Problemas da autenticação RADIUS na versão 6.0 ONS15454

Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenções](#)
[Informações de Apoio](#)
[shared secret](#)
[Mapeamento do grupo de segurança do usuário](#)
[Senha](#)
[Informações Relacionadas](#)

Introdução

Este documento descreve um par problemas conhecidos com autenticação de servidor do Remote Authentication Dial-In User Service (RADIUS) na versão 6.0 ONS15454 em um ambiente do Cisco ONS 15454.

Pré-requisitos

Requisitos

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:

- Versão 6.0 do Cisco ONS 15454

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Informações de Apoio

O RAIO é um sistema de segurança distribuída que fixa o Acesso remoto às redes e aos serviços de rede contra o acesso não autorizado. O RAIO compreende estes três componentes:

- Um protocolo com um formato de frame que utilize o User Datagram Protocol (UDP) /IP
- Um server
- Um cliente

Um nó ONS15454 opera-se como um cliente de RADIUS. O cliente passa a informação sobre o usuário aos servidores radius designados, e atua então na resposta. Os servidores Radius recebem pedidos de conexão do usuário, autenticam o usuário, e retornam toda a informação de configuração necessária para que o cliente entregue o serviço ao usuário.

Um segredo compartilhado autentica transações entre o cliente RADIUS e o server. O segredo compartilhado é enviado nunca sobre a rede. Além, todas as senhas do usuário são cifradas quando trocadas entre o cliente e o servidor Radius. O processo da criptografia elimina a possibilidade de alguém que monitora uma rede não protegida para determinar a senha de um usuário.

shared secret

Um segredo compartilhado é uma sequência de caracteres de texto que serva como uma senha entre o cliente RADIUS ONS15454 e o servidor Radius. Termine estas etapas a fim criar um segredo compartilhado:

1. Log no Cisco Transport Controller (CTC).
2. Vá à vista de rede.
3. Selecione um ONS15454 específico a fim ir à opinião da prateleira.
4. Clique o **> segurança > o servidor Radius do abastecimento**.
5. Datilografe o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius no campo do endereço IP de Um ou Mais Servidores Cisco ICM NT (veja a seta A em figura 1).
6. Datilografe um segredo compartilhado no campo secreto compartilhado. Um segredo compartilhado é uma sequência de caracteres de texto que saques como uma senha entre um cliente RADIUS e um servidor Radius (veja a seta B em figura 1).
7. Datilografe o número de porta da autenticação RADIUS no campo de porta de autenticação (veja o C da seta em figura 1).O número de porta da autenticação padrão é 1812. Se o nó é um ENE, ajuste a porta de autenticação a um número dentro da escala de 1860 e de 1869.
8. Datilografe o número de porta de relatório do RAIO no campo de porta de relatório (veja a seta D em figura 1).O número de porta de relatório do padrão é 1813. Se o nó é um ENE, ajuste a porta de relatório a um número dentro da escala de 1870 e de 1879.**Figura 1 – Segurança: Servidor Radius**

Use segredos compartilhados para assegurar-se de que um dispositivo habilitado por radius que você configure com o mesmo segredo compartilhado envie todos os mensagens de RADIUS exceto a mensagem da solicitação de acesso.

Os segredos compartilhados certificam-se de que o mensagem de RADIUS não obtém alterado no trânsito. Ou seja os segredos compartilhados mantêm a integridade de mensagem. Os segredos compartilhados igualmente cifram alguns atributos RADIUS, por exemplo, Senha do usuário e Túnel-senha.

A versão 6.0 ONS15454 limita o comprimento de um segredo compartilhado a 16 caráteres. Contudo, da versão 6.2 ONS15454 avante, Cisco planeia aumentar o comprimento máximo aos caráteres 128. Refira a identificação de bug Cisco CSCsc16614 (clientes registrados somente) para mais informação.

Apoios secretos compartilhados do grupo do caráter:

- Letras (caixas e lowercase), por exemplo, A, B, a e B.
- Numerais, por exemplo, 1, 2 e 3.
- Símbolos, que representam todos os caráteres que não são definidos como letras ou numerais, por exemplo, >, (, e *.

Mapeamento do grupo de segurança do usuário

Um par do valor de atributo (AV) representa uma variável e esse dos valores possíveis que a variável pode sustentar. Dentro do ONS15454, os usuários são traçados aos grupos de segurança diferentes baseados em pares do AV Cisco. Aqui está um exemplo:

“shell: priv-lvl=X” onde X pode ser valor de 0 a 3:

- 0 representam o RTRV.
- 1 representa PROV.
- 2 representam o MAINT.
- 3 representam SUPER.

Senha

O servidor Radius e o cliente não limitam os caráteres que você se usa para uma senha. Contudo, o CTC tem uma limitação. Para a versão 6.0 ONS15454, estão aqui os caráteres que o CTC apoia:

- Letras (caixas e lowercase), por exemplo, A, B, a e B.
- Numerais, por exemplo, 1, 2 e 3.
- Somente #, %, e + símbolos especiais.

Planos de Cisco para remover a limitação de símbolos especiais em versões mais atrasadas do ONS15454. Refira a identificação de bug Cisco CSCsc16604 (clientes registrados somente) para mais informação.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems