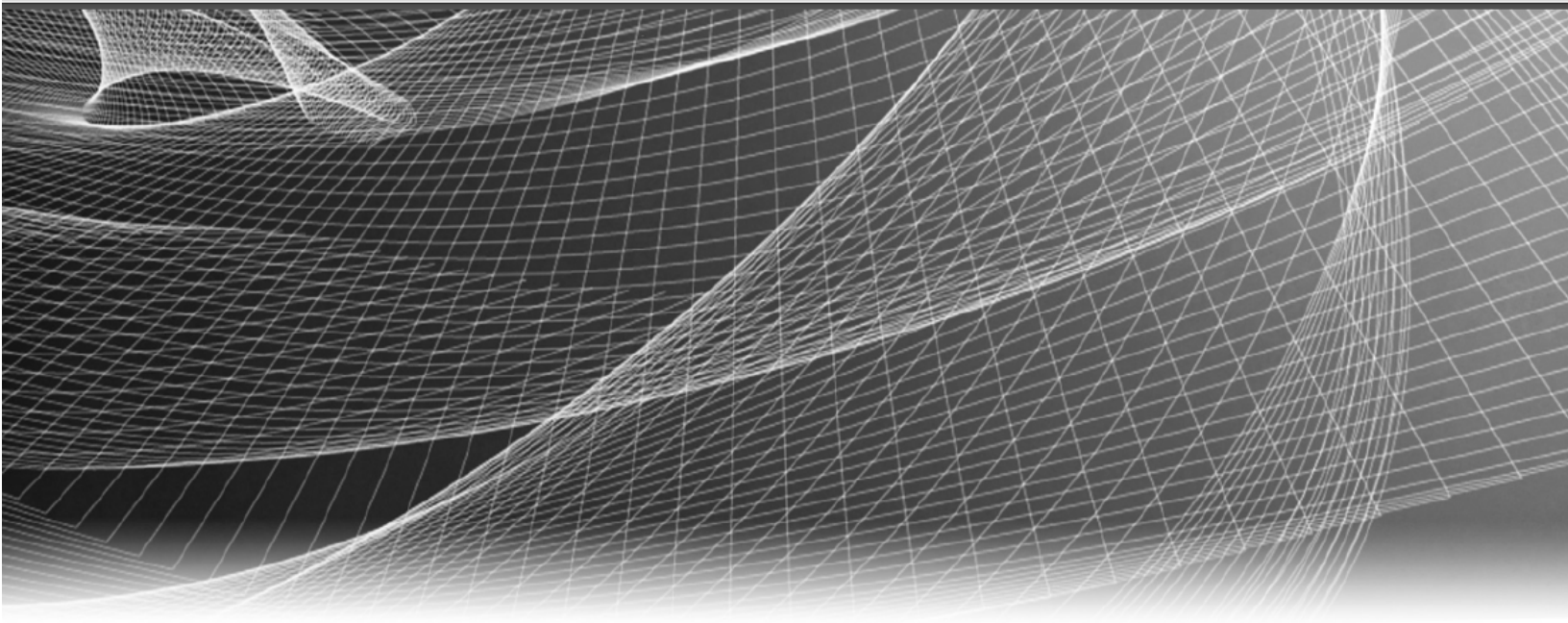


RSA Security Analytics

Guide de configuration de Workbench

pour la version 10.6

RSA EMC²

Copyright © 2016 EMC Corporation. Tous droits réservés.

Marques commerciales

RSA, le logo RSA et EMC sont des marques commerciales ou des marques déposées d'EMC Corporation aux États-Unis et/ou dans d'autres pays. Toutes les autres marques citées dans le présent document sont la propriété de leurs détenteurs respectifs. Pour obtenir la liste des marques commerciales d'EMC, consultez france.emc.com/legal/emc-corporation-trademarks.htm.

Contrat de licence

Ce logiciel et la documentation qui l'accompagne sont la propriété d'EMC et considérés comme confidentiels. Délivrés sous licence, ils ne peuvent être utilisés et copiés que conformément aux modalités de ladite licence et moyennant l'inclusion de la note de copyright ci-dessous. Ce logiciel et sa documentation, y compris toute copie éventuelle, ne peuvent pas être remis ou mis de quelque façon que ce soit à la disposition d'un tiers.

Aucun droit ou titre de propriété sur le logiciel ou sa documentation ni aucun droit de propriété intellectuelle ne vous est cédé par la présente. Toute utilisation ou reproduction non autorisée de ce logiciel et de sa documentation peut faire l'objet de poursuites civiles et/ou pénales. Ce logiciel est modifiable sans préavis et ne doit nullement être interprété comme un engagement de la part d'EMC.

Licences tierces

Ce produit peut inclure des logiciels développés par d'autres entreprises que RSA. Le texte des accords de licence applicables aux logiciels tiers de ce produit peut être consulté dans le fichier thirdpartylicenses.pdf.

Remarque sur les technologies de chiffrement

Ce produit peut intégrer une technologie de chiffrement. Étant donné que de nombreux pays interdisent ou limitent l'utilisation, l'importation ou l'exportation des technologies de chiffrement, il convient de respecter les réglementations en vigueur lors de l'utilisation, de l'importation ou de l'exportation de ce produit.

Distribution

L'utilisation, la copie et la diffusion de tout logiciel EMC décrit dans cette publication nécessitent une licence logicielle en cours de validité. EMC estime que les informations figurant dans ce document sont exactes à la date de publication. Ces informations sont modifiables sans préavis.

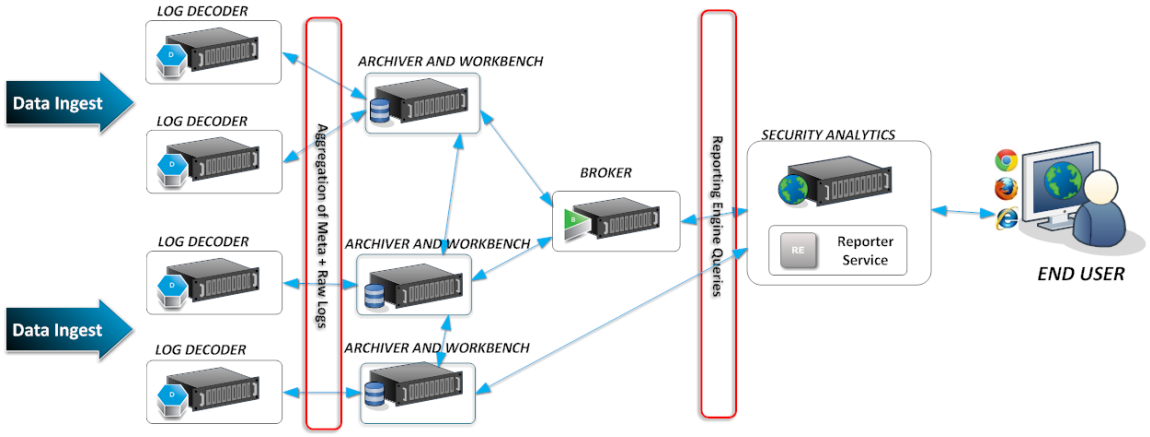
LES INFORMATIONS CONTENUES DANS CETTE PUBLICATION SONT FOURNIES « EN L'ÉTAT ». EMC CORPORATION NE FOURNIT AUCUNE DÉCLARATION OU GARANTIE D'AUCUNE SORTE CONCERNANT LES INFORMATIONS CONTENUES DANS CETTE PUBLICATION ET REJETTE PLUS SPÉCIALEMENT TOUTE GARANTIE IMPLICITE DE QUALITÉ COMMERCIALE OU D'ADÉQUATION À UNE UTILISATION PARTICULIÈRE.

Sommaire

Présentation de Workbench

Le service Security Analytics Workbench permet de créer des collections avec des données restaurées, sauvegardées hors ligne à partir d'un Archiver. Une fois les données copiées et enregistrées dans une collection, elles peuvent être analysées depuis les vues Investigation et Reporting.

Le schéma suivant présente l'architecture d'un réseau Security Analytics mettant en œuvre Workbench.



Procédures de configuration de Workbench

Conditions préalables

Avant de configurer le service Workbench, vous devez :

- Ajouter le service Security Analytics Workbench à l'hôte de votre environnement réseau. (Reportez-vous à la section Présentation de Workbench.)
- Installez l'hôte Security Analytics Workbench dans votre environnement réseau. Pour plus d'informations, reportez-vous au Guide de mise en route de l'hôte et des services.

Les étapes pour configurer le service Workbench sont les suivantes :

1. Ajouter le service Workbench comme source de données au Broker
2. Ajouter Workbench comme source de données au Reporting Engine

Lorsque la configuration est terminée, vous pouvez créer et gérer des collections tel que décrit dans Gérer les collections.

Ajouter le service Workbench comme source de données au Broker

Conditions préalables

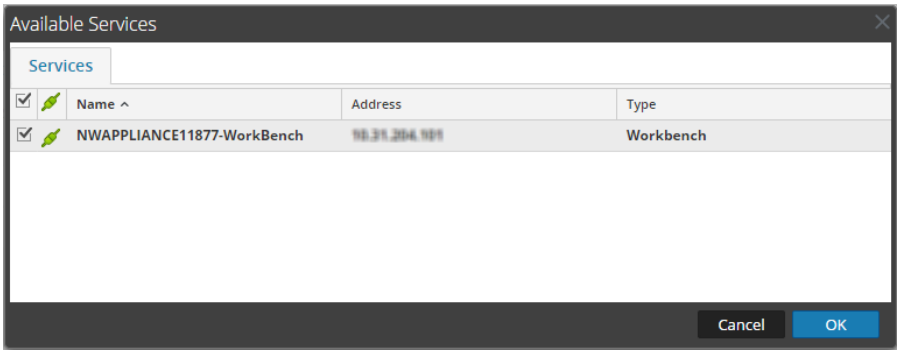
Avant d'ajouter le service Workbench, vous devez :

- Installer le service Workbench sur l'appliance Archiver.
- Ajouter une collection au service Workbench.

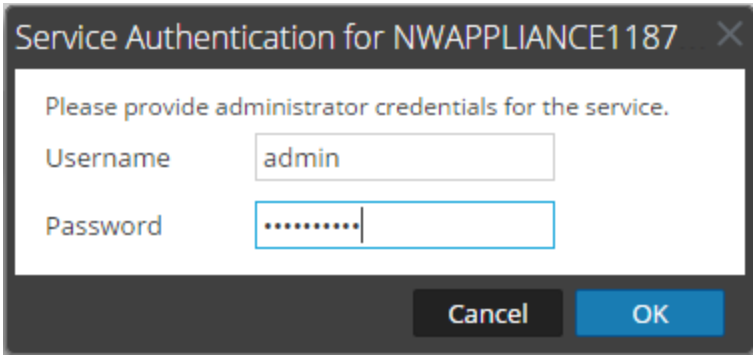
Pour ajouter le service Workbench en tant que source de données sur le Broker :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Sélectionnez un service Broker et cliquez sur  **> Vue > Config.**
   La vue Configuration des services s'affiche.
3. Cliquez sur l'onglet **Général**.

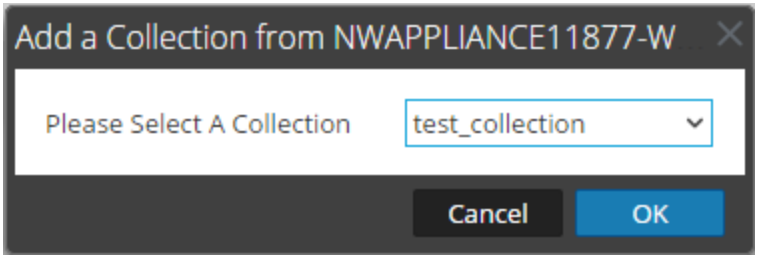
4. Cliquez sur + et sélectionnez **Services disponibles**.
   La boîte de dialogue Services disponibles s'affiche.



5. Sélectionnez le service Workbench et cliquez sur **OK**.
6. Si le service Workbench utilise un modèle de confiance, une boîte de dialogue Authentification de service pour le service sélectionné s'affiche.



7. Saisissez le nom d'utilisateur et le mot de passe administrateur du service.
8. Cliquez sur **OK**.
   La boîte de dialogue Ajouter une collection s'affiche.



9. Sélectionnez une collection dans la liste déroulante et cliquez sur **OK**.
   Le service Workbench est maintenant ajouté en tant que source de données au Broker et répertorié dans la liste de sources NWDATA.

Remarque : Cette procédure doit être réalisée pour chaque collection.

Ajouter Workbench comme source de données au Reporting Engine

Conditions préalables

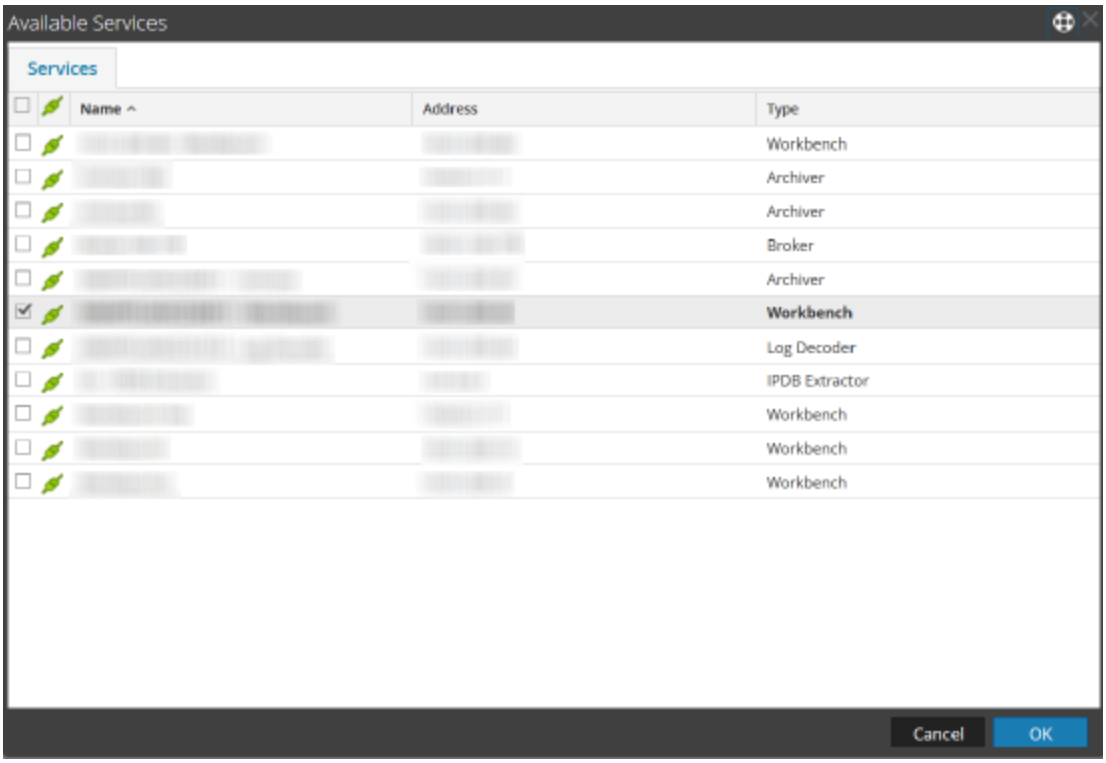
Voici les tâches requises avant d'ajouter le Workbench en tant que source de données à Reporting :

1. Ajouter Reporting Engine en tant que service à votre déploiement Security Analytics.
2. Ajouter le Workbench en tant que service à votre hôte Security Analytics Archiver (le cas échéant).

L'ajout de collections Workbench comme source de données à Reporting Engine dépend d'une connexion approuvée. Si Workbench est établi avec une connexion approuvée, vous devez ajouter manuellement les collections Workbenchcomme source au Reporting Engine.

Pour associer la source de données Workbench au Reporting Engine, procédez comme suit :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Dans la grille Services, sélectionnez un service **Reporting Engine**. Sélectionnez  **Vue > Config**.
3. Accédez à l'onglet **Sources**.
4. Select +
5. Sélectionnez **Services disponibles**. Sélectionnez un service Workbench dans la boîte de dialogue Services disponibles.
6. Cliquez sur **OK**.
   La boîte de dialogue Informations de gestion s'affiche.



8. Saisissez votre nom d'utilisateur et votre mot de passe.
   - Obligatoires si le service Workbench est approuvé.
   - Facultatifs si le service Workbench n'est pas approuvé (ajouté manuellement).
9. Cliquez sur **OK**.
10. Sélectionnez **Collection** dans la boîte de dialogue Ajouter une collection depuis Workbench.
11. Cliquez sur **OK**.

Résultat

Vous pouvez maintenant créer des rapports sur les données collectées par Workbench.

Gérer les collections

Un administrateur peut créer et supprimer des collections Workbench, et afficher les statistiques et logs Workbench. Cette section fournit toutes les procédures et un exemple de procédure de restauration d'une collection pour Reporting et Investigation.

- Monter des répertoires Archiver
- Créer une collection
- Supprimer une collection
- Enquêter sur une collection
- VueWorkbenchCollection Statistics
- Afficher les logs Workbench

Monter des répertoires Archiver

Si les données se trouvent dans un stockage hors ligne ou à froid, vous devez monter les répertoires Archiver afin de restaurer les données à des fins de reporting et de procédure d'enquête :

1. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
2. Sélectionnez un **Archiver** à partir de la grille Services et sélectionnez **> Vue> Explorer**.
   La vue Explorer d'Archiver s'affiche
3. Cliquez avec le bouton droit de la souris sur le nœud **Base de données** dans l'arborescence de gauche puis sélectionnez les propriétés **Base de données** pour les ouvrir dans le volet de droite.
4. Exécutez la commande **manifest** pour une période, du 1er au 10 avril 2015.
   La recherche renvoie tous les fichiers qui ont besoin d'être restaurés pour la requête sélectionnée.

Créer une collection

Les administrateurs peuvent créer des collections de données restaurées à partir d'une sauvegarde ou d'un ensemble existant de données.

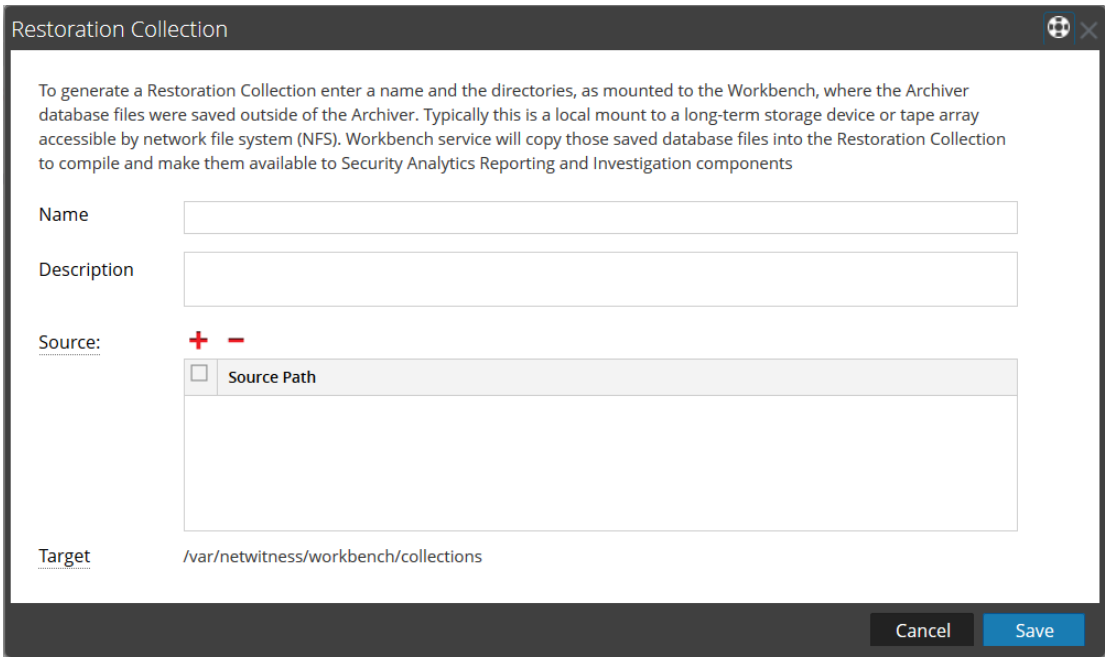
Remarque : Vous pouvez indiquer l'emplacement des fichiers de base de données comme chemin source et la commande de restauration les copie vers Workbench. Vous devez monter ces répertoires dans Archiver (où Workbench est installé) avant de pouvoir créer une collection de restauration.

Pour créer une collection à l'aide de données restaurées à partir des données sauvegardées ou d'un sous-ensemble existant de données :

1. Dans le menu Security Analytics, sélectionnez **Administration > Services.**
2. Dans la vue Services, sélectionnez un **Workbench,** puis cliquez sur **> Vue > Config**.
   La vue Configuration des services s'ouvre sur l'onglet Général.

3. Cliquez sur l'onglet **Collections**.
   La grille Collections s'affiche.

4. Cliquez sur + dans la barre d'outils.
   La boîte de dialogue Collection de restauration s'affiche.



5. Fournissez les informations suivantes :

   - **Nom :** Nom de la collection Workbench que vous souhaitez restaurer.
   - **Source:** Emplacement où les fichiers de base de données Archiver ont été déplacés du stockage à froid.

Remarque : La **cible** est l'emplacement où la collection est créée.

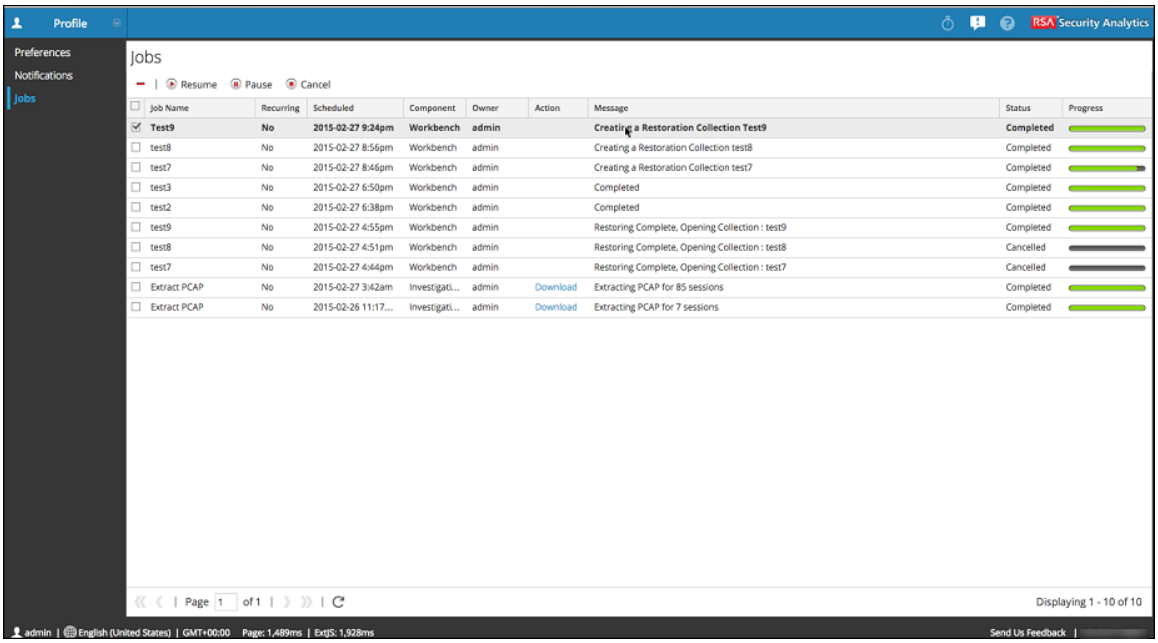
6. Cliquez sur **Enregistrer** pour restaurer la collection.

Remarque : Si le chemin source proposé pour créer la collection de restauration n'existe pas, le message d'erreur suivant apparaît :
`Ce chemin source n'existe pas « /xxx/xxx/ ».`

Si vous ne disposez pas d'assez de stockage pour restaurer la collection, le message d'erreur suivant s'affiche :
`Une erreur est survenue lors de la vérification de l'espace disque. Espace disque insuffisant à l'emplacement « /xxx/xxx ».`

La boîte de dialogue Planifier une tâche s'affiche avec le message suivant :
`Restauration des données dans une nouvelle collection. Consultez la page des tâches pour afficher la progression.`

7. Cliquez sur l'icône **Tâches** dans la barre d'outils Security Analytics pour développer la liste de tâches de la collection de restauration et afficher son état actuel.



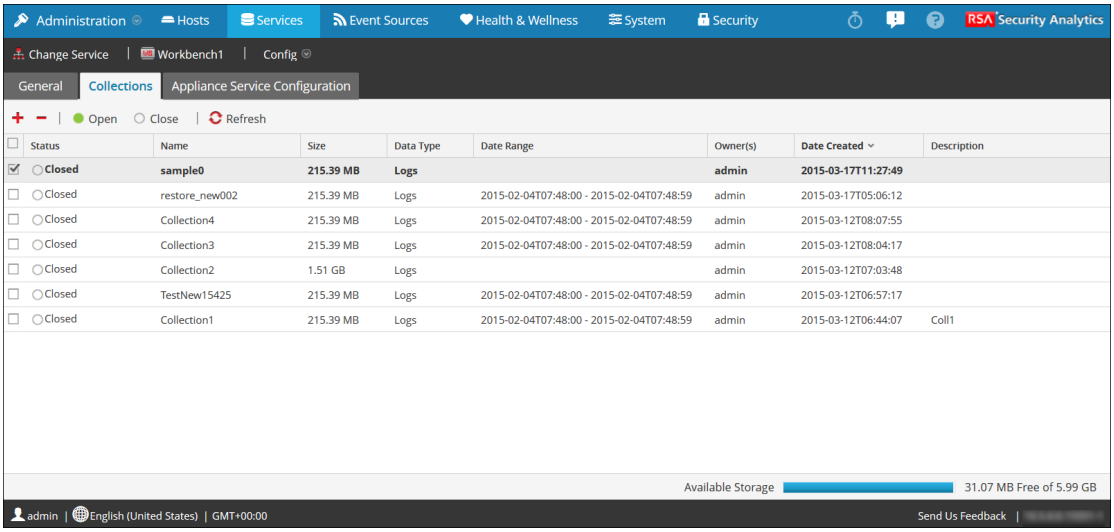
Remarque : La restauration d'une collection supérieure à 550 Go peut prendre plusieurs heures à traiter.

Supprimer une collection

Les administrateurs peuvent supprimer des collections à partir du service Workbench.

Procédez comme suit pour supprimer une collection :

1. Dans le menu Security Analytics, sélectionnez **Administration > Services.**
2. À partir de la vue Services, sélectionnez un **Workbench**, puis cliquez sur > **Vue** > **Config**.
   La vue Configuration des services s'ouvre en affichant l'onglet Général.
3. Sélectionnez l'onglet **Collections**.
   La grille Collections s'affiche.



4. Dans la grille Collections, sélectionnez la collection que vous souhaitez supprimer.
5. Cliquez sur dans la barre d'outils.
   Une boîte de dialogue d'avertissement demande confirmation.
6. Si vous voulez supprimer la collection, cliquez sur **Oui**.
   La collection est supprimée du service Workbench.

Exemple de procédure : Comment restaurer une collection pour reporting et analyse

Les étapes suivantes indiquent comment restaurer des données situées dans un stockage hors ligne ou à froid (données peu actives) dans un but de reporting et d'investigation. Dans l'exemple suivant, les données sont restaurées pour une période de temps allant du 1er avril 2015 au 10 avril 2015.

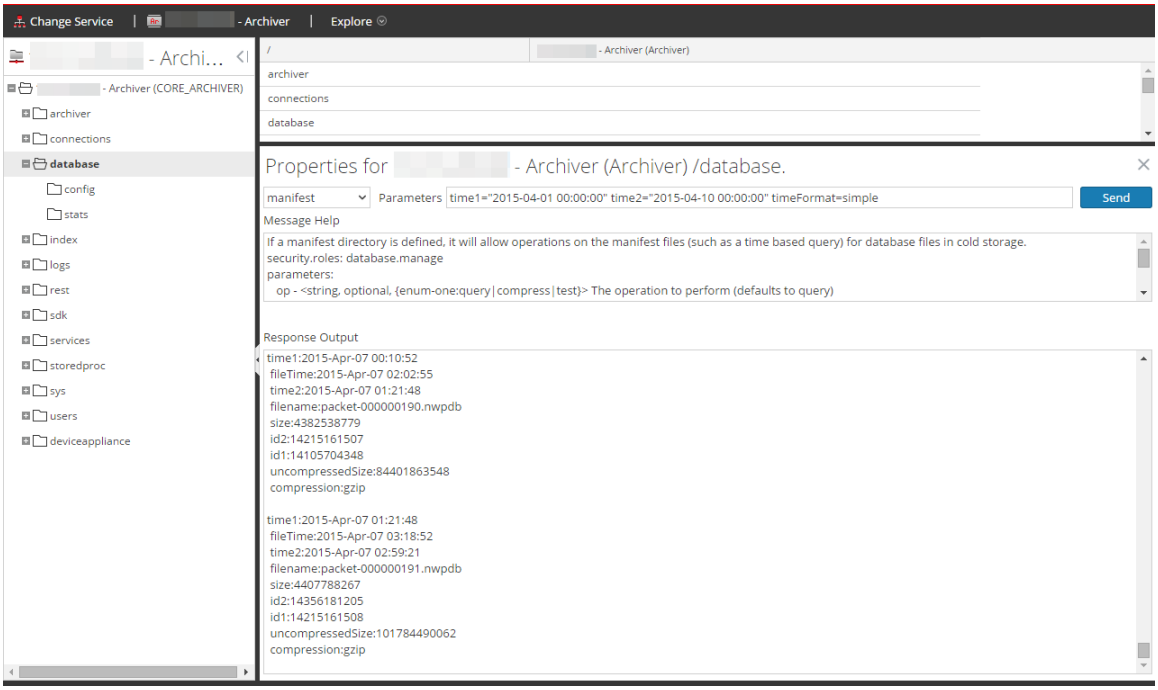
Pour restaurer des données à des fins de reporting et d'analyse :

1. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
2. Sélectionnez **Archiver** dans la grille Services.

3. Naviguez jusqu'à la vue Explorer de l'appliance Archiver en sélectionnant > **Vue** > **Explorer**.
   La vue Explorer d'Archiver s'affiche
4. Cliquez avec le bouton droit de la souris sur le nœud **Base de données** dans l'arborescence de gauche puis sélectionnez les propriétés **Base de données** pour les ouvrir dans le volet de droite.
5. Exécutez la commande **manifest** pour la période sélectionnée : du 1er au 10 avril 2015.
   La recherche renvoie tous les fichiers qui ont besoin d'être restaurés pour la requête sélectionnée.

Exemple de recherche :

```
time1="2015-04-01 00:00:00" time2="2015-04-10 00:00:00"
timeFormat=simple
```



6. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
7. Dans la vue Services, sélectionnez un **Workbench**, puis cliquez sur > **Vue > Config**.
   La vue Configuration des services s'ouvre sur l'onglet Général.
8. Sélectionnez l'onglet **Collections.**
9. Créez une collection de restauration avec le chemin source menant à des fichiers répertoriés dans le résultat de commande de manifeste.

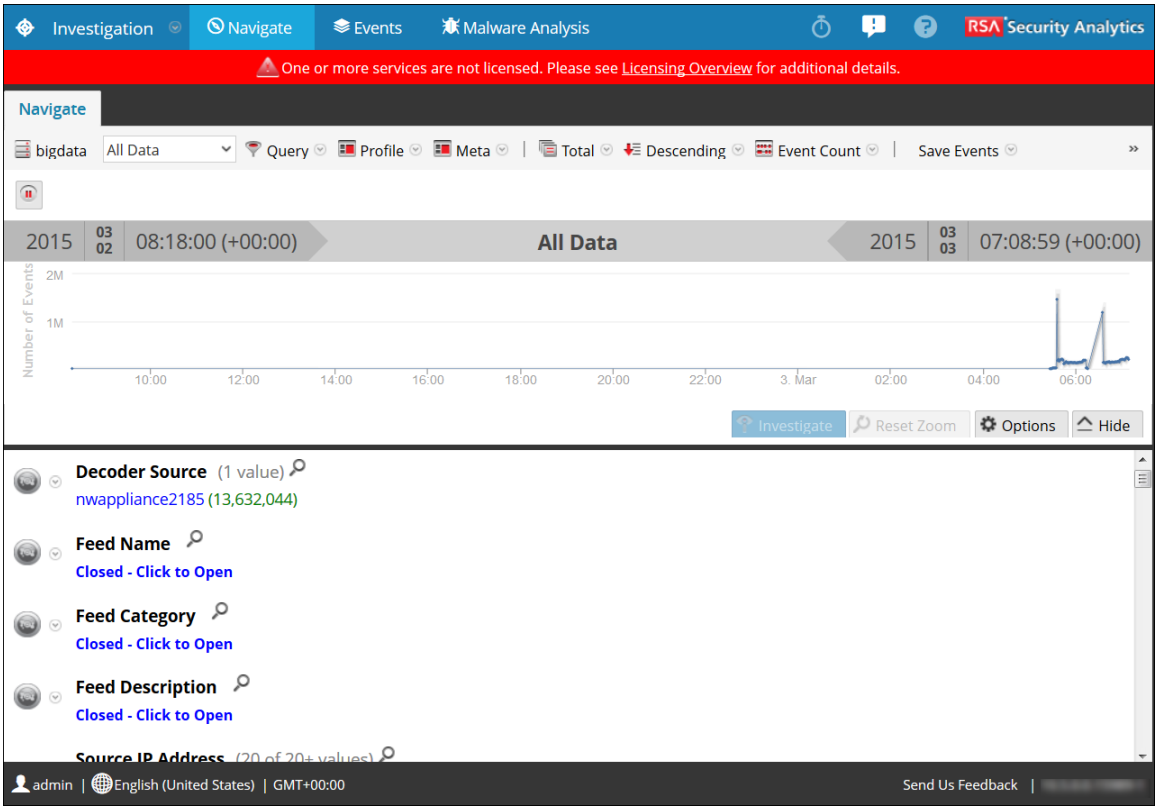
10. Enregistrez la collection.
    Après avoir réussi la création d'une collection, vous pouvez l'utiliser à des fins de reporting et d'analyse.

Enquêter sur une collection

Pour réaliser une procédure d'enquête sur une collection Workbench :

1. Dans le menu **Security Analytics**, sélectionnez **Procédure d'enquête > Naviguer.**
   La boîte de dialogue Examiner s'affiche.
2. Cliquez sur l'onglet **Collections** dans la boîte de dialogue Enquêter.
3. Sélectionnez un service Workbench dans le volet de gauche.
4. Sélectionnez la collection que vous souhaitez analyser dans le panneau de droite.
5. Cliquez sur **Naviguer**.

La vue Naviguer s'affiche et affiche les données relatives à la collection Workbench que vous avez sélectionnée.



Remarque : Pour obtenir des informations détaillées sur l'utilisation de l'Investigation, reportez-vous à la section Investigation et Malware Analsis.

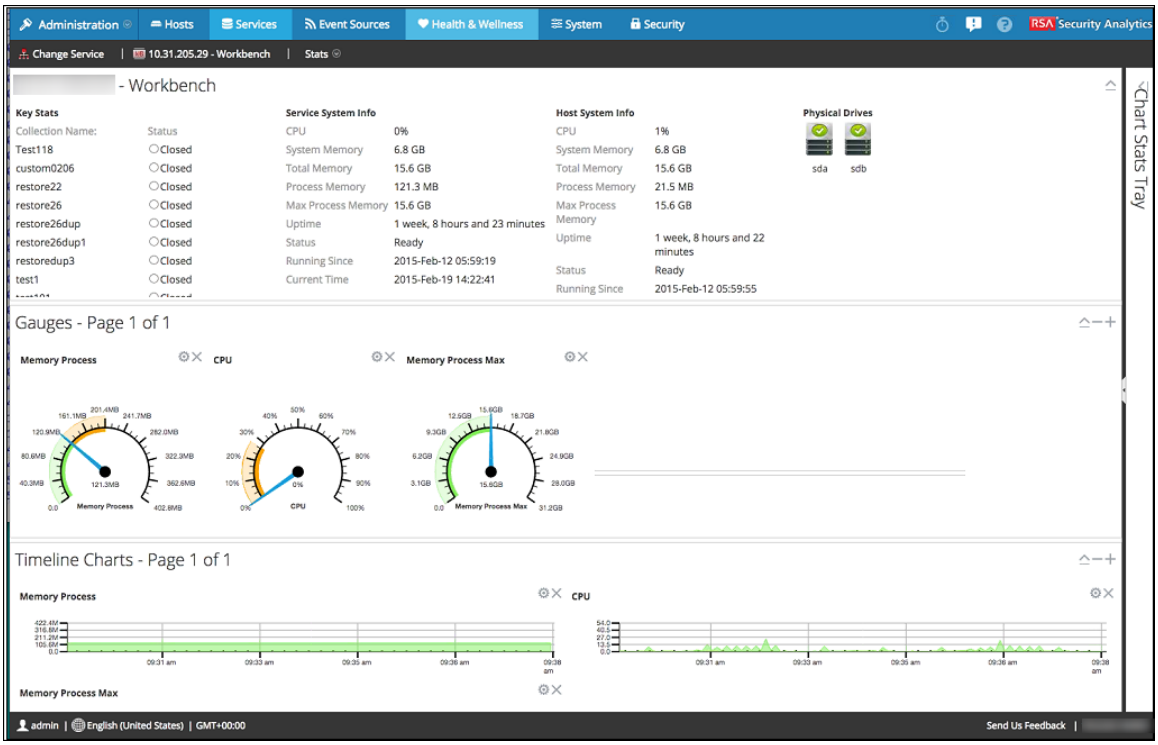
Vue Workbench Collection Statistics

Les mêmes statistiques disponibles pour d'autres services sont fournies pour le service Workbench. La vue Statistiques des services affiche les statistiques clés et les informations système qui se rapportent à votre service Workbench sélectionné. Les informations s'affichent dans plusieurs sections différentes de la vue Statistiques : Workbench, Jauges, Graphiques chronologiques et Barre de statistiques graphiques. La barre de statistiques graphiques répertorie toutes les statistiques disponibles pour le Workbench. Toute statistique de la barre de statistiques graphiques peut être affichée sous forme de graphique en jauge ou chronologique.

Procédez comme suit pour afficher les statistiques Workbench :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Dans la vue Services, sélectionnez un **Workbench**, puis cliquez sur > **Vue** > **Statistiques.**

   La vue Statistiques des services s'affiche.



Remarque : Pour plus d'informations sur les statistiques Workbench, reportez-vous à Guide de mise en route de l'hôte et des services.

Afficher les logs Workbench

Procédez comme suit pour afficher les logs sur un service Workbench :

1. Dans le menu Security Analytics, sélectionnez **Administration > Services.**
2. Dans la vue Services, sélectionnez un **Workbench**, puis cliquez sur  **> Vue > Logs.**
   La grille Logs de services s'affiche.

Remarque : Pour plus d'informations sur l'affichage et la configuration des logs d'audit, reportez-vous à Configuration système.

Références

Rubriques de référence Workbench :

- Vue Configuration des Services - Workbench
- Vue Configuration des services - onglet Collections
- Vue Configuration des services - onglet Général

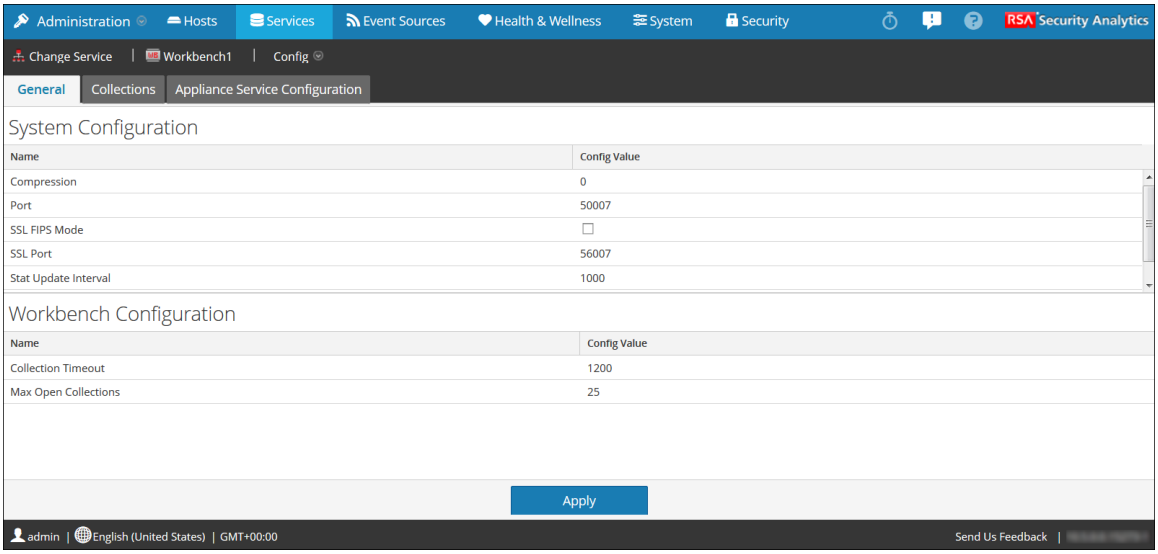
Vue Configuration des Services - Workbench

La vue Configuration des services Workbench permet de configurer un service Workbench. Dans la vue Configuration des services pour Workbench, certains paramètres sont les mêmes que les autres services Security Analytics, tandis que d'autres sont propres au service Workbench.

Pour accéder à la vue Configuration des Services :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Sélectionnez un service Workbench et cliquez sur **> Vue > Config.**

   La vue Configuration des services s'affiche.



Fonctions

Le service Workbench comporte trois onglets dans la vue Configuration :

- General
- Collections
- Configuration du service Appliance

Onglet General

L'état Vue Configuration des services - onglet Généralpour le service Workbench fournit un moyen de gérer la configuration du service de base.

Onglet Collections

L’état Vue Configuration des services - onglet Collections vous permet de traiter les fichiers à partir d'une collection Workbench.

Configuration du service Appliance

L'onglet de Configuration du service Appliance est le même pour tous les services Security Analytics. Il fournit des informations de configuration sur les appliances qui sont connectées à votre service Workbench. Pour obtenir des informations sur l'onglet **Configuration du service Appliance**, reportez-vous à l'« onglet Configuration du service Appliance » dans le Guide de mise en route de l'hôte et des services.

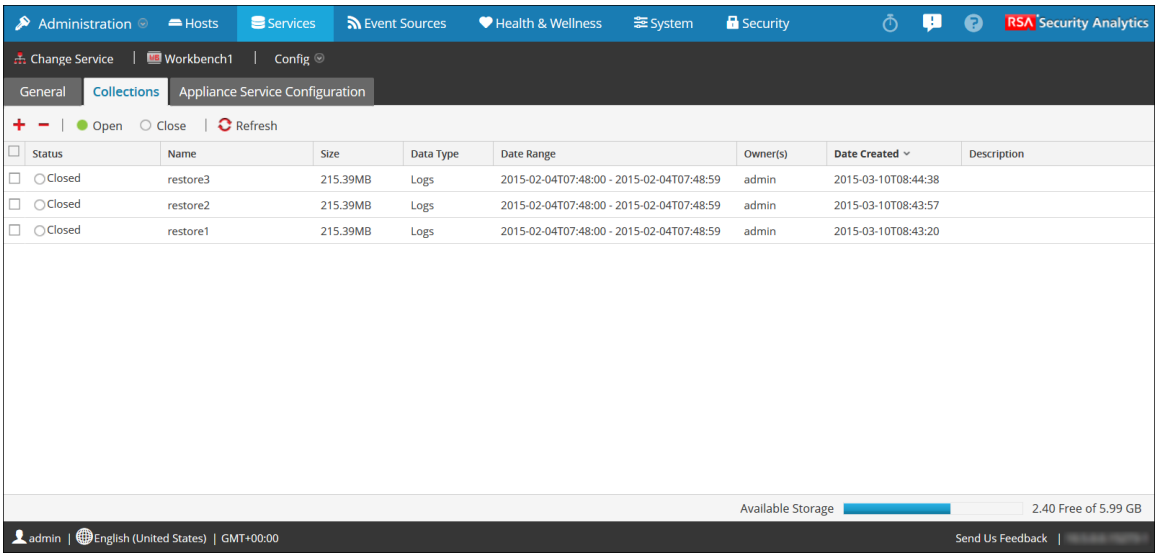
Vue Configuration des services - onglet Collections

L'onglet Collections du service Workbench fournit un moyen de gérer des collections Workbench. Les procédures associées sont disponibles dans Gérer les collections.

Pour accéder à l'onglet Collections :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Dans la grille **Services**, sélectionnez un service Workbench, puis > **Vue>Configuration**.
3. Sélectionnez l'onglet **Collections**.

La figure suivante donne un exemple de la grille Collections.



Fonctions

L'onglet Collections comporte une barre d'outils et une grille qui répertorient des informations pertinentes sur les collections Workbench.

Barre d'outils

Voici les options de la barre d'outils :

Paramètre	Description :
+	Crée une nouvelle collection de restauration.

Paramètre	Description :
	Supprime la collection Workbench sélectionnée.
Ouvrir et fermer - Se réfère à l'état de la collection de restauration.	Ouvrir - Met la collection à disposition pour les procédures d'enquêtes et le reporting. Fermer - Rend la collection indisponible pour les procédures d'enquêtes et le reporting tout en préservant les ressources.
	Actualise la liste des collections Workbench.

Grille

Le tableau suivant décrit les fonctionnalités de la grille :

Fonctionnalité	Description :
État de la collection de restauration	• **Données en cours de restauration** - La restauration de données est en cours. • **Clôturé** - Les données ont été restaurées. • **Ouverture en cours** - Les données sont en cours d'indexation. • **Prêt** - L'indexation est terminée. • **Clôture en cours** - La collection est en cours de clôture
Name	Nom du fichier en cours de restauration.
Taille	Taille de la collection.
Type de données	Logs.
Propriétaire	Indique le créateur de la collection.
Période	Indique l'heure de début et de fin des données contenues dans la collection.
Propriétaire	Répertorie l'utilisateur qui a restauré la collection.
Date de création	Affiche la date de création de la collection.

Description :	Description de la collection de restauration.
Indicateur de stockage disponible	Affiche l'espace disque disponible, exprimé en gigaoctets (Go). Le Workbench valide pour s'assurer qu'il y a suffisamment d'espace disponible lors de la tentative de création d'une collection de restauration.

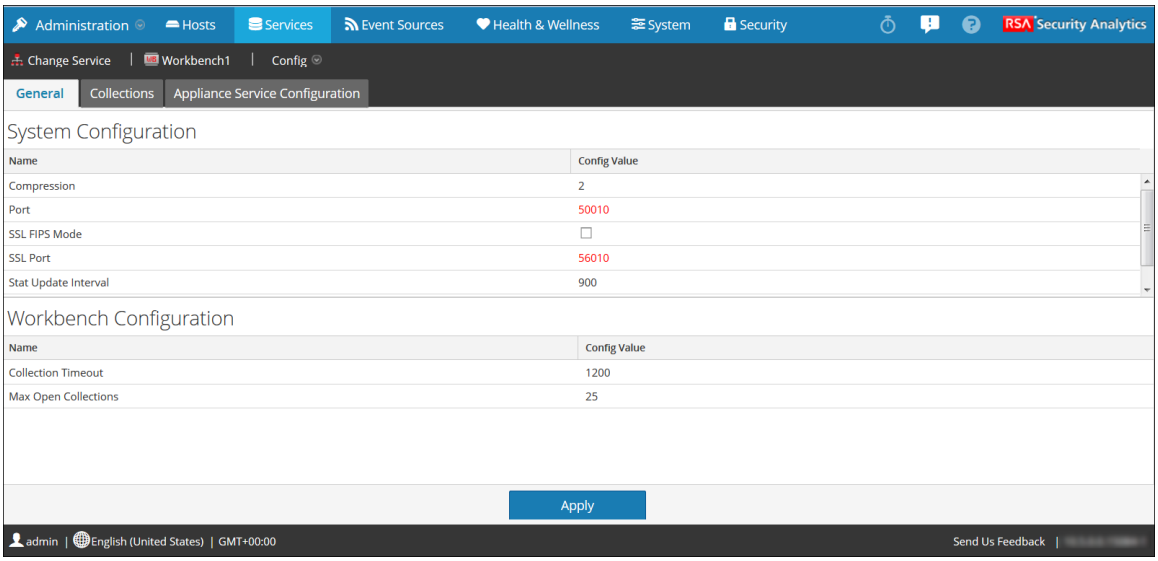
Vue Configuration des services - onglet Général

L'onglet Général du service Workbench fournit un moyen de gérer la configuration du service de base. Les procédures associées sont décrites dans la rubrique Procédures de configuration du Workbench.

Pour accéder à l'onglet Général :

1. Dans le menu **Security Analytics**, sélectionnez **Administration** > **Services**.
2. Sélectionnez un service et sélectionnez > **Vue** > **Configuration**.

La figure suivante donne un exemple de l'onglet Général.



Fonctions

L'onglet Général comporte deux panneaux :

- Configuration système
- Workbench Configuration

Panneau Configuration système

Le panneau Configuration système affiche les paramètres de configuration du service Workbench. Le tableau suivant décrit les fonctions du panneau Configuration système.

Paramètre	Description :
Compression	Lorsque sa valeur est positive, elle indique le nombre minimum d'octets avant la compression d'un message. **0** indique aucune compression pour aucun message. La modification prend effet aux connexions suivantes.
Port	Port chiffré sur lequel écoutera ce service. **0** indique désactivé. Les modifications prendront effet au redémarrage du service.
Mode FIPS SSL	Détermine si la bibliothèque OpenSSL entrera en mode FIPS. Les modifications prendront effet au redémarrage du service.
Port SSL	Port SSL sur lequel écoutera ce service. **0** indique désactivé. Les modifications prendront effet au redémarrage du service.
Intervalle de mise à jour des statistiques	Détermine la fréquence (en millisecondes) à laquelle les nœuds statistiques sont mis à jour dans le système. La modification prend effet immédiatement.
Threads	Nombre de threads dans le pool de threads permettant de gérer les requêtes entrantes. La modification prend effet immédiatement.

Panneau Configuration de Workbench

Le panneau Configuration de Workbench affiche les paramètres de configuration des collections Workbench. Le tableau suivant décrit les fonctions du panneau Configuration de Workbench

Paramètre	Description :
Expiration du délai de collection	Nombre de secondes avant qu'une collection inactive se ferme automatiquement.
Nombre max. de collections ouvertes	Nombre de collections qui peuvent être ouvertes en même temps. Un paramètre de 0 désactive la limite.
Appliquer	Met à jour les configurations modifiées dans le panneau.

Dépannage

Security Analytics notifie les utilisateurs de problèmes en utilisant des notifications contextuelles.

Problèmes Workbench possibles

Security Analytics Workbench renvoie les types de messages d'erreur suivants, comme l'explique ce tableau.

Problème	Causes possibles	Solutions

Impossible de se connecter au service Workbench à partir de la page Administration de l'interface utilisateur de Security Analytics.	Le service Security Analytics ne fonctionne pas.	Vérifiez que votre service Security Analytics est en cours d'exécution. Connectez-vous à votre serveur Security Analytics et exécutez la commande suivante :
		`status nwworkbench`
		Les règles du pare-feu doivent autoriser les connexions à partir de 50007, 50607 et 50107.
		Vérifiez votre connexion en exécutant la commande suivante :
		`service iptables status`
		
		Vérifiez que vous êtes en mesure de lancer REST. Exécutez la commande suivante pour votre appliance :
		`https://<IPAddress>:50107 service`
		Si vous êtes en mesure de lancer le service REST à partir de votre appliance, vous pouvez confirmer qu'il n'y a pas de problème avec l'appliance. Accédez au côté Security Analytics pour poursuivre la procédure d'enquête comme suit :
		Activez le mode débogage et

Problème	Causes possibles	Solutions
		recherchez les erreurs sa.log situées à l'emplacement suivant : `/var/lib/netwitness/uax/-logs` Activez les outils du développeur à l'aide du raccourci `Ctrl+Shift+I` pour Chrome et vérifiez l'aperçu et la réponse à la demande.
Impossible de visualiser l'onglet Configuration du service Appliance pour l'appliance Workbench s'exécutant en mode SSL.		Activez SSL pour le service d'appliance et redémarrez le service d'appliance.

Problème	Causes possibles	Solutions

Le message d'erreur suivant s'affiche lorsque vous essayez de charger des métas afin de créer un rapport sur une collection Workbench :
« Impossible d'extraire le schéma de la source de données lors de la tentative de chargement de métas. »
		Chargez les métas pour l'appliance à partir de la bibliothèque de règles de l'interface utilisateur Security Analytics et surveillez les erreurs
		dans le log Reporting Engine situé à l'emplacement suivant :
		`/home/rsasoc/rsa/soc/reporting-engine/logs`
		Lancez REST pour le périphérique et vérifiez les erreurs si vous exécutez la requête suivante
		`/sdk?msg=language&force-content-type=text-/plain&expiry=600&size=10`

Problème	Causes possibles	Solutions
Aucun résultat ne s'affiche après que vous avez exécuté la requête depuis l'interface utilisateur de Security Analytics via le Reporting Engine.		Exécutez la requête sur le Reporting Engine et recherchez `/var/log/messages` sur la source de données. Recherchez une requête exacte correspondant à la source de données. **ASTUCE :** Recherchez `[SDK-Query]` dans le fichier log. Copiez la requête exacte et exécutez depuis SDK de REST pour voir si vous obtenez un résultat. `REST Query: /sdk?msg=query&force-content-type=text/plain&expiry=600&query=select%20user.dst&size`
L'indicateur de stockage disponible de Workbench dans l'onglet Collections - Workbench n'est pas précis.	L'indicateur de stockage disponible dans l'Interface utilisateur affiche le répertoire Collections par défaut présenté ci-dessous : `/VAR/NETWITNESS/WORKBENCH-/COLLECTIONS`	Aucun.

Problème	Causes possibles	Solutions
Impossible d'ouvrir de nouvelles collections après avoir ouvert des collections existantes.	Il y a une configuration Workbench appelée « Max Open Collections » qui est définie sur 25 par défaut. Cette configuration spécifie le nombre de collections qui peuvent être ouvertes simultanément.	Vous pouvez modifier ce nombre. Un réglage de zéro désactive la limite du nombre maximum de collections ouvertes.
Ouverture réussie d'une collection qui est allée en état Ready. Mais après un certain temps, la collection est passée automatiquement à l'état Fermé.	Il y a une configuration Workbench appelée « collection.timeout » qui est définie sur 1 200 secondes par défaut. Cette configuration spécifie le nombre de secondes avant qu'une collection inactive soit automatiquement fermée. Le temps maximum autorisé avant l'expiration du délai est de 86 400 secondes (24 heures).	Un réglage de zéro désactive l'expiration du délai.
La recherche d'une période à l'aide de la commande `/database manifest` a renvoyé un résultat nul.	Un résultat nul indique qu'il n'y a pas de fichiers nwdb disponibles pour la période.	Aucun.

Problème	Causes possibles	Solutions
La collection a été créée, mais son état indique Non disponible dans les Tâches et la collection ne s'affiche pas dans l'onglet Collections de Workbench.	Vous exécutez peut-être un environnement en mode mixte (par exemple, création d'une collection sur une version 10.4.x de Workbench à partir de l'interface utilisateur Security Analytics 10.5.	La collection s'affiche dans l'onglet Collections de Workbench après que vous avez rechargé la page.
Valeurs vierges de Période et de Date de création notées pour les collections.	Toutes les collections affichent des valeurs vierges de Période et de Date de création.	Les valeurs de Période et de Date de création s'affichent après la mise à niveau vers 10.5.

Problème	Causes possibles	Solutions
Divergence des comportements lors de l'ajout de collections Workbench comme source de données au Reporting Engine.	Ce comportement dépend de si vous avez une connexion approuvée ou non-approuvée.	Si votre service Workbench est établi avec une connexion approuvée, vous devez ajouter manuellement les collections Workbench comme source vers le Reporting Engine. Si votre service Workbench n'est pas établi avec une connexion approuvée lorsque la collection de restauration Workbench a été créée, il envoie automatiquement un message au Reporting Engine pour l'ajouter en tant que source dans le Reporting Engine.

Problème	Causes possibles	Solutions
Les attributs de collection (taille, période et date de création) ne s'affichent pas.	La période ne s'affiche pas pour une collection si le service Jetty est redémarré pendant que la restauration est en cours. Les collections de restauration créées à partir d'une vue Explorer affichent une période vierge. Toutes les collections créées sur un Workbench 10.4 afficheront des valeurs vierges de Période et de Date de création après la mise à niveau vers 10.5. Dans un environnement de mode mixte (serveur Security Analytics 10.5 et Workbench 10.4.x), la taille, la période et la date de création ne s'affichent pas.	Aucun.
Les exceptions ou les pages vierges s'affichent lorsque l'on descend dans la hiérarchie d'une collection Workbench.	La collection s'est fermée car elle a dépassé son délai d'expiration.	Analysez la collection depuis le début.

Problème	Causes possibles	Solutions
Une collection vide est créée.	Une collection vide s'affiche si la restauration échoue car le service Workbench est redémarré pendant la création de la collection.	Aucun.
Le service s'arrête brutalement.		Exécutez le service depuis la ligne de commande et vérifiez s'il y a des erreurs. Par exemple, exécutez la commande à partir de la console du serveur `/usr/sbin/NwWorkbench` pour Workbench.
Demande REST refusée.		Vérifiez la configuration user.agent.whitelist dans `/rest/config/` Si elle n'est pas vide, il s'agit d'une expression regex qui correspond à des agents utilisateurs HTTP valides. Si le regex ne correspond pas, toutes les demandes REST seront refusées (voir allow.missing.user.agent pour l'exception potentielle). S'il 'est vierge, toutes les demandes sont autorisées.

Problème	Causes possibles	Solutions
Les requêtes avec méta brut renvoient des valeurs vierges pour champ Brut.		Vérifiez que vous avez un `packet db`.