

UBA - Ferramentas de suporte:

uba_pre_check.sh e uba_health_check.sh

Aplicabilidade

UBA

Descrição

Para coletar informações sobre uma implantação de UBA, o Suporte Splunk UBA geralmente solicita a execução de dois scripts: uba_pre_check.sh e uba_health_check.sh. Esses scripts capturam a configuração UBA e o estado atual, respectivamente.

Ambas as ferramentas são mantidas pela Engenharia da UBA fora do ciclo normal de lançamento do produto, pois são revisadas à medida que novos problemas de suporte são levantados. A versão que vem com uma versão de plataforma UBA é a que está disponível no congelamento de código semanas antes da data de disponibilidade geral e das revisões ocorrerem.

Investigação

Faça o download dos scripts do 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 os scripts em node1:

Conecte-se ao nó 1 (o nó mestre em um cluster) via SSH como usuário caspida.
Salve uma cópia dos scripts atualmente instalados executando:

```
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 os novos scripts baixados no local padrão ***/opt/caspida/bin/utils/*** substituindo os existentes e torne-os executáveis:

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

NOTE: Às vezes, ^M caracteres são adicionados a esses scripts durante o download para sistemas Windows. Estes são os comandos que podem ser usados para remover os 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
```

Em um ambiente de cluster, sincronize os arquivos em ***/opt/caspida/bin/utils/*** através dos nós executando:

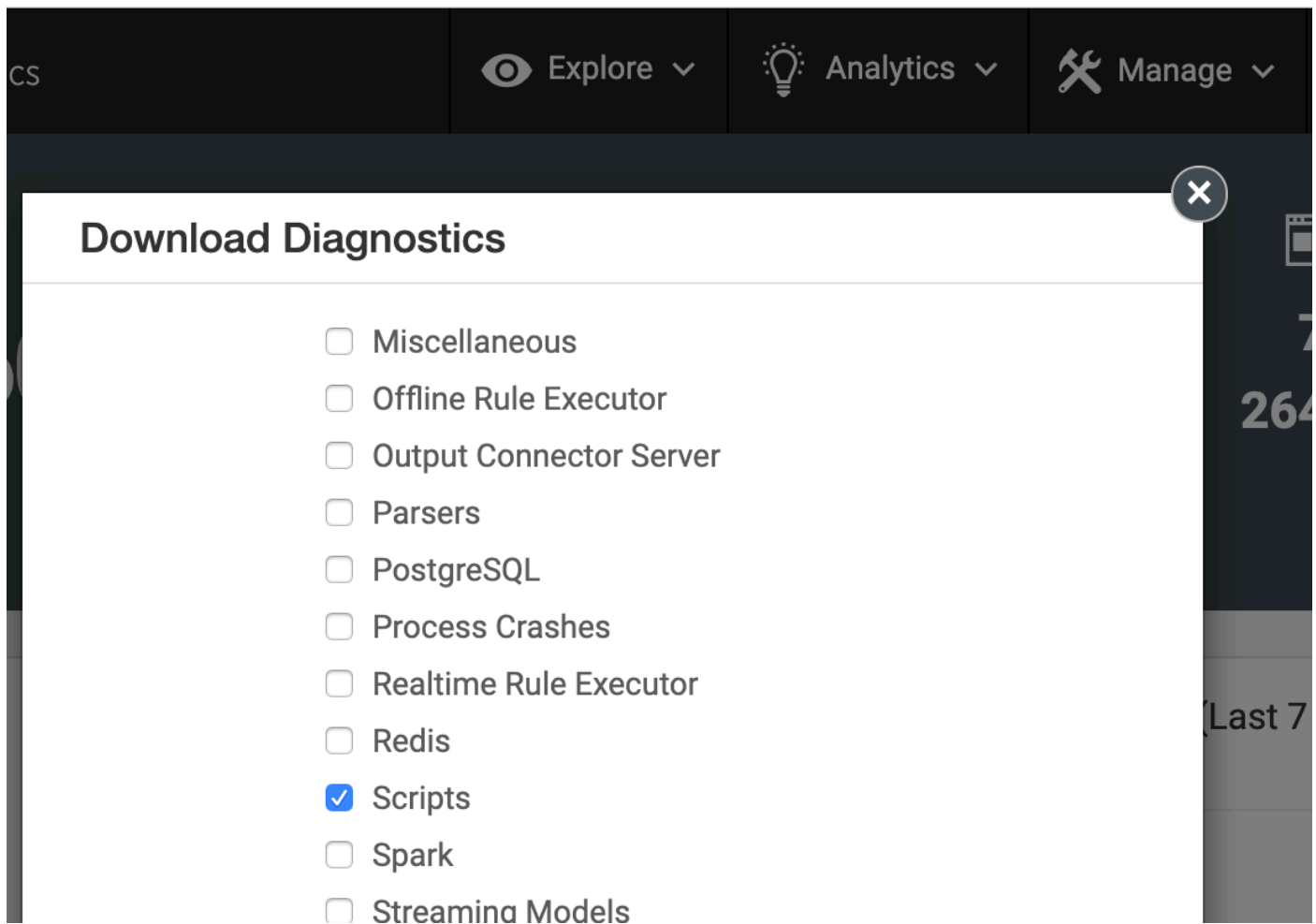
```
/opt/caspida/bin/Caspida sync-cluster /opt/caspida/bin/utils/
```

Executando os scripts quando a interface do usuário estiver disponível:

Para executar os scripts e coletar os arquivos de saída usando a UBA UI, clique em " Sistema —> Download Diagnostics"

Na janela pop-up, defina 1 em "Últimos dias".

Desmarque todos os itens da lista, exceto " Scripts":



Em seguida, pressione OK. A execução do script pode demorar um pouco para ser concluída. Será exibida uma mensagem informando que o arquivo de diagnóstico está pronto para download.

Carregue o arquivo de diagnóstico no gabinete para que ele possa ser analisado pelo suporte.

Executando manualmente os scripts quando a interface do usuário não está disponível:

Conecte-se ao nó 1 (o nó mestre em um cluster) via SSH como usuário caspida e execute estes comandos:

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

Ambos os scripts produzirão arquivos de saída como ***/var/log/caspida/check/u*.txt*** que incluem nome de host e carimbo de data e hora.

Colete os seguintes arquivos e carregue-os no caso para que eles possam ser analisados pelo suporte:

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

Resolução

Ambos os scripts são constantemente melhorados e atualizados, por isso é altamente recomendável baixar e executar a versão mais recente disponível.

Eles são compatíveis com versões anteriores de todas as versões de UBA suportadas.

As revisões mais recentes podem conter lógica para acesso antecipado ou versões futuras.

Links relacionados

Faça o download dos seguintes scripts do 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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.