Tidal Enterprise Scheduler: Problemen oplossen bij verzenden van SNMPTraps

Inhoud

Inleiding

Dit document bevat basistips voor het oplossen van problemen bij Tidal Enterprise Scheduler (TES) bij het verzenden van SNMP-traps.

Voorwaarden

Vereisten

- Lijst van vangsystemen en de havennummers die deze systemen gebruiken om vallen te ontvangen
- Toestemming/mogelijkheid om het Master.props-bestand van het TES-systeem te bewerken of een bestand in de directory van de Master's Config te maken
- Toestemming/mogelijkheid om het TES-systeem opnieuw op te starten nadat een dergelijke configuratie is uitgevoerd
- Een functionerend TES-systeem en een of meer systemen met de mogelijkheid om SNMP-vallen te ontvangen

Gebruikte componenten

De informatie in dit document is gebaseerd op Tidal Master (Windows of Unix).

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor

meer informatie over documentconventies.

Oplossing

Configuratie-controle

Voer de volgende stappen uit:

1. Controleer de SNMP-configuratiebestanden zoals gespecificeerd in Tidal Enterprise Scheduler: SNMP configureren. Er dient slechts één van de twee in dat document omschreven methoden te worden gebruikt. Als beide worden gebruikt, kunnen onvoorspelbare resultaten worden veroorzaakt.
2. Controleer dat de configuratiebestanden correct in de Master gelezen zijn.Selecteer in de Master de optie **Activiteiten > Scheduler instellen** in het menu.Stel in het tabblad Logging het logbestand van Event Manager in op **High Debug** en klik vervolgens op **OK**. Let op de vorige waarde zodat deze later opnieuw kan worden ingesteld. Meestal is het ernstig.Onderzoek het meest recente Masterlogbestand, en kijk naar deze fout:
   ```
   Could not parse snmp configuration file: Content is not allowed in prolog.
   ```
   Dit betekent dat er een fout is in het bestand snmpenig.xml.Corrigeer dit en start de Master opnieuw.Nadat de fout is gegaan, stelt u het logniveau van Event Manager opnieuw in op de vorige waarde.

Controleer of de trap is verzonden

Voltooi deze stappen om te verifiëren dat de kapitein de val probeerde te verzenden:

1. Selecteer in de Master de optie **Activiteiten > Scheduler instellen** in het menu.
2. Stel in het tabblad Logging het logbestand van Event Manager in op **High Debug** en klik vervolgens op **OK**. Let op de vorige waarde zodat deze later opnieuw kan worden ingesteld. Meestal is het ernstig.
3. In het logbestand van de Master, zoek dan naar soortgelijke items (waarbij u uiteraard de eenheid van uw systeem kunt waarborgen):
   ```
   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
   ```
   Deze berichten geven aan dat de Meester de val wel heeft gestuurd.Onjuiste bestemming in deze regel geeft aan dat het configuratiebestand fouten in het bestand kan bevatten (zie het gedeelte Configuratie controleren):
   ```
   No IP address accessable for SNMP manager, hostname = 'localhost'
   ```
4. Nadat deze test is voltooid, stelt u het niveau van het logboek van Event Manager in op de vorige waarde.

Besturingssysteem zonder trap

Indien het doelsysteem geen vallen ontvangt die zijn geverifieerd dat zij aan de hand van het

bovenstaande zijn verzonden, moet dit worden gecontroleerd:

- Routing kwesties-Doet een ‘ping’ of ‘traceroute’ (‘traceroute’ op Unix) naar de doelhost volledig.
- Firewallregels-SNMP-trap worden verzonden met een bestemmingspoorts van 162 (tenzij gewijzigd in de hierboven genoemde TES SNMP-configuratie) door gebruik van UDP. Controleer zowel lokale (software) firewalls op Master- en ontvangsthosts als op infrastructuur-niveau (hardware) firewalls.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems