

UBA — 支持工具：uba_pre_check.sh和uba_health_check.sh

适用范围

UBA

描述

要收集有关UBA部署的信息，Splunk UBA支持通常会请求运行两个脚本：uba_pre_check.sh和uba_health_check.sh。这些脚本分别捕获UBA配置和当前状态。

这两种工具都由UBA Engineering在正常的产品发布周期之外进行维护，因为出现新的支持问题时会对其进行修订。随UBA平台版本一起提供的版本是代码冻结时提供的版本，该版本将在正式上市前的几周内发布，并将进行修订。

调查

从**Google Drive**下载脚本：

- 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

复制node1上的脚本：

以caspida用户身份通过SSH连接到node1（集群中的主节点）。
保存当前安装的脚本的副本，执行：

```
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
```

在默认位置/opt/caspida/bin/utils/中复制下载的新脚本，以替换现有脚本，然后使这些脚本成为可执行脚本：

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

NOTE:下载到Windows系统时，有时会将^M个字符添加到这些脚本中。以下是可用于删除^M字符的命令：

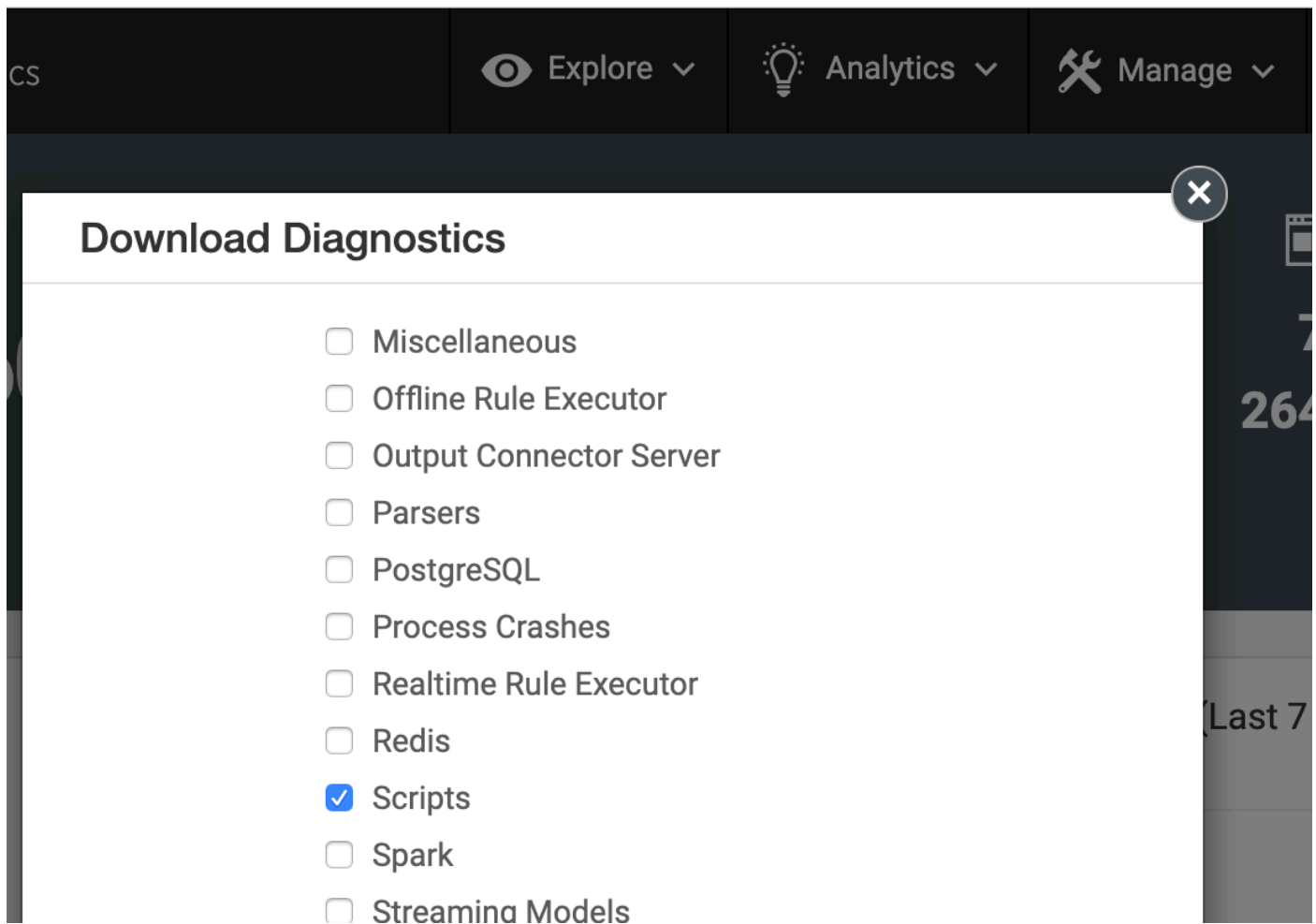
```
cd ~/bin  
tr -d '\r' < uba_pre_check.sh > /tmp/x  
cp /tmp/x uba_pre_check.sh  
tr -d '\r' < uba_health_check.sh > /tmp/x  
cp /tmp/x uba_health_check.shrm /tmp/x
```

在群集环境中，通过执行以下操作在节点间同步`/opt/caspida/bin/utils/`中的文件：

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

在UI可用时运行脚本：

要使用UBA UI运行脚本并收集输出文件，请点击“System —> Download Diagnostics”。
在弹出窗口中，在“Past Days”（过去）中设置1。
取消选择列表中的每个项目，但选择“脚本”：



然后按OK。脚本执行可能需要一段时间才能完成。
系统将显示一条消息，告知您诊断文件已准备好下载。
将诊断文件上传到案例，以便支持人员对其进行分析。

在UI不可用时手动执行脚本：

以caspida用户身份通过SSH连接到node1（集群中的主节点），然后执行以下命令：

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

两个脚本都将生成输出文件`/var/log/caspida/check/u*.txt`，其中包含主机名和时间戳。
收集以下文件并将其上传到案例，以便支持人员对其进行分析：

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

分辨率

这两个脚本都会不断改进和更新，因此强烈建议您下载并运行可用的最新版本。它们与所有支持的UBA版本向后兼容。最新修订可能包含提前访问或未来版本的逻辑。

相关链接

从Google Drive下载以下脚本：

- 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

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。