Konfigurieren der NTP-Authentifizierung für sichere Netzwerkanalysen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Secure Network Analytics (SNA) Appliance so konfigurieren, dass die Verbindung zum konfigurierten NTP-Server authentifiziert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Administration der Cisco Secure Network Analytics Appliance
- Network Time Protocol (NTP)

Verwendete Komponenten

Die für dieses Dokument verwendete Cisco Secure Network Analytics Manager-Appliance ist Version 7.4.2.

Dieser Prozess gilt für alle Cisco Secure Network Analytics-Appliance-Typen.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

NTP-Konfigurationsanforderungen

Die für die Authentifizierung der NTP-Kommunikation verwendeten Werte müssen folgende Anforderungen erfüllen:

- Der Wert für die Schlüssel-ID muss kleiner oder gleich 65535 sein.
- Die Schlüsselvalidierung ist SHA1.
- Der Schlüsselwert darf nicht länger als 32 druckbare alphanumerische Zeichen (ASCII) sein: 0-9, A-Z, a-z und Symbole (außer #).

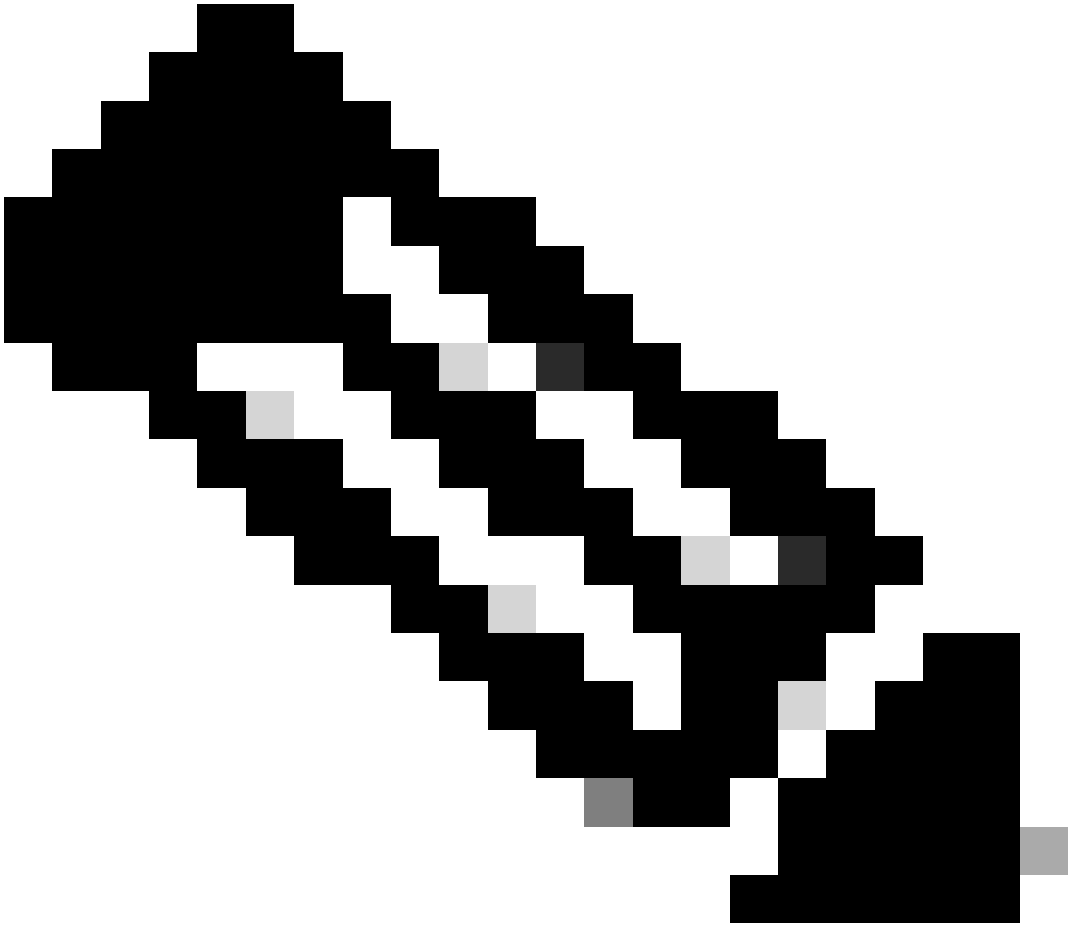
Wichtigste Details

Beim NTP wird davon ausgegangen, dass Schlüsselwerte, die länger als 20 Byte sind, als Hexadezimalwert angenommen werden.

Die maximale Länge des Schlüsselwerts beträgt 64 Byte, sodass ein enthexter Schlüssel nicht länger als 32 Byte sein darf.

In der Tabelle finden Sie Beispiele für die Schlüsselwerte für den NTP-Server und die Secure Network Analytics-Appliance.

Schlüsselbyte	Konfiguration des NTP-Serverschlüssels	Secure Schlüs
Weniger als 20 Byte	Lan1cope!	Lan1cc
Zwischen 20 Byte und 32 Byte	4C616E31636F7065214C616E31636F7065214C616E31636F7065214C616E3163	Lan1cc



Hinweis: Die in der Tabelle verwendeten Werte dienen lediglich als Beispiele und sind kein empfohlener Wert für die Umgebung.

Konfiguration SNA Manager NTP-Authentifizierung

NTP-Servereinstellungen öffnen

Melden Sie sich bei an, **SNA Manager** und öffnen Sie die **NTP Server** Einstellungen.

- Wählen Sie im Hauptmenü die Option Configure > GLOBAL Central Management.
- Klicken Sie auf der Registerkarte Inventar auf das ... (Ellipsis) Symbol für die Appliance.

- Auswählen Edit Appliance Configuration.
- Wählen Sie die Network Services Registerkarte.

NTP-Server hinzufügen

Verwenden Sie diese Anweisungen, um der ausgewählten Appliance-Konfiguration bei Bedarf einen NTP-Server hinzuzufügen.

- Klicken Sie im Abschnitt "NTP-Server" auf Add New.
- Klicken Sie im NTP Servers Feld auf den Dropdown-Pfeil. Wählen Sie einen NTP-Server aus der Liste aus.
- Geben Sie den Servernamen oder die IP-Adresse ein.
- Klicken Sie auf .Add
- Klicken Sie auf .Apply Settings
- Akzeptieren Sie die Aufforderungen auf dem Bildschirm. Die Appliance wird automatisch neu gestartet.

Authentifizierung hinzufügen

Verwenden Sie diese Anweisungen, um die Verbindung zum ausgewählten NTP-Server zu authentifizieren.

Vorbereitung: Stellen Sie sicher, dass Sie die Schlüssel-ID und den Schlüsselwert für den NTP-Server haben.

- Klicken Sie im Abschnitt "NTP-Server" auf das ... (Ellipsis) Symbol für den NTP-Server.
- Auswählen Authenticate Connection.
- Geben Sie die Schlüssel-ID und den Schlüsselwert ein.
- Klicken Sie auf Authentifizierung anwenden.
- Klicken Sie auf .Apply Settings
- Akzeptieren Sie die Aufforderungen auf dem Bildschirm. Die Appliance wird automatisch neu gestartet.

Überprüfung

Authentifizierung bestätigen

Wenn Sie einem Server eine Authentifizierung hinzufügen, zeigt das Schlüsselsymbol an, dass die Authentifizierung konfiguriert ist. Überprüfen Sie das Überwachungsprotokoll, um sicherzustellen, dass die Authentifizierung erfolgreich ist.

- Wählen Sie im Hauptmenü die Option Configure > GLOBAL Central Management.
- Klicken Sie auf der Registerkarte Inventar auf das ... (Ellipsis) Symbol für die Appliance.
- Auswählen Support.
- Wählen Sie die Audit Logs Registerkarte.
- Wählen Sie im Category Feld die Option Management aus.
- Klicken Sie auf .Search
- Bestätigen Sie, dass der NTP-Kommunikationsstatus und die Änderungen der Systemzeit als erfolgreich angezeigt werden. (Überprüfen Sie in der Spalte Erfolg, ob das Ereignis als Ja angezeigt wird.)

Fehlerbehebung

Byteanzahl bestätigen

Sie können eine Shell auf einem Linux-Gerät verwenden, um die Byteanzahl der Schlüsselwerte zu testen.

Die Schlüsselwerte in den Beispielen stammen aus der Tabelle im Abschnitt Länge der Schlüsselwerte in diesem Dokument.

Führen Sie den echo -n '{key_value}' | wc -c Befehl aus, um die Byteanzahl anzuzeigen, die {key_value} durch den zu verwendenden Schlüsselwert ersetzt.

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

Die Ausgabe in den Zeilen 2, 4 und 6 zeigt an, dass die Schlüsselwertbytezählungen 9, 32 bzw. 64 betragen.

Zeichenverwendung bestätigen

Wenn die Byteanzahl weniger als 20 beträgt, stellen Sie sicher, dass Sie, wie in den NTP-Konfigurationsanforderungen angegeben, druckbare ASCII-Zeichen verwenden.

Sie können den echo '{key_value}' | xxd -r -p && echo Befehl ausführen, um die HEX-Werte in ASCII zu konvertieren, und {key_value} durch den zu verwendenden Schlüsselwert ersetzen.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.