Falha de Configuração de Autenticação NTP no ISE 3.4 Devido ao Tratamento de Prefixo HEX

Contents

Problema

O Patch 1 do Cisco Identity Services Engine (ISE) 3.4.0.608 falha ao sincronizar com servidores NTP ao usar NTP autenticado com chaves SHA1 com 40 caracteres de comprimento. Os comandos da chave de autenticação NTP são aceitos na CLI sem erros, mas a sincronização NTP não ocorre quando a autenticação está habilitada. Sem autenticação, a sincronização NTP funciona corretamente. Outros dispositivos de rede, incluindo switches Cisco, autenticam com êxito com o mesmo servidor NTP usando ID de chave e valores de chave idênticos.

Durante a identificação e solução de problemas, a análise de captura de pacotes revelou que o ISE envia solicitações de NTP autenticadas com os campos Key ID e MAC/authenticator adequados. No entanto, as respostas do servidor contêm um Key ID com somente zeros e sem MAC/authenticator, fazendo com que o ISE rejeite a autenticação. A saída de depuração nos switches Cisco que atuam como servidores NTP exibiram "SHA1-Match: 0" indicando falha de autenticação.

Ambiente

- Cisco Identity Services Engine (ISE) versão 3.4.0.608 com Patch 1
- Autenticação NTP usando algoritmo SHA1
- Chaves de autenticação NTP com 40 caracteres
- Switches Cisco Catalyst 9500 (C9500-24Y4C) executando a versão 17.12.04
- Dispositivos de servidor NTP com configuração NTP autenticada

Resolução

Este problema é causado pela ID do bug da Cisco: CSCwq7972, que afeta a forma como o ISE trata chaves de autenticação NTP longas quando o prefixo HEX é necessário. Esse bug foi corrigido no ISE 3.4 Patch 8 e ISE 3.5 Patch 3.

Entendendo a causa raiz

Ao configurar chaves de autenticação NTP em dispositivos Cisco, as chaves com 20 caracteres ou mais são automaticamente tratadas como strings hexadecimais em vez de texto simples. Isso exige que o ISE use o prefixo "HEX:" ao configurar a chave. No entanto, devido ao bug, o ISE aceita somente 36 caracteres de uma chave de 40 caracteres devido ao tratamento adicional de prefixo "HEX:", resultando em falha de autenticação.

Opções de solução imediata

Até que o software ISE possa ser atualizado para uma versão que contenha a correção, use uma destas soluções:

Opção 1: Usar uma chave SHA1 de 36 caracteres

Configure o servidor NTP e o ISE com uma chave SHA1 de 36 caracteres em vez da chave de 40 caracteres.

No ISE:

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

No servidor NTP (exemplo de switch Cisco):

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

Opção 2: Usar Autenticação MD5

Mude da autenticação SHA1 para a autenticação MD5, que não exibe a mesma limitação de comprimento.

No ISE:

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

No servidor NTP:

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

Etapas de verificação

Depois de implementar qualquer uma das alternativas, verifique a sincronização NTP:

No ISE:

```
show ntp
show clock
```

No switch (se estiver usando o switch como servidor NTP):

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

Procure indicadores de sincronização bem-sucedidos e verifique se a autenticação está funcionando confirmando a falha da sincronização NTP quando a autenticação está desabilitada em um lado, mas habilitada no outro.

Resolução Permanente

Atualize o ISE para uma destas versões que contenha a correção da ID de bug da Cisco: CSCwq7972:

- ISE 3.4 Patch 8 (quando disponível)
- ISE 3.5 Patch 3 ou posterior

Após a atualização, a configuração original da chave SHA1 de 40 caracteres funciona corretamente com o prefixo HEX.

Causa

Este problema é causado pela ID do bug da Cisco: CSCwq79772, nas versões do ISE anteriores à 3.4 Patch 8 e à 3.5 Patch 3. Quando as chaves de autenticação do NTP têm 20 caracteres ou mais, os dispositivos Cisco as tratam como strings hexadecimais, exigindo o prefixo "HEX:" na configuração. Devido a esse erro, o ISE manipula incorretamente o cálculo do comprimento da chave quando o prefixo HEX é usado, aceitando apenas 36 caracteres de uma chave de 40 caracteres. Isso resulta em uma incompatibilidade de chave entre o ISE e o servidor NTP, causando falha de autenticação durante tentativas de sincronização NTP.

Conteúdo relacionado

- Bug CSCwq79772 da Cisco
- Referência de Comandos do Cisco Wireless Controller - Autenticação NTP
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.