

Tidal Enterprise Scheduler: Fehlerbehebung

Senden von SNMPTraps

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Lösung](#)

[Konfigurationsprüfung](#)

[Überprüfen Sie, ob Trap gesendet wurde.](#)

[Zielsystem empfängt Trap nicht](#)

[Zugehörige Informationen](#)

[Einführung](#)

Dieses Dokument enthält grundlegende Tipps zur Fehlerbehebung bei Problemen mit dem Senden von SNMP-Traps durch Tidal Enterprise Scheduler (TES).

[Voraussetzungen](#)

[Anforderungen](#)

- Liste der Trap Receiving-Systeme und der Portnummern, die diese Systeme zum Empfang von Traps verwenden
- Berechtigung/Möglichkeit zum Bearbeiten der Master.props-Datei des TES-Systems oder zum Erstellen einer Datei im Konfigurationsverzeichnis des Master
- Berechtigung/Möglichkeit zum Neustart des TES-Systems nach einer solchen Konfiguration
- Ein funktionierendes TES-System und ein oder mehrere Systeme, die SNMP-Traps empfangen können

[Verwendete Komponenten](#)

Die Informationen in diesem Dokument basieren auf Tidal Master (Windows oder Unix).

[Konventionen](#)

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Lösung

Konfigurationsprüfung

Gehen Sie wie folgt vor:

1. Überprüfen Sie die SNMP-Konfigurationsdateien, wie in Tidal Enterprise Scheduler festgelegt: SNMP konfigurieren. Beachten Sie, dass nur eine der beiden in diesem Dokument definierten Methoden verwendet werden sollte. Wenn beide verwendet werden, können unvorhersehbare Ergebnisse verursacht werden.
2. Überprüfen Sie, ob die Konfigurationsdateien korrekt in den Master eingelesen wurden. Wählen Sie im Master im Menü **Aktivitäten > Scheduler konfigurieren** aus. Legen Sie auf der Registerkarte Protokollierung für das Event Manager-Protokoll die Option **High Debug fest**, und klicken Sie auf **OK**. Beachten Sie den vorherigen Wert, damit er später zurückgesetzt werden kann. In der Regel handelt es sich um einen Schweregrad. Überprüfen Sie die neueste Master-Protokolldatei, und suchen Sie nach diesem Fehler:
`Could not parse snmp configuration file: Content is not allowed in prolog.`
Dies weist darauf hin, dass in der Datei snmpconfig.xml ein Fehler aufgetreten ist. Korrigieren Sie dies, und starten Sie den Master neu. Nachdem der Fehler behoben wurde, setzen Sie die Event Manager-Protokollstufe auf den vorherigen Wert zurück.

Überprüfen Sie, ob Trap gesendet wurde.

Gehen Sie wie folgt vor, um zu überprüfen, ob der Master versucht hat, das Trap zu senden:

1. Wählen Sie im Master im Menü **Aktivitäten > Scheduler konfigurieren** aus.
2. Legen Sie auf der Registerkarte Protokollierung für das Event Manager-Protokoll die Option **High Debug fest**, und klicken Sie auf **OK**. Beachten Sie den vorherigen Wert, damit er später zurückgesetzt werden kann. In der Regel handelt es sich um einen Schweregrad.
3. Suchen Sie in der Master-Protokolldatei nach Einträgen, die diesen ähneln (was natürlich die Einzigartigkeit Ihres Systems zulässt):

```
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
```

Diese Meldungen weisen darauf hin, dass der Master das Trap gesendet hat. Falsches Ziel in dieser Zeile weist darauf hin, dass die Konfigurationsdatei darin möglicherweise Fehler enthalten kann (siehe Abschnitt [Konfigurationsprüfung](#)):

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

4. Setzen Sie nach Abschluss dieses Tests die Ereignismanager-Protokollstufe auf den vorherigen Wert zurück.

Zielsystem empfängt Trap nicht

Wenn das Zielsystem keine Traps empfängt, für die überprüft wurde, dass sie mit dem oben genannten Verfahren gesendet wurden, muss Folgendes überprüft werden:

- Routing-Probleme - Wird ein "Ping" oder "tracert" (Traceroute auf Unix) zum Ziel-Host erfolgreich abgeschlossen.
- Firewall-Regeln - SNMP-Traps werden mit UDP mit einem Zielport von 162 gesendet (sofern in der oben aufgeführten TES-SNMP-Konfiguration nicht geändert wurde). Überprüfen Sie sowohl lokale (Software-) Firewalls auf Master- und empfangenden Hosts als auch Hardware-Firewalls auf Infrastrukturebene.

Zugehörige Informationen

- [Technischer Support und Dokumentation - Cisco Systems](#)