Gestire gli avvisi SNMP

SANtricity 11.7

NetApp
February 12, 2024

Sommario

Gestire gli avvisi SNMP

Configurare gli avvisi SNMP

Per configurare gli avvisi SNMP (Simple Network Management Protocol), è necessario identificare almeno un server in cui il monitor degli eventi dell'array di storage può inviare trap SNMP. La configurazione richiede un nome di comunità o un nome utente e un indirizzo IP per il server.

Prima di iniziare

- Un server di rete deve essere configurato con un'applicazione di servizio SNMP. È necessario l'indirizzo di rete di questo server (un indirizzo IPv4 o IPv6), in modo che il monitor eventi possa inviare messaggi trap a tale indirizzo. È possibile utilizzare più di un server (sono consentiti fino a 10 server).
- Il file MIB (Management Information base) è stato copiato e compilato sul server con l'applicazione del servizio SNMP. Questo file MIB definisce i dati monitorati e gestiti.

  Se non si dispone del file MIB, è possibile ottenerlo dal sito NetApp Support:

  - Passare a. "Supporto NetApp".
  - Fare clic sulla scheda **Downloads**, quindi selezionare **Downloads**.
  - Fare clic su **Software controller OS SANtricity e-Series**.
  - Selezionare **Scarica ultima release**.
  - Effettuare l'accesso.
  - Accettare la dichiarazione di attenzione e il contratto di licenza.
  - Scorrere verso il basso fino a visualizzare il file MIB per il tipo di controller in uso, quindi fare clic sul collegamento per scaricare il file.

A proposito di questa attività

Questa attività descrive come identificare il server SNMP per le destinazioni trap, quindi verificare la configurazione.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Al primo setup, nella scheda SNMP viene visualizzato "Configure Communities/Users" (Configura community/utenti).

3. Selezionare **Configura community/utenti**.

   Viene visualizzata la finestra di dialogo Select SNMP version (Seleziona versione SNMP).

4. Selezionare la versione SNMP per gli avvisi, **SNMPv2c** o **SNMPv3**.

   A seconda della selezione effettuata, viene visualizzata la finestra di dialogo Configura comunità o Configura utenti SNMPv3.

5. Seguire le istruzioni appropriate per SNMPv2c (community) o SNMPv3 (utenti):

- **SNMPv2c (community)** — nella finestra di dialogo Configura community, immettere una o più stringhe di community per i server di rete. Un nome di comunità è una stringa che identifica un set noto di stazioni di gestione e viene in genere creato da un amministratore di rete. È costituito solo da caratteri ASCII stampabili. Puoi aggiungere fino a 256 community. Al termine, fare clic su **Save** (Salva).
- **SNMPv3 (utenti)** — nella finestra di dialogo Configure SNMPv3 Users (Configura utenti SNMPv3), fare clic su **Add** (Aggiungi), quindi immettere le seguenti informazioni:
  - **Nome utente** — immettere un nome per identificare l'utente, che può contenere fino a 31 caratteri.
  - **ID motore** — selezionare l'ID motore, utilizzato per generare chiavi di autenticazione e crittografia per i messaggi, che deve essere univoco nel dominio amministrativo. Nella maggior parte dei casi, selezionare **locale**. Se si dispone di una configurazione non standard, selezionare **Custom**; viene visualizzato un altro campo in cui inserire l'ID del motore autorevole come stringa esadecimale, con un numero pari di caratteri compreso tra 10 e 32 caratteri.
  - **Authentication credentials** — selezionare un protocollo di autenticazione che garantisca l'identità degli utenti. Quindi, inserire una password di autenticazione, necessaria quando si imposta o si modifica il protocollo di autenticazione. La password deve contenere da 8 a 128 caratteri.
  - **Privacy credentials** — selezionare un protocollo per la privacy utilizzato per crittografare il contenuto dei messaggi. Quindi, inserire una password per la privacy, necessaria quando il protocollo per la privacy viene impostato o modificato. La password deve contenere da 8 a 128 caratteri. Al termine, fare clic su **Aggiungi**, quindi su **Chiudi**.

6. Dalla pagina Avvisi con la scheda SNMP selezionata, fare clic su **Aggiungi destinazioni trap**.

   Viene visualizzata la finestra di dialogo Add Trap Destinations (Aggiungi destinazioni trap).

7. Immettere una o più destinazioni trap, selezionare i nomi di comunità o utenti associati, quindi fare clic su **Aggiungi**.
   - **Destinazione trap** — immettere un indirizzo IPv4 o IPv6 del server che esegue un servizio SNMP.
   - **Nome di comunità o Nome utente** — dal menu a discesa, selezionare il nome di comunità (SNMPv2c) o il nome utente (SNMPv3) per questa destinazione trap. (Se ne è stata definita una sola, il nome viene già visualizzato in questo campo).
   - **Send Authentication Failure Trap** — selezionare questa opzione (la casella di controllo) se si desidera avvisare la destinazione trap ogni volta che una richiesta SNMP viene rifiutata a causa di un nome di comunità o di un nome utente non riconosciuto. Dopo aver fatto clic su **Aggiungi**, le destinazioni trap e i nomi associati vengono visualizzati nella scheda **SNMP** della pagina **Avvisi**.
8. Per assicurarsi che un trap sia valido, selezionare una destinazione trap dalla tabella, quindi fare clic su **Test Trap Destination** (destinazione trap test) per inviare un trap di test all'indirizzo configurato.

Risultati

Il monitor degli eventi invia trap SNMP ai server ogni volta che si verifica un evento verificabile.

Aggiungere destinazioni trap per gli avvisi SNMP

È possibile aggiungere fino a 10 server per l'invio di trap SNMP.

Prima di iniziare

- Il server di rete che si desidera aggiungere deve essere configurato con un'applicazione di servizio SNMP. È necessario l'indirizzo di rete di questo server (un indirizzo IPv4 o IPv6), in modo che il monitor eventi possa inviare messaggi trap a tale indirizzo. È possibile utilizzare più di un server (sono consentiti fino a 10 server).

- Il file MIB (Management Information base) è stato copiato e compilato sul server con l'applicazione del servizio SNMP. Questo file MIB definisce i dati monitorati e gestiti.

  Se non si dispone del file MIB, è possibile ottenerlo dal sito NetApp Support:

  - Passare a. "Supporto NetApp".
  - Fare clic su **Downloads**, quindi selezionare **Downloads**.
  - Fare clic su **Software controller OS SANtricity e-Series**.
  - Selezionare **Scarica ultima release**.
  - Effettuare l'accesso.
  - Accettare la dichiarazione di attenzione e il contratto di licenza.
  - Scorrere verso il basso fino a visualizzare il file MIB per il tipo di controller in uso, quindi fare clic sul collegamento per scaricare il file.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Le destinazioni trap attualmente definite vengono visualizzate nella tabella.

3. Selezionare **Add Trap Desinations** (Aggiungi Desination trap).

   Viene visualizzata la finestra di dialogo Add Trap Destinations (Aggiungi destinazioni trap).

4. Immettere una o più destinazioni trap, selezionare i nomi di comunità o utenti associati, quindi fare clic su **Aggiungi**.
   - **Destinazione trap** — immettere un indirizzo IPv4 o IPv6 del server che esegue un servizio SNMP.
   - **Nome di comunità o Nome utente** — dal menu a discesa, selezionare il nome di comunità (SNMPv2c) o il nome utente (SNMPv3) per questa destinazione trap. (Se ne è stata definita una sola, il nome viene già visualizzato in questo campo).
   - **Send Authentication Failure Trap** — selezionare questa opzione (la casella di controllo) se si desidera avvisare la destinazione trap ogni volta che una richiesta SNMP viene rifiutata a causa di un nome di comunità o di un nome utente non riconosciuto. Dopo aver fatto clic su **Aggiungi**, nella tabella vengono visualizzate le destinazioni trap e i nomi di comunità o utenti associati.
5. Per assicurarsi che un trap sia valido, selezionare una destinazione trap dalla tabella, quindi fare clic su **Test Trap Destination** (destinazione trap test) per inviare un trap di test all'indirizzo configurato.

Risultati

Il monitor degli eventi invia trap SNMP ai server ogni volta che si verifica un evento verificabile.

Configurare le variabili SNMP MIB

Per gli avvisi SNMP, è possibile configurare facoltativamente le variabili MIB (Management Information base) che vengono visualizzate nei trap SNMP. Queste variabili possono restituire il nome dell'array di storage, la posizione dell'array e una persona di contatto.

Prima di iniziare

Il file MIB deve essere copiato e compilato sul server con l'applicazione di servizio SNMP.

Se non si dispone di un file MIB, è possibile ottenerlo come segue:

- Passare a. "Supporto NetApp".
- Fare clic su **Downloads**, quindi selezionare **Downloads**.
- Fare clic su **Software controller OS SANtricity e-Series**.
- Selezionare **Scarica ultima release**.
- Effettuare l'accesso.
- Accettare la dichiarazione di attenzione e il contratto di licenza.
- Scorrere verso il basso fino a visualizzare il file MIB per il tipo di controller in uso, quindi fare clic sul collegamento per scaricare il file.

A proposito di questa attività

Questa attività descrive come definire le variabili MIB per i trap SNMP. Queste variabili possono restituire i seguenti valori in risposta a SNMP GetRequests:

- `sysName` (nome dell'array di storage)
- `sysLocation` (posizione dello storage array)
- `sysContact` (nome di un amministratore)

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.
3. Selezionare **Configure SNMP MIB variables** (Configura variabili SNMP MIB).

   Viene visualizzata la finestra di dialogo Configura variabili MIB SNMP.

4. Immettere uno o più dei seguenti valori, quindi fare clic su **Save** (Salva).
   - **Name** — il valore per la variabile MIB `sysName`. Ad esempio, inserire un nome per l'array di storage.
   - **Location** — il valore della variabile MIB `sysLocation`. Ad esempio, inserire una posizione dell'array di storage.
   - **Contatto** — il valore della variabile MIB `sysContact`. Ad esempio, inserire un amministratore responsabile dello storage array.

Risultati

Questi valori vengono visualizzati nei messaggi trap SNMP per gli avvisi degli array di storage.

Modificare le community per le trap SNMPv2c

È possibile modificare i nomi di comunità per i trap SNMPv2c.

Prima di iniziare

È necessario creare un nome di comunità.

Fasi

1. Selezionare **impostazione › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Le destinazioni trap e i nomi di comunità vengono visualizzati nella tabella.

3. Selezionare **Configura community**.
4. Immettere il nuovo nome di comunità, quindi fare clic su **Salva**. I nomi di comunità possono essere costituiti solo da caratteri ASCII stampabili.

Risultati

La scheda SNMP della pagina Avvisi visualizza il nome di comunità aggiornato.

Modificare le impostazioni utente per i trap SNMPv3

È possibile modificare le definizioni utente per i trap SNMPv3.

Prima di iniziare

È necessario creare un utente per la trap SNMPv3.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Le destinazioni trap e i nomi utente vengono visualizzati nella tabella.

3. Per modificare una definizione utente, selezionare l'utente nella tabella, quindi fare clic su **Configura utenti**.
4. Nella finestra di dialogo, fare clic su **Visualizza/Modifica impostazioni**.
5. Modificare le seguenti informazioni:
   - **Nome utente** — consente di modificare il nome che identifica l'utente, che può contenere fino a 31 caratteri.
   - **ID motore** — selezionare l'ID motore, utilizzato per generare chiavi di autenticazione e crittografia per i messaggi, che deve essere univoco nel dominio amministrativo. Nella maggior parte dei casi, selezionare **locale**. Se si dispone di una configurazione non standard, selezionare **Custom**; viene visualizzato un altro campo in cui inserire l'ID del motore autorevole come stringa esadecimale, con un numero pari di caratteri compreso tra 10 e 32 caratteri.
   - **Authentication credentials** — selezionare un protocollo di autenticazione che garantisca l'identità degli utenti. Quindi, inserire una password di autenticazione, necessaria quando si imposta o si modifica il protocollo di autenticazione. La password deve contenere da 8 a 128 caratteri.
   - **Privacy credentials** — selezionare un protocollo per la privacy utilizzato per crittografare il contenuto dei messaggi. Quindi, inserire una password per la privacy, necessaria quando il protocollo per la privacy viene impostato o modificato. La password deve contenere da 8 a 128 caratteri.

Risultati

La scheda SNMP della pagina Avvisi visualizza le impostazioni aggiornate.

Aggiungere community per le trap SNMPv2c

È possibile aggiungere fino a 256 nomi di comunità per le trap SNMPv2c.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Le destinazioni trap e i nomi di comunità vengono visualizzati nella tabella.

3. Selezionare **Configura community**.

   Viene visualizzata la finestra di dialogo Configura comunità.

4. Selezionare **Aggiungi un'altra community**.
5. Immettere il nuovo nome di comunità, quindi fare clic su **Salva**.

Risultati

Il nuovo nome di comunità viene visualizzato nella scheda SNMP della pagina Avvisi.

Aggiungere utenti per le trap SNMPv3

È possibile aggiungere fino a 256 utenti per i trap SNMPv3.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Le destinazioni trap e i nomi utente vengono visualizzati nella tabella.

3. Selezionare **Configure Users** (Configura utenti).

   Viene visualizzata la finestra di dialogo Configure SNMPv3 Users (Configura utenti SNMPv3).

4. Selezionare **Aggiungi**.
5. Inserire le seguenti informazioni, quindi fare clic su **Aggiungi**.
   - **Nome utente** — immettere un nome per identificare l'utente, che può contenere fino a 31 caratteri.
   - **ID motore** — selezionare l'ID motore, utilizzato per generare chiavi di autenticazione e crittografia per i messaggi, che deve essere univoco nel dominio amministrativo. Nella maggior parte dei casi, selezionare **locale**. Se si dispone di una configurazione non standard, selezionare **Custom**; viene visualizzato un altro campo in cui inserire l'ID del motore autorevole come stringa esadecimale, con un numero pari di caratteri compreso tra 10 e 32 caratteri.
   - **Authentication credentials** — selezionare un protocollo di autenticazione che garantisca l'identità degli utenti. Quindi, inserire una password di autenticazione, necessaria quando si imposta o si modifica il protocollo di autenticazione. La password deve contenere da 8 a 128 caratteri.
   - **Privacy credentials** — selezionare un protocollo per la privacy utilizzato per crittografare il contenuto dei messaggi. Quindi, inserire una password per la privacy, necessaria quando il protocollo per la privacy viene impostato o modificato. La password deve contenere da 8 a 128 caratteri.

Rimuovere le community per le trap SNMPv2c

È possibile rimuovere un nome di comunità per i trap SNMPv2c.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Le destinazioni trap e i nomi di comunità vengono visualizzati nella pagina **Avvisi**.

3. Selezionare **Configura community**.

   Viene visualizzata la finestra di dialogo Configura comunità.

4. Selezionare il nome della community che si desidera eliminare, quindi fare clic sull'icona **Rimuovi** (X) all'estrema destra.

   Se le destinazioni trap sono associate a questo nome di comunità, la finestra di dialogo Conferma rimozione comunità mostra gli indirizzi di destinazione trap interessati.

5. Confermare l'operazione, quindi fare clic su **Rimuovi**.

Risultati

Il nome di comunità e la destinazione trap associata vengono rimossi dalla pagina Avvisi.

Rimuovere gli utenti per i trap SNMPv3

È possibile rimuovere un utente per i trap SNMPv3.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Le destinazioni trap e i nomi utente vengono visualizzati nella pagina Avvisi.

3. Selezionare **Configure Users** (Configura utenti).

   Viene visualizzata la finestra di dialogo Configure SNMPv3 Users (Configura utenti SNMPv3).

4. Selezionare il nome utente che si desidera eliminare, quindi fare clic su **Delete** (Elimina).
5. Confermare l'operazione, quindi fare clic su **Delete** (Elimina).

Risultati

Il nome utente e la destinazione trap associata vengono rimossi dalla pagina Avvisi.

Eliminare le destinazioni trap

È possibile eliminare un indirizzo di destinazione trap in modo che il monitor eventi dell'array di storage non invii più trap SNMP a tale indirizzo.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Gli indirizzi di destinazione trap vengono visualizzati nella tabella.

3. Selezionare una destinazione trap, quindi fare clic su **Delete** (Elimina) in alto a destra nella pagina.
4. Confermare l'operazione, quindi fare clic su **Delete** (Elimina).

   L'indirizzo di destinazione non viene più visualizzato nella pagina Avvisi.

Risultati

La destinazione dei trap cancellati non riceve più trap SNMP dal monitor degli eventi dell'array di storage.