Solucionar problemas de falhas de autenticação de VPN e RADIUS do ISE 3.4

Contents

Problema

As implantações do ISE 3.4 Patch 4 apresentam falhas de autenticação quando um nó de administração secundário (SAN) sofre uma interrupção. As solicitações de autenticação direcionadas ao PPAN (Primary Policy Administration Node, nó primário de administração de política) também falham, causando interrupções nas conexões VPN ASA e nas autenticações RADIUS. O nó SAN é exibido como desconectado no painel de implantação do ISE e os registros indicam erros relacionados a EAP/TLS e problemas de controle de sessão.

Ambiente

- Cisco Identity Services Engine (ISE)
- Dispositivos de acesso à rede (NADs): Inclui dispositivos Meraki e/ou firewall ASA
- Topologia: Implantação do ISE em vários nós com SAN e PPAN

Resolução

1.- Remova todos os personagens do nó SAN através da interface de administração do Cisco ISE navegando até Administração > Sistema > Implantação. Isso interrompe as tentativas de autenticação para o nó com falha e permite que os nós não afetados continuem o processamento.


Note: Após a remoção da persona, o nó SAN continua a ser exibido como desconectado (Red X) no painel de implantação.

2.- Force manualmente o firewall ASA a considerar o nó SAN como FALHA, evitando que outras tentativas de autenticação sejam direcionadas para a SAN indisponível. Essa ação é executada na configuração do ASA, garantindo o failover para os nós operacionais do ISE.

3.- Reveja a implantação do ISE para obter a sincronização apropriada e monitore as métricas de integridade, incluindo CPU, memória e utilização de disco.

4.- Verifique se os serviços de autenticação estão operacionais, verificando se as novas solicitações Dot1x e RADIUS são processadas pelos nós ISE não afetados.

5.- Colete registros DEBUG e capturas de pacotes durante falhas de autenticação para analisar a temporização da negociação EAP/TLS e as redefinições de sessão.

6.- Continuar monitorando as métricas de integridade do sistema ISE e o comportamento de autenticação após eventos de failover da SAN.

7.- Valide o comportamento de failover do Meraki RADIUS, observando que o ISE não suporta pacotes RADIUS de "Status-Server" para detecção de disponibilidade de servidor.

Exemplo de mensagens de registro

```
Accounting start was received for non-existing session
```

```
Error getting peer certificate from SSL Connection
```

```
packet for this endpoint 58-6D-67-XX-XX-XX is being processed right now so drop the new EAP session
```

```
Long step latency ;2=57290
```

```
Endpoint 58-6D-67-XX-XX-XX abandoned EAP session xxxxxxxxx/552628443/4183334 and started EAP session
```

Causa

A causa principal é uma paralisação do nó de SAN devido a uma falha de link do ISP, que leva a inconsistências de controle de sessão e erros de negociação EAP/TLS entre os nós suplicante, NAD e ISE. Além disso, os dispositivos Meraki dependem de pacotes RADIUS de "servidor de status" para detecção de failover, que o Cisco ISE não suporta, resultando em tentativas contínuas de autenticação para o nó SAN com falha.

Conteúdo relacionado

- Como: Integre as redes Meraki ao ISE
- Configurar a VPN de acesso remoto com autenticação RADIUS no ISE e mapeamento de política de grupo
- 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.