Tidal Enterprise Scheduler: Risoluzione dei problemi relativi all'invio di SNMPrap

Sommario

Introduzione

In questo documento vengono forniti suggerimenti di base per la risoluzione dei problemi relativi all'invio di trap SNMP da parte di Tidal Enterprise Scheduler (TES).

Prerequisiti

Requisiti

- Elenco dei sistemi di ricezione delle trap e numeri di porta utilizzati da tali sistemi per ricevere le trap
- Autorizzazione/capacità di modificare il file master.props del sistema TES o di creare un file nella directory di configurazione del sistema TES
- Autorizzazione/possibilità di riavviare il sistema TES dopo aver eseguito una configurazione di questo tipo
- Un sistema TES funzionante e uno o più sistemi in grado di ricevere trap SNMP

Componenti usati

Le informazioni fornite in questo documento si basano su Tidal Master (Windows o Unix).

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Soluzione

Controllo configurazione

Attenersi alla seguente procedura:

1. Controllare i file di configurazione SNMP come specificato in Tidal Enterprise Scheduler: Configurazione di SNMP. Si noti che deve essere utilizzato solo uno dei due metodi definiti in tale documento. Se vengono utilizzati entrambi, è possibile che si verifichino risultati imprevedibili.
2. Verificare che i file di configurazione siano stati letti correttamente nel master.Nel Master, selezionare **Attività > Configura scheduler** dal menu.Nella scheda Log, impostare il registro del Gestore eventi su **High Debug** e fare clic su **OK**. Annotare il valore precedente in modo da poterlo reimpostare in seguito. In genere è grave.Esaminare il file di log master più recente e individuare l'errore seguente:
   ```
   Could not parse snmp configuration file: Content is not allowed in prolog.
   ```
   Ciò indica la presenza di un errore nel file snmpconfig.xml.Correggere e riavviare il master.Quando l'errore non viene più visualizzato, ripristinare il livello del registro del Gestore eventi sul valore precedente.

Verifica Dell'Invio Della Trap

Per verificare che il dispositivo master abbia tentato di inviare la trap, completare la procedura seguente:

1. Nel Master, selezionare **Attività > Configura scheduler** dal menu.
2. Nella scheda Log, impostare il registro del Gestore eventi su **High Debug** e fare clic su **OK**. Annotare il valore precedente in modo da poterlo reimpostare in seguito. In genere è grave.
3. Nel file di registro master cercare le voci simili a quelle seguenti (tenendo conto dell'univocità del 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
   ```
   Questi messaggi indicano che il Master ha inviato la trap.Una destinazione errata in questa riga indica che il file di configurazione potrebbe contenere errori (vedere la sezione Controllo configurazione):
   ```
   No IP address accessable for SNMP manager, hostname = 'localhost'
   ```
4. Al termine del test, reimpostare il livello del registro del Gestore eventi sul valore precedente.

Sistema di destinazione che non riceve la trap

Se il sistema di destinazione non riceve trap di cui è stata verificata l'invio mediante le procedure di cui sopra, verificare quanto segue:

- Problemi di routing - Il comando "ping" o "traceroute" ("traceroute" su Unix) viene eseguito

correttamente sull'host di destinazione.
- Regole del firewall: le trap SNMP vengono inviate con una porta di destinazione di 162 (a meno che non vengano modificate nella configurazione TES SNMP indicata in precedenza) utilizzando UDP. Controllare i firewall locali (software) sugli host master e di ricezione e i firewall a livello di infrastruttura (hardware).

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems