Configurazione dell'autenticazione NTP su Secure Network Analytics

Sommario

- Introduzione
- Prerequisiti
  - Requisiti
  - Componenti usati
- Configurazione
  - Requisiti di configurazione NTP
  - Dettagli valore chiave
  - Autenticazione NTP di Configuration SNA Manager
    - Apri impostazioni server NTP
    - Aggiungi server NTP
    - Aggiungi autenticazione
- Verifica
    - Conferma autenticazione
- Risoluzione dei problemi
  - Conferma conteggio byte
  - Conferma utilizzo caratteri

Introduzione

In questo documento viene descritto come configurare l'Secure Network Analytics (SNA)accessorio in modo che autentichi la connessione al server NTP configurato.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione di Cisco Secure Network Analytics
- Protocollo NTP (Network Time Protocol)

Componenti usati

La versione dell'appliance Cisco Secure Network Analytics Manager utilizzata per questo documento è 7.4.2.

questo processo è valido per tutti i tipi di appliance Cisco Secure Network Analytics.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Requisiti di configurazione NTP

I valori utilizzati per l'autenticazione della comunicazione NTP devono soddisfare i seguenti requisiti:

- Il valore dell'ID chiave deve essere minore o uguale a 65535
- La convalida della chiave è SHA1
- Il valore della chiave non deve superare i 32 caratteri alfanumerici stampabili (ASCII): 0-9, A-Z, a-z e simboli (ad eccezione di #)

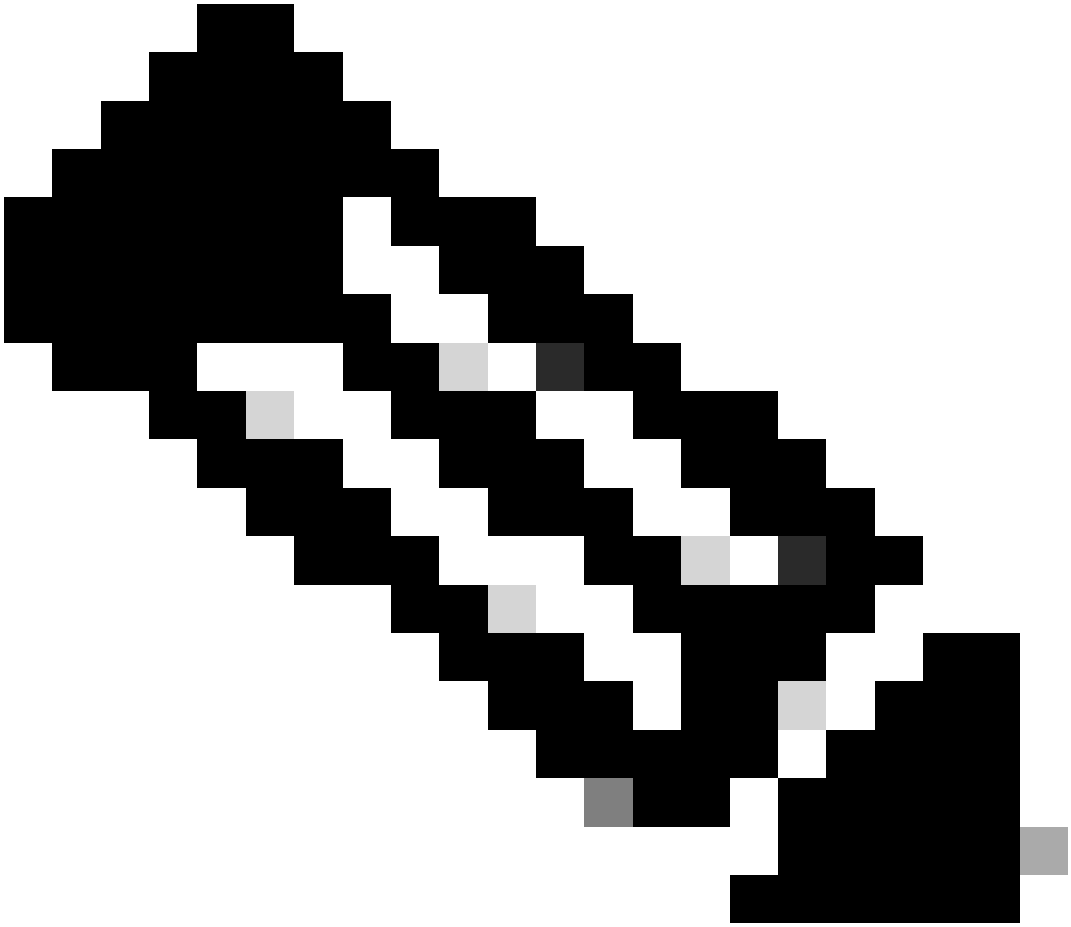
Dettagli valore chiave

NTP presume che i valori di chiave più lunghi di 20 byte siano in formato ESADECIMALE.

La lunghezza massima del valore della chiave è di 64 byte, pertanto una chiave deesadecimata non può superare i 32 byte.

Fare riferimento alla tabella, ad esempio i valori delle chiavi per il server NTP e l'appliance Secure Network Analytics.

Byte chiave	Configurazione valore chiave server NTP	Configurazione chiave di anali
Meno di 20 byte	Lan1cope!	Lan1cope!
Tra 20 byte e 32 byte	4C616E31636F7065214C616E31636F7065214C616E31636F7065214C616E3163	Lan1cope!Lan



Nota: I valori utilizzati nella tabella sono solo esempi e non sono consigliati per l'utilizzo nell'ambiente in uso

Autenticazione NTP di Configuration SNA Manager

Apri impostazioni server NTP

Accedere a **SNA Manager** e aprire le **NTP Server** impostazioni.

1. Dal menu principale, selezionareConfigure > GLOBAL Central Management.
2. Nella scheda Inventario fare clic sull'icona ...(Ellipsis) dell'accessorio.
3. SelezionareEdit Appliance Configuration.
4. Selezionare laNetwork Servicesscheda.

Aggiungi server NTP

Utilizzare queste istruzioni per aggiungere un server NTP alla configurazione dell'accessorio

selezionata, se necessario.

1. Nella sezione Server NTP fare clic suAdd New.
2. Nel campo,NTP Serversfare clic sulla freccia dell'elenco a discesa. Selezionare un server NTP dall'elenco.
3. Immettere il nome o l'indirizzo IP del server.
4. Fare clic su .Add
5. Fare clic su .Apply Settings
6. Accettare le istruzioni visualizzate. L'accessorio verrà riavviato automaticamente.

Aggiungi autenticazione

Utilizzare queste istruzioni per autenticare la connessione al server NTP selezionato.

Preparazione: Verificare di disporre dell'ID e del valore della chiave del server NTP.

1. Nella sezione Server NTP, fare clic sull'icona... (Ellipsis) del server NTP.
2. SelezionareAuthenticate Connection.
3. Immettere l'ID e il valore della chiave.
4. Fare clic su Applica autenticazione.
5. Fare clic su .Apply Settings
6. Accettare le istruzioni visualizzate. L'accessorio verrà riavviato automaticamente.

Verifica

Conferma autenticazione

Se si aggiunge l'autenticazione a un server, l'icona a forma di chiave indica che l'autenticazione è configurata. Controllare il registro di controllo per verificare che l'autenticazione sia stata eseguita correttamente.

1. Dal menu principale, selezionareConfigure > GLOBAL Central Management.
2. Nella scheda Inventario fare clic sull'icona ...(Ellipsis) dell'accessorio.
3. SelezionareSupport.
4. Selezionare laAudit Logsscheda.
5. Nel campo,Categoryselezionare Management.
6. Fare clic su .Search
7. Confermare che lo stato della comunicazione NTP e le modifiche all'ora di sistema siano corrette. (Controllare la colonna Operazione riuscita per verificare che l'evento sia visualizzato come Sì).

Risoluzione dei problemi

Conferma conteggio byte

È possibile utilizzare una shell su un dispositivo Linux per verificare il numero di byte dei valori

chiave.

I valori chiave negli esempi derivano dalla tabella riportata nella sezione Lunghezza valore chiave di questo documento.

Eseguire il comando per `echo -n '{key_value}' | wc -c`visualizzare il conteggio dei byte che sostituisce {key_value} con il valore della chiave che si desidera utilizzare.

```
742smc:~# echo -n 'Lan1cope!' | wc -c
9
742smc:~# echo -n 'Lan1cope!Lan1cope!Lan1cope!Lan1c' | wc -c
32
742smc:~# echo -n '4C616E31636F7065214C616E31636F7065214C616E31636F7065214C616E3163' | wc -c
64
742smc:~#
```

L'output nelle righe 2, 4 e 6 mostra che i conteggi dei byte dei valori chiave sono rispettivamente 9, 32 e 64.

Conferma utilizzo caratteri

Se il numero di byte è inferiore a 20, accertarsi di utilizzare i caratteri stampabili ASCII come indicato nei requisiti di configurazione NTP.

È possibile eseguire il comando per`echo '{key_value}' | xxd -r -p && echo`convertire i valori HEX in ASCII sostituendo {key_value} con il valore della chiave che si desidera utilizzare.

```
742smc:~# echo '4C616E31636F7065214C616E31636F7065214C616E31636F7065214C616E3163' | xxd -r -p && echo
Lan1cope!Lan1cope!Lan1cope!Lan1c
742smc:~#
```

Informazioni su questa traduzione
Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).