Configuración de la autenticación NTP en ISE

Contenido

Introducción

Este documento describe cómo configurar la autenticación NTP en Cisco Identity Services Engine (ISE) y cómo solucionar los problemas de autenticación NTP.

Colaboración de Ankush Kaidalwar, ingeniero del TAC de Cisco.

Prerequisites

Requirements

Se recomienda que tenga conocimiento de estos temas:

- Configuración de Cisco ISE CLI
- Conocimientos básicos de Network Time Protocol (NTP)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Nodo independiente ISE 2.7
- CISCO2911/K9 Versión 15.2(1)T2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red

Configuraciones

Antes de comenzar

Debe tener el rol de superadministrador o de administrador del sistema asignado para acceder a ISE.

Asegúrese de que el puerto NTP no esté bloqueado en la ruta de tránsito entre los servidores ISE y NTP.

Se supone que tiene sus servidores NTP configurados en ISE. Si desea cambiar los servidores NTP, vaya a **Administration > System > Settings > System Time**. Para ver un breve vídeo, visite https://www.youtube.com/watch?v=Bl7loWfb6TE

> **Nota**: en el caso de una implementación distribuida, elija el mismo servidor de protocolo de tiempo de la red (NTP) para todos los nodos. Para evitar problemas de zona horaria entre los nodos, debe proporcionar el mismo nombre de servidor NTP durante la instalación de cada nodo. Esto garantiza que los informes y registros de los distintos nodos de la implementación siempre estén sincronizados con las marcas de tiempo.

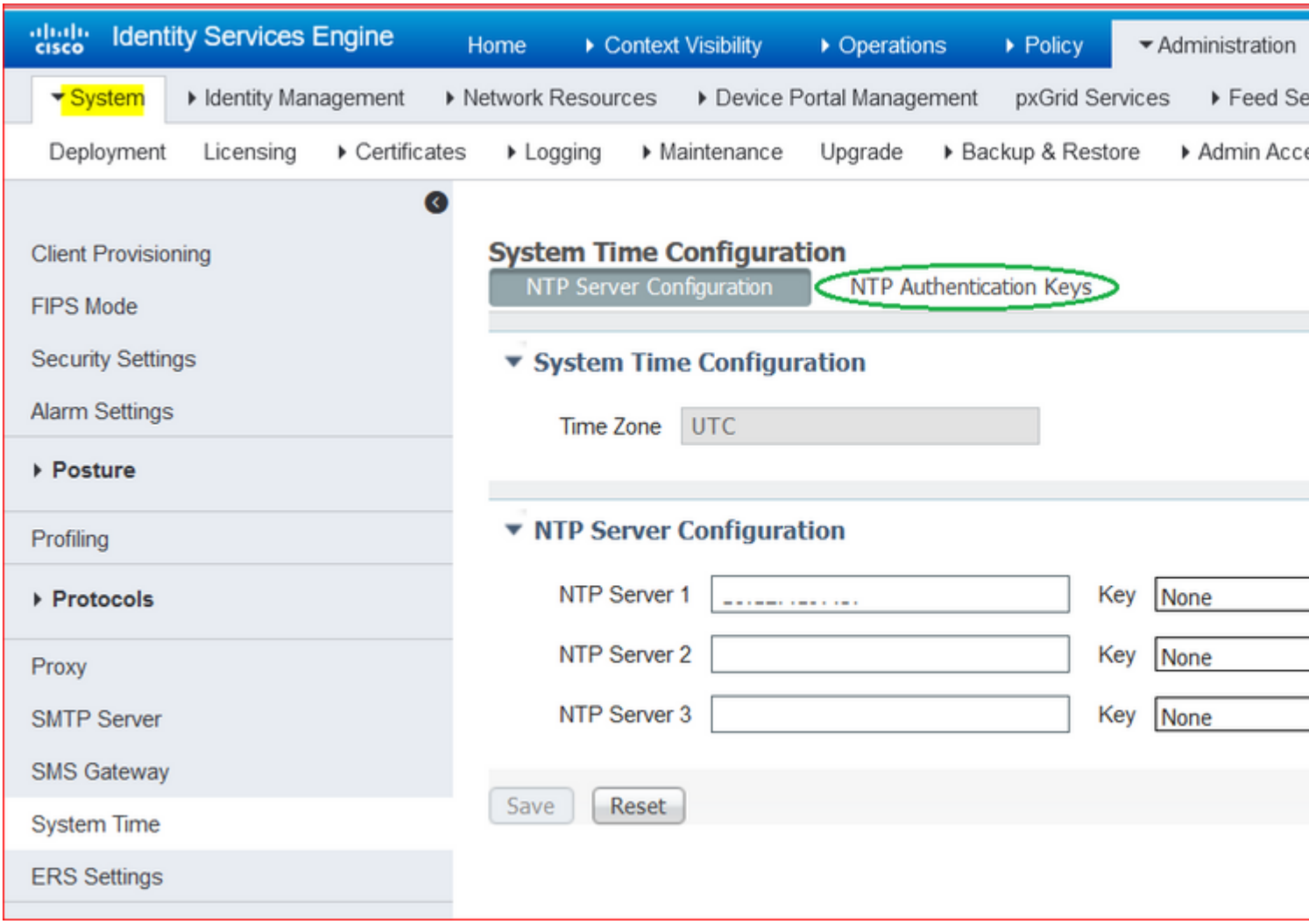
> **Nota**: No puede cambiar la zona horaria desde la GUI. Puede hacerlo a través de CLI, que requiere el reinicio del servicio ISE para ese nodo concreto. Se recomienda utilizar la zona horaria preferida (UTC predeterminado) en el momento de la instalación cuando el asistente de configuración inicial le solicite las zonas horarias. Consulte el ID de bug de Cisco CSCvo49755 relacionado con habilitar el comando de zona horaria de reloj CLI.

Si tiene nodos Cisco ISE primarios y secundarios en la implementación, debe iniciar sesión en la interfaz de usuario de cada nodo y configurar la hora del sistema y los parámetros del servidor de protocolo de tiempo de la red (NTP).

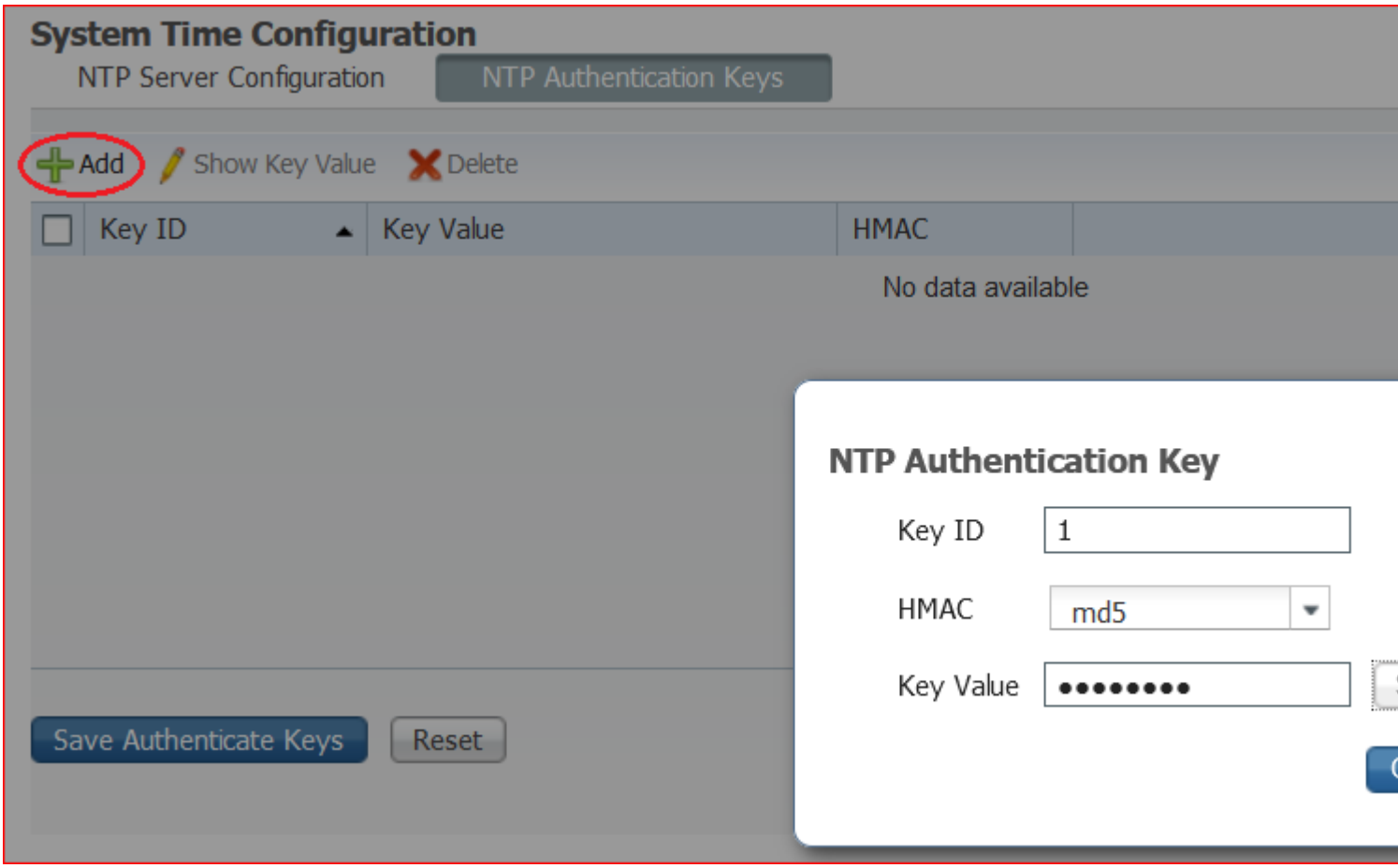
Puede configurar la autenticación NTP en ISE desde la GUI o desde la CLI.

Pasos de GUI

Paso 1. Navegue hasta **Administration > System > Settings > System Time** y haga clic en **NTP Authentication Keys**, como se muestra en esta imagen.

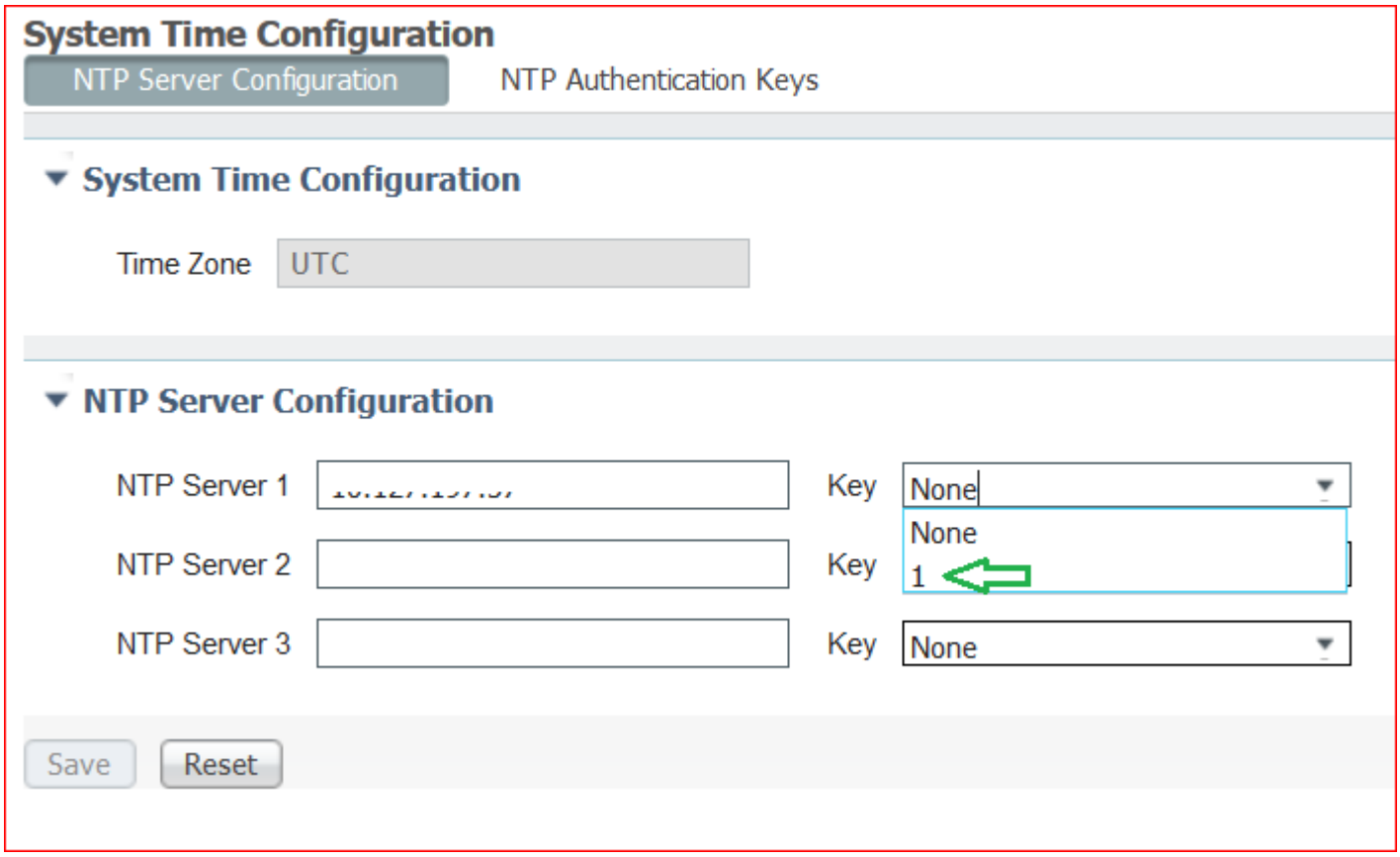


Paso 2. Aquí puede agregar una o más claves de autenticación. Haga clic en **Agregar**, aparecerá una ventana emergente. Aquí, el campo Key ID admite valores numéricos entre 1 y 65535 y el campo Key Value admite hasta 15 caracteres alfanuméricos. El **valor de clave** es la clave NTP real que se utiliza para autenticar ISE como cliente en el servidor NTP. Además, el ID de clave debe coincidir con el configurado en el servidor NTP. Elija el valor requerido del código de autenticación de mensajes hash (HMAC) en la lista desplegable HMAC.



Paso 3. Haga clic en Aceptar y luego en **Guardar claves de autenticación**. Vuelva a la ficha **Configuración del servidor NTP**.

Paso 4. Ahora, en la lista desplegable de claves, verá el ID de claves que configuró en el paso 3. Haga clic en el ID de clave correspondiente si tiene varios ID de clave configurados. A continuación, haga clic en **Guardar**.



Pasos de CLI

Paso 1. Configure la clave de autenticación NTP.

```
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
```

Paso 2. Defina el servidor NTP y asocie el ID de clave configurado en el paso 1.

```
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
```

Configuración en el router

El router actúa como un servidor NTP. Configure estos comandos para habilitar el router como un servidor NTP con autenticación NTP.

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

Verificación

En ISE:

Utilice el comando **show ntp**. Si la autenticación de NTP se realiza correctamente, debe ver que ISE se sincroniza con el servidor NTP.

```
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#
```

Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

1. Si la autenticación NTP no funciona, el primer paso para garantizar es la disponibilidad entre ISE y el servidor NTP.

2. Asegúrese de que la configuración de ID de clave coincida en ISE y en el servidor NTP.

3. Asegúrese de que el ID de clave esté configurado como **clave de confianza** en el servidor NTP.

4. Las versiones anteriores de ISE, como 2.4 y 2.6, admiten el comando **ntp trusted-key**. Asegúrese de haber configurado la clave NTP como **clave de confianza** en estas versiones de ISE.

5. ISE 2.7 introduce un cambio en el comportamiento para la sincronización NTP. Mientras que las versiones anteriores utilizan ntpd, las versiones 2.7 y posteriores utilizan chrony. Chrony tiene diferentes requisitos que ntpd. Una de las más notables es que mientras ntpd se sincroniza con servidores que tienen una dispersión de raíz de hasta 10 segundos, chrony sólo se sincroniza cuando la dispersión de raíz es inferior a 3 segundos. Esto hace que los servidores NTP que pudieron sincronizar antes de la actualización, se desincronicen en 2.7 sin ninguna razón evidente.

   Debido a este cambio, los problemas de sincronización de NTP se verían con frecuencia si utiliza el servidor NTP de Windows, ya que informan una dispersión de raíz muy grande (3 o más segundos) y esto hace que el cronyd ignore el servidor NTP como demasiado impreciso.

Defectos de referencia

ID de falla de funcionamiento de Cisco CSCvw78019

ID de falla de funcionamiento de Cisco CSCvw03693

Información Relacionada

- **Guía de depuración y solución de problemas con el protocolo de tiempo de red (NTP)**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).