Redefinir a configuração do ISE para os padrões de fábrica

Contents

Problema

Você precisa redefinir a configuração de um nó do Cisco Identity Services Engine (ISE) para os padrões de fábrica.

Ambiente

- Versão do Cisco ISE: versão 3.1 e posterior
- Tipo de implantação: Distribuído
- Nó de administração de política (PAN)
- Nó de monitoramento (MNT)
- Nó de serviço de política (PSN)
- Network Access Device (NAD), por exemplo, um switch ou controlador sem fio

Resolução

Avaliação de impacto

- Se você redefinir o PAN Principal, promova primeiro um PAN Secundário para Principal.

    - Um PAN principal deve sempre existir em sua implantação.
- Se você redefinir uma PSN:
    - Verifique se há uma PSN restante disponível.
    - Certifique-se de que os NADs estejam configurados para direcionar as autenticações RADIUS e TACACS+ para as PSNs restantes.
    - Teste a autenticação com as PSNs restantes.
- Se você redefinir um MNT:
    - Certifique-se de que um nó de monitoramento restante esteja disponível.
- Verifique se nenhuma operação de sincronização está em andamento nos nós restantes.

Antes de redefinir a configuração

Você deve documentar a configuração do nó de destino antes de redefinir a configuração, caso pretenda reconstruir e/ou registrar novamente o nó de destino padrão de fábrica posteriormente.

Note: Redefinir um nó do ISE para os padrões de fábrica faz com que o nó seja reiniciado.

Etapas de redefinição da configuração

1.- Use o Shell Seguro (SSH) para fazer login no nó de destino.

2.- No prompt CLI do ISE, digite:

```
application reset-config ise
```

Note: Esse comando redefine as configurações no nível do aplicativo, incluindo todas as políticas definidas pelo usuário, usuários e logs, e retém apenas as entradas padrão do sistema.

3.- Prompts do ISE:

```
Initialize your Application configuration to factory defaults? (y/n):
```

4.- Inserir: y

5.- O ISE então solicita:

```
Retain existing Application server certificates? (y/n):
```

6.- Escolha uma das opções descritas nas próximas seções.

Opção A - Reter certificados de servidor existentes

O ISE salva os certificados do servidor localmente antes de apagar a configuração e, em seguida, importa-os após a redefinição.

Insira: y


Note: A opção de reter certificados não substitui a exportação manual de certificados. Em particular, as chaves privadas internas da CA não são incluídas quando você usa a opção para reter certificados.

Opção B - Excluir certificados existentes e usar certificados com assinatura automática

O ISE exclui os certificados de servidor existentes e cria novos certificados autoassinados.

Insira: n

Note: Use esta opção somente se:

7.- O ISE interrompe os serviços, limpa e recria os bancos de dados do ISE, desliga o banco de dados e reinicia os serviços de aplicativos.

Aguarde a confirmação:

```
application reset-config is success
```

Note: Não interrompa ou reinicialize o nó enquanto este processo estiver em execução.

8.- Valide a execução do serviço de aplicativo do ISE após inicializá-lo com este comando:

```
show application status ise
```

Causa

Esse processo pode ser necessário para:

- Desativação ou reconstrução de nós do ISE.
- Substituição de hardware.
- Alterações na topologia.
- Resolução de falhas persistentes de sincronização/replicação.

Conteúdo relacionado

- Exportar backup de dados de configuração e operação do ISE

- Guia de referência da CLI do Cisco Identity Services Engine

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.