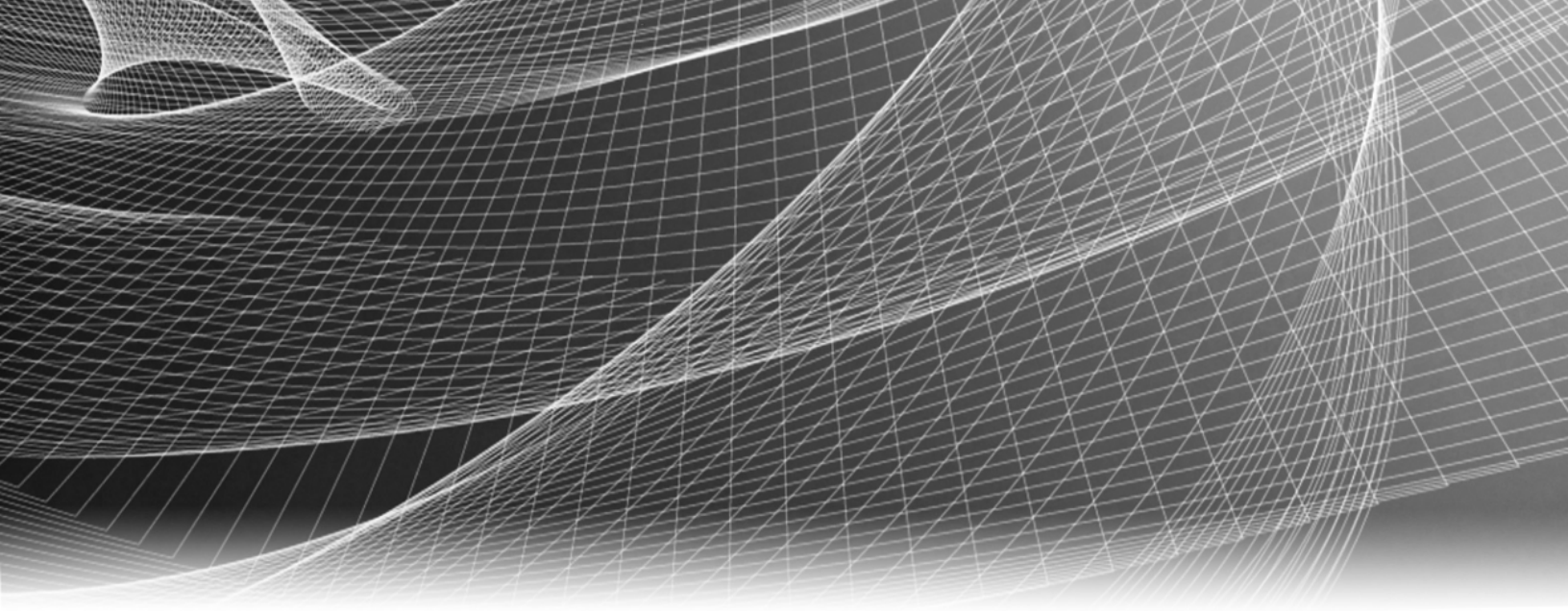


RSA Security Analytics

Guide de configuration des appliances Security Analytics de la gamme 5

RSA

EMC²

Trademarks

License Agreement

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 des appliances Security Analytics de la gamme 5

RSA

Guide de configuration des appliances Security Analytics de la gamme 5

Présentation

Ce document est un guide étape par étape pour installer les appliances RSA Security Analytics de la gamme 5 et les connecter à votre réseau.

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, veuillez continuer l'installation et la configuration des appliances Security Analytics, comme décrit dans la documentation en ligne Security Analytics sur le site sadocs.emc.com/fr-fr.

Ce document ne remplace pas la documentation du fabricant d'origine. Il contient des informations spécifiquement pour les appliances Security Analytics.

Last Modified: August 10 2016, 9:33AM

Description matérielle des appliances R630 S5

Introduction

Toutes sauf une des appliances RSA Security Analytics de la gamme 5 sont basées sur le châssis Dell PowerEdge R630. L'exception est l'appliance hybride, qui est basée sur le châssis Dell PowerEdge R730xd. Les appliances de la gamme 5 sont fournies avec le logiciel Security Analytics 10.5 installé.

Cette rubrique décrit les appliances de la gamme 5 basées sur le châssis Dell PowerEdge R630 :

- Decoder et Log Decoder
- Concentrator
- Broker
- Archiver
- Machines Security Analytics
- Malware Analysis
- Event Stream Analysis (ESA)

À l'exception de l'appliance ESA, toutes les appliances basées sur Dell PowerEdge R630 ont les mêmes composants et caractéristiques physiques. L'appliance ESA a des disques durs supplémentaires, plus de mémoire et une UC différente. Les spécifications de l'appliance Security Analytics ESA fournissent des informations détaillées.

La configuration initiale d'une appliance de la gamme 5 de votre réseau comprend ces étapes :

1. Vérifiez les exigences en matière de site et les informations de sécurité dans le Guide de déploiement pour votre version du logiciel Security Analytics : Security Analytics 10.5
2. Montez ou placez le matériel de l'appliance en toute sécurité, conformément aux exigences de votre site.
3. Connectez l'appliance à votre réseau et configurez les paramètres réseau sur l'appliance : Connectez l'appliance et configurez les paramètres réseau.
4. Terminez la configuration de l'appliance dans Security Analytics : Terminez la configuration de l'appliance dans Security Analytics.

Caution: Pour éviter d'endommager les appliances et les serveurs Security Analytics, retirez-les du rack et démontez le rack avant de les déplacer vers un autre emplacement. Suivez les recommandations du fabricant du serveur et du fabricant du rack pour l'emballage, le transport et l'installation.
RSA ne prend pas en charge la réexpédition des serveurs en rack. Le client prend en charge tous les risques et est le seul responsable lors du transport des serveurs et appliances Security Analytics montés en rack.

Last Modified: August 10 2016, 9:33AM

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 appliance.

- Appliance Security Analytics de la gamme 5 (Decoder, Concentrator, Broker, Archiver, Security Analytics Server, Malware Analysis ou ESA)
- Glissières prêtes statiques (1 jeu)
- Adaptateur de glissière gauche pour rack profond EMC
- Panneau RSA (1) - Les clés sont fixées au panneau.
- Cordon d'alimentation (2)
- Guide d'information sur le produit Dell (1)
- Dossier de la documentation RSA (1)
- CLUF RSA (1)

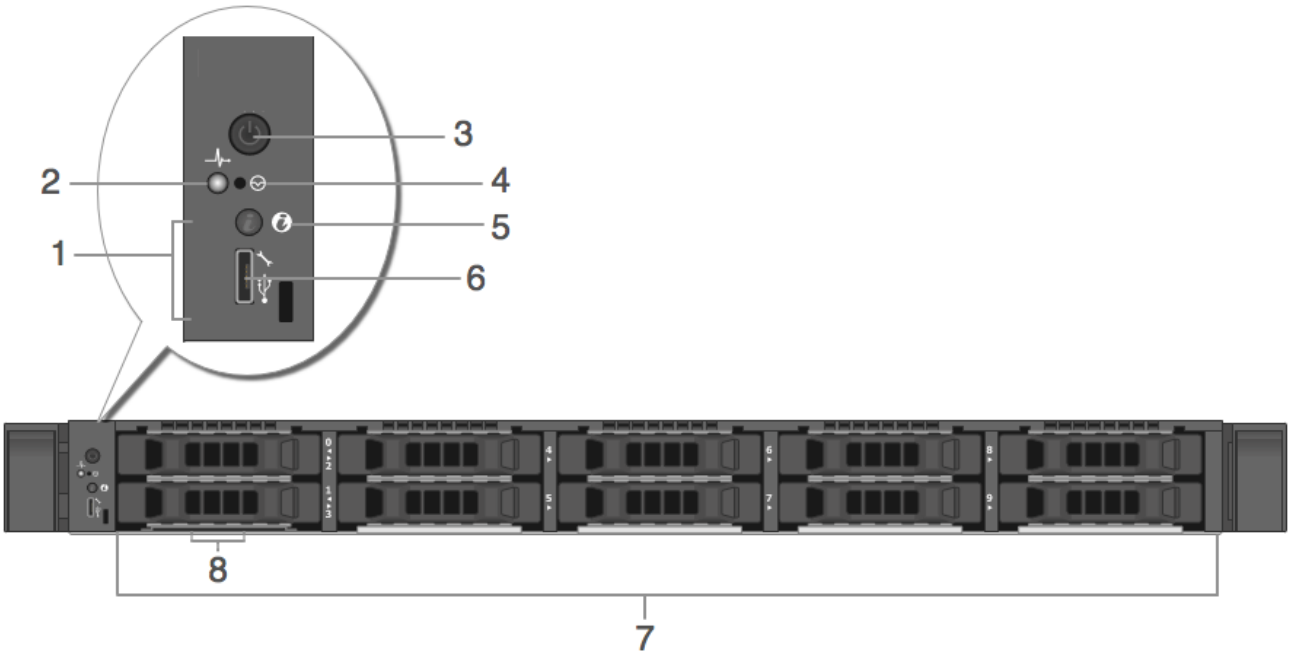
Matériel fourni par le client

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

- Un câble 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

Last Modified: August 10 2016, 9:33AM

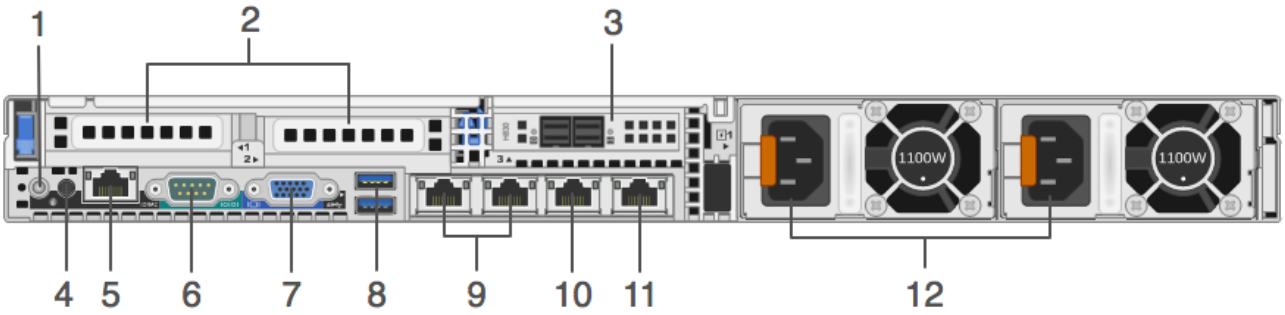
Vue avant des appliances de la gamme 5 (sauf hybride)



Clé	Description
1	Emplacement des voyants de diagnostic. Les voyants de diagnostic s'affichent et indiquent le statut si des erreurs se produisent.
2	Voyant d'état de santé du système. Il clignote de la couleur ambre lorsqu'une défaillance du système est détectée.
3	Marche/Arrêt
4	Bouton d'interruption non masquable encastré
5	Bouton d'identification du système
6	Micro port USB / iDRAC Direct
7	Dix baies de disque dur 2,5 pouces (remplaçables sur site). Les caractéristiques techniques ci-dessous identifient le nombre et les types de disques durs installés sur les appliances.
8	Emplacement des balises d'informations

Last Modified: August 10 2016, 9:33AM

Vue arrière des appliances de la gamme 5 (sauf hybride)



Clé	Description
1	Bouton d'identification du système
2	Slots d'extension LP PCIe 1 et 2. Le Decoder 10G peut utiliser un slot LP PCIe pour une carte d'interface réseau optique Intel X520 en option.
3	Contrôleur RAID PERC H830. Il est indiqué dans le slot 3 LP PCIe, mais il peut être installé dans un autre slot LP PCIe. Le PERC H830 est le contrôleur RAID pour le DAC d'extension de stockage. Il nécessite un câble avec un port Mini-SAS pour se connecter au DAC.
4	Connecteur d'identification du système
5	Port iDRAC
6	Port série RS232 (connexion série pour les ordinateurs portables via DB9 ou serveur série)
7	Port vidéo VGA (moniteur)
8	Ports USB (clavier, souris, clé USB, etc.)
9	Ports Ethernet 10GBASE-T em3 et em4
10	Port de gestion 1000BASE-T de réseau principal : em1
11	Port 1000BASE-T de réseau secondaire : em2
12	Alimentations 1 et 2 remplaçables à chaud (remplaçable sur site)

Note: Le contrôleur RAID PERC H830 nécessite un câble avec un port Mini-SAS pour se connecter au DAC.

Last Modified: August 10 2016, 9:33AM

Spécifications de l'appliance de la gamme 5 (à l'exception de hybride et ESA)

Élément	Description
Encombrement	1U, profondeur complète
Poids (approximatif)	18,4 kg
Dimensions (approximatives)	Avec panneau : 482,43 mm [l] x 808,59 mm [p] x 42,80 mm [h] Sans panneau : 482,43 mm [l] x 776,16 mm [p] x 42,80 mm [h]
Les alimentations	Alimentation double, installable à chaud, redondante (1+1), 1 100 W
Processeurs	2 * E5-2667v3
RAM	16 * RDIMM 8 Go 2133 MT/s (128 Go)
Disques durs (remplacement sur site)	2 * Disque dur 2,5 pouces 1 To 7,2 K RPM NLSAS 6 Gbit/s installable à chaud 2 * disque dur 2,5 pouces de 2 To 7, 2 K RPM NLSAS 12 Gbit/s 512e installable à chaud
Contrôleur RAID	Externe : PERC H830 RAID Interne : PERC H730P
Carte d'interface réseau	Carte fille réseau Intel Ethernet X540 10 Go BT DP + I350 1 Go BT DP

Spécifications de l'appliance Security Analytics ESA

Élément	Description
Encombrement	1U, profondeur complète
Poids (approximatif)	18,4 kg
Dimensions (approximatives)	Avec panneau : 482,43 mm [l] x 808,59 mm [p] x 42,80 mm [h] Sans panneau : 482,43 mm [l] x 776,16 mm [p] x 42,80 mm [h]
Les alimentations	Alimentation double, installable à chaud, redondante (1+1), 1 100 W
Processeurs	2 * E5-2680v3
RAM	8 * RDIMM 32 Go 2133 MT/s (256 Go)
Disques durs (remplaçables sur site)	2 * Disque dur 2,5 pouces 1 To 7,2 K RPM NLSAS 6 Gbit/s installable à chaud 4 * disque dur 2,5 pouces 2 To 7,2 K RPM NLSAS 12 Gbit/s 512e installable à chaud

Last Modified: August 10 2016, 9:33AM

Élément	Description
Contrôleur RAID	Externe : PERC H830 RAID Interne : PERC H730P
Carte d'interface réseau	Carte fille réseau Intel Ethernet X540 10 Go BT DP + I350 1 Go BT DP

⚠ **Caution:** L'ouverture du châssis de l'appliance entraînera l'annulation de la garantie, sauf si vous êtes spécifiquement invité à le faire par l'assistance clientèle de RSA. Les disques durs et les alimentations sont remplaçables sur site par un technicien qualifié.

Last Modified: August 10 2016, 9:33AM

Installation d'un adaptateur de rack profond pour une appliance R630

Procédure

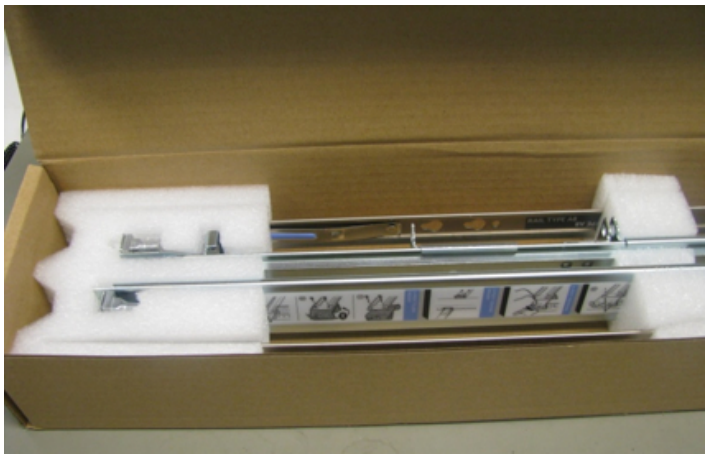
Note: Cette procédure s'applique uniquement si vous installez l'appliance S5 R630 dans un rack EMC Titan D Ultra.

Lors de l'installation de l'appliance S5 R630 dans un rack EMC Titan D Ultra, un adaptateur de rack profond 1U est obligatoire. Suivez cette procédure pour installer un nouveau support sur les glissières du serveur.

1. Dans la boîte d'accessoires du carton de l'appliance R630, cherchez le support de l'autre glissière.

Last Modified: August 10 2016, 9:33AM

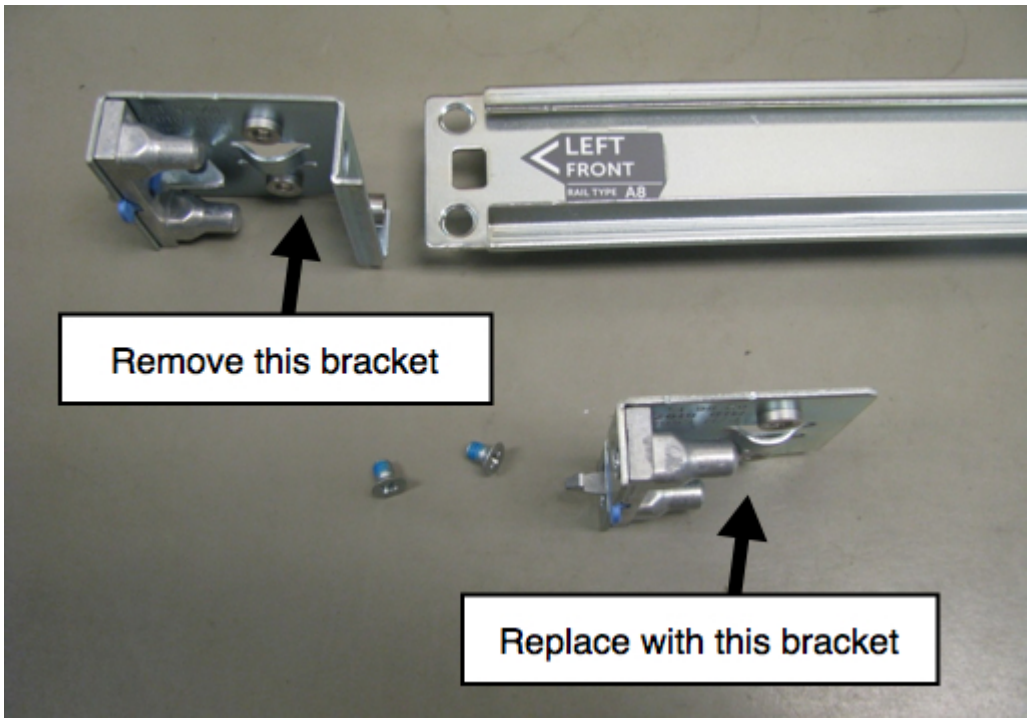
2. Retirez la glissière gauche du carton de la glissière.



Chaque glissière est marquée.

3. Utilisez un tournevis cruciforme pour retirer les deux vis de montage.

4. Retirez le support et remplacez-le par le nouveau support.



5. Réutilisez les vis pour fixer le support de nouveau en place.

La glissière est désormais prête pour l'installation de l'appliance R630.

Description matérielle de l'appliance hybride R730xd S5

Introduction

L'appliance hybride RSA Security Analytics de la gamme 5 est basée sur le châssis Dell PowerEdge R730xd. L'appliance hybride RSA Security Analytics de la gamme 5 est fournie avec le logiciel de l'appliance hybride Security Analytics 10.5 installé. Le logiciel d'appliance hybride inclut le Concentrator et le Decoder (log ou paquets, pas les deux).

La configuration initiale d'une appliance de la gamme 5 de votre réseau comprend ces étapes :

1. Vérifiez les exigences en matière de site et les informations de sécurité dans le Guide de déploiement pour votre version du logiciel Security Analytics : Security Analytics 10.5
2. Montez ou placez le matériel de l'appliance en toute sécurité, conformément aux exigences de votre site.
3. Connectez l'appliance à votre réseau et configurez les paramètres réseau sur l'appliance : Connectez l'appliance et configurez les paramètres réseau.
4. Terminez la configuration de l'appliance dans Security Analytics : Terminez la configuration de l'appliance dans Security Analytics.

Caution: Pour éviter d'endommager les appliances et les serveurs Security Analytics, retirez-les du rack et démontez le rack avant de les déplacer vers un autre emplacement. Suivez les recommandations du fabricant du serveur et du fabricant du rack pour l'emballage, le transport et l'installation.
RSA ne prend pas en charge la réexpédition des serveurs en rack. Le client prend en charge tous les risques et est le seul responsable lors du transport des serveurs et appliances Security Analytics montés en rack.

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 appliance hybride.

- Appliance hybride de la gamme 5
- Glissières statiques ReadyRails (1 jeu)
- Adaptateur 2U de glissière gauche pour rack profond EMC
- Panneau RSA 2U (1) - Les clés sont fixées au panneau.
- Cordon d'alimentation (2)
- Guide d'information sur le produit Dell (1)
- Dossier de la documentation RSA (1)

Last Modified: August 10 2016, 9:33AM

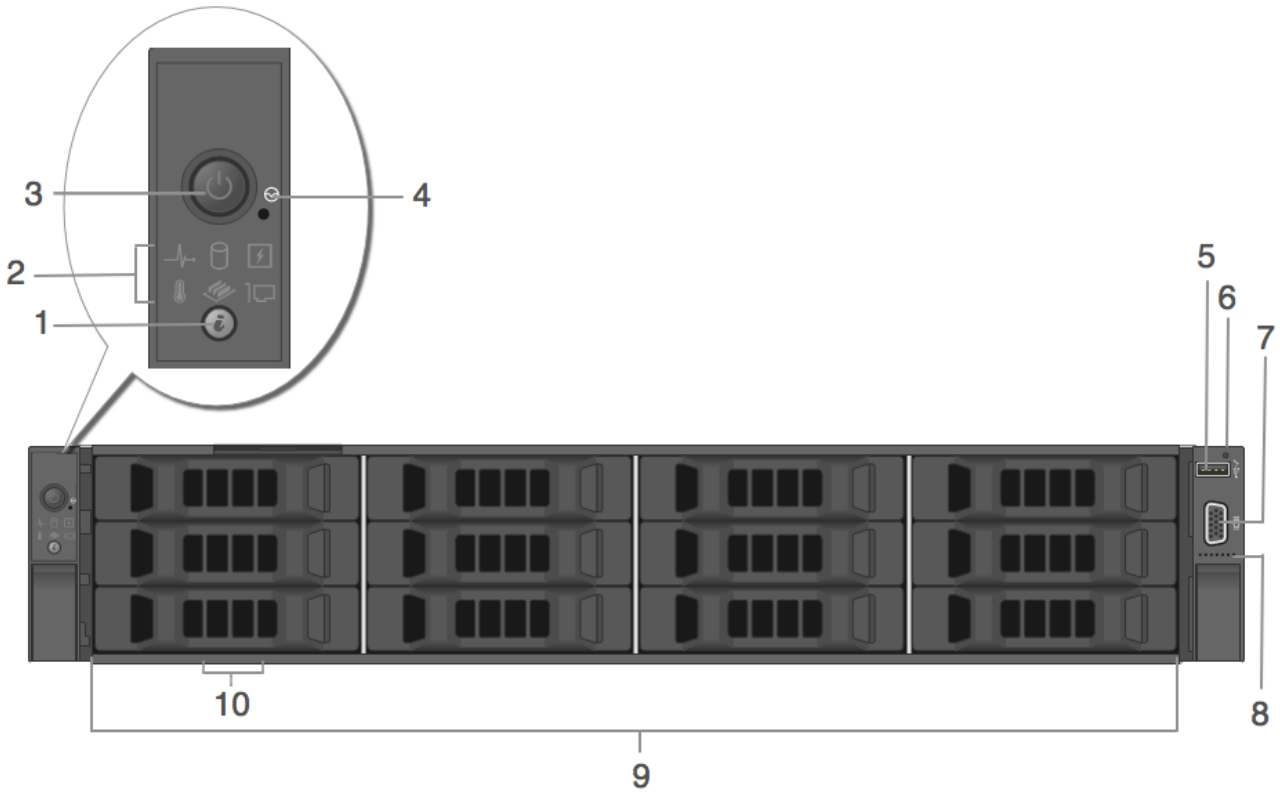
- CLUF RSA (1)

Matériel fourni par le client

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

- Un câble 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

Vue avant de l'appliance hybride Security Analytics

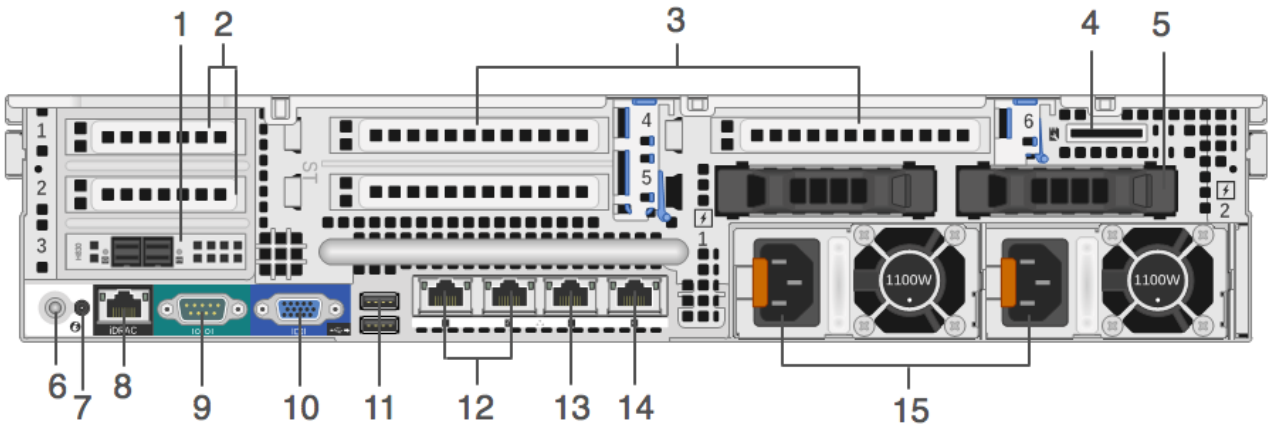


Clé	Description
1	Bouton d'identification du système
2	Indicateurs de diagnostic
3	Marche/Arrêt

Last Modified: August 10 2016, 9:33AM

Clé	Description
4	Bouton d'interruption non masquable encastré
5	Port de gestion USB/iDRAC Direct
6	Voyant indicateur iDRAC Direct
7	Connecteur vidéo
8	Synchronisation rapide (facultative)
9	12 disques durs 3,5 pouces (remplaçables sur site). L'appliance hybride Security Analytics a un total de 14 disques. Il y a 12 disques durs à l'avant et 2 disques SSD à l'arrière. Consultez les caractéristiques techniques de l'appliance ci-dessous pour plus d'informations.
10	Emplacement des balises d'informations

Vue arrière de l'appliance hybride Security Analytics



Clé	Description
1	Contrôleur RAID PERC H830. Il est indiqué dans le slot de carte PCIe 3, mi-hauteur, mais il peut être installé dans un autre slot pour carte PCIe, mi-hauteur. Le PERC H830 est le contrôleur RAID pour le DAC d'extension de stockage. Il nécessite un câble avec un port Mini-SAS pour se connecter au DAC.
2	Slots de carte d'extension PCIe mi-hauteur 1 et 2
3	Slots de carte d'extension PCIe, hauteur complète (3)
4	Slot de carte media vFlash
5	Deux disques SSD 2,5 pouces (remplaçables à chaud)
6	Bouton d'identification du système

Last Modified: August 10 2016, 9:33AM

Clé	Description
7	Connecteur d'identification du système
8	Port d'entreprise iDRAC8
9	Port série RS232 (connexion série pour les ordinateurs portables via DB9 ou serveur série)
10	Port vidéo VGA (moniteur)
11	Ports USB (clavier, souris, clé USB, etc.)
12	Ports Gigabit Ethernet 10GBASE-T : em3-4
13	Port de gestion 1000BASE-T de réseau principal : em1
14	Port 1000BASE-T de réseau secondaire : em2
15	Alimentations 1 et 2 remplaçables à chaud (remplaçable sur site)

Note: Le contrôleur RAID PERC H830 nécessite un câble avec un port Mini-SAS pour se connecter au DAC.

Spécifications de l'appliance hybride Security Analytics

Élément	Description
Encombrement	2U, profondeur complète
Poids (approximatif)	36,5 kg
Dimensions (approximatives)	H : 8,73 cm x L : 48,2 cm x P : 75,58 cm
Les alimentations	Alimentation double, installable à chaud, redondante (1+1), 1 100 W
Processeurs	2 * E5-2680v3
RAM	16 * RDIMM 8 Go 2133 MT/s (128 Go)
Disques durs	L'appliance hybride Security Analytics a un total de 14 disques. Il y a 12 disques durs à l'avant et 2 disques SSD à l'arrière. 2 * disque SSD 800 Go (arrière) 4 x disque NLSAS 1 To 7,2 K t/min 6 Gbit/s 8 x disque NLSAS 6 To 7,2 K t/min 6 Gbit/s
Contrôleur RAID	Externe : PERC H830 RAID Interne : PERC H730P
Carte d'interface réseau	Carte fille réseau Intel Ethernet X540 10 Go BT DP + I350 1 Go BT DP

Last Modified: August 10 2016, 9:33AM

Caution: L'ouverture du châssis de l'appliance entraînera l'annulation de la garantie, sauf si vous êtes spécifiquement invité à le faire par l'assistance clientèle de RSA. Les disques durs et les alimentations sont remplaçables sur site par un technicien qualifié.

Last Modified: August 10 2016, 9:33AM

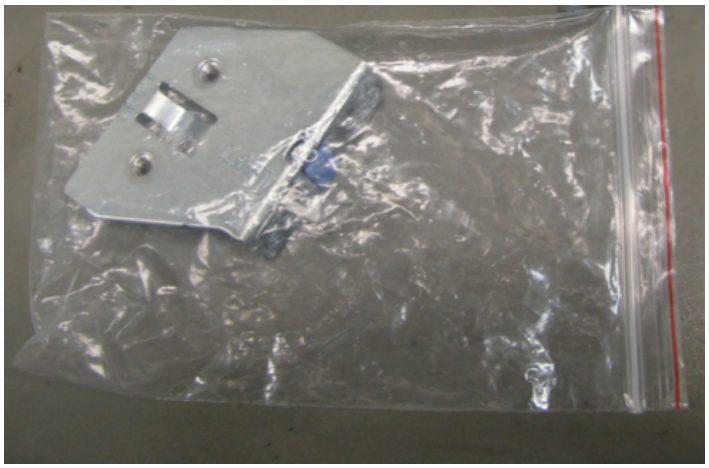
Installation d'un adaptateur de rack profond pour un hybride R730xd

Procédure

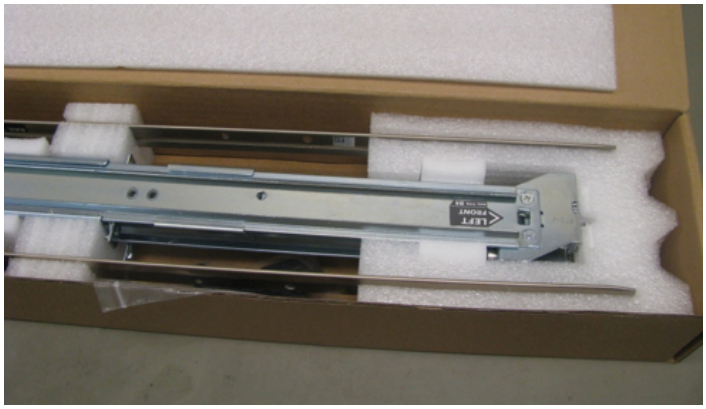
Note: Cette procédure s'applique uniquement si vous installez l'appliance hybride S5 R730xd dans un rack EMC Titan D Ultra.

Lors de l'installation de l'appliance hybride S5 R730xd dans un rack EMC Titan D Ultra, un adaptateur de rack profond 2U est obligatoire. Suivez cette procédure pour installer un nouveau support sur les glissières du serveur.

1. Dans la boîte d'accessoires du carton de l'appliance hybride R730xd, cherchez le support de l'autre glissière.



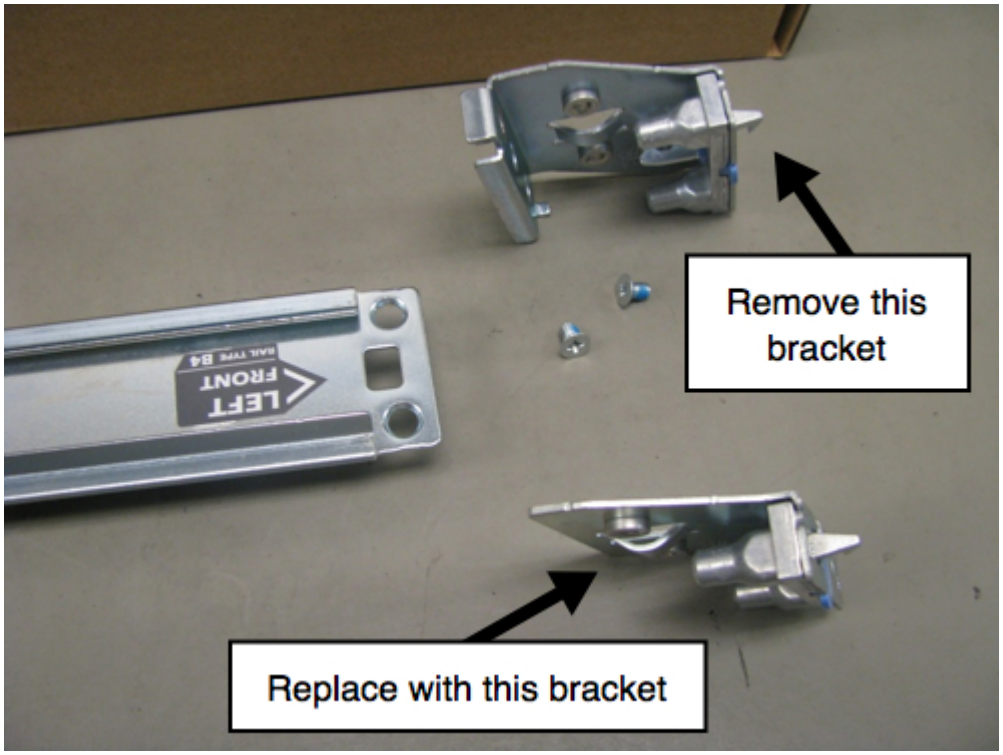
2. Retirez la glissière gauche du carton de la glissière. Chaque glissière est marquée.



Last Modified: August 10 2016, 9:33AM

3. Utilisez un tournevis cruciforme pour retirer les deux vis de montage.

4. Retirez le support et remplacez-le par le nouveau support.



Last Modified: August 10 2016, 9:33AM

5. Réutilisez les vis pour fixer le support de nouveau en place.

La glissière est désormais prête pour l'installation de l'appliance hybride R730xd.

RSA

Connecter l'appliance et configurer les paramètres réseau

Présentation

Cette section fournit des instructions pour connecter une appliance Security Analytics S5 à votre réseau et configurer les paramètres de gestion initiaux sur l'appliance.

Conditions préalables

Pour chaque appliance Security Analytics de la gamme 5, obtenez et écrivez les informations dans le tableau suivant.

Configuration	Standard	Votre appliance
Connexion	racine	
Password	netwitness	
Adresse IP du système	192.168.1.1	
Masque de réseau système	255.255.255.0	
Passerelle par défaut		
Serveur DNS principal Adresse IP		
Serveur DNS secondaire IP		
Nom de domaine local (ou aucun)		
Nom d'hôte non complet	NWAPPLIANCE<xxxxxx>, où <xxxxxx> est un nombre aléatoire généré.	
Adresse IP du serveur Security Analytics		

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

Last Modified: August 10 2016, 9:33AM

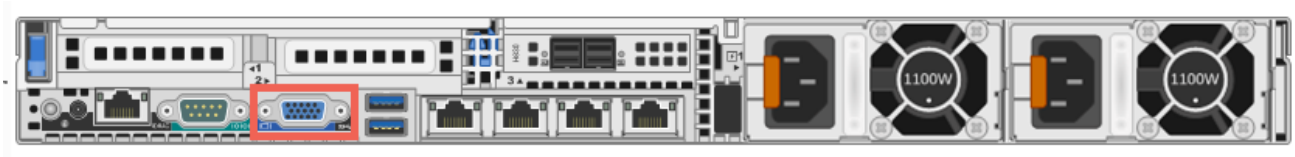
Introduction

La configuration des paramètres réseau pour une appliance RSA Security Analytics S5 inclut la définition de l'adresse IP par défaut, de la source d'horloge réseau et du nom d'hôte, puis la configuration de vos serveurs DNS. Pour définir ces paramètres, vous pouvez vous connecter à la console de l'appliance à l'aide d'un clavier et d'une souris.

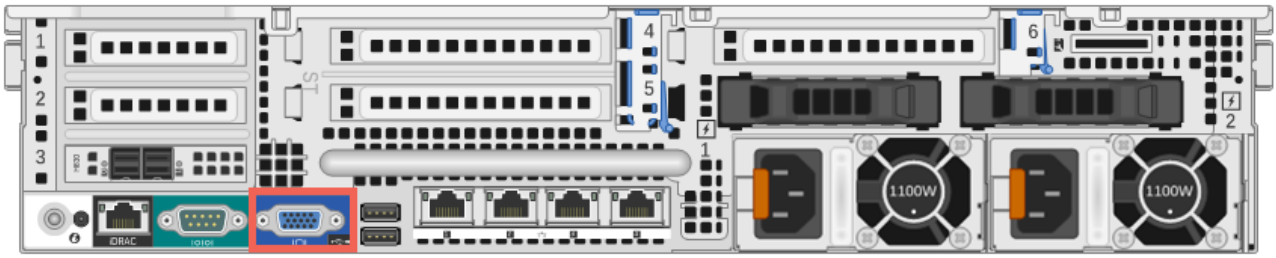
La pratique privilégiée consiste à provisionner le serveur Security Analytics avant de configurer les autres appliances Security Analytics.

Se connecter à la console de l'appliance

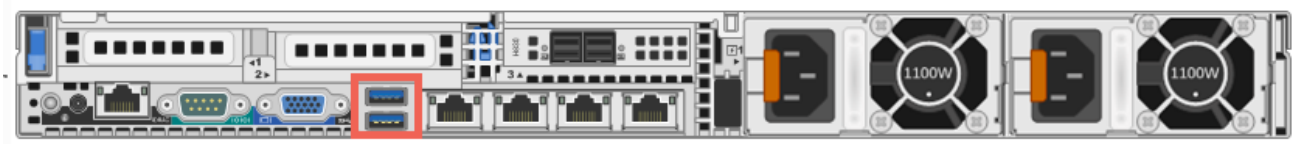
1. Connectez un moniteur ou un adaptateur KVM au port VGA à l'arrière de l'appliance.



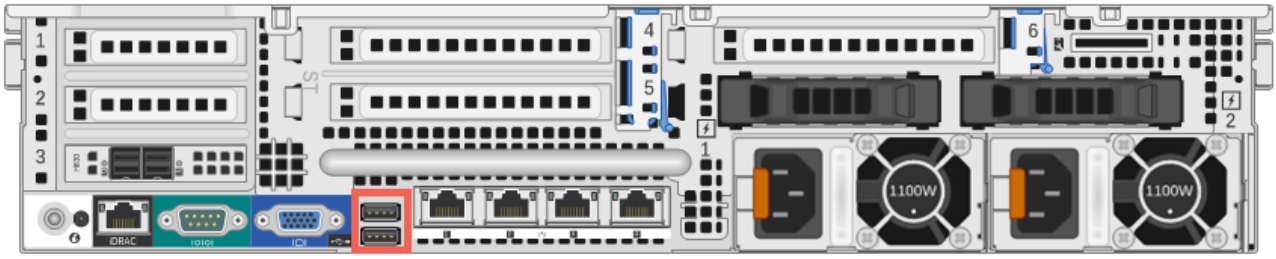
La figure suivante montre l'emplacement de port VGA pour l'appliance hybride.



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

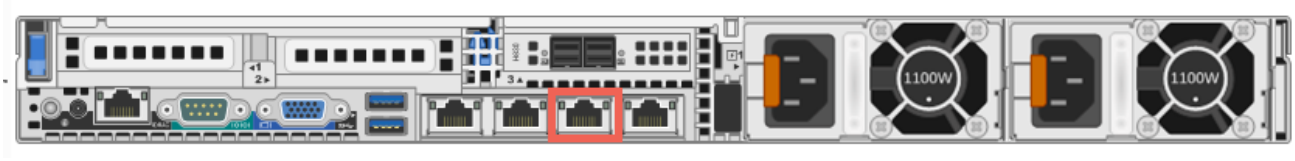


La figure suivante montre l'emplacement de port USB pour l'appliance hybride.

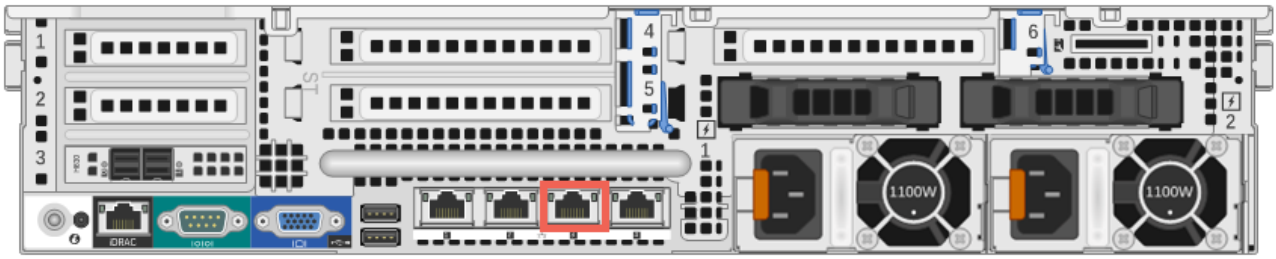


Last Modified: August 10 2016, 9:33AM

3. Connectez un câble Ethernet à partir du réseau au port em1 à l'arrière de l'appliance.



La figure suivante montre l'emplacement de port em1 pour l'appliance hybride.



4. Connectez un câble d'alimentation à chacun 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.

5. Mettez l'appliance sous tension et passez à la section Configurer les paramètres réseau.

Configurer les paramètres réseau

1. À l'invite de connexion, utilisez les informations d'identification par défaut pour accéder au système d'exploitation :

```
NWAPPLIANCE<xxxxxx> login: root
Password: netwitness
```

> **Note:** Si vous n'avez pas reçu les invites pour configurer les paramètres réseau, vous pouvez exécuter `#netconfig.sh` à partir de la ligne de commande pour vous inviter à saisir les options de configuration.

2. Saisissez les informations suivantes à l'invite :
   a. Adresse IP du système (ou **d** pour DHCP)
   b. Masque de réseau système
   c. Passerelle par défaut
   d. Adresse IP du serveur DNS principal
   e. Adresse IP du serveur DNS secondaire (ou appuyez sur **Entrée** pour aucune)
   f. Nom de domaine local (ou appuyez sur **Entrée** pour aucun)
   g. Nom d'hôte non complet

Last Modified: August 10 2016, 9:33AM

Au terme de la configuration initiale, vous devez voir une invite qui vous permet d'enregistrer la configuation, comme illustré sur la figure suivante.

3. Vérifiez les informations saisies, puis saisissez `y` pour enregistrer la configuration.
   Cela permet de définir les informations de réseau et de redémarrer les services réseau.
4. Si votre appliance n'est pas un serveur Security Analytics, **attendez environ 15 secondes pour recevoir une invite**, puis entrez l'adresse IP du serveur Security Analytics à l'invite.
5. Vérifiez la connectivité réseau en envoyant une requête ping à votre serveur DNS.
6. Passez à la section Spécifier la source de l'horloge réseau.

Spécifier la source de l'horloge réseau

La configuration de la synchronisation horaire entre les appliances et les services est obligatoire. Il est vivement recommandé d'utiliser une source d'heure NTP pour la synchronisation. Non seulement l'heure est essentielle pour les communications sous-jacentes entre les services, mais si les appliances ne sont pas synchronisées, cela peut entraîner une non-concordance des heures indiquées lors de l'analyse des données. Si le serveur NTP n'est pas configuré ou accessible à ce stade, la configuration de la source d'horloge réseau échouera, mais elle peut être effectuée à partir de l'interface Security Analytics ultérieurement.

Last Modified: August 10 2016, 9:33AM

Bonnes pratiques

RSA recommande de suivre les bonnes pratiques suivantes :

Pour une meilleure intégrité des données, configurez le serveur Security Analytics en tant que source de l'horloge de toutes les autres appliances. Toutes les appliances, y compris Event Stream Analysis (ESA), obtiennent l'heure à partir du serveur Security Analytics. Seul le serveur Security Analytics est configuré à une source d'heure NTP externe.

Pour l'appliance du serveur Security Analytics, utilisez l'utilitaire NwConsole pour vous connecter à la source de temps NTP.

Si les autres appliances ont Security Analytics 10.5.1 ou version ultérieure, l'heure est automatiquement définie sur toutes les appliances rattachées à l'appliance de serveur Security Analytics. Si les autres appliances n'ont pas Security Analytics 10.5.1 ou ultérieure, définissez l'heure pour pointer vers le serveur Security Analytics manuellement.

Définir l'heure sur le serveur Security Analytics à l'aide de l'utilitaire NwConsole

Pour définir la source de l'horloge réseau sur le serveur Security Analytics à l'aide de l'utilitaire NwConsole :

1. À l'invite racine `[root@NwAppliance~]#`, saisissez la commande suivante :
   `NwConsole`
   NwConsole démarre et le message de démarrage s'affiche avec une version et une date :
   `Console RSA Security Analytics`
2. Dans NwConsole, saisissez la commande suivante :
   `login localhost:50006 <username> <password>`
   Le nom d'utilisateur du compte administrateur système pour Security Analytics est **admin** et le mot de passe par défaut est **netwitness**.
   Vous êtes connecté à l'appliance et le message suivant s'affiche :
   `Successfully logged in as session <session #>`
3. À l'invite de l'hôte local `[localhost:50006] />` effectuez l'une des opérations suivantes :
   a. Si vous souhaitez utiliser votre source d'horloge de réseau, entrez la commande suivante :Si vous souhaitez utiliser votre source d'horloge réseau, entrez la commande suivante :
      `appliance setNTP source=<NTP_server_hostname or IP_address>`
      Par exemple : `appliance setNTP source=0.pool.ntp.org`
   b. Si vous souhaitez utiliser l'horloge de l'appliance comme source de l'horloge, saisissez : `appliance setNTP source=local`
4. Lorsque le résultat de la commande est `Success`, saisissez **`exit`** pour vous déconnecter, puis quittez le programme NwConsole.

> **Note:** Si vous avez spécifié une source d'horloge NTP locale, l'horloge de l'appliance constitue la source de l'horloge et l'heure est configurée à l'aide de Définir l'horloge intégrée de l'appliance, comme décrit dans l'aide en ligne Security Analytics.

Fin de la configuration de l'appliance dans Security Analytics

Introduction

Pour terminer la configuration d'une appliance de la gamme 5, vous devez vous connecter à Security Analytics et utiliser les options de configuration disponibles dans le module Security Analytics Administration. Chaque type d'appliance a une configuration un peu différente. Cette section fournit des informations de base et des liens vers des documents d'aide en ligne pour vous guider tout au long du processus.

Se connecter à Security Analytics

RSA Security Analytics est une application basée sur le web qui vous lancez dans une fenêtre de navigateur. Les navigateurs compatibles incluent n'importe quel navigateur qui prend en charge le protocole WebSocket, LocalStrorage et les API d'historique HTML5 : Google Chrome, Apple Safari, Mozilla Firefox et Internet Explorer 10 ou version ultérieure.

1. Dans votre navigateur Web, saisissez ce qui suit :
   `https://<hostname or IP address>/login`
   Où `<hostname or IP address>`est le nom d'hôte ou l'adresse IP de votre serveur Security Analytics.

Last Modified: August 10 2016, 9:33AM

L'écran de connexion de Security Analytics s'affiche.

2. Entrez votre nom d'utilisateur et votre mot de passe, puis cliquez sur **Se connecter**.
   Le nom d'utilisateur du compte administrateur système pour Security Analytics est **admin** et le mot de passe par défaut est **netwitness**.

Ouvrir l'aide en ligne

Les instructions pour la configuration des appliances individuelles sont fournies en fonction de la version du logiciel installée sur l'appliance.

Pour Security Analytics 10.5, lisez ces documents : Guides de configuration de l'hôte et des services et Guide d'octroi de licence. Un bon point de départ pour comprendre le processus général de configuration et commencer la configuration est le *Host and Service Getting Started Guide*.

Last Modified: August 10 2016, 9:33AM