

Agendador do Tidal Enterprise: Troubleshooting de Envio de SNMPTraps

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Solução](#)

[Verificação de configuração](#)

[Verifique se a interceptação foi enviada](#)

[Sistema de destino não está recebendo interceptação](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento fornece dicas básicas de solução de problemas para problemas com o Tidal Enterprise Scheduler (TES) enviando interceptações SNMP.

[Prerequisites](#)

[Requirements](#)

- Lista de sistemas de recebimento de interceptação (trap) e os números de porta que esses sistemas utilizam para receber interceptações (traps)
- Permissão/capacidade para editar o arquivo master.props do sistema TES ou criar um arquivo no diretório de configuração Master
- Permissão/capacidade de reiniciar o sistema TES após essa configuração
- Um sistema TES em funcionamento e um ou mais sistemas com a capacidade de receber armadilhas SNMP

[Componentes Utilizados](#)

As informações neste documento são baseadas no Tidal Master (Windows ou Unix).

[Conventions](#)

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.](#)

Solução

Verificação de configuração

Conclua estes passos:

1. Verifique os arquivos de configuração SNMP especificados no Tidal Enterprise Scheduler: Configurando o SNMP. Observe que apenas um dos dois métodos definidos nesse documento deve ser usado. Se ambos forem usados, resultados imprevisíveis podem ser causados.
2. Verifique se os arquivos de configuração foram lidos corretamente no mestre. No Mestre, selecione **Atividades > Configurar Agendador** no menu. Na guia Registro, defina o Log do Event Manager como **High Debug** e clique em **OK**. Observe o valor anterior para que ele possa ser redefinido posteriormente. Normalmente, é grave. Examine o arquivo de log mestre mais recente e procure este erro:
`Could not parse snmp configuration file: Content is not allowed in prolog.`
Isso indica que há um erro no arquivo `snmpconfig.xml`. Corrija isso e reinicie o Mestre. Quando o erro for eliminado, redefina o nível de log do Event Manager para o valor anterior.

Verifique se a interceptação foi enviada

Conclua estes passos para verificar se o Mestre tentou enviar a armadilha:

1. No Mestre, selecione **Atividades > Configurar Agendador** no menu.
2. Na guia Registro, defina o Log do Event Manager como **High Debug** e clique em **OK**. Observe o valor anterior para que ele possa ser redefinido posteriormente. Normalmente, é grave.
3. No arquivo de log Master, procure entradas semelhantes a estas (permitindo, é claro, a exclusividade do seu sistema):

```
enter: snmp handle(ActionSNMP: 9)
enter: snmp execute(ActionSNMP: 9)
try to send SNMP trap message
SNMP job trap is sent to host 'vlillico_4.tidalsoft.local'. Alert ID is '4'
SNMP trap message is sent.
SNMP trap is sent successfully. Snmp ID : 9
exit: snmp execute(ActionSNMP: 9)
Executed action Action: 9
```

Essas mensagens indicam que o Mestre enviou a armadilha. O destino incorreto nesta linha indica que o arquivo de configuração pode conter erros (consulte a seção [Verificação de configuração](#)):

```
No IP address accessible for SNMP manager, hostname = 'localhost'
```

4. Quando este teste estiver concluído, redefina o nível de log do Event Manager para seu valor anterior.

Sistema de destino não está recebendo interceptação

Se o sistema de destino não estiver recebendo armadilhas que foram verificadas como sendo enviadas usando o acima, isso deve ser verificado:

- Problemas de roteamento—Um "ping" ou "tracert" ("traceroute" no Unix) ao host de destino é concluído com êxito.
- Regras de firewall—as interceptações SNMP são enviadas com uma porta de destino 162 (a menos que sejam alteradas na configuração de TES SNMP listada acima) usando UDP. Verifique os firewalls locais (software) nos hosts Master e de recebimento, bem como os firewalls de nível de infraestrutura (hardware).

[Informações Relacionadas](#)

- [Suporte Técnico e Documentação - Cisco Systems](#)