Problemas de autenticación RADIUS en ONS 15454 Versión 6.0

Contenido

Introducción

Este documento describe un par de problemas conocidos con la autenticación de servidor RADIUS (Servicio de usuario de acceso telefónico de autenticación remota) en ONS 15454 versión 6.0 en un entorno Cisco ONS 15454.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco ONS 15454
- servidor RADIUS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ONS 15454 versión 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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

RADIUS es un sistema de seguridad distribuida que protege el acceso remoto a redes y servicios de red contra el acceso no autorizado. RADIUS comprende estos tres componentes:

- Protocolo con un formato de trama que utiliza el protocolo de datagramas de usuario (UDP)/IP
- Un servidor
- Un cliente

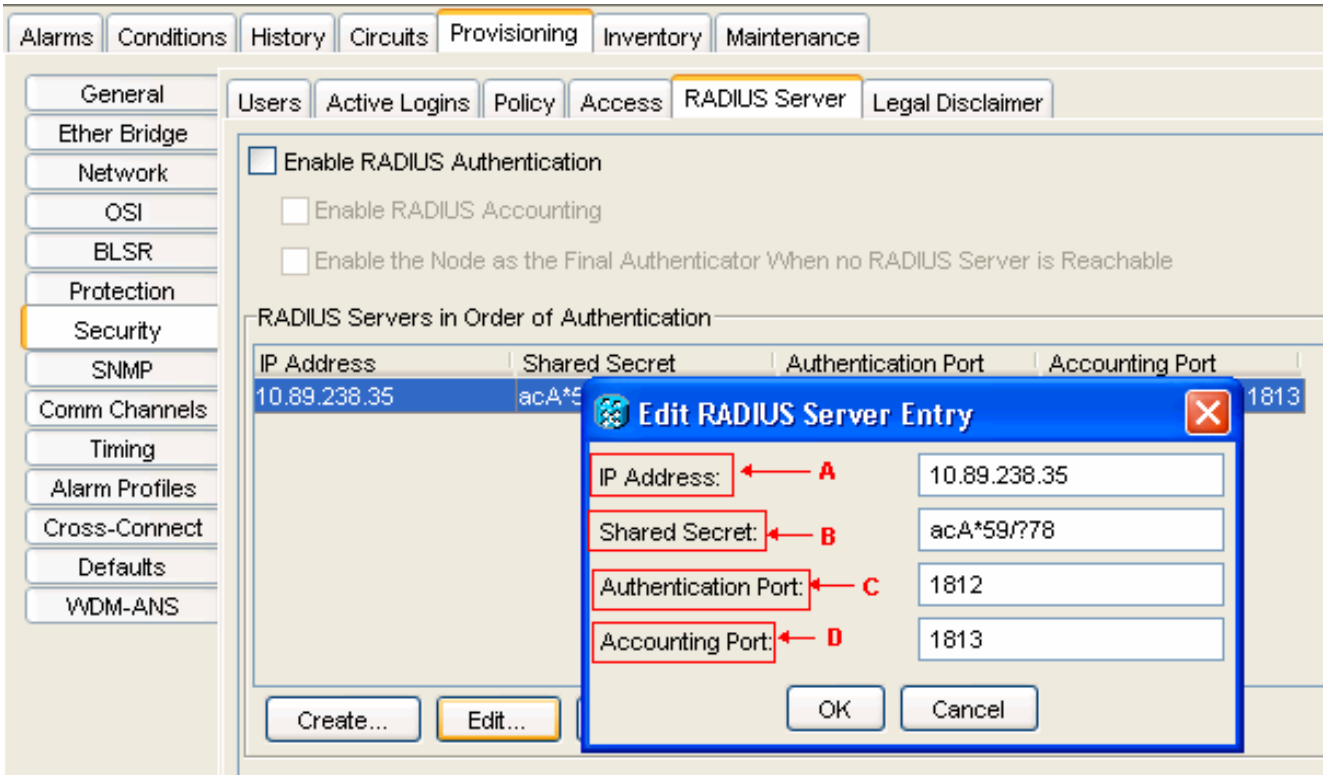
Un nodo ONS 15454 funciona como cliente de RADIUS. El cliente pasa la información del usuario a los servidores RADIUS designados y luego actúa sobre la respuesta. Los servidores RADIUS reciben solicitudes de conexión de usuario, autentican al usuario y devuelven toda la información de configuración necesaria para que el cliente entregue el servicio al usuario.

Un secreto compartido autentica las transacciones entre el cliente RADIUS y el servidor. El secreto compartido nunca se envía a través de la red. Además, cualquier contraseña de usuario se cifra cuando se intercambia entre el cliente y el servidor RADIUS. El proceso de cifrado elimina la posibilidad de que alguien que supervisa una red no segura determine la contraseña de un usuario.

secreto compartido

Un secreto compartido es una cadena de texto que sirve como contraseña entre el cliente RADIUS ONS15454 y el servidor RADIUS. Complete estos pasos para crear un secreto compartido:

1. Inicie sesión en Cisco Transport Controller (CTC).
2. Vaya a la vista Red.
3. Seleccione un ONS 15454 específico para ir a la vista Shelf.
4. Haga clic en **Provisioning > Security > RADIUS Server**.
5. Escriba la dirección IP del servidor RADIUS en el campo IP Address (Dirección IP) (consulte la flecha A en la Figura 1).
6. Escriba un secreto compartido en el campo Secreto compartido. Un secreto compartido es una cadena de texto que sirve como contraseña entre un cliente RADIUS y un servidor RADIUS (consulte la flecha B en la Figura 1).
7. Escriba el número de puerto de autenticación RADIUS en el campo Authentication Port (consulte la flecha C en la Figura 1).El número de puerto de autenticación predeterminado es 1812. Si el nodo es un ENE, configure el puerto de autenticación en un número dentro del rango de 1860 y 1869.
8. Escriba el número de puerto de contabilización RADIUS en el campo Puerto de Contabilización (consulte la flecha D en la Figura 1).El número de puerto de contabilidad predeterminado es 1813. Si el nodo es un ENE, establezca el puerto de contabilidad en un número dentro del rango de 1870 y 1879.**Figura 1: Seguridad: Servidor RADIUS**



Utilice secretos compartidos para asegurarse de que un dispositivo habilitado para RADIUS que haya configurado con el mismo secreto compartido envíe todos los mensajes RADIUS excepto el mensaje Access-Request.

Los secretos compartidos se aseguran de que el mensaje RADIUS no se modifique en tránsito. En otras palabras, los secretos compartidos mantienen la integridad del mensaje. Los secretos compartidos también cifran algunos atributos RADIUS, por ejemplo, User-Password y Tunnel-Password.

ONS 15454 versión 6.0 limita la longitud de un secreto compartido a 16 caracteres. Sin embargo, a partir de la versión 6.2 de ONS 15454, Cisco planea aumentar la longitud máxima a 128 caracteres. Consulte Cisco bug ID CSCsc16614 (sólo clientes registrados) para obtener más información.

El grupo de caracteres secreto compartido admite:

- Cartas (mayúsculas y minúsculas), por ejemplo, A, B, a y b.
- Numerales, por ejemplo, 1, 2 y 3.
- Símbolos, que representan todos los caracteres no definidos como letras o números, por ejemplo, >, (y *.

Asignación de grupo de seguridad de usuario

Un par attribute-value (AV) representa una variable y uno de los valores posibles que la variable puede contener. Dentro de ONS 15454, los usuarios se asignan a diferentes grupos de seguridad según el par AV de Cisco. Aquí tiene un ejemplo:

"shell:priv-lvl=X", donde X puede tener un valor de 0 a 3:

- 0 representa RTRV.
- 1 representa PROV.

- 2 representa MAINT.
- 3 representa SUPER.

Contraseña

El servidor RADIUS y el cliente no limitan los caracteres que utiliza para una contraseña. Sin embargo, el Comité contra el Terrorismo tiene una limitación. Para ONS 15454 versión 6.0, estos son los caracteres que CTC admite:

- Cartas (mayúsculas y minúsculas), por ejemplo, A, B, a y b.
- Numerales, por ejemplo, 1, 2 y 3.
- Sólo los símbolos especiales #, % y +.

Cisco planea eliminar la limitación de los símbolos especiales en versiones posteriores de ONS 15454. Consulte Cisco bug ID CSCsc16604 (sólo clientes registrados) para obtener más información.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems