O dispositivo Sourcefire/FirePOWER pesquisa defeitos procedimentos de geração do arquivo

Índice

Introdução

Este documento descreve como gerar um arquivo da pesquisa de defeitos em um dispositivo de Sourcefire/FirePOWER. Um arquivo da pesquisa de defeitos contém uma coleção dos mensagens de registro, dos dados de configuração, e das saídas do comando. É usado a fim determinar o estado de um sistema de Sourcefire/FirePOWER. Se um engenheiro de suporte da Cisco pede que você envia um arquivo da pesquisa de defeitos de seu dispositivo de Sourcefire/FirePOWER, você pode usar as instruções fornecidas neste documento.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Dispositivos do Gerenciamento de Sourcefire, tais como o centro da defesa/FireSIGHT/centro de gerenciamento de FirePOWER (FMC)
- Dispositivos gerenciado de Sourcefire, tais como os modelos do dispositivo de FirePOWER (Series-3), os modelos do dispositivo 3D (Series-2), e o módulo do dispositivo virtual/ASA FirePOWER com fora de Gerenciamento da caixa.

Note: Você pode usar o centro ou o centro de gerenciamento da defesa a fim gerar um arquivo para o dispositivo do Gerenciamento próprio da pesquisa de defeitos, ou para um dispositivo gerenciado. Os modelos do dispositivo de FirePOWER (Series-3) incluem o 7000

Series, o 7100 Series, e os dispositivos gerenciado do 8000 Series. Os modelos do dispositivo gerenciado Series-2 incluem 3D500, 3D1000, 3D2000, 3D2100, 3D2500, 3D3500, 3D4500, 3D6500, 3D9900, e ASA com serviços de FirePOWER.

Componentes Utilizados

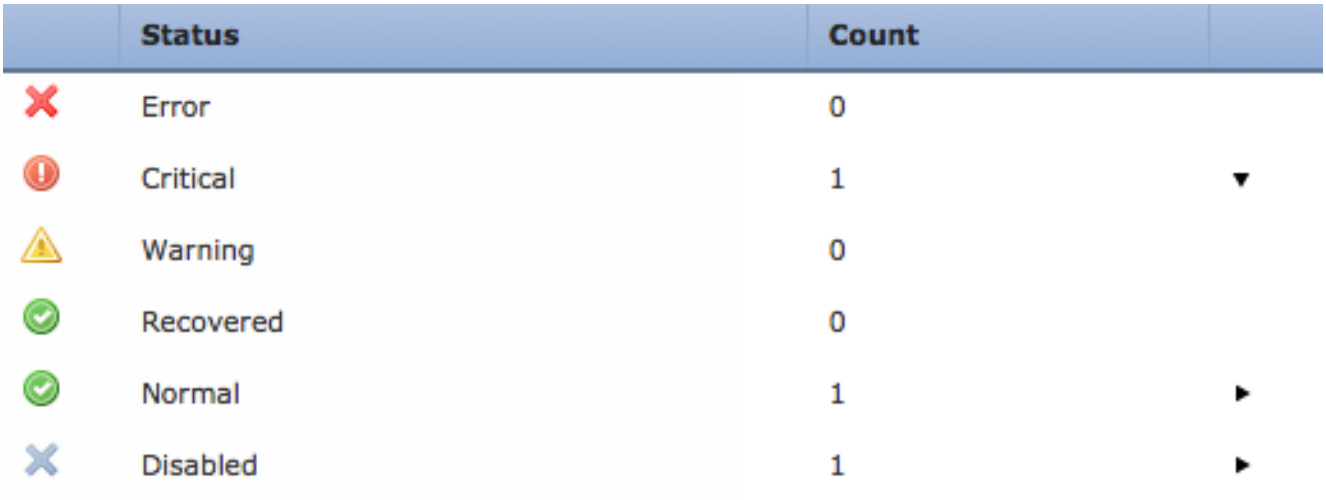
Esta informação neste documento é baseada em um dispositivo de Sourcefire /FirePOWER que execute a versão de software 5.0 ou mais atrasado.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Gerencia pesquisam defeitos arquivos com uma interface da WEB

Termine estas etapas a fim gerar pesquisam defeitos arquivos:

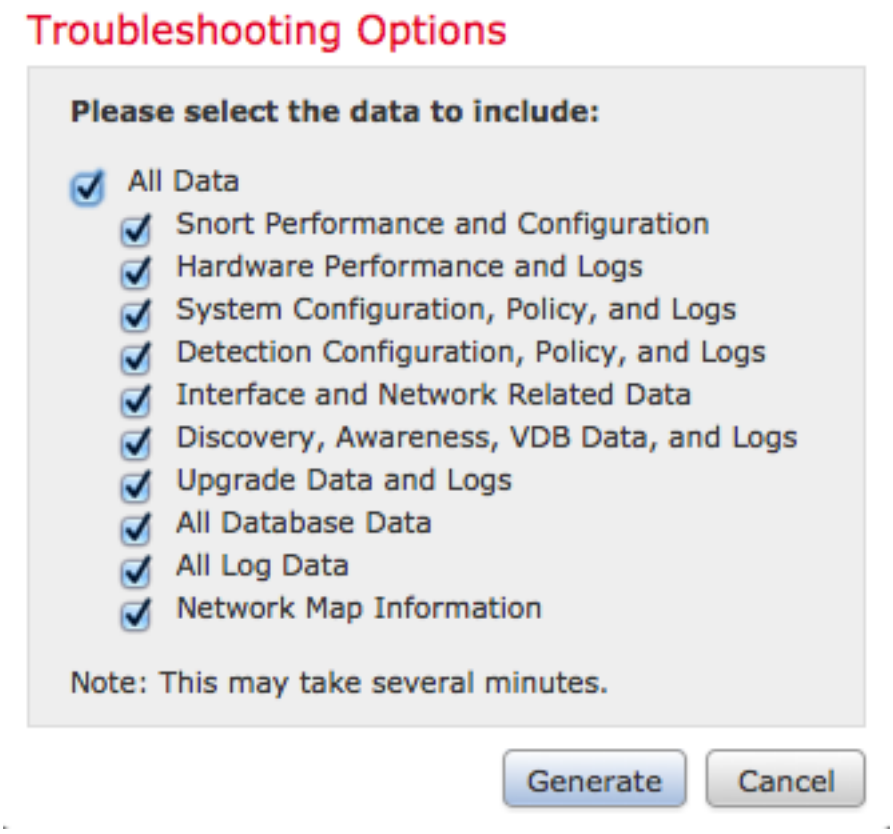
1. Na versão 5.x.x, navegue à **saúde > ao monitor de funcionamento na** interface da WEB do dispositivo do Gerenciamento a fim alcançar a página do monitor de funcionamento.
   Na versão 6.x.x, navegue ao **sistema > à saúde > ao monitor na** interface da WEB do dispositivo do Gerenciamento a fim alcançar a página do monitor de funcionamento.
2. A fim expandir a lista do dispositivo e ver os dispositivos com um estado particular, clique a seta no fim da fileira:



   Tip: Se a seta no fim da fileira para pontos nivelados de um estado para baixo, a lista do dispositivo para esse estado aparece na tabela mais baixa. Se a seta aponta certo, a lista do dispositivo é hidden.
3. Na coluna do dispositivo da lista do dispositivo, clique o nome do dispositivo para que você quer ver detalhes. A página do dispositivo do monitor de funcionamento publica-se.

4. O clique **gerencie arquivos do Troubleshooting**. A janela pop-up das opções do Troubleshooting aparece.

5. Verifique **toda a** caixa de **verificação de dados** a fim gerar um relatório com todos os dados possíveis do Troubleshooting, ou verifique as caixas de seleção individuais a fim personalizar seu relatório:



6. O clique **gerencie** e o centro de gerenciamento gerencie os arquivos da pesquisa de defeitos.

   Tip: Na versão 5.x.x, a fim monitorar o processo de geração do arquivo na fila de tarefa, navegue ao **sistema > ao estado da monitoração > da tarefa**. Na versão 6.x.x, a fim monitorar o processo de geração do arquivo no estado da tarefa, navegue ao **ícone do centro da mensagem** (uma opção no meio distribui e sistema) **> tarefas**.

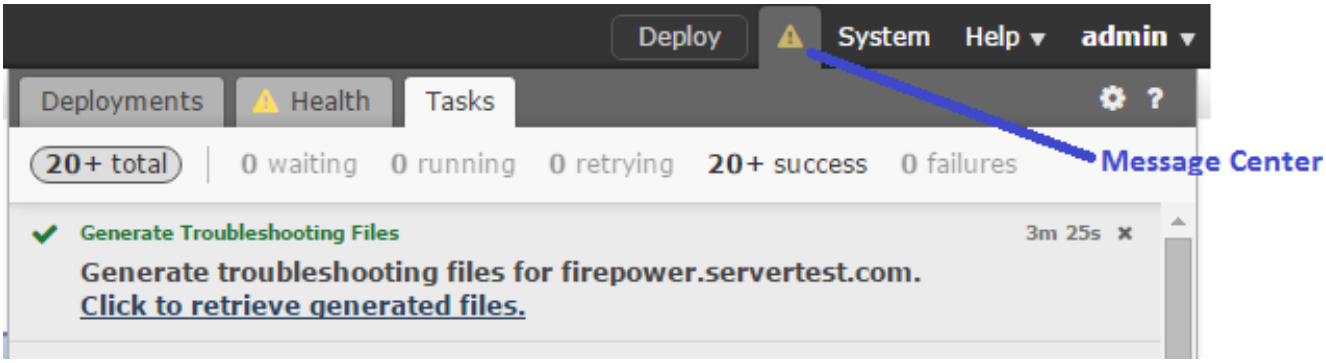
A transferência pesquisa defeitos arquivos

Termine estas etapas a fim transferir cópias do seu gerado pesquisam defeitos arquivos:

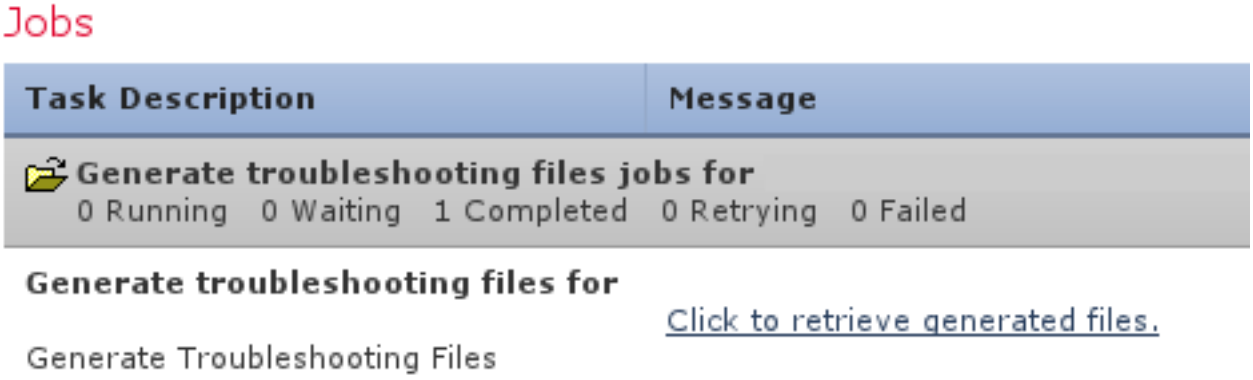
1. Na versão 5.x.x, navegue ao **estado do sistema > da monitoração > da tarefa na** interface da WEB do dispositivo do Gerenciamento a fim alcançar a página do estado da tarefa.
   Na versão 6.x.x**,** navegue ao **ícone do centro da mensagem** (uma opção no meio distribui e sistema) **> tarefas na** interface da WEB do dispositivo do Gerenciamento a fim alcançar a página do estado da tarefa.
2. Depois que o dispositivo gerencie os arquivos da pesquisa de defeitos e as alterações de status da tarefa ao **terminado**, encontre a tarefa que corresponde aos arquivos da pesquisa de defeitos que você gerou.
3. Clique o **clique para recuperar o** link de **arquivos gerado** e para seguir as alertas do

navegador a fim transferir o arquivo.

Versão 5.x.x



da versão 6.x.x



4. **Note**: Os arquivos são transferidos a seu desktop em um único arquivo de **.tar.gz**.

Métodos alternativos da geração

Se você tenta usar o método da geração que está descrito nas seções anterior e é incapaz de alcançar a interface da WEB do dispositivo do Gerenciamento, ou se há um problema de conectividade entre o dispositivo do Gerenciamento e os dispositivos gerenciado, a seguir você não pode gerar o arquivo da pesquisa de defeitos. Neste caso, você pode usar o CLI de seu dispositivo a fim gerar o arquivo da pesquisa de defeitos.

Gerencia pesquisam defeitos arquivos com o CLI

Centro da defesa e dispositivos Series-2

Incorpore este comando ao centro, ao centro de gerenciamento, e aos dispositivos gerenciado Series-2 da defesa a fim gerar um arquivo da pesquisa de defeitos:

```
admin@3DSystem:~$ sudo sf_troubleshoot.pl

Starting /usr/local/sf/bin/sf_troubleshoot.pl...
Please, be patient.  This may take several minutes.
Troubleshooting information successfully created at /var/common/xxxxxx.tar.gz
```

FirePOWER e dispositivos virtuais

Incorpore este comando em dispositivos de FirePOWER/módulos e em dispositivos gerenciado virtuais a fim gerar um arquivo da pesquisa de defeitos:

```
> system generate-troubleshoot all
Starting /usr/local/sf/bin/sf_troubleshoot.pl... Please, be patient. This may take several
minutes. The troubleshoot option code specified is ALL. Troubleshooting information successfully
created at /var/common/xxxxxx.tar.gz
```

A cópia pesquisa defeitos arquivos

Centro da defesa e dispositivos Series-2

Incorpore este comando ao centro, ao centro de gerenciamento e aos dispositivos gerenciado Series-2 da defesa a fim copiar os arquivos da pesquisa de defeitos:

```
admin@3DSystem:~$ sudo scp troubleshoot_file_name username@destination_host:
 destination_folder
```

FirePOWER e dispositivos virtuais

Incorpore este comando em dispositivos de FirePOWER e em dispositivos gerenciado virtuais a fim copiar os arquivos da pesquisa de defeitos:

```
> system file secure-copy hostname username destination_folder troubleshoot_file
```

> **Note**: Neste exemplo, o **hostname** refere o nome ou o endereço IP de Um ou Mais Servidores Cisco ICM NT do host remoto do alvo, o **username** especifica o nome do usuário no host remoto, o **destination_folder** especifica o caminho de destino no host remoto, e o **troubleshoot_file** especifica o local pesquisa defeitos o arquivo para transferência.