

UBA - Herramientas de asistencia:

uba_pre_check.sh y uba_health_check.sh

Aplicabilidad

UBA

Descripción

Para recopilar información sobre una implementación de UBA, el Soporte de Splunk UBA a menudo solicita la ejecución de dos scripts: uba_pre_check.sh y uba_health_check.sh. Estos scripts capturan la configuración de UBA y el estado actual, respectivamente.

Ingeniería de UBA mantiene ambas herramientas fuera del ciclo normal de lanzamiento de productos, ya que se revisan a medida que surgen nuevos problemas de asistencia. La versión que se envía con una versión de la plataforma UBA es la que está disponible en la congelación de código que es semanas antes de GA y las revisiones se producirán.

Investigación

Descargue los guiones 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

Copie las secuencias de comandos en node1:

Conéctese al nodo 1 (el nodo maestro en un clúster) a través de SSH como usuario caspida. Guardar una copia de los scripts instalados actualmente en ejecución:

```
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
```

Copie las nuevas secuencias de comandos descargadas en la ubicación predeterminada ***/opt/caspida/bin/utils/*** reemplazando las existentes, luego conviértalas en ejecutables:

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

NOTE: A veces se agregan ^M caracteres a estas secuencias de comandos al descargarlas en sistemas Windows. Estos son los comandos que se pueden utilizar para quitar los caracteres ^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
```

En un entorno de clúster, sincronice los archivos en ***/opt/caspida/bin/utils/*** a través de los nodos mediante la ejecución de:

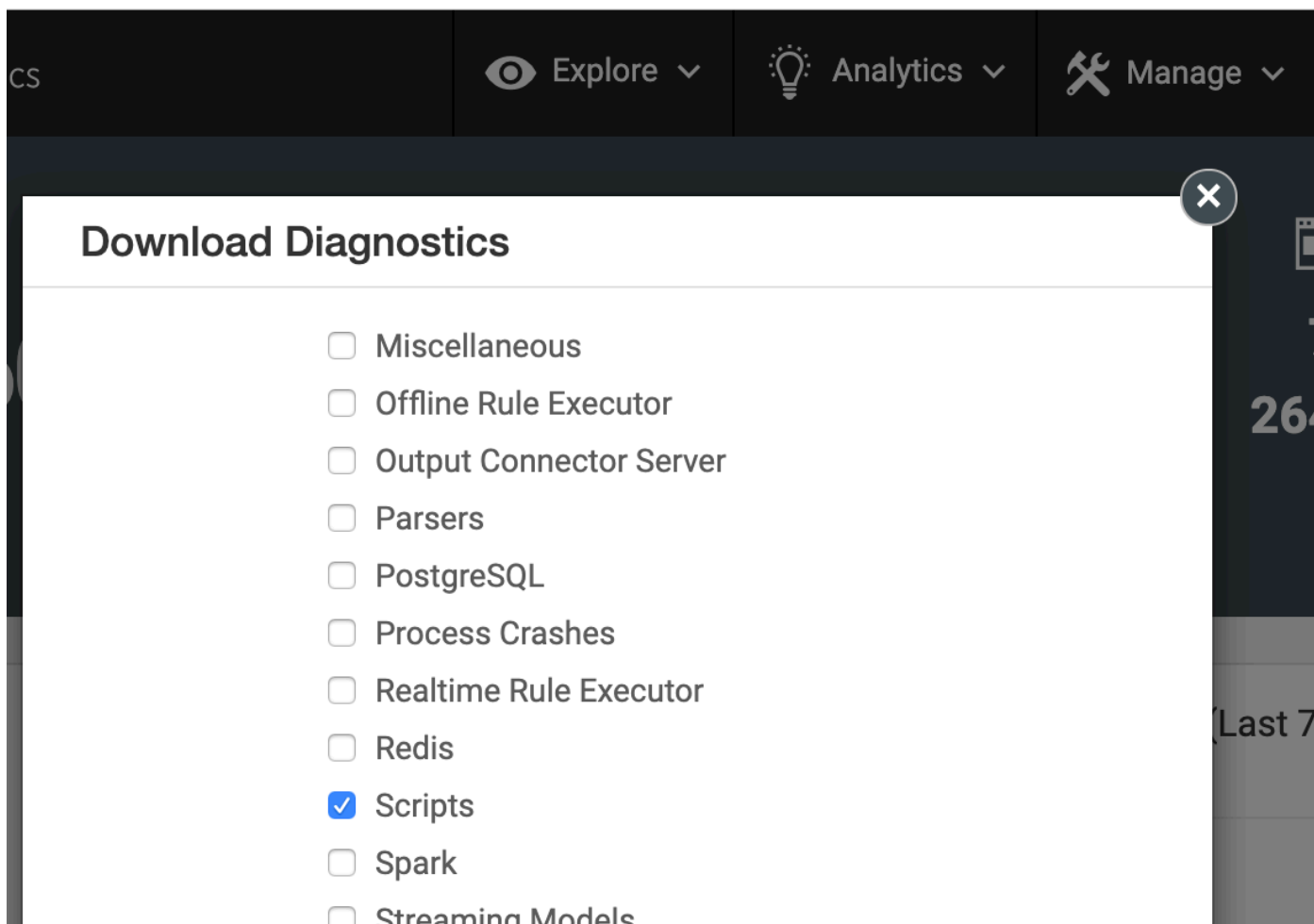
```
/opt/caspida/bin/Caspida sync-cluster /opt/caspida/bin/utils/
```

Ejecutar las secuencias de comandos cuando la interfaz de usuario esté disponible:

Para ejecutar las secuencias de comandos y recopilar los archivos de salida mediante la interfaz de usuario de UBA, haga clic en " System —> Download Diagnostics" (Sistema —> Descargar diagnósticos)

En la ventana emergente, establezca 1 en "Días anteriores".

Anule la selección de todos los elementos de la lista excepto " Scripts":



A continuación, pulse Aceptar. La ejecución del script puede tardar un tiempo en completarse. Aparecerá un mensaje que le informará de que el archivo de diagnóstico está listo para su descarga.

Cargue el archivo de diagnóstico en el caso para que el equipo de soporte técnico pueda analizarlo.

Ejecutar manualmente los scripts cuando la interfaz de usuario no está disponible:

Conéctese al nodo node1 (el nodo maestro en un cluster) vía SSH como usuario caspida y ejecute estos comandos:

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

Ambos scripts producirán archivos de salida como ***/var/log/caspida/check/u*.txt*** que incluye nombre de host y marca de tiempo.

Recopile los siguientes archivos y cárguelos en el caso para que el equipo de soporte técnico pueda analizarlos:

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

Resolución

Ambos scripts se mejoran y actualizan constantemente, por lo que es muy recomendable descargar y ejecutar la última versión disponible.

Son compatibles con todas las versiones UBA compatibles.

Las últimas revisiones pueden contener lógica de acceso anticipado o versiones futuras.

Enlaces relacionados

Descargue los siguientes scripts 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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).