Konfigurieren der NTP-Authentifizierung in der ISE

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die NTP-Authentifizierung auf der Cisco Identity Services Engine (ISE) konfigurieren und die NTP-Authentifizierungsprobleme beheben.

Beitrag von Ankush Kaidalwar, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Es wird empfohlen, dass Sie über Kenntnisse in den folgenden Themen verfügen:

- Konfiguration der Cisco ISE CLI
- Grundkenntnisse des Network Time Protocol (NTP)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ISE 2.7 Standalone-Knoten
- CISCO2911/K9 Version 15.2(1)T2

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

Netzwerkdiagramm

Konfigurationen

Vorbereitungen

Ihnen muss entweder die Administratorrolle "Super Admin" oder "System Admin" für den ISE-Zugriff zugewiesen sein.

Stellen Sie sicher, dass der NTP-Port im Transitpfad zwischen ISE und NTP-Server(n) nicht blockiert wird.

Es wird davon ausgegangen, dass die NTP-Server auf der ISE konfiguriert sind. Wenn Sie die NTP-Server ändern möchten, navigieren Sie zu **Administration > System > Settings > System Time**. Ein kurzes Video finden Sie unter https://www.youtube.com/watch?v=Bl7loWfb6TE

> **Hinweis**: Wählen Sie bei einer verteilten Bereitstellung für alle Knoten denselben NTP-Server (Network Time Protocol) aus. Um Zeitzonenprobleme zwischen den Knoten zu vermeiden, müssen Sie bei der Installation jedes Knotens denselben NTP-Servernamen angeben. Dadurch wird sichergestellt, dass die Berichte und Protokolle der verschiedenen Knoten in Ihrer Bereitstellung immer mit Zeitstempeln synchronisiert werden.

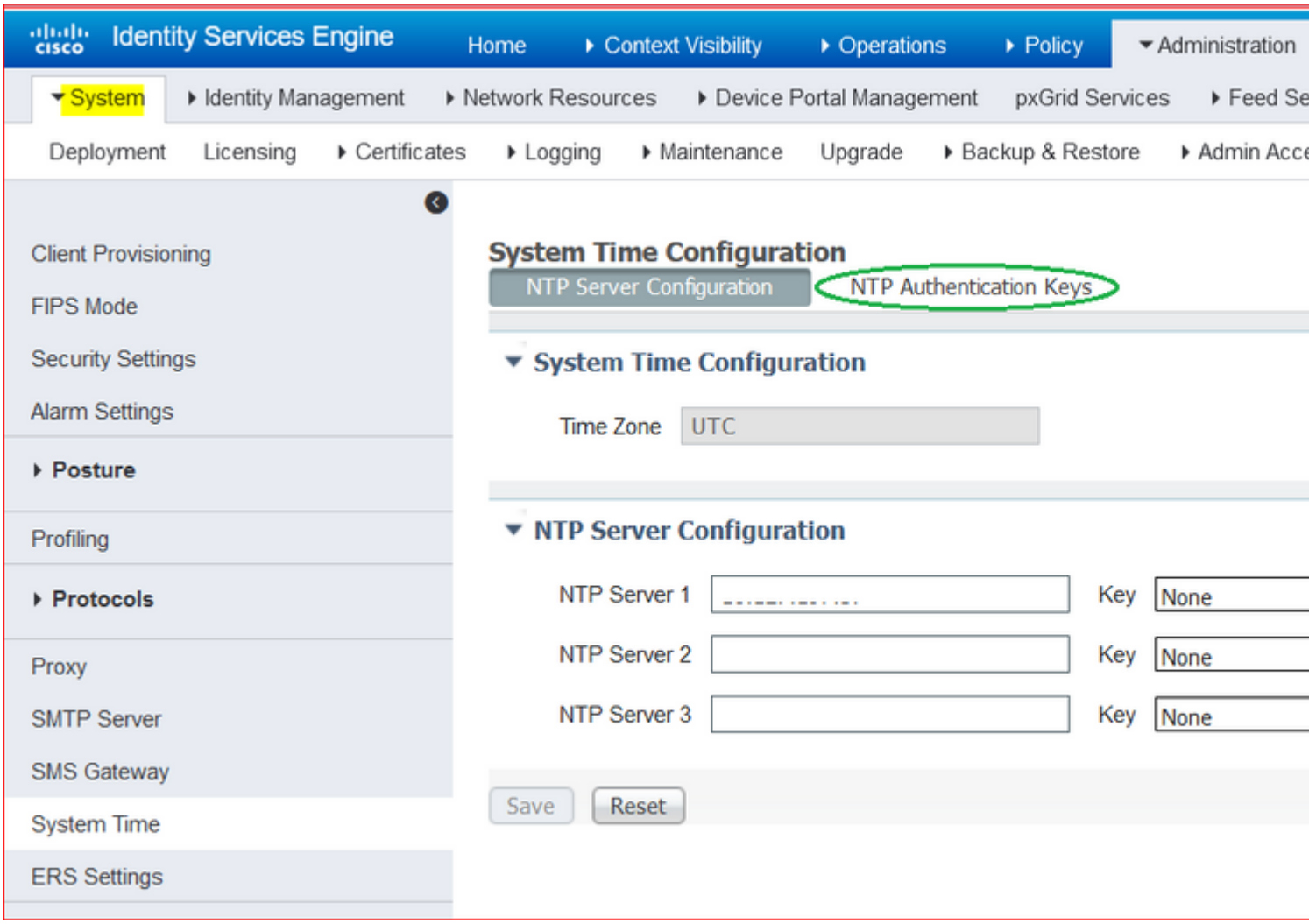
> **Hinweis**: Sie können die Zeitzone nicht über die GUI ändern. Dies ist über die CLI möglich, die einen Neustart des ISE-Service für diesen bestimmten Knoten erfordert. Es wird empfohlen, zum Zeitpunkt der Installation die bevorzugte Zeitzone (Standard-UTC) zu verwenden, wenn Sie vom Assistenten zur Ersteinrichtung zur Eingabe der Zeitzonen aufgefordert werden. Siehe Cisco Bug-ID CSCvo49755 zur Aktivierung des CLI-Befehls clock timezone.

Wenn Sie in Ihrer Bereitstellung sowohl primäre als auch sekundäre Cisco ISE-Knoten haben, müssen Sie sich bei den Benutzeroberflächen der einzelnen Knoten anmelden und die Systemzeit- und NTP-Servereinstellungen (Network Time Protocol) konfigurieren.

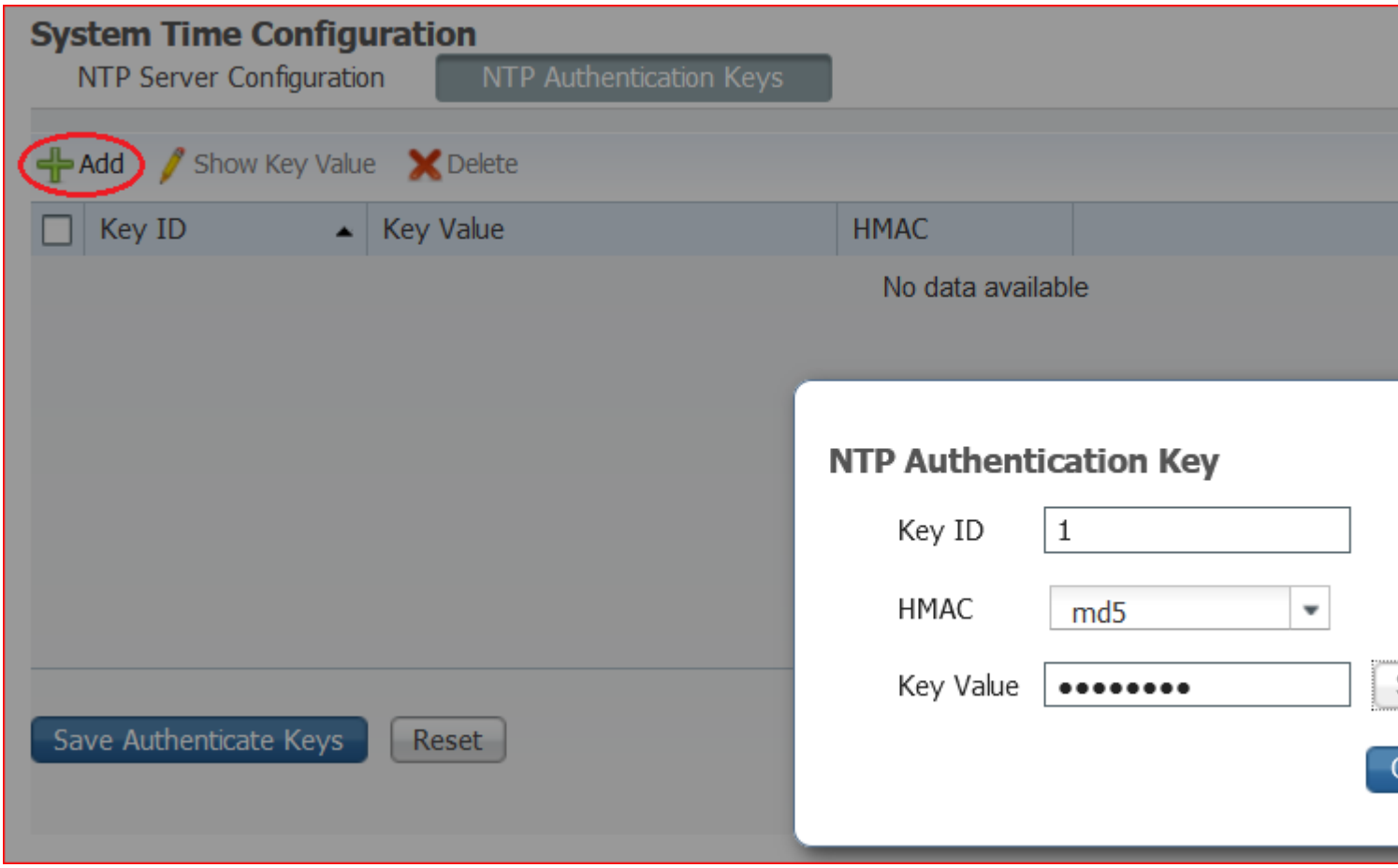
Sie können die NTP-Authentifizierung in der ISE entweder über die GUI oder die CLI konfigurieren.

Schritte der Benutzeroberfläche

Schritt 1: Navigieren Sie zu **Administration > System > Settings > System Time**, und klicken Sie auf **NTP Authentication Keys**. (NTP-Authentifizierungsschlüssel), wie in dieser Abbildung dargestellt.

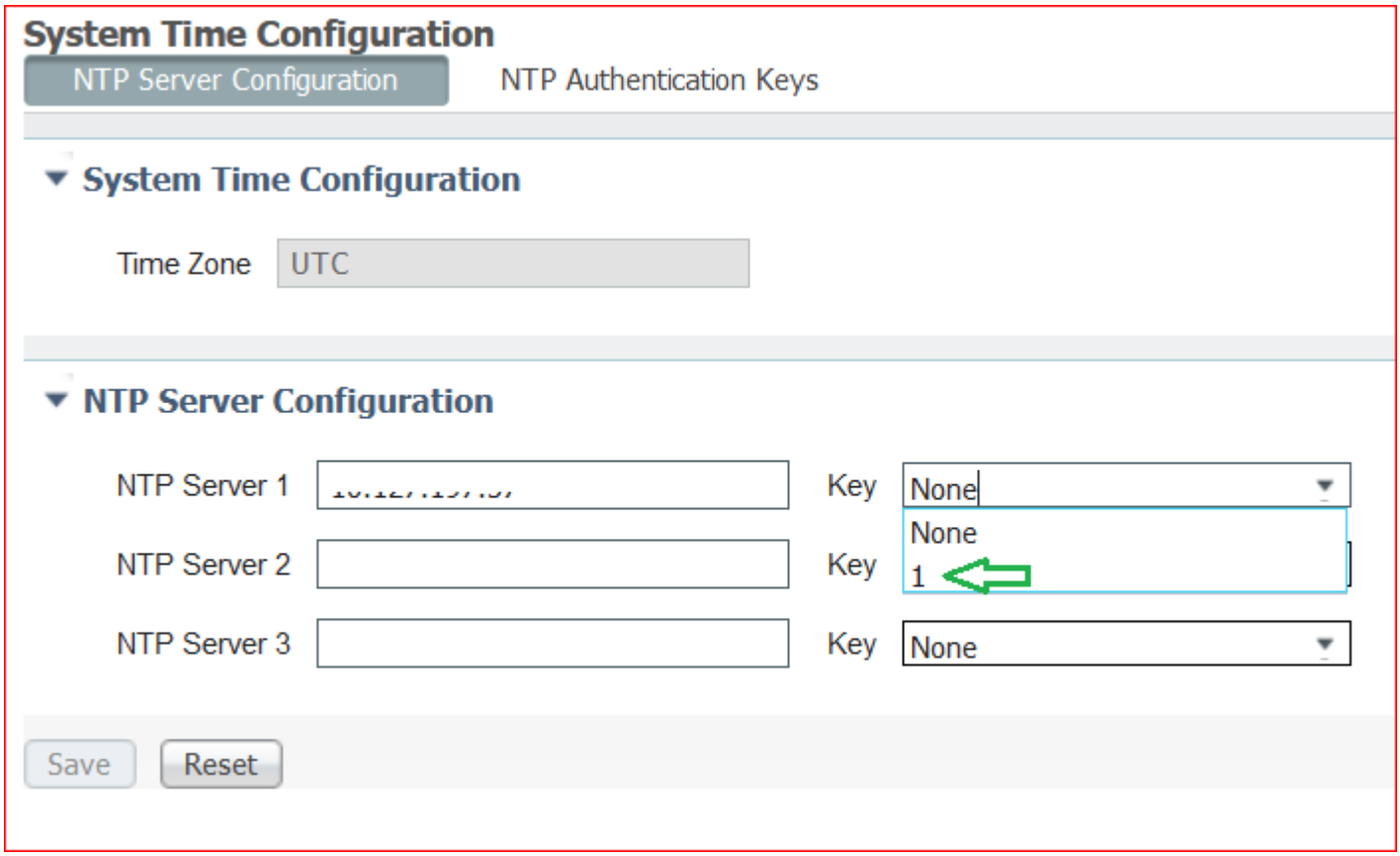


Schritt 2: Hier können Sie einen oder mehrere Authentifizierungsschlüssel hinzufügen. Klicken Sie auf **Hinzufügen**, um ein Popup-Fenster zu öffnen. Hier unterstützt das Feld Schlüssel-ID numerische Werte zwischen 1 und 65535, und das Feld Schlüsselwert unterstützt bis zu 15 alphanumerische Zeichen. Der **Schlüsselwert** ist der tatsächliche NTP-Schlüssel, mit dem die ISE als Client beim NTP-Server authentifiziert wird. Außerdem muss die Schlüssel-ID mit der Schlüssel-ID übereinstimmen, die auf dem NTP-Server konfiguriert wurde. Wählen Sie den erforderlichen HMAC-Wert (Hashed Message Authentication Code) aus der HMAC-Dropdown-Liste aus.



Schritt 3: Klicken Sie auf OK und dann auf **Authentifizierungsschlüssel speichern**. Kehren Sie zur Registerkarte "**NTP-Serverkonfiguration" zurück**.

Schritt 4: Im Dropdown-Menü "Key" (Schlüssel) wird die Schlüssel-ID angezeigt, die Sie in Schritt 3 konfiguriert haben. Klicken Sie auf die entsprechende Schlüssel-ID, wenn Sie mehrere Schlüssel-IDs konfiguriert haben. Klicken Sie dann auf **Speichern**.



CLI-Schritte

Schritt 1: Konfigurieren Sie den NTP-Authentifizierungsschlüssel.

```
admin(config)# ntp authentication-key ?
<1-65535> Key number >>> This is the Key ID
admin(config)# ntp authentication-key 1 ? >>> Here you can choose the HMAC value
md5 MD5 authentication
sha1 SHA1 authentication
sha256 SHA256 authentication
sha512 SHA512 authentication
admin(config)# ntp authentication-key 1 md5 ? >>> You can choose either to paste the hash of the actual
hash Specifies an ENCRYPTED (hashed) key follows
plain Specifies an UNENCRYPTED plain text key follows

admin(config)# ntp authentication-key 1 md5 plain Ntp123 >>> Ensure there are no spaces given at the enc
```

Schritt 2: Definieren Sie den NTP-Server, und ordnen Sie die in Schritt 1 konfigurierte Schlüssel-ID zu.

```
admin(config)# ntp server IP/HOSTNAME ?
key Peer key number
<cr> Carriage return.

admin(config)# ntp serve IP/HOSTNAME key ?
<1-65535>

admin(config)# ntp serve IP/HOSTNAME key 1 ?
```

```
<cr> Carriage return.

admin(config)# ntp serve IP/HOSTNAME key 1
```

Konfiguration auf Router

Der Router fungiert als NTP-Server. Konfigurieren Sie diese Befehle, um den Router als NTP-Server mit NTP-Authentifizierung zu aktivieren.

```
ntp authentication-key 1 md5 Ntp123 >>> The same key that you configured on ISE
ntp authenticate
ntp master STRATUM
```

Überprüfung

Auf der ISE:

Verwenden Sie den Befehl **show ntp**. Wenn die NTP-Authentifizierung erfolgreich ist, muss die ISE angezeigt werden, die mit dem NTP-Server synchronisiert werden soll.

```
admin# sh ntp
Configured NTP Servers:
NTP_SERVER_IP

Reference ID : 0A6A23B1 (NTP_SERVER_IP)
Stratum : 3
Ref time (UTC) : Fri Mar 26 09:14:31 2021
System time : 0.000008235 seconds fast of NTP time
Last offset : +0.000003193 seconds
RMS offset : 0.000020295 seconds
Frequency : 10.472 ppm slow
Residual freq : +0.000 ppm
Skew : 0.018 ppm
Root delay : 0.000571255 seconds
Root dispersion : 0.000375993 seconds
Update interval : 519.3 seconds
Leap status : Normal >>> If there is any issue in NTP synchronization, it shows "Not synchronised".

210 Number of sources = 1
MS Name/IP address Stratum Poll Reach LastRx Last sample
===============================================================================
^* NTP_SERVER_IP 2 9 377 100 +3853ns[+7046ns] +/- 684us

M indicates the mode of the source.
^ server, = peer, # local reference clock.

S indicates the state of the sources.
* Current time source, + Candidate, x False ticker, ? Connectivity lost, ~ Too much variability

Warning: Output results can conflict at the time of changing synchronization.

admin#
```

Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

1. Wenn die NTP-Authentifizierung nicht funktioniert, muss als erster Schritt die Erreichbarkeit zwischen ISE und NTP-Server sichergestellt werden.

2. Stellen Sie sicher, dass die Konfiguration der Schlüssel-ID auf der ISE und dem NTP-Server übereinstimmt.

3. Stellen Sie sicher, dass die Schlüssel-ID auf dem NTP-Server als **vertrauenswürdiger Schlüssel** konfiguriert ist.

4. Ältere ISE-Versionen wie 2.4 und 2.6 unterstützen den Befehl **ntp trusted-key**. Stellen Sie daher sicher, dass Sie den NTP-Schlüssel auf diesen ISE-Versionen als **Trusted-Key** konfiguriert haben.

5. ISE 2.7 führt eine Verhaltensänderung für die NTP-Synchronisierung ein. Während frühere Versionen ntpd verwenden, nutzen 2.7 und höhere Versionen die Chronik. Chrony hat andere Anforderungen als ntpd. Eines der auffälligsten ist, dass ntpd zwar mit Servern synchronisiert wird, die eine Root-Dispersion von bis zu 10 Sekunden aufweisen, Chrony jedoch nur synchronisiert, wenn die Root-Dispersion unter 3 Sekunden liegt. Dies führt dazu, dass die NTP-Server, die vor dem Upgrade synchronisiert werden konnten, ohne ersichtlichen Grund nicht mit 2.7 synchronisiert werden.

   Aufgrund dieser Änderung treten NTP-Synchronisierungsprobleme häufig auf, wenn Sie den Windows NTP-Server verwenden, da dieser eine sehr große Root-Dispersion (3 oder mehr Sekunden) meldet. Dies führt dazu, dass der NTP-Server in der Chronik als zu ungenau ignoriert wird.

Referenzfehler

Cisco Bug-ID CSCvw78019

Cisco Bug-ID CSCvw03693

Zugehörige Informationen

- **Network Time Protocol (NTP) â€“ Leitfaden zur Fehlerbehebung und -suche**

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.