

RSA Security Analytics

Guide de configuration du service IPDB Extractor pour la Version 10.6





Copyright © 2010 - 2016 RSA, the Security Division of EMC. All rights reserved.

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.

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 du service IPDB Extractor

٠

4
5
7
8
17
19
20
22
24
28
29
30
31
36

.

Guide de configuration du service IPDB Extractor

Ce guide fournit des instructions pour configurer le service ainsi qu'une liste de contrôle permettant de guider les utilisateurs tout au long de la configuration du service IPDB Extractor. Chaque tâche de la liste de contrôle fait l'objet d'une description dans une procédure distincte, et une rubrique de référence séparée donne des détails sur les paramètres de configuration. Lorsque toutes les tâches de la liste sont réalisées ou jugées inutiles dans le cas des tâches facultatives, Security Analytics est prêt à générer des rapports à l'aide d'IPDB pour les analystes.

IPDB et le service IPDB Extractor

Cette rubrique présente le service IPDB Extractor et son rôle dans le module Reporting. Vous pouvez choisir IPDB (Internet Protocol Database) comme source de données lorsque vous générez des rapports dans le module RSA Security Analytics Reporting. Le service IPDB Extractor envoie les données issues d'IPDB au Reporting Engine. IPDB est le référentiel des messages d'événements normalisés et bruts. IPDB stocke tous les messages collectés dans un système de fichiers organisé par source d'événement (service), adresse IP et date (jour/mois/année) avec les fichiers d'index pour faciliter les recherches (rapport et requêtes).

Note: IPDB Extractor ne prend en charge que les sources d'événement Content 2.x.

Vous pouvez utiliser la boîte de dialogue Déploiement manuel de la ressource de Live pour déployer le dernier contenu sur le service IPDB Extractor. Le processus de déploiement stocke le contenu du service IPDB Extractor dans le répertoire **/etc/netwitness/ng/envision/etc**. Le contenu se compose des éléments suivants :

- Le service xml pour tous les types de service pris en charge par RSA.
- Le fichier ipaddr.tab : un fichier d'adresses IP.
- Le fichier ecat.ini.
- Le fichier table-map.xml : mappage de contenu Envision vers des métadonnées NetWitness.

IPDB File System





.

Configurer le service IPDB Extractor

Cette rubrique constitue un ensemble de procédures de configuration du service IPDB Extractor. Les étapes requises pour la configuration sont présentées dans l'ordre dans lequel l'administrateur les réalise. Une fois la configuration terminée, les analystes et les opérateurs peuvent générer des rapports de données dans IPDB.

Étape 1. Monter IPDB

Cette rubrique décrit comment configurer le service Internet Protocol Database (IPDB) Extractor afin d'en faire une source de données disponible pour Reporting Engine.

Le service Internet Protocol Database (IPDB) Extractor facilite l'utilisation de la base de données de sources d'événements IPDB RSA enVision en tant que source de données pour Reporting Engine. Avant de pouvoir utiliser le service IPDB comme source de données pour Reporting Engine, vous devez le monter dans votre environnement Security Analytics, et inclure les instructions de montage dans le fichier /etc/fstab afin que l'IPDB soit monté automatiquement à l'avenir.

Dans cette version, Security Analytics :

- prend en charge deux types de déploiements IPDB :
 - sur une appliance ES,
 - · sur un périphérique de stockage rattaché au réseau (NAS) distinct,
- ne prend pas en charge un IPDB qui s'exécute sur un périphérique de stockage en attachement direct (DAS).

Note: Dans un environnement comprenant plusieurs sites RSA enVision, chaque site nécessite qu'une instance IPDB Extractor distincte s'exécute sur une appliance distincte (virtuelle ou physique) pour pouvoir s'intégrer avec la source de données IPDB du site.

Monter un IPDB s'exécutant sur une appliance ES

Vous devez effectuer les tâches suivantes pour monter un IPDB s'exécutant sur une appliance ES :

- Tâche 1 Se connecter à l'appliance ES.
- Tâche 2 Créer un utilisateur système dans Active Directory, puis partager les répertoires IPDB et csd.
- Tâche 3 Noter le Broker Reporting Engine et configurer le parefeu.
- Tâche 4 Configurer IPDB et le fichier d'emplacement de périphérique.
- Tâche 5 (facultatif) Si IPDB a plusieurs emplacements de stockage, les mapper.

Note: Les exemples de ces tâches utilisent Microsoft Windows 2003. Si vous avez une autre version de Windows, les écrans et l'accès à ces derniers peuvent différer.

Tâche 1 Se connecter à l'appliance ES

Connectezvous à l'appliance ES afin de monter un IPDB résidant sur cette appliance ES.

Note: Vous devez utiliser les informations d'identification du compte maître RSA enVision pour vous connecter à l'appliance ES.

.og On to Win	dows
/	Windows Server 2003 R2 Enterprise x64 Edition
Copyright © 2005 N	Alcrosoft Corporation Alignment
User name:	master
Password:	1
	OK Cancel Options >>

Tâche 2 Créer un utilisateur système dans Active Directory, puis partager les répertoires IPDB et CSD

Pour créer un utilisateur système dans Active Directory avec une autorisation de lecture seule pour l'accès au répertoire IPDB :

1. Accédez au dossier Active Directory.



2. Créez un utilisateur système dans Active Directory.

Interstory Users and Comp	outers	
	elp	
$\leftarrow \rightarrow \boxdot \blacksquare \& \circledast \times $	' 🖻 🖻 😰 💷 🦉 💯 🐜 🖓 🍕 🙍	
Active Directory Users and Computer	Users 25 objects	
ESIPDB.nic	Name Tupe Description	
Builtin Computers Computers Ormain Controllers ForeignSecurityPrincipals Users	Create in: ESIPDB.nic/Users	
	Eirst name: ipdbuser Initials:	
	Last name:	
	Full name: ipdbuser	
	Ser logon name:	
	ipdbuser @ESIPDB.nic	
	Q i User logon name (pre- <u>₩</u> indows 2000):	
	ESIPDB\ ipdbuser	

Partagez le répertoire IPDB (par exemple e:\nic\lsnode\data) :<
 <p>Le programme d'installation télécharge le fichier lockdown.zip contenant le script doit.bat dans l'appliance Broker. Le script doit.bat vous donne la possibilité de partager IPDB. Le partage exporte le dossier afin que vous puissiez y accéder à partir de Linux dans votre environnement Security Analytics.

- a. Copiez le fichier lockdown.zip à partir du répertoire /etc/netwitness/ng/envision du Broker vers l'appliance ES.
- b. Extrayez tous les fichiers de lockdown.zip.
- c. Exécutez le script doit.bat sur l'appliance ES.
- d. Cliquez avec le bouton droit de la souris sur le répertoire IPDB (par exemple e:\nic\lsnode\data).

e. Sélectionnez l'accès Lecture sous l'onglet Autorisations du partage pour accorder au nouvel utilisateur (par exemple ipdbuser@ESIPDB.nic) un accès en lecture au répertoire IPDB.

Address 🛅 E:\nic\lsnode\dat	a				
Name 🔺	Size	Туре	Date Modified	Attribute	is 🛛
ESIPDB-ES Prope	erties	eta estas.	2012 4:20 PM		
General Sharin	9 Security Customize	Permissions for E	SIPDB-ES		? ×
You o	can share this folder with o	th Share Permissions			
folder	ork. To enable sharing for	Group or user na	mes:		
C Do not st	hare this folder	🕵 ipdbuser (ip	dbuser@ESIPDB.nic)		
<u>Share this</u>	s folder				
S <u>h</u> are name:	ESIPDB-ES				
<u>C</u> omment:					
User limit:	Maximum allowed		/	Add	Bemove
	C Allo <u>w</u> this number o	f u <u>P</u> ermissions for ip	 odbuser	Allow	Deny
To set permis folder over th	sions for users who acces e network, click Permissio	s Full Control		2	
To configure	settings for offline access,	c Read			

- 4. Partagez le répertoire csd (par exemple e:\nic\csd).
 - a. Cliquez avec le bouton droit de la souris sur le répertoire csd (par exemple e:\nic\csd).

b. Sélectionnez l'accès Lecture sous l'onglet Autorisations du partage pour accorder au nouvel utilisateur (par exemple csd) un accès en lecture au répertoire csd.

	🗁 E:\nic					
	Eile Edit View Favorites I	ools <u>H</u> elp				
	🔾 Back 🔹 🌍 🔹 🏂 🔎 Searc	h 防 Folders	\$ D 🗙	19		
	Address 🛅 E:\nic					
	Name A	Size	Туре	Date Modified	Attributes	
	6 4000		File Folder	5/31/2012 8:25 AM		
	ackup		File Folder	11/30/2012 1:54 PM		
	Csd		File Folder	12/24/2012 10:44 AM		
	Cinstallables		File Folder	1/25/2013 9:16 PM		
	Snode		File Folder	12/12/2012 4:55 AM		
	tasktriage		File Folder	5/31/2012 4:33 AM		
			_	Permissions for csd		? ×
csd Propert	ies	?	×	Chara Deminiana I		
General	Sharing Security Customize			Share Permissions		
	- [1	Group or user names:		
	You can share this folder with other use	rs on your		C Everyone		
	folder.	er, click share this		indbuser (indbuser@ES34	40 nic)	
C Do	not chare this folder				10.1809	
- • Sha	not shale this folder					
- <u>2</u> 16						
Share r	hame: Csd			1		
Comme	nt:				Add	<u>R</u> emove
User lin	nit: <u>M</u> aximum allowed			Permissions for ipdbuser	Allow	Deny
	Allow this number of users:			Full Control	F	
				Change	ň	ā
To set p folder o	permissions for users who access this ver the network, click Permissions.	Permissions		Read		ā
To con Caching	figure settings for offline access, click g.	Caching				
		New Share		,		
Windows	s Firewall will be configured to allow this	folder to be				
shared w	with other computers on the network.					1
View you	# Windows Firewall settings			OK	Cancel	Apply

Tâche 3 Noter le Broker Reporting Engine et configurer le parefeu

Pour noter l'adresse IP du Broker pour la configuration ultérieure, et pour configurer le parefeu :

- 1. Notez l'adresse IP de l'appliance Broker sur laquelle vous souhaitez exécuter Reporting Engine.
- 2. Configurez le parefeu afin que le Broker exécutant Reporting Engine puisse accéder au répertoire partagé sur l'appliance ES.

Tâche 4 Configurer IPDB et le fichier d'emplacement de périphérique

Pour configurer IPDB et le fichier d'emplacement de périphérique :

1. Mettez à jour /etc/fstab pour créer le point de montage d'IPDB :

a. Exécutez les commandes suivantes pour autoriser l'utilisation d'un fichier de mot de passe pour les informations d'identification :

yum install cifsutils

Le package cifsutils s'installe sur l'appliance.

- b. Procédez de la manière suivante pour insérer le répertoire du point de montage IPDB dans le fichier /etc/fstab :
 - Si vous n'utilisez pas de fichier d'informations d'identification : //1.1.1.1/ESIPDB-ES /var/netwitness/ipdbextractor/ipdb/ cifs auto,nouser,noexec,ro, username=*username*, password=*credentials-of-ipdb-user* 0 0
 - Si vous utilisez un fichier d'informations d'identification : //1.1.1.1/ESIPDB-ES /var/netwitness/ipdbextractor/ipdb/ cifs auto,nouser,noexec,ro,credentials=/root/cred 0 0

Vous pouvez créer un fichier d'informations d'identification pour fournir le nom d'utilisateur et le mot de passe d'IPDB-USER. Le contenu du fichier serait le suivant :

username=*username* password=*password*

- c. Effectuez l'une des opérations suivantes pour insérer le répertoire du point de montage csd dans le fichier /etc/fstab :
 - Si vous n'utilisez pas de fichier d'informations d'identification : //1.1.1.1/csd /var/netwitness/ipdbextractor/devicelocation cifs auto,nouser,noexec,ro, username=username, password=credentialsofipdbuser 0 0
 - Si vous utilisez un fichier d'informations d'identification : //1.1.1.1/csd /var/netwitness/ipdbextractor/devicelocation cifs auto,nouser,noexec,ro,credentials=/root/cred 0 0
- 2. Saisissez mount -a.

Tâche 5 (facultatif) Mapper les emplacements de stockage d'un IPDB ayant plusieurs emplacements de stockage

Pour mapper les emplacements de stockage pour IPDB avec de multiples emplacements de stockage :

- 1. Dans le menu Security Analytics, sélectionnez Administration > Services.
- 2. Dans la grille **Services**, sélectionnez un service IPDB Extractor.
- Dans la barre d'outils, sélectionnez Vue > Explorer. Security Analytics affiche l'arborescence de dossiers de paramètres IPDB Extractor.
- 4. Cliquez avec le bouton droit de la souris sur /ipdbextractor/config/storage.mapping dans l'arborescence de dossiers de paramètres.
- 5. Entrez la valeur e:\nic\lsnode~storage1,d:\seclocation~storage2.

Change Davides 🔪 🚞 Evolute V 🔪 IPDB-One

change bevice / = explore / / h	00-0112		
IPDB-One (IPDB Extractor)	<1	/ipdbextractor/configIPDB-0	One (IPDB Extractor)
IPDB-One (IPDB Extractor)		🗱 sqlite.filter	yes
) 🖨 ipdbextractor		🔅 storage.mapping	e:\nic\lsnode~storage1,d:\seclocation~storage2

- 6. Redémarrez le service IPDB Extractor.
- Sur l'appliance Broker, créez les répertoires storage1 et storage2 dans le répertoire ES. En outre, vous devez modifier les points de montage /etc/fstab afin qu'ils reflètent les divers répertoires de stockage. Par exemple : //1.1.1./storage1 /var/netwitness/ipdbextractor/ipdb/storage1 cifs auto,nouser,noexec,ro,credentials=/root/creds 0 0

//1.1.1.1/storage2 /var/netwitness/ipdbextractor/ipdb/storage2 cifs auto,nouser,noexec,ro,credentials=/root/creds 0 0

© 2010 - 2016 RSA, The Security Division of EMC. Last Modified: August 10 2016, 9:33AM Note: Dans cet exemple, storage1 est un nom partagé donné à e:\nic\lsnode\data sur une appliance ES avec l'adresse IP 1.1.1.1. De même, storage2 est un nom partagé donné à d:\alternatestorage\data sur la même appliance. En outre, lorsque vous disposez de plusieurs emplacements de stockage, les emplacements de stockage mappés d'une appliance Broker deviennent leurs noms de nœuds respectifs sur l'appliance ES ou le NAS (en d'autres termes, storage1 et storage2 sont créés dans le répertoire /var/ netwitness/ipdbextractor/ipdb/ de l'appliance Broker

Monter un IPDB s'exécutant sur un périphérique de stockage rattaché au réseau

Vous devez effectuer les tâches suivantes pour monter un IPDB s'exécutant sur un NAS :

- Tâche 1 Créer un utilisateur en lecture seule IPDB et csd.
- Tâche 2 Se connecter physiquement au NAS.
- Tâche 3 Configurer IPDB et le fichier d'emplacement de périphérique.
- Tâche 4 (facultatif) Si IPDB a plusieurs emplacements de stockage, les mapper.

Tâche 1 Créer un utilisateur en lecture seule IPDB et CSD

Accédez au contrôleur d'administration du NAS, puis créez un utilisateur en lecture seule dans les répertoires IPDB et **csd** sur le NAS.

Tâche 2 Se connecter physiquement au NAS

Connecter physiquement le NAS à l'appliance Broker exécutant Reporting Engine via un commutateur privé. Vous devez appliquer une adresse IP au point Ethernet auquel vous rattachez le NAS (par exemple **10.203.2.***x*, où *x* est supérieur à 60).

Tâche 3 Configurer IPDB et le fichier d'emplacement de périphérique

Pour configurer IPDB et le fichier d'emplacement de périphérique :

IPDB et le fichier d'emplacement de périphérique résident sur un périphérique de stockage rattaché au réseau (NAS) dans un déploiement d'appliance LS. Le fichier d'emplacement de périphérique (**.dir**) réside sur le partage **vol0**, et IPDB réside dans **vol1/vol2/vol3**, selon la façon dont vous avez configuré IPDB pour votre environnement.

- 1. Mettez à jour /etc/fstab pour créer le point de montage d'IPDB :
 - a. Exécutez les commandes suivantes pour autoriser l'utilisation d'un fichier de mot de passe pour les informations d'identification :
 yum install cifsutils

Le package cifsutils s'installe sur l'appliance.

- b. Procédez de la manière suivante pour insérer le répertoire du point de montage IPDB dans le fichier /etc/fstab :
 - Si vous n'utilisez pas de fichier d'informations d'identification : //1.1.1.1/vol1 /var/netwitness/ipdbextractor/ipdb/LSIPDB-LC1/ cifs auto,nouser,noexec,ro,prefixpath=/nic/ Isnode/LSIPDB-LC1/data/LSIPDB-LC1, username=username, password=credentials-of-ipdb-user 0 0
 - Si vous utilisez un fichier d'informations d'identification : //1.1.1.1/vol1 /var/netwitness/ipdbextractor/ipdb/LSIPDBLC1/ cifs auto,nouser,noexec,ro,prefixpath=/nic/ Isnode/LSIPDBLC1/data/LSIPDBLC1,credentials=/root/cred 0 0
 Vous pouvez créer un fichier d'informations d'identification pour fournir le nom d'utilisateur et le mot de passe d'IPDB-USER. Le contenu du fichier serait le suivant : username=username password=password
 Pour vérifier si IPDB est monté correctement, assurezvous que le répertoire /var/netwitness/ipdbextractor/ipdb contient le NODENAME suivi de divers types de périphériques.
 - Si vous avez plusieurs LC :

//1.1.1.1/LSIPDBLC1 /var/netwitness/ipdbextractor/ipdb/LSIPDBLC1 cifs auto,nouser,noexec,ro, username=username, password=credentialsofipdbuser 0 0

//1.1.1.1/LSIPDBLC2 /var/netwitness/ipdbextractor/ipdb/LSIPDBLC2 cifs auto,nouser,noexec,ro, username=username, password=credentialsofipdbuser 0 0

- c. Effectuez l'une des opérations suivantes pour insérer le répertoire du point de montage csd dans le fichier /etc/fstab :
 - Si vous n'utilisez pas de fichier d'informations d'identification : //1.1.1.1/vol0 /var/netwitness/ipdbextractor/devicelocation cifs auto,nouser,noexec,ro,prefixpath=/nic/csd, username=username, password=credentialsofipdbuser 0 0
 - Si vous utilisez un fichier d'informations d'identification : //1.1.1.1/vol0 /var/netwitness/ipdbextractor/devicelocation cifs auto,nouser,noexec,ro,prefixpath=/nic/ csd,credentials=/root/cred 0 0

Pour vérifier si le fichier d'emplacement de périphérique est monté correctement, assurezvous que le répertoire /var/ netwitness/ipdbextractor/devicelocation/global/local/ contient le fichier d'emplacement de périphérique.

2. Saisissez mount -a.

Tâche 4 (facultatif) Mapper les emplacements de stockage d'un IPDB ayant plusieurs emplacements de stockage

Pour mapper les emplacements de stockage pour IPDB avec de multiples emplacements de stockage :

- 1. Dans Security Analytics, sélectionnez Administration > Services.
- 2. Dans la grille Services, sélectionnez un service IPDB Extractor.
- Dans la barre d'outils, sélectionnez Vue > Configuration.
 Security Analytics affiche l'onglet Général des paramètres de configuration d'IPDB Extractor.
- 4. Sous l'onglet Configuration d'IPDB Extractor, dans le paramètre Mappage de l'emplacement de stockage au point de montage, entrez \\1.1.1.1\vol1\nic\lsnode\LSIPDBLC1~storage1,\\1.1.1.1\vol2\nic\lsnode\LSIPDBLC1~storage2 pour la valeur de configuration.
- 5. Redémarrez le service IPDB Extractor.
- 6. Sur l'appliance Broker, créez les répertoires **storage1** et **storage2** dans le répertoire **LSIPDBLC1**. En outre, vous devez modifier les points de montage /etc/fstab afin qu'ils reflètent les divers répertoires de stockage. Par exemple :

//1.1.1.1/vol1 /var/netwitness/ipdbextractor/ipdb/LSIPDBLC1/storage1 cifs auto,nouser,noexec,ro,prefixpath=/nic/ Isnode/LSIPDBLC1/data/LSIPDBLC1,credentials=/root/cred 0 0 //1.1.1.1/vol2 /var/netwitness/ipdbextractor/ipdb/LSIPDBLC1/storage2 cifs auto,nouser,noexec,ro,prefixpath=/nic/ Isnode/LSIPDBLC1/data/LSIPDBLC1,credentials=/root/cred 0 0

Note: Dans cet exemple, storage1 est un nom partagé donné à \\1.1.1.1\vol1\nic\Isnode\LSIPDBLC1 sur un périphérique NAS ayant l'adresse IP 1.1.1.1 De même, storage2 est un nom partagé donné à \\1.1.1.1\vol2\ nic\Isnode\LSIPDBLC1 sur la même appliance. En outre, lorsque vous disposez de plusieurs emplacements de stockage, les emplacements de stockage mappés d'une appliance Broker deviennent leurs noms de nœuds respectifs sur le NAS (en d'autres termes, storage1 et storage2 sont créés dans le répertoire LSIPDBLC1 de l'appliance Broker.

Étape 2. Associer un Reporting Engine à IPDB

Cette rubrique décrit la procédure permettant d'associer l'IPDB à un Reporting Engine. Pour associer un service IPDB Extractor à un Reporting Engine, vous devez ajouter le service Reporting Engine et le service IPDB Extractor qui lui est associé au même hôte Broker. Ajouter ou mettre à jour un hôte donne les étapes générales pour ajouter un hôte Broker.

Procédure

Vous devez ajouter le service Reporting Engine et le service PDB Extractor qui lui est associé au même hôte Broker.

 Ajoutez le service Reporting Engine à l'hôte Broker. Lorsque vous ajoutez un service Reporting Engine, ce dernier est paramétré par défaut sur le port approprié (51113) comme illustré ci-dessous :

Add Service		₽×
Service	Reporting Engine	- 1
Host	~	- 1
Name		- 1
Connection Deta	ails	- I
Port	51113	
Test Connection	n	
	Cancel Save	

Le service Reporting Engine est ajouté à l'hôte Broker 10.31.205.50 :

2. Ajoutez le service IPDB Extractor.

Lorsque vous ajoutez le service IPDB Extractor, ce dernier est paramétré par défaut sur le port (50025 pour les connexions non-SSL et 56025 pour les connexions SSL). Par défaut, les connexions SSL sont désactivées. Pour les utiliser, vous devez configurer le paramètre **SSL** dans la section **Configuration système** de l'onglet Général d'IPDB Extractor et redémarrer ce service.

Note: Veillez à ce que le port natif approprié du service IPDB Extractor soit spécifié et, le cas échéant, remplacez le port par défaut par le port qui convient. Après la mise à niveau, vérifiez que le port du service IPDB Extractor corresponde au port natif approprié.

3. Le service IPDB Extractor est ajouté à l'hôte Broker 10.31.205.50 :

Add Service		×
Service	IPDB Extractor	
Host	10.31.205.50	~
Name	IPDB	
Connection De	tails	
Port	50025	
SSL		
Username	admin	
Password	***	
Test Connecti	on	
	Cancel	Save

- 4. Dans le menu Security Analytics, sélectionnez Administration > Services.
- 5. Pour un **Reporting Engine** dans la colonne **Actions**, cliquez sur **Sources**.
- 6. Sous l'onglet Sources, ajoutez un service IPDB Extractor en tant que source de données.

🔎 A	dministration		🖴 Hosts			S Eve	nt Sources	🛡 Health	& Wellness	; #	System	📑 Securi	ty				P	?	RSA S	ecurity Analy	ytics
🚠 Ch	ange Service	RE	SA - Reportir	ng Engi	ne C	Config 😔															
Gen	eral Source	ces	Output Ac	tions	Manage	Logos															
+ ⊙	- 🗷 😵	🗹 S	et default																		
	Name							Address						Port	Туре					Thread cou	unt
	B Data Sources																				
	Analyst - Conce	entrato	or					101 12-1						1000	Concentrator					5	
	DPO - Concent	rator						111 12-1						8665	Concentrator					5	
	Log Decoder - I	Log De	coder					111 121						-	Log Decoder					5	
	Decoder - Deco	oder						112-12-1						0000	Decoder					5	
	Broker - Broker	r						111 121						1000	Broker					5	
	Concentrator -	Conce	entrator					111-12-12-1						-	Concentrator					5	
■ Ware	house Data Sou	rces																			
	warehouse							111-00-0						1000	Warehouse					5	
👤 adr	nin @English	(Unite	ed States) G	MT+00:0	00												Se	end Us	Feedback	10.6.0.0.220	018-4

Note: Si vous ajoutez plusieurs services IPDB Extractor au même service Reporting Engine, vérifiez que l'option Utiliser le filtre Sqlite est la même pour tous les services. Si une initialisation du filtre Sqlite échoue pour l'un des services IPDB Extractor, vous devez désactiver l'option Utiliser le filtre Sqlite pour tous les services IPDB Extractor associés au service Reporting Engine.

© 2010 - 2016 RSA, The Security Division of EMC. Last Modified: August 10 2016, 9:33AM

Étape 3. (Facultatif) Mapper plusieurs emplacements de stockage

Cette rubrique décrit comment mapper plusieurs emplacements de stockage pour IPDB Extractor. L'onglet Général d'IPDB Extractor dans la vue Configuration des services permet de mapper l'emplacement de stockage sur le point de montage.

Procédure

Pour mapper plusieurs emplacements de stockage pour l'IPDB :

- 1. Dans le menu Security Analytics, sélectionnez Administration > Services.
- 2. Dans la vue Services, sélectionnez le service IPDB Extractor.
- Dans la colonne Actions, cliquez sur ^{See} > Vue > Config. La vue Configuration des services s'ouvre sur l'onglet Général du service IPDB Extractor.
- 4. Dans le volet **Configuration d'IPDB Extractor**, champ **Mappage de l'emplacement de stockage sur le point de montage**, saisissez l'emplacement de stockage d'IPDB.
- 5. Cliquez sur Appliquer.

Étape 4. Réinitialiser le mot de passe utilisateur de nwipdbadptr postgreSQL

Cette rubrique décrit les étapes permettant de réinitialiser le mot de passe de l'utilisateur nwipdbadptr postgreSQL (composant du service IPDB Extractor). IPDB Adaptor est un composant du service IPDB Extractor. **nwipdbadptr** est l'utilisateur de la base de données postgreSQL dont IPDB Adaptor doit obtenir les métadonnées d'événement pour le module {REP}}.

Pour configurer IPDB Adaptor, exécutez les deux tâches suivantes :

- · Réinitialisez le mot de passe par défaut de l'utilisateur nwipdbadptr.
- · Ajoutez IPDB Adaptor au Reporting Engine.

Procédure

Pour réinitialiser un mot de passe pour l'utilisateur nwipdbadptr :

1. Connectez-vous à Reporting Engine Appliance à l'aide des informations d'identification d'un superutilisateur.

```
2. Exécutez les commandes suivantes :
   su - postgres
   psql -d nwtmpdb
   ALTER ROLE nwipdbadptr WITH PASSWORD 'password';
    \q
   Exit
```

```
service postgresql restart
```

3. Remplacez le mot de passe sous **Configuration de la base de données IPDB** sous l'onglet Général du Reporting Engine par le mot de passe que vous avez réinitialisé à l'étape 2.

Administration Administration	Health & Wellness	😂 System	Security	Ō 👎	?	RSA Security Analytics
👬 Change Service 🧰 SA - Reporting Engine Config \odot						
General Sources Output Actions Manage Logos						
All the data source parameters are automatically populated and RSA recommends they r	not be changed as they are optin	mal configurations. (Optionally, if you want to change any parameter, select any of the values and click Apply.			
System Configuration						+
Logging Configuration						+
IPDB Database Configuration						-
Name			Config Value			
Username			nwipdbadptr			
Warehouse Analytics Output Configuration						+
Warehouse Analytics Model Configuration						+
Warehouse Kerberos Configuration						+
						Apply
👤 admin 🌐 English (United States) GMT+00:00					Send Us F	eedback 10.6.0.0.22018-4

Note: Vous utilisez ce mot de passe lorsque vous ajoutez une source de données à un Reporting Engine.

Étape 5. Configurer les sources de données IPDB Extractor dans le Reporting Engine

Cette rubrique décrit la configuration des sources de données IPDB Extractor pour le Reporting Engine. Cette rubrique vous indique comment :

- · Ajouter une source de données au Reporting Engine
- · Définir une source de données comme source par défaut

Ajouter une source de données au Reporting Engine

Pour associer une source de données au Reporting Engine :

- 1. Dans le menu Security Analytics, sélectionnez Tableau de bord Administration > Services.
- 2. Dans la grille Services, sélectionnez un service IPDB Extractor .
- Cliquez sur ^{Son} > Vue > Config. La vue Configuration des services s'ouvre sur l'onglet Général du service IPDB Extractor.
- 4. Sous l'onglet Configuration, effectuez les tâches suivantes :
 - 1. Cliquez sur + · · · > Services disponibles.
 - 2. Dans la boîte de dialogue Services disponibles, effectuez l'opération suivante :
 - a. Sélectionnez le service que vous souhaitez ajouter comme source de données au Reporting Engine, puis cliquez sur OK.

Security Analytics l'ajoute comme une source de données à la disposition des alertes par rapport à ce Reporting Engine.

se i	dministration ⊗ ← Hosts	🛡 Health & Wellness 🛛 🚟 System	🔒 Security			Ō	P	?	RSA Security Analytics
🙏 CI	ange Service 醒 SA - Reporting Engine Config 👳								
Ger	eral Sources Output Actions Manage Logos								
+ .	- 🗹 💲 🗹 Set default								
	Name	Address		Port	Туре				Thread count
	Data Sources								
	SA - IPDB Extractor	10.00		100121	IPDB Extractor				
■ NW	DB Data Sources								
	Analyst - Concentrator	11.1 12.7		0.007	Concentrator				5
	DPO - Concentrator	0.00		10000	Concentrator				5
	Log Decoder - Log Decoder	11.10.10.10.10		0000	Log Decoder				5
	Decoder - Decoder	11-1 12-12		-8693	Decoder				5
	Broker - Broker	01.0 12.00		0.000	Broker				5
	Concentrator - Concentrator	11-1 - 12-2		1000	Concentrator				5
🗉 War	ehouse Data Sources								
	warehouse	0110-020		1000	Warehouse				5
9 ad	nin						S	end Us Fe	eedback 10.6.0.0.22018-4

Définir une source de données comme source par défaut

Pour définir une source de données comme source par défaut pour créer des alertes :

- 1. Dans le menu Security Analytics, sélectionnez Tableau de bord > Administration > Services.
- 2. Dans la grille Services, sélectionnez un service Reporting Engine.
- Cliquez sur ^{\$\$} ^{\$\$} > Vue > Config. La vue Configuration des services du Reporting Engine s'affiche.
- 4. Sélectionnez l'onglet **Sources**. La vue Configuration des services s'ouvre sur l'onglet Sources du Reporting Engine.
- 5. Sélectionnez la source à définir par défaut (par exemple, IPDB Extractor).
- Cochez la case Définir la valeur par défaut. Security Analytics est défini sur cette source de données par défaut lorsque vous créez des alertes par rapport à ce Reporting Engine.

Étape 6. Créer une liste de sources d'événements IPDB pour les rapports

Cette rubrique décrit comment vous pouvez créer une liste de sources d'événements à partir de la source de données IPDB et utiliser cette liste dans un rapport. Dans le cadre de la configuration du service IPDB Extractor, vous devez créer des listes de sources d'événements pour la source de données IPDB. Après avoir créé une telle liste, utilisez-la dans vos rapports pour extraire les données de l'IPDB uniquement pour ces sources d'événements.

Procédure

Pour créer un groupe de sources d'événements pour une source de données IPDB :

- Dans le menu Security Analytics, cliquez sur Tableau de bord > Rapports. L'onglet Gérer s'affiche.
- 2. Créez un groupe de règles pour les listes de sources d'événements (par exemple, Aix_listepériph).
- Créez une règle (par exemple, AIX LISTEPERIPH) pour obtenir les adresses des sources d'événements desquelles vous souhaitez que la source de données IPDB extraie des données. L'exemple suivant illustre une règle qui crée une adresse de liste de sources d'événements avec les éléments suivants : domaine NIC, site ESIPDB, nœud ESIPDB-ES et type de service AIX.

Note: Vous devez utiliser le format domaine:site:noeud:type-périphérique pour spécifier le format de la source d'événements. Par exemple, NIC:ESIPDB:ESIPDB-ES:AIX. La spécification de la source d'événements et la clause WHERE doivent être identiques.

Build Rule	
Rule Type	IPDB
Name	AIX_DEVICELIST
Select	device.host
Event Source	NIC:ESIPDB:ESIPDB-ES:AIX:*
	Enter the event source
	•
Where	domain = 'NIC' AND site = 'ESIPDB' AND node = 'ESIPDB-ES' AND device.type = "AIX"
Group By	
Order By	Column Name Sort By
	Enter the column name Ascending
Limit	20 0
Use	Save Reset Test Rule

- 4. Ajouter une liste. Il se peut que vous ne puissiez ajouter aucune valeur à la liste. Par exemple : LISTE DES PERIPHERIQUES.
- 5. Créez un rapport et ajoutez la règle avec la règle AIX LISTEPERIPHERIQUES.

6. Planifiez un rapport dont la sortie s'effectue sous forme de liste, comme illustré ci-dessous.

Schedule F	Report
Enable	
Report Name	AIX DEVICE LIST
Schedule Name	AIXDEVICELIST
Run	Daily 🖌 At 00:00 🗸
On	Past 🗸 I Hours V 🗆 Use relative time calculation
Variables	No variables defined
Output Action Output	15
+ - 6	Z
List Name	
\$[/Per Use	r Report/List of Services]
•	•
- 🕑 Logo	
Previous	Schedule Reset 🌣 Configure

Lorsque vous exécutez le rapport (règle), Security Analytics renseigne la sortie dans la liste.

7. Lorsque le rapport est généré, Security Analytics renseigne la liste. Par exemple :

Manage	View [LIST] List of Services 🛛
Build Lis	st
Name	List of Services
Description	
List Values	Insert Values
	Value
	0.0.0.206
	66.66.66.5
	0.0.208
	0.0.203
	0.0.0.213
	0.0.0.209
	0.0.0.150
	Enter value 🔻
	↓
	Quotes will be inserted for all the values
Save	Reset

Utiliser une liste de sources d'événements pour la source de données IPDB dans un rapport

Pour utiliser une liste de sources d'événements pour la source de données IPDB dans un rapport :

- 1. Créez une règle. Spécifiez la liste Liste des services comme source d'événements.
- Créez un rapport avec cette règle. Lorsque vous générez le rapport, tous les services répertoriés dans la liste servent à sa génération.

Étape 7. Déployer du contenu Live vers IPDB Extractor

Cette rubrique décrit comment télécharger du contenu depuis NetWitness Live vers IPDB Extractor. Utilisez Security Analytics Live pour déployer le dernier contenu sur le service IPDB Extractor. Le téléchargement stocke le contenu du service IPDB Extractor dans le répertoire **/etc/netwitness/ng/envision/etc**. Le contenu se compose des éléments suivants :

- · Le service xml pour tous les types de service pris en charge par RSA.
- Le fichier ipaddr.tab.
- Le fichier ecat.ini.
- Le fichier table-map.xml : mappage de contenu Envision vers des métadonnées NetWitness.

Procédure

Pour télécharger du contenu sur le service IPDB Extractor :

- 1. Dans le menu Security Analytics, cliquez sur **Tableau de' bord > Live > Search** Security Analytics affiche la Vue Live Search.
- Dans la liste déroulante Types de ressourcess, sélectionnez RSA Log Device et cliquez sur Rechercher. Security Analytics affiche un lien de ContenuNWFL (NetWitness for Logs) dans les Ressources correspondantes. Vous pouvez saisir le mot-clé à rechercher pour ce contenu.
- 3. Double-cliquez sur le fichier de contenu Envision (Contenu NWFL) ou sélectionnez le fichier.
- 4. Cliquez sur Déployer.
- 5. Sélectionnez la ressource (Fichier de contenu Envision) et cliquez sur Suivant.
- 6. Sélectionnez le service IPDB Extractor dans lequel vous souhaitez déployer le contenu et cliquez sur Suivant.
- 7. Vérifiez les informations et cliquez sur Déployer.
- 8. Accédez au répertoire /etc/netwitness/ng/envision/etc dans l'appliance Broker qui exécute le service IPDB Extractor pour vérifier que Live a bien téléchargé le contenu.
- 9. Redémarrez le service IPDB Extractor pour déployer le contenu.

Étape 8. (Facultatif) Configurer le déploiement multisite

Cette rubrique décrit comment mettre à jour le paramètre Transport Vives URI pour l'IPDB déployée dans un environnement multisite. Pour un environnement multisite, vous devez mettre à jour le paramètre pour la base de données IPDB déployée.

Pour un déploiement IPDB multisite uniquement, mettez à jour le paramètre Transport Vives URI.

- 1. Dans le menu Security Analytics, sélectionnez Administration > Services.
- 2. Dans la grille Services, sélectionnez le service IPDB Extractor exécuté sur le site distant.
- 3. Dans la colonne Actions, cliquez sur 🔅 🗹 > Vue > Configuration.
- 4. Sous l'onglet IPDB Extractor Général, dans Paramètres Extractor, cliquez sur la colonne Valeur de configuration du paramètre URI de transport.
- 5. Remplacez la valeur par défaut vives://127.0.0.1:50009 par l'adresse IP du service IPDB Extractor qui réside sur le site distant (soit vives://<remote-site-ip-address>:50009) et cliquez sur Appliquer.
- 6. Redémarrez le service IPDB Extractor.

.

Références

Cette rubrique rassemble des références qui décrivent l'interface utilisateur du service IPDB Extractor dans Security Analytics. Utilisez cette section si vous recherchez la description des attributions de droits et définitions des fonctions de l'interface utilisateur.

Vue Configuration des services - Configuration d'IPDB Extractor

Cette rubrique décrit les paramètres de configuration de l'onglet Général pour le service IPDB Extractor. L'onglet **Général** de la vue Configuration des services correspondant à un IPDB Extractor permet de gérer la configuration du service, de paramétrer l'extraction de données et de sélectionner les parsers appliqués aux données récupérées.

- 1. Dans le menu Security Analytics, sélectionnez Administration > Services.
- 2. Dans la vue Services, sélectionnez le service IPDB Extractor.
- Dans la colonne Actions, cliquez sur ^{Son} > Vue > Configuration. La vue Configuration des services s'ouvre sur l'onglet Général du service IPDB Extractor.

Administration Hosts	🚡 Event Sources 💎 Health & Wellness	📰 System	🖶 Security	💿 🗭 ? 🔀 Security Analytics
🚓 Change Service SA - IPDB Extractor Config \odot				
General Appliance Service Configuration				
System Configuration			Parsers Configuration	
Name	Config Value		Name	Config Value
Compression	0		A B ALERTS	Enabled
Port	50025		FeedParser	Enabled
SSL FIPS Mode			GeoIP	Disabled
SSL Port	56025		⊞ Log Parser	Enabled
Caral Hardware Incoment	1000		■ LogTokens	Enabled
IPDB Extractor Configuration			NETWORK	Enabled
Name	Config Value			
Extractor Settings			A	
BufferSize (MB)	1 MB		Service Parsers Configuration	
Mapping of storage location to mount point	e:\nic\lsnode~storage1,d:\testsl~storage2		Name	Config Value
Num Of Buffers	4		accurey	
Num Of Buffers in the pool	500		actioner	
Num Of requests in the pool	500		actividentity	
Num Of Threads in threadpool	50		aforerloudlink	E Contraction of the second se
Parse Threads	0		airdefence	
Transport URI	vives://127.0.0.1:50009		almanat	
Transport Worker Threads	50		airtiatme	
Use L1 Bloom			airegrane	
Heal D Plaam	2			•
		A	Apply	
👤 admin 🌐 English (United States)				Send Us Feedback

Caractéristiques

Configuration système

La section Configuration système gère le paramétrage d'un service. Lorsqu'un service est ajouté pour la première fois, les valeurs par défaut s'appliquent. Vous pouvez modifier ces valeurs pour optimiser les performances.

La Configuration système dispose des paramètres suivants.

Paramètre	Description
Compression	Le nombre minimum d'octets devant être transmis par réponse avant la compression. Le paramètre 0 désactive la compression. La valeur par défaut est 0 . La modification d'une valeur prend effet immédiatement pour toutes les connexions suivantes.
Port	 Port d'écoute du service. Les ports par défaut sont les suivants : 50001 pour les Log Collectors 50002 pour les Log Decoders 50003 pour les Brokers 50004 pour les Decoders 50005 pour les Concentrators 50007 pour les autres services Le port par défaut du service IPDB Extractor est 50025.
SSL	En cas d'activation (on), la sécurité de la transmission des données est gérée par le chiffrement des informations et l'authentification avec les certificats SSL. La valeur par défaut est off .
Intervalle de mise à jour des statistiques	Nombre de millisecondes entre les mises à jour statistiques sur le système. Les petites valeurs engendrent des mises à jour plus fréquentes et peuvent ralentir d'autres processus. La valeur par défaut est 1000 . La modification de la valeur prend effet immédiatement.
Threads	Nombre de threads dans le pool de threads permettant de gérer les requêtes entrantes. Le paramètre 0 laisse le système décider. La valeur par défaut est 15. Les modifications prendront effet au redémarrage du service.

Configuration d'IPDB Extractor

Les paramètres du panneau **Configuration d'IPDB Extractor** permettent de gérer le paramétrage du service IPDB Extractor. Lorsque vous ajoutez un service IPDB Extractor, les valeurs par défaut s'appliquent. Les valeurs par défaut proposées par RSA s'adaptent à la plupart des environnements et il est recommandé de ne pas modifier ces valeurs car cela pourrait avoir un impact négatif sur les performances.

Les paramètres qui définissent et optimisent l'extraction de données englobent les suivants :

- · Paramètres d'Extractor
- · Paramètres des requêtes

Paramètres d'Extractor

Le tableau suivant décrit les paramètres d'Extractor.

Nom	Valeur de configuration		
Taille du tampon (Mo)	Taille du tampon d'extraction des données (en Mo). La valeur par défaut est 1 . Il faut redémarrer le service IPDB Extractor après avoir apporté des modifications pour que cette valeur soit prise en compte.		
Mappage de l'emplacement de stockage sur le point de montage	Réservé à un IPDB avec plusieurs emplacements de stockage. Si un IPDB compte plusieurs emplacements de stockage, il convient de les mapper sur les points de montage correspondants pour que le service IPDB Extractor puisse extraire des données. Par exemple : \\1.1.1.1\vol1\nic\lsnode\LSIPDB-LC1~storage1,\\1.1.1.1\vol2\nic\lsnode\LSIPDB-LC1~storage2 II faut redémarrer le service IPDB Extractor après avoir apporté des modifications pour que cette valeur soit prise en compte.		
Nbre de tampons	Nombre de tampons d'extraction de données. Les valeurs valides sont comprises entre 1 et 4. La valeur par défaut est 4 tampons. Il faut redémarrer le service IPDB Extractor après avoir apporté des modifications pour que cette valeur soit prise en compte.		
Nbre de tampons dans le pool	Nombre d'éléments dans le pool de tampons disponibles. Les valeurs valides sont comprises entre 500 et 700. La valeur par défaut est 500 tampons. Il faut redémarrer le service IPDB Extractor après avoir apporté des modifications pour que cette valeur soit prise en compte.		
Nbre de demandes dans le pool	Nombre d'éléments dans le pool de demandes. Les valeurs valides sont comprises entre 500 et 6000. La valeur par défaut est 500 demandes. Il faut redémarrer le service IPDB Extractor après avoir apporté des modifications pour que cette valeur soit prise en compte.		
Nbre de threads dans le pool	Nombre d'éléments dans le pool de threads. Les valeurs valides sont comprises entre 50 et 200. La valeur par défaut est 50 threads. Il faut redémarrer le service IPDB Extractor après avoir apporté des modifications pour que cette valeur soit prise en compte.		
Threads d'analyse	Nombre de threads utilisés lors de l'analyse des sessions. Pour être valide, la valeur doit être un nombre. La valeur par défaut est 0 thread d'analyse. Si vous définissez la valeur 0 , le serveur détermine le nombre de threads en fonction du volume de données. Il faut redémarrer le service IPDB Extractor après avoir apporté des modifications pour que cette valeur soit prise en compte.		
URI de transport	Adresse URI (Uniform Resource Identifier) de transport utilisée pour assurer la communication entre le client IPDB et le serveur IPDB Extractor. La valeur par défaut est vives://127.0.0.1:50009 . Il faut redémarrer le service IPDB Extractor après avoir apporté des modifications pour que cette valeur soit prise en compte.		
Threads de travail de transport	Nombre de threads de travail permettant de traiter les demandes de transport du client. Il faut redémarrer le service IPDB Extractor après avoir apporté des modifications pour que cette valeur soit prise en compte.		
Utiliser Bloom L1	Utiliser Bloom L1 pour accélérer l'extraction de données à partir d'IPDB. Si l'index du filtre de Bloom est activé pour une méta et si les logs d'événements contiennent la métavaleur demandée dans la requête du rapport, alors les fichiers de données correspondants sont lus. Sinon, ils sont ignorés. Cette option est activée par défaut (Utiliser Bloom L1).		

Nom	Valeur de configuration		
	Note: Le package de contenu datant d'août 2013 (ou version ultérieure) doit être installé pour pouvoir spécifier les options Utiliser Bloom L1 et Utiliser Bloom L2.		
Utiliser Bloom L2	Utiliser Bloom L2 pour accélérer l'extraction de données à partir d'IPDB. Si l'index du filtre de Bloom est activé pour une méta et si les logs d'événements contiennent la métavaleur demandée dans la requête du rapport, alors les fichiers de données correspondants sont lus. Sinon, ils sont ignorés. Cette option est activée par défaut (Utiliser Bloom L2).		
Utiliser l'indexation L2	Utiliser l'indexation L2 lors de l'extraction de données à partir d'IPDB. Cette option est activée par défaut (Utiliser l'indexation L2).		
Utiliser le filtre Sqlite	Appliquer le filtre Sqlite aux événements. Cette option est activée par défaut (Utiliser le filtre Sqlite).		

Paramètres des requêtes

Le tableau suivant décrit les	paramètres des requêtes	IPDB Extractor.
-------------------------------	-------------------------	-----------------

Nom	Valeur de configuration		
Limite d'inactivité de requête	Délai (en secondes) que doit respecter Security Analytics entre deux extractions de données avant de fermer une requête. La valeur par défaut est 3600 .		
Intervalle d'état de requête	Délai (en secondes) que doit respecter Security Analytics entre deux mises à jour des statistiques de requête. Pour être valide, la valeur doit être comprise entre 1 et 200 . La valeur par défaut est 10 . Security Analytics reprend la valeur de l'option Intervalle de mise à jour des statistiques figurant dans la vue Profil > panneau Préférences > onglet Général si le paramètre Intervalle d'état de requête est inférieur à Intervalle de mise à jour des statistiques .		

Configuration des analyseurs

Le panneau Configuration des analyseurs permet de sélectionner les parsers à utiliser sur le service IPDB Extractor.

Le tableau décrit les fonctions de la section Configuration des analyseurs.

Fonction	Description		
Nom	Nom des parsers disponibles dans IPDB Extractor. Le signe plus indique que les métadonnées générées par l'analyseur sont configurables. Lorsque vous cliquez sur le signe plus, les métadonnées que l'analyseur peut créer s'affichent.		
Valeur de configuration	Une case à cocher permet d'activer ou de désactiver l'analyseur ou les métadonnées. Lorsque cette case est cochée, le service IPDB Extractor filtre le trafic à l'aide de l'analyseur. Dans le cas contraire, l'IPDB Extractor n'utilise pas		

Fonction	Description
	l'analyseur. Si les métadonnées générées sont configurables, une case à cocher détermine celles que l'analyseur doit créer.

Configuration des analyseurs de servicess

Le panneau Configuration des analyseurs de services permet de sélectionner les parsers à utiliser sur le service IPDB Extractor.

Dépannage d'IPDB Extractor

Cette rubrique fournit des informations sur les problèmes que vous pouvez éventuellement rencontrer lors de l'utilisation d'IPDB Extractor.

Problèmes possibles

Problème	Causes possibles	Solutions	
Dans un environnement Linux, lorsqu'IPDB Extractor est installé sur une machine virtuelle, le chargement échoue et vous ne voyez pas la métadonnée qui définit une règle IPDB. <dyou <br="" at="" can="" in="" log="">look="" the="">/var/log/messages file où le message suivant s'affiche : Impossible d'allouer de la mémoire dans le constructeur MemPages. </dyou>	Le service IPDB Extractor ne peut peut-être pas allouer suffisamment de mémoire au parser.	 Pour modifier les paramètres du pool : Dans le menu Security Analytics, sélectionnez Administration Services > IPDB Extractor > Vue > Explorer. Remplacez la valeur de /ipdbextractor/config/ pool. packet.pages par une valeur inférieure à la valeur configurée. Remplacez la valeur de /ipdbextractor/config/ pool.session.pages par une valeur inférieure à la valeur configurée. Redémarrez le service IPDB Extractor. 	

Valeurs recommandées

Taille de la mémoire de la machine virtuelle	Pages de paquets	Pages de sessions
>=24 Go	50000	25000
>=17 Go	30000	10000
>=9 Go	20000	7000
>=4 Go	10000	5000

Note: Les valeurs ci-dessus ne sont que des suggestions. Si le problème persiste même après avoir modifié les valeurs de configuration, pensez à réduire encore les valeurs.