Problemas de autenticação RADIUS no ONS 15454 versão 6.0

Contents

Introduction

Este documento descreve alguns problemas conhecidos com a autenticação de servidor RADIUS (Remote Authentication Dial-In User Service) no ONS 15454 versão 6.0 em um ambiente Cisco ONS 15454.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco ONS 15454
- servidor RADIUS

Componentes Utilizados

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

- Cisco ONS 15454 versão 6.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

RADIUS é um sistema de segurança distribuída que protege o acesso remoto a redes e serviços de rede contra acesso não autorizado. O RADIUS compreende estes três componentes:

- Um protocolo com um formato de quadro que utiliza UDP (User Datagram Protocol)/IP
- Um server
- Um cliente

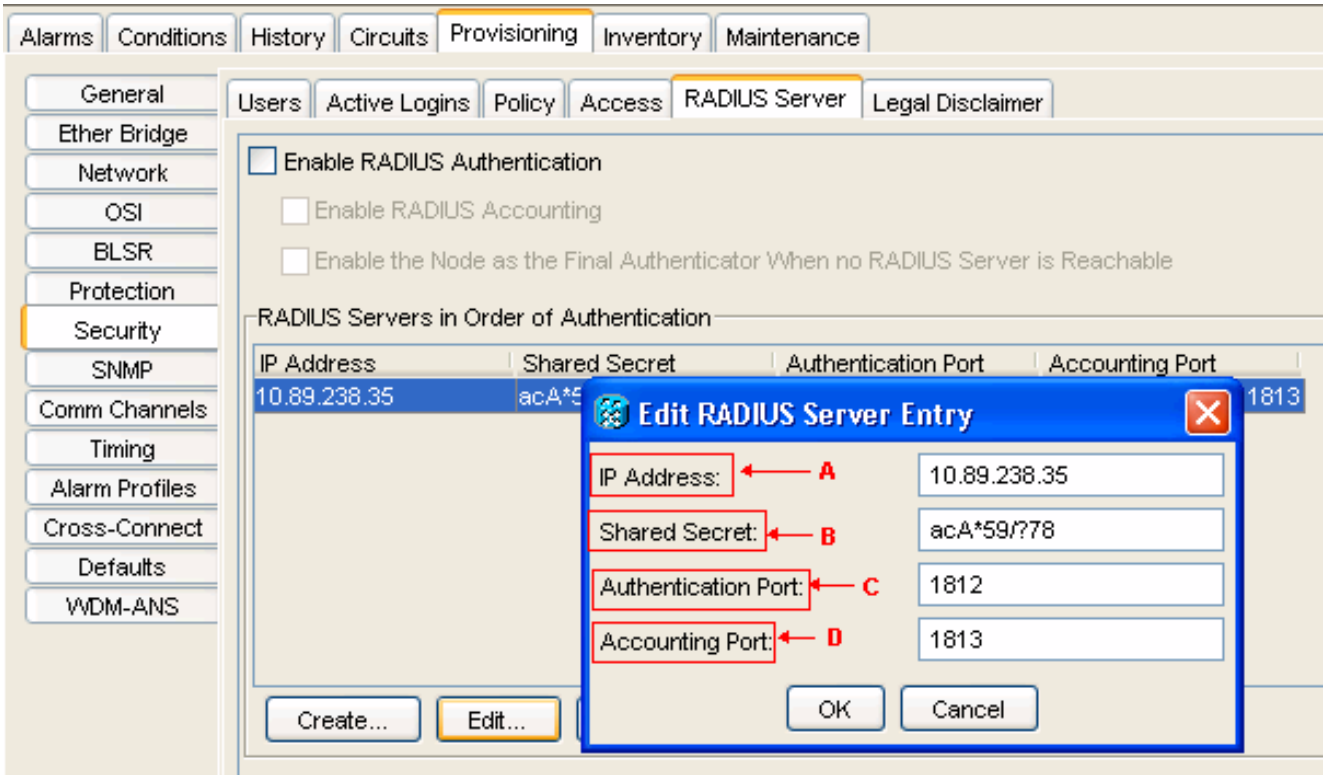
Um nó ONS 15454 opera como um cliente de RADIUS. O cliente passa as informações do usuário para os servidores RADIUS designados e, em seguida, age na resposta. Os servidores RADIUS recebem solicitações de conexão do usuário, autenticam o usuário e retornam todas as informações de configuração necessárias para que o cliente forneça o serviço ao usuário.

Um segredo compartilhado autentica transações entre o cliente e o servidor RADIUS. O segredo compartilhado nunca é enviado pela rede. Além disso, quaisquer senhas de usuário são criptografadas quando trocadas entre o cliente e o servidor RADIUS. O processo de criptografia elimina a possibilidade de alguém monitorar uma rede não segura para determinar a senha de um usuário.

shared secret

Um segredo compartilhado é uma string de texto que serve como senha entre o cliente RADIUS ONS15454 e o servidor RADIUS. Conclua estes passos para criar um segredo compartilhado:

1. Faça login no Cisco Transport Controller (CTC).
2. Vá para a exibição Rede.
3. Selecione um ONS 15454 específico para ir para a visualização da Prateleira.
4. Clique em **Provisioning > Security > RADIUS Server**.
5. Digite o endereço IP do servidor RADIUS no campo IP Address (Endereço IP) (consulte a seta A na Figura 1).
6. Digite um segredo compartilhado no campo Shared Secret. Um segredo compartilhado é uma string de texto que serve como senha entre um cliente RADIUS e o servidor RADIUS (consulte a seta B na Figura 1).
7. Digite o número da porta de autenticação RADIUS no campo Authentication Port (consulte a seta C na Figura 1).O número da porta de autenticação padrão é 1812. Se o nó for um ENE, defina a porta de autenticação como um número dentro do intervalo de 1860 e 1869.
8. Digite o número da porta contábil RADIUS no campo Porta de contabilidade (consulte a seta D na Figura 1).O número da porta de contabilidade padrão é 1813. Se o nó for um ENE, defina a porta de contabilização como um número dentro do intervalo de 1870 e 1879.**Figura 1: Segurança: Servidor RADIUS**



Use segredos compartilhados para garantir que um dispositivo habilitado para RADIUS configurado com o mesmo segredo compartilhado envie todas as mensagens RADIUS, exceto a mensagem Solicitação de acesso.

Os segredos compartilhados garantem que a mensagem RADIUS não seja modificada em trânsito. Em outras palavras, segredos compartilhados mantêm a integridade da mensagem. Os segredos compartilhados também criptografam alguns atributos RADIUS, por exemplo, User-Password e Tunnel-Password.

O ONS 15454 versão 6.0 limita o comprimento de um segredo compartilhado a 16 caracteres. Entretanto, a partir do ONS 15454 versão 6.2, a Cisco planeja aumentar o comprimento máximo para 128 caracteres. Consulte o bug da Cisco ID CSCsc16614 (somente clientes registrados) para obter mais informações.

O grupo de caracteres secretos compartilhados oferece suporte a:

- Letras (maiúsculas e minúsculas), por exemplo, A, B, a e b.
- Numerais, por exemplo, 1, 2 e 3.
- Símbolos, que representam todos os caracteres não definidos como letras ou números, por exemplo, >, (, e *.

Mapeamento do grupo de segurança do usuário

Um par atributo-valor (AV) representa uma variável e um dos valores possíveis que a variável pode conter. No ONS 15454, os usuários são mapeados para diferentes grupos de segurança com base no Cisco AV Pair. Aqui está um exemplo:

"shell:priv-lvl=X" onde X pode ter um valor de 0 a 3:

- 0 representa RTRV.
- 1 representa PROV.

- 2 representa MAINT.
- 3 representa SUPER.

Senha

O servidor e o cliente RADIUS não limitam os caracteres usados para uma senha. No entanto, o CTC tem uma limitação. Para o ONS 15454 versão 6.0, aqui estão os caracteres que o CTC suporta:

- Letras (maiúsculas e minúsculas), por exemplo, A, B, a e b.
- Numerais, por exemplo, 1, 2 e 3.
- Apenas os símbolos especiais #, % e +.

A Cisco planeja remover a limitação de símbolos especiais em versões posteriores do ONS 15454. Consulte o bug da Cisco ID CSCsc16604 (somente clientes registrados) para obter mais informações.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems