

UBA — 支援工具：uba_pre_check.sh和uba_health_check.sh

適用性

UBA

說明

要收集有關UBA部署的資訊，Splunk UBA支援部門通常會請求運行兩個指令碼：uba_pre_check.sh和 uba_health_check.sh。這些指令碼分別捕獲UBA配置和當前狀態。

這兩種工具都由UBA Engineering在正常產品發佈週期之外進行維護，因為出現新的支援問題時會對其進行修訂。隨UBA平台版本提供的版本是代碼凍結時提供的版本，該版本將在正式上市前幾週提供，並將進行修訂。

調查

從Google Drive下載指令碼：

- 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

複製node1上的指令碼：

以caspida使用者身份通過SSH連線到node1（集群中的主節點）。
儲存當前正在執行的已安裝指令碼的副本：

```
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
```

將下載的新指令碼複製到預設位置`/opt/caspida/bin/utils/`以替換現有指令碼，然後將其設定為執行檔：

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

附註：下載到Windows系統時，有時會將^M個字元新增到這些指令碼中。以下是可用於刪除^M字元的命令：

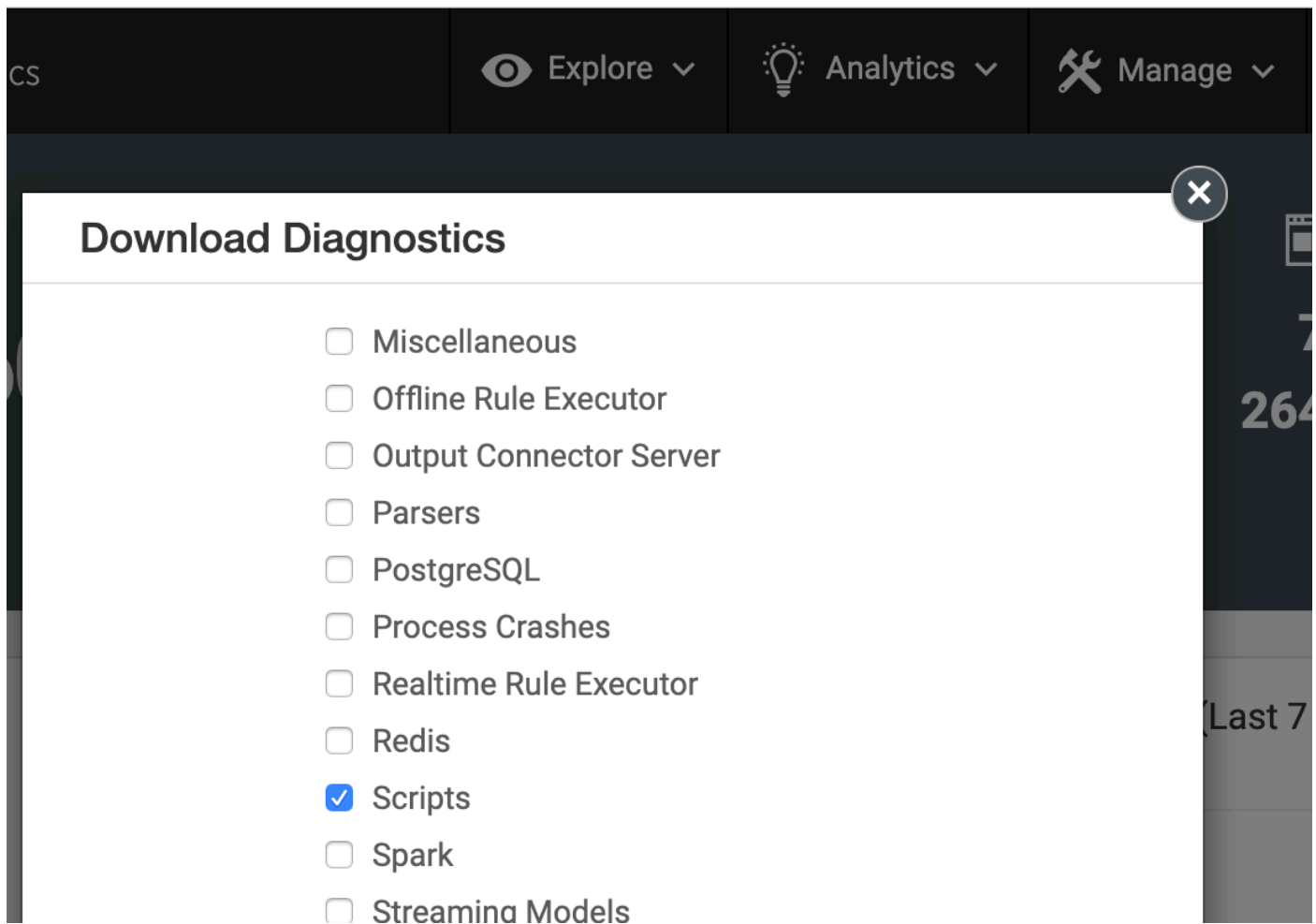
```
cd ~/bin  
tr -d '\r' < uba_pre_check.sh > /tmp/x  
cp /tmp/x uba_pre_check.shtr -d '\r' < uba_health_check.sh > /tmp/x  
cp /tmp/x uba_health_check.shrm /tmp/x
```

在群集環境中，通過執行以下操作跨節點同步`/opt/caspida/bin/utils/`中的檔案：

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

在UI可用時運行指令碼：

要使用UBA UI運行指令碼並收集輸出檔案，請按一下「System -> Download Diagnostics」在彈出視窗的「Past Days (過去天)」中設定1。
取消選擇清單中的每個專案，但選擇「Scripts」：



然後按確定。指令碼執行可能需要一段時間才能完成。
系統將顯示一條消息，通知您診斷檔案已準備好下載。
將診斷檔案上傳到案件，以便支援部門進行分析。

在UI不可用時手動執行指令碼：

以caspida使用者身份通過SSH連線到node1（ 集群中的主節點 ），然後執行以下命令：

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

這兩個指令碼都將生成輸出檔案 ***/var/log/caspida/check/u*.txt***，其中包括主機名和時間戳。
收集以下檔案並將其上傳到案件，以便支援部門可以分析這些檔案：

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

解析

這兩個指令碼都不斷改進和更新，因此極建議下載並運行可用的最新版本。

它們與所有支援的UBA版本向後相容。

最新版本可能包含提前訪問或將來版本的邏輯。

相關連結

從Google Drive下載以下指令碼：

- 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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。