

UBA : サポートツール : uba_pre_check.shおよびuba_health_check.sh

適用性

ウバ

説明

UBAの展開に関する情報を収集するために、Splunk UBAサポートでは uba_pre_check.shと uba_health_check.shの2つのスクリプトの実行を要求することがよくあります。これらのスクリプトは、UBAの設定と現在の状態をそれぞれキャプチャします。

どちらのツールも、新しいサポートの問題が発生すると改訂されるため、通常の製品リリースサイクルの範囲外でUBA Engineeringによって維持されます。UBAプラットフォームリリースとともに出荷されるバージョンは、GAおよびリビジョンが発生する数週間前のコードフリーズ時に利用可能なバージョンです。

調査

Google ドライブからスクリプトをダウンロードします。

- uba_pre_check.sh (引用符は付けません) :
 - https://drive.google.com/file/d/1FUMtUiyWYynBHwM24J7fNbyHC8tvZ2Sb/view?usp=share_link
- uba_health_check.sh (有効な場合) :
 - https://drive.google.com/file/d/1IXtTHz3BNN20pyJDh52kcZyArwxAQk2x/view?usp=share_link

node1にスクリプトをコピーします。

caspidaユーザとしてSSH経由でnode1 (クラスタ内のマスターノード) に接続します。
現在インストールされているスクリプトのコピーを保存します。実行中 :

```
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
```

ダウンロードした新しいスクリプトをデフォルトの場所である`/opt/caspida/bin/utils/`にコピーして、既存のスクリプトと置き換え、実行可能ファイルにします。

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

注：Windowsシステムへのダウンロード時に、`^M`文字がスクリプトに追加されることがあります。`^M`文字を削除するために使用できるコマンドを次に示します。

```
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
```

クラスタ環境では、次のコマンドを実行して、ノード間で`/opt/caspida/bin/utils/`のファイルを同期します。

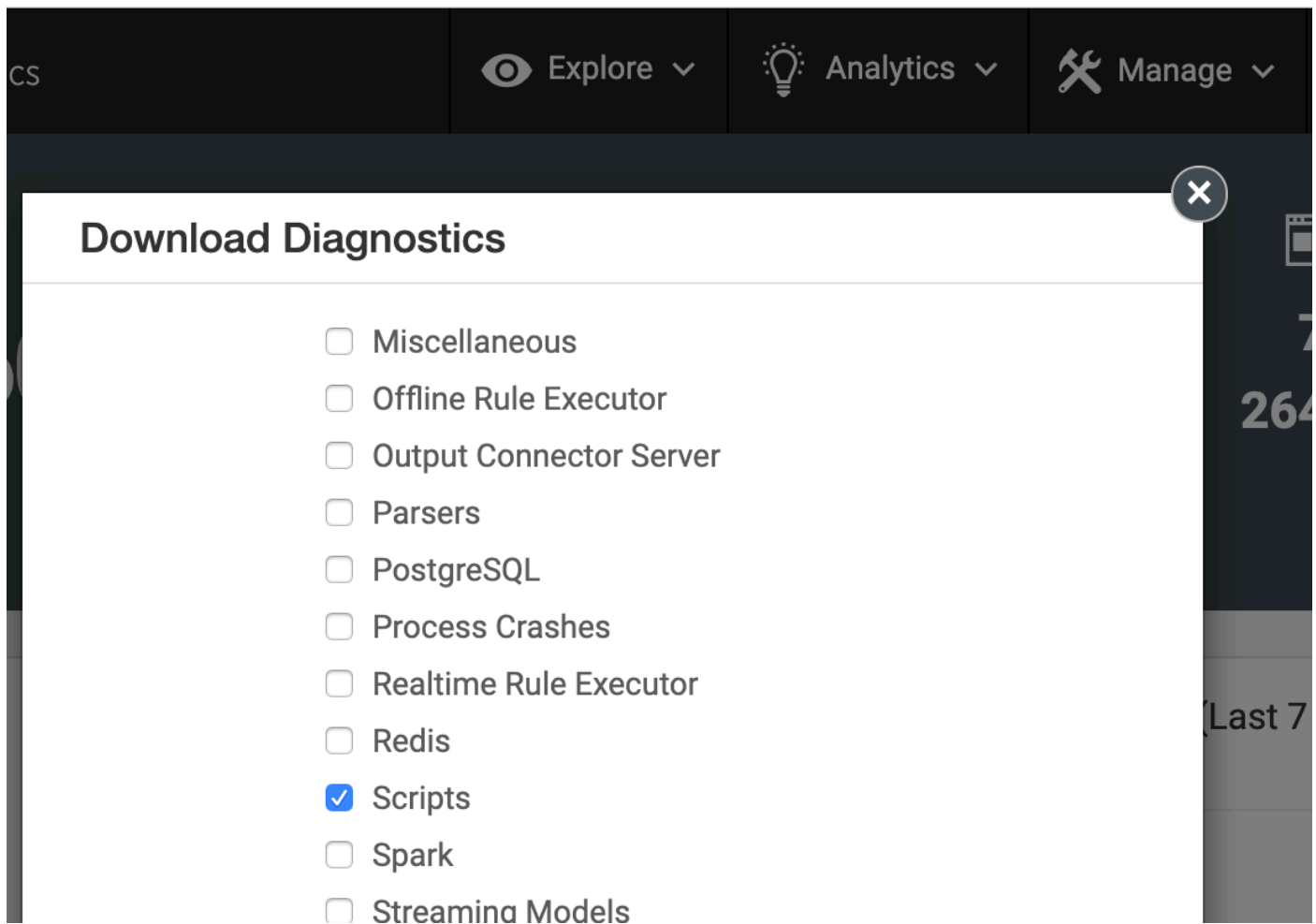
```
/opt/caspida/bin/Caspida sync-cluster /opt/caspida/bin/utils/
```

UIが使用可能なときにスクリプトを実行する：

UBA UIを使用してスクリプトを実行し、出力ファイルを収集するには、「System → Download Diagnostics」をクリックします。

ポップアップウィンドウで、「Past Days」に「1」を設定します。

リスト内のすべての項目の選択を解除しますが、「スクリプト」は選択しません。



次に、OKを押します。スクリプトの実行が完了するまでに時間がかかる場合があります。診断ファイルをダウンロードする準備が整ったことを知らせるメッセージが表示されます。診断ファイルをケースにアップロードして、サポート担当者が分析できるようにします。

UIが使用できないときに手動でスクリプトを実行する：

SSH経由でcaspidaユーザとしてnode1（クラスタ内のマスターノード）に接続し、次のコマンドを実行します。

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

どちらのスクリプトでも、ホスト名とタイムスタンプを含む出力ファイルが **`/var/log/caspida/check/u*.txt`** として生成されます。

次のファイルを収集してケースにアップロードし、サポートによって分析できるようにします。

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

解決方法

両方のスクリプトは常に改善および更新されるため、入手可能な最新バージョンをダウンロードして実行することを強くお勧めします。

サポートされるすべてのUBAリリースと下位互換性があります。

最新リリースには、早期アクセスまたは将来のリリースのためのロジックが含まれる場合があります。

関連リンク

Googleドライブから次のスクリプトをダウンロードします。

- uba_pre_check.sh (引用符は付けません) :
 - https://drive.google.com/file/d/1FUMtUiyWYynBHwM24J7fNbyHC8tvZ2Sb/view?usp=share_link
- uba_health_check.sh (有効な場合) :
 - https://drive.google.com/file/d/1IXtTHz3BNN20pyJDh52kcZyArwxAQk2x/view?usp=share_link

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。