

UBA - Outils d'assistance : uba_pre_check.sh et uba_health_check.sh

Applicabilité

UBA

Description

Pour collecter des informations sur un déploiement UBA, Splunk UBA Support demande souvent l'exécution de deux scripts : uba_pre_check.sh et uba_health_check.sh. Ces scripts capturent respectivement la configuration UBA et l'état actuel.

Les deux outils sont gérés par UBA Engineering en dehors du cycle normal de publication des produits, car ils sont révisés à mesure que de nouveaux problèmes d'assistance sont soulevés. La version fournie avec une plate-forme UBA est disponible au gel du code qui se produit quelques semaines avant la mise à jour générale et les révisions.

Enquête

Téléchargez les scripts depuis Google Drive :

- uba_pre_check.sh :
 - https://drive.google.com/file/d/1FUMtUiyWYynBHwM24J7fNbyHC8tvZ2Sb/view?usp=share_link
- uba_health_check.sh :
 - https://drive.google.com/file/d/1IXtTHz3BNN20pyJDh52kcZyArwxAQk2x/view?usp=share_link

Copiez les scripts sur node1 :

Connectez-vous au node1 (le noeud maître dans un cluster) via SSH en tant qu'utilisateur caspida. Enregistrez une copie des scripts actuellement installés qui s'exécutent :

```
cd /opt/caspida/bin/utils/  
cp -p uba_pre_check.sh uba_pre_check.sh.OLD  
cp -p uba_health_check.sh uba_health_check.sh.OLD
```

Copiez les nouveaux scripts téléchargés dans l'emplacement par défaut ***/opt/caspida/bin/utils/*** en remplaçant les scripts existants, puis faites-les exécutable :

```
cd /opt/caspida/bin/utils/  
chmod 755 uba_pre_check.sh  
chmod 755 uba_health_check.sh
```

NOTE: Parfois, ^M caractères sont ajoutés à ces scripts lors du téléchargement sur des systèmes Windows. Voici les commandes qui peuvent être utilisées pour supprimer les caractères ^M :

```
cd ~/bin  
tr -d '\r' < uba_pre_check.sh > /tmp/x  
cp /tmp/x uba_pre_check.shtr -d '\r' < uba_health_check.sh > /tmp/x  
cp /tmp/x uba_health_check.shrm /tmp/x
```

Dans un environnement de cluster, synchronisez les fichiers dans ***/opt/caspida/bin/utils/*** sur les noeuds en exécutant :

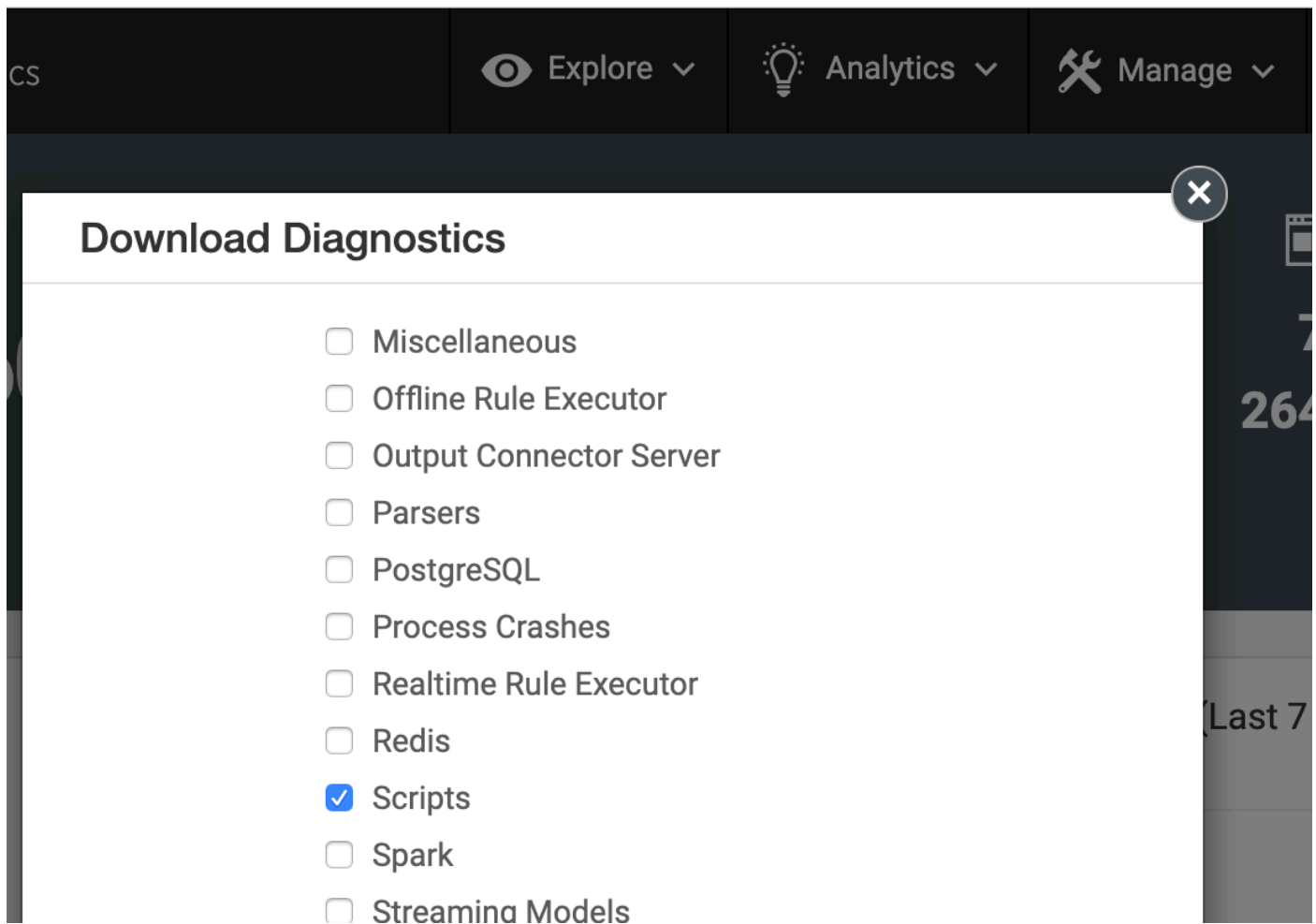
```
/opt/caspida/bin/Caspida sync-cluster /opt/caspida/bin/utils/
```

Exécution des scripts lorsque l'interface utilisateur est disponible :

Pour exécuter les scripts et collecter les fichiers de sortie à l'aide de l'interface utilisateur UBA, cliquez sur " System —> Download Diagnostics"

Dans la fenêtre contextuelle, définissez 1 dans « Jours passés ».

Désélectionnez tous les éléments de la liste sauf " Scripts" :



Appuyez ensuite sur OK. L'exécution du script peut prendre un certain temps.

Un message s'affiche pour vous indiquer que le fichier de diagnostic est prêt à être téléchargé. Téléchargez le fichier de diagnostic sur le dossier afin de pouvoir l'analyser par le support.

Exécution manuelle des scripts lorsque l'interface utilisateur n'est pas disponible :

Connectez-vous au node1 (le noeud maître dans un cluster) via SSH en tant qu'utilisateur caspida et exécutez ces commandes :

```
cd /opt/caspida/bin/utils/  
./uba_pre_check.sh  
./uba_health_check.sh
```

Les deux scripts produiront des fichiers de sortie sous la forme ***/var/log/caspida/check/u*.txt*** qui incluront le nom d'hôte et l'horodatage.

Collectez les fichiers suivants et téléchargez-les dans le dossier afin qu'ils puissent être analysés par le support technique :

```
/var/log/caspida/check/uhc*<last_time_stamp>  
/var/log/caspida/check/upc*<last_time_stamp>
```

Résolution

Les deux scripts sont constamment améliorés et mis à jour, il est donc fortement conseillé de télécharger et d'exécuter la dernière version disponible.

Ils sont rétrocompatibles avec toutes les versions UBA prises en charge.

Les dernières révisions peuvent contenir une logique d'accès anticipé ou de versions futures.

Liens connexes

Téléchargez les scripts suivants à partir de Google Drive :

- uba_pre_check.sh :
 - https://drive.google.com/file/d/1FUMtUiyWYynBHwM24J7fNbyHC8tvZ2Sb/view?usp=share_link
- uba_health_check.sh :
 - https://drive.google.com/file/d/1IXtTHz3BNN20pyJDh52kcZyArwxAQk2x/view?usp=share_link

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.