由于十六进制前缀处理，在ISE 3.4上配置NTP身份验证失败

目录

问题

当使用经过身份验证的NTP和长度为40个字符的SHA1密钥时，思科身份服务引擎(ISE)3.4.0.608补丁1无法与NTP服务器同步。NTP authentication key命令在CLI上被接受，没有错误，但是启用身份验证时不会发生NTP同步。如果没有身份验证，NTP同步将正常工作。其他网络设备（包括思科交换机）使用相同的密钥ID和密钥值成功通过同一NTP服务器进行身份验证。

在故障排除期间，数据包捕获分析显示ISE发送具有正确密钥ID和MAC/身份验证器字段的已验证NTP请求，但是，服务器回复包含全零的密钥ID且没有MAC/身份验证器，从而导致ISE拒绝身份验证。充当NTP服务器的思科交换机上的调试输出显示“SHA1-Match:0”表示身份验证失败。

环境

- 思科身份服务引擎(ISE)版本3.4.0.608，带补丁1
- 使用SHA1算法的NTP身份验证
- 长度为40个字符的NTP身份验证密钥
- 运行版本17.12.04的Cisco Catalyst 9500交换机(C9500-24Y4C)
- 具有经过身份验证的NTP配置的NTP服务器设备

分辨率

此问题是由思科漏洞ID导致的：CSCwq79772,影响ISE在需要十六进制前缀时处理长的NTP身份验证密钥的方式。此Bug已在ISE 3.4补丁8和ISE 3.5补丁3中修复。

了解根本原因

在Cisco设备上配置NTP身份验证密钥时，20个字符或更长的密钥将自动视为十六进制字符串，而不是纯文本。这要求ISE在配置密钥时使用“HEX：”前缀。但是，由于Bug，ISE仅接受36个字符的40字符密钥，因为额外的“HEX：”前缀处理，导致身份验证失败。

即时解决方法选项

在将ISE软件升级到包含修复程序的版本之前，请使用以下解决方法之一：

选项 1：使用36个字符的SHA1密钥

为NTP服务器和ISE配置36个字符的SHA1密钥，而不是40个字符的密钥。

在ISE上：

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

在NTP服务器上（Cisco交换机示例）：

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

选项 2：使用MD5身份验证

从SHA1切换到MD5身份验证，此身份验证未显示相同的长度限制。

在ISE上：

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

在NTP服务器上：

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

验证步骤

在实施任一解决方法后，验证NTP同步：

在ISE上：

```
show ntp
show clock
```

在交换机上（如果使用交换机作为NTP服务器）：

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

在一端禁用身份验证而在另一端启用身份验证时，通过确认NTP同步失败来查找成功的同步指示符，并验证身份验证是否正常工作。

永久解决方案

将ISE升级到包含思科Bug ID修复程序的以下版本之一：CSCwq79772:

- ISE 3.4补丁8（如果可用）
- ISE 3.5补丁3或更高版本

升级后，原始40字符SHA1密钥配置可与HEX前缀配合使用。

原因

此问题是由思科漏洞ID导致的：CSCwq79772，在3.4补丁8和3.5补丁3之前的ISE版本中。当NTP身份验证密钥为20个字符或更长时，思科设备会将这些密钥视为十六进制字符串，在配置中需要“HEX：”前缀。由于此Bug，ISE错误地处理使用HEX前缀时的密钥长度计算，仅接受40字符密钥的36个字符。这会导致ISE和NTP服务器之间的密钥不匹配，从而在NTP同步尝试期间导致身份验证失败。

相关内容

- Cisco Bug CSCwq79772
- 思科无线控制器命令参考 — NTP身份验证
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。