Solucione problemas de falha de troca de tráfego (peering) de alta disponibilidade devido à incompatibilidade da chave de autenticação no Evolved Programmable Network Manager

Contents

Introdução

Este documento descreve como resolver o erro de incompatibilidade de chave de autenticação ao configurar o peering de alta disponibilidade entre servidores EPNM primários e secundários.

Pré-requisitos

Requisitos

A Cisco recomenda que você conheça estes tópicos:

- Evolved Programmable Network Manager (EPNM)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

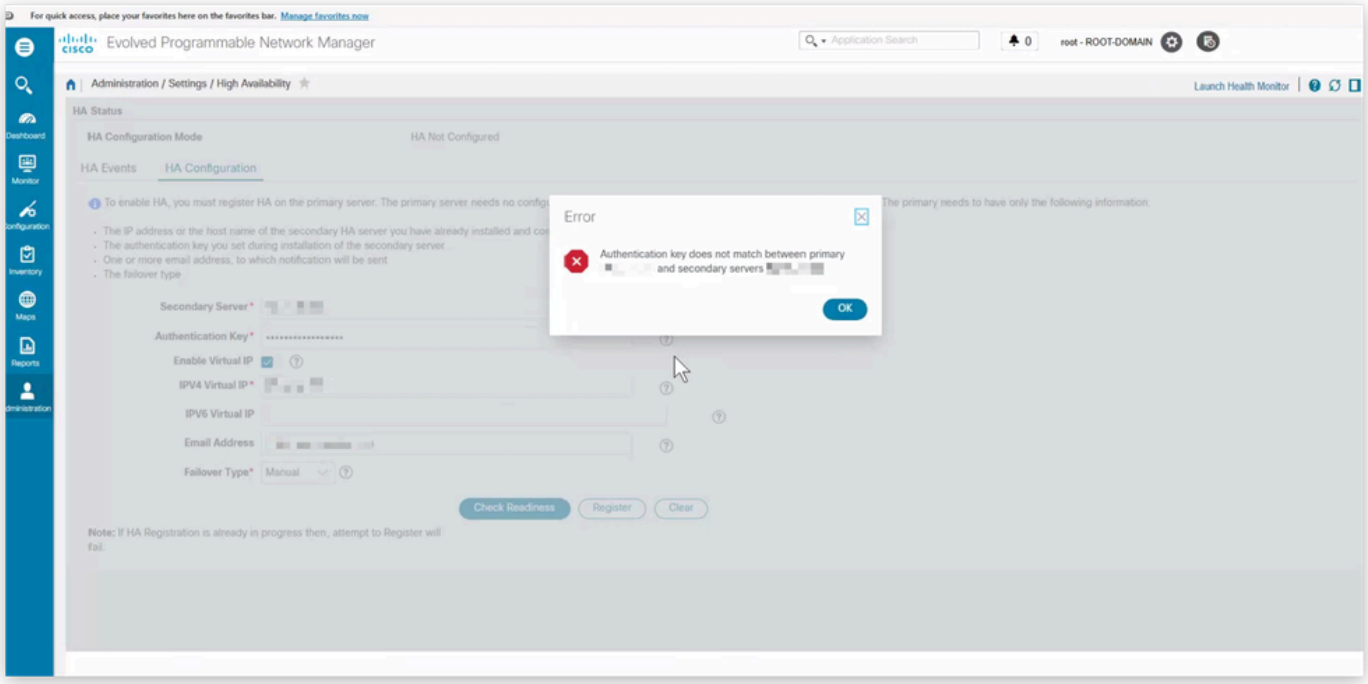
- Software EPNM versão 8.x

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Instrução do problema

As tentativas de configurar o peering de Alta Disponibilidade (HA) entre os servidores Cisco Evolved Programmable Network Manager (EPNM) primário e secundário falham. Uma mensagem de erro informa que a chave HA não corresponde entre os servidores primário e secundário. Redefinir a chave HA secundária e tentar novamente o processo de troca de tráfego (peering) não resolve o problema.

- Mensagem de Erro: "A chave de autenticação não corresponde entre os servidores primário <IP Primário> e secundário <IP Secundário>"
- A falha ocorre durante a configuração de HA entre os nós primário e secundário do EPNM
- As tentativas de redefinir a chave HA no servidor secundário não foram bem-sucedidas



Ambiente

- Tecnologia: Serviços de gerenciamento de rede (NMS)
- Produto: Cisco Evolved Programmable Network Manager
- Versão de software: 8.1.0
- Servidores EPNM primários e secundários configurados para HA
- Ação recente: Tentativa de redefinir a chave de alta disponibilidade no servidor secundário e restabelecer o emparelhamento de alta disponibilidade
- Erro observado: "A chave de autenticação não corresponde entre os servidores primário <IP Primário> e secundário <IP Secundário>"

Resolução

1. Alterar a Chave de Autenticação HA em Ambos os Servidores

Atualize a chave de autenticação HA em ambos os servidores EPNM primário e secundário para garantir que eles correspondam.

Execute o comando em cada servidor (substitua `<newkey>` pela chave de autenticação desejada):

<#root>

ncs ha authkey

Exemplo:

<#root>

epnm/admin#

ncs ha authkey HAAuthKey123

Going to update Secondary authentication key
Successfully updated Secondary authentication key in standalone server
epnm/admin#

2. Certificados Tofu Limpos

Para eliminar possíveis incompatibilidades de certificado, limpe os certificados Tofu associados ao processo de emparelhamento de alta disponibilidade em ambos os servidores.

No servidor primário:

Liste os certificados Tofu existentes:

<#root>

ncs certvalidation tofu-certs listcerts

Se você vir uma entrada para o IP do servidor secundário, exclua-a com:

<#root>

ncs certvalidation tofu-certs deletecert host

```
_8082
```

No servidor secundário:

Liste os certificados Tofu existentes:

<#root>

```
ncs certvalidation tofu-certs listcerts
```

Se você vir uma entrada para o IP do servidor primário, exclua-a com:

<#root>

```
ncs certvalidation tofu-certs deletecert host
```

```
_8082
```

3. Reinicie os Serviços NCS no Servidor Primário

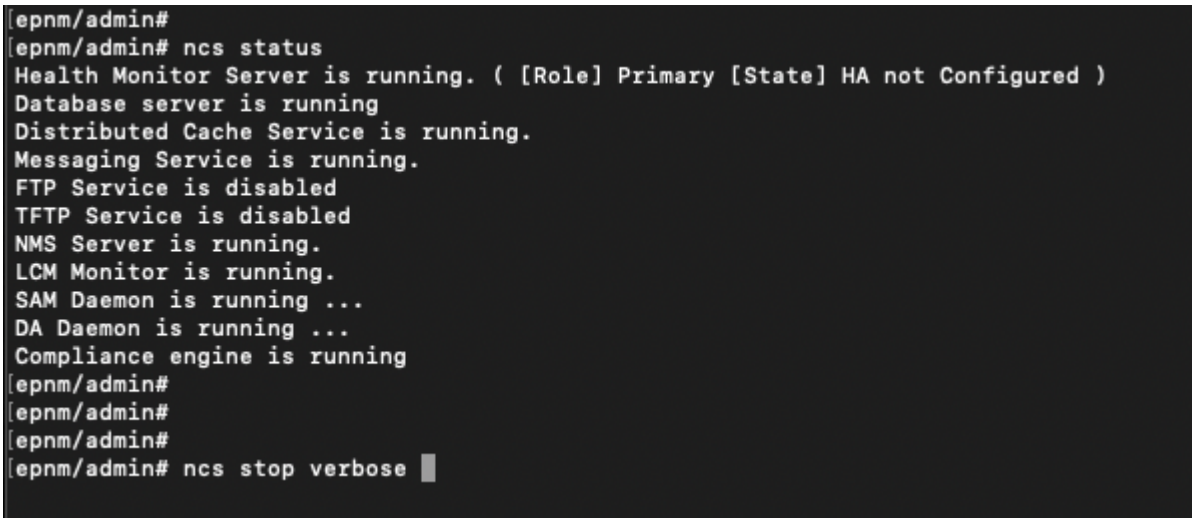
Após atualizar a chave HA e limpar os certificados Tofu relevantes, reinicie os serviços NCS no servidor primário para aplicar as alterações.

Observação: esta etapa afeta o serviço; o acesso ao aplicativo fica indisponível durante a reinicialização do servidor primário.

Pare os serviços do NCS:

<#root>

```
ncs stop verbose
```



- Aguarde até que todos os serviços sejam interrompidos e verifique o status usando o comando:
  <#root>

  ncs status

- Inicie todos os serviços usando o comando:
  <#root>

  ncs start verbose

- Aguarde até que todos os serviços sejam iniciados e verifique o status novamente usando o comando:
  <#root>

  ncs status

4. Repetir a configuração de HA através da GUI do servidor primário

Depois que o servidor primário for reiniciado, prossiga com o fluxo de trabalho de configuração de HA normal usando a interface gráfica do usuário (GUI) do servidor primário.

Causa

A causa subjacente da falha de peering HA é uma incompatibilidade na chave de autenticação HA entre os servidores Cisco EPNM primário e secundário. Isso resulta no erro:"Authentication key does not match between primary <Primary IP> and secondary servers <Secondary IP>" (A chave de autenticação não corresponde entre os servidores primário <Primary IP> e secundário <Secondary IP>). Incompatibilidades adicionais de certificado (certificados Tofu) também podem impedir o estabelecimento bem-sucedido de HA.

Informações Relacionadas

- Redefinir a chave de autenticação de alta disponibilidade
- Procedimento de reinicialização do serviço Cisco EPNM (Vídeo)
- 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.