Configuración de un error de autenticación NTP en ISE 3.4 debido a la gestión de prefijos HEX

Contenido

Problema

El parche 1 de Cisco Identity Services Engine (ISE) 3.4.0.608 no se puede sincronizar con los servidores NTP cuando se utiliza NTP autenticado con claves SHA1 de 40 caracteres de longitud. Los comandos de clave de autenticación NTP se aceptan en CLI sin errores, pero la sincronización NTP no se produce cuando la autenticación está habilitada. Sin autenticación, la sincronización NTP funciona correctamente. Otros dispositivos de red, incluidos los switches de Cisco, se autentican correctamente con el mismo servidor NTP utilizando idénticos valores de clave e ID de clave.

Durante la resolución de problemas, el análisis de captura de paquetes reveló que ISE envía solicitudes NTP autenticadas con el ID de clave y los campos MAC/autenticador adecuados; sin embargo, las respuestas del servidor contienen un ID de clave de todos ceros y sin MAC/autenticador, lo que hace que ISE rechace la autenticación. La salida de depuración en los switches Cisco que actúan como servidores NTP muestra "SHA1-Match: 0" que indica un fallo de autenticación.

Entorno

- Cisco Identity Services Engine (ISE) versión 3.4.0.608 con parche 1
- Autenticación NTP mediante el algoritmo SHA1
- Claves de autenticación NTP de 40 caracteres de longitud
- Switches Cisco Catalyst 9500 (C9500-24Y4C) que ejecutan la versión 17.12.04
- Dispositivos de servidor NTP con configuración NTP autenticada

Resolución

Este problema es causado por el ID de bug de Cisco: CSCwq7972, que afecta a la forma en que ISE administra las claves de autenticación NTP largas cuando se requiere el prefijo HEX. Este error se ha corregido en el parche 8 de ISE 3.4 y en el parche 3 de ISE 3.5.

Comprensión de la causa raíz

Al configurar las claves de autenticación NTP en los dispositivos Cisco, las claves de 20 caracteres o más se tratan automáticamente como cadenas hexadecimales en lugar de como texto sin formato. Esto requiere que ISE utilice el prefijo "HEX:" al configurar la clave. Sin embargo, debido al error de funcionamiento, ISE solo acepta 36 caracteres de una clave de 40 caracteres debido a la gestión adicional del prefijo "HEX:", lo que provoca un error de autenticación.

Opciones de solución alternativa inmediata

Hasta que el software de ISE se pueda actualizar a una versión que contenga la corrección, utilice una de estas soluciones alternativas:

Opción 1: Utilizar una clave SHA1 de 36 caracteres

Configure el servidor NTP e ISE con una clave SHA1 de 36 caracteres en lugar de la clave de 40 caracteres.

En ISE:

```
ntp authentication-key 1 sha1 plain HEX:1d3f35b762ab7c21e5f1265dc9762fe421fa
```

En el servidor NTP (ejemplo de switch de Cisco):

```
ntp authentication-key 1 sha1 1d3f35b762ab7c21e5f1265dc9762fe421fa
ntp authenticate
```

```
ntp trusted-key 1
```

Opción 2: Usar autenticación MD5

Cambie de la autenticación SHA1 a MD5, que no presenta la misma limitación de longitud.

En ISE:

```
ntp authentication-key 1 md5 plain [MD5-key-value]
ntp server [NTP-server-IP] key 1
```

En el servidor NTP:

```
ntp authentication-key 1 md5 [MD5-key-value]
ntp authenticate
ntp trusted-key 1
```

Pasos de verificación

Después de implementar cualquier solución alternativa, verifique la sincronización NTP:

En ISE:

```
show ntp
show clock
```

En el switch (si utiliza el switch como servidor NTP):

```
show ntp associations
show ntp status
```

Busque indicadores de sincronización exitosos y verifique que la autenticación esté funcionando al confirmar que la sincronización NTP falla cuando la autenticación está inhabilitada en un lado

pero habilitada en el otro.

Resolución permanente

Actualice ISE a una de estas versiones que contenga la corrección de la ID de bug de Cisco: CSCwq7972:

- ISE 3.4 Parche 8 (cuando esté disponible)
- ISE 3.5 Parche 3 o posterior

Después de la actualización, la configuración original de la clave SHA1 de 40 caracteres funciona correctamente con el prefijo HEX.

Causa

Este problema es causado por el ID de bug de Cisco: CSCwq7972, en las versiones de ISE anteriores a la 3.4 Parche 8 y 3.5 Parche 3. Cuando las claves de autenticación NTP tienen 20 caracteres o más, los dispositivos de Cisco las tratan como cadenas hexadecimales, lo que requiere el prefijo "HEX:" en la configuración. Debido a este error, ISE gestiona incorrectamente el cálculo de la longitud de la clave cuando se utiliza el prefijo HEX, aceptando solo 36 caracteres de una clave de 40 caracteres. Esto da lugar a una discordancia de clave entre ISE y el servidor NTP, lo que provoca un error de autenticación durante los intentos de sincronización NTP.

Contenido relacionado

- Error de Cisco CSCwq79772
- Referencia de Comandos del Controlador Inalámbrico de Cisco - Autenticación NTP
- Soporte técnico y descargas de Cisco

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).