Problemas de la autenticación de RADIUS en la versión 6.0 ONS15454

Contenido

Introducción

Este documento describe un par de problemas conocidos con la autenticación de servidor del Remote Authentication Dial-In User Service (RADIUS) en la versión 6.0 ONS15454 en un entorno del Cisco ONS 15454.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco ONS 15454
- Servidor de RADIUS

Componentes Utilizados

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

- Versión 6.0 del Cisco ONS 15454

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Antecedentes

El RADIUS es un sistema de seguridad distribuida que asegure el Acceso Remoto a las redes y a los servicios de red contra el acceso no autorizado. El RADIUS comprende estos tres componentes:

- Un protocolo con un formato de trama que utiliza el User Datagram Protocol (UDP) /IP
- Un servidor
- Un cliente

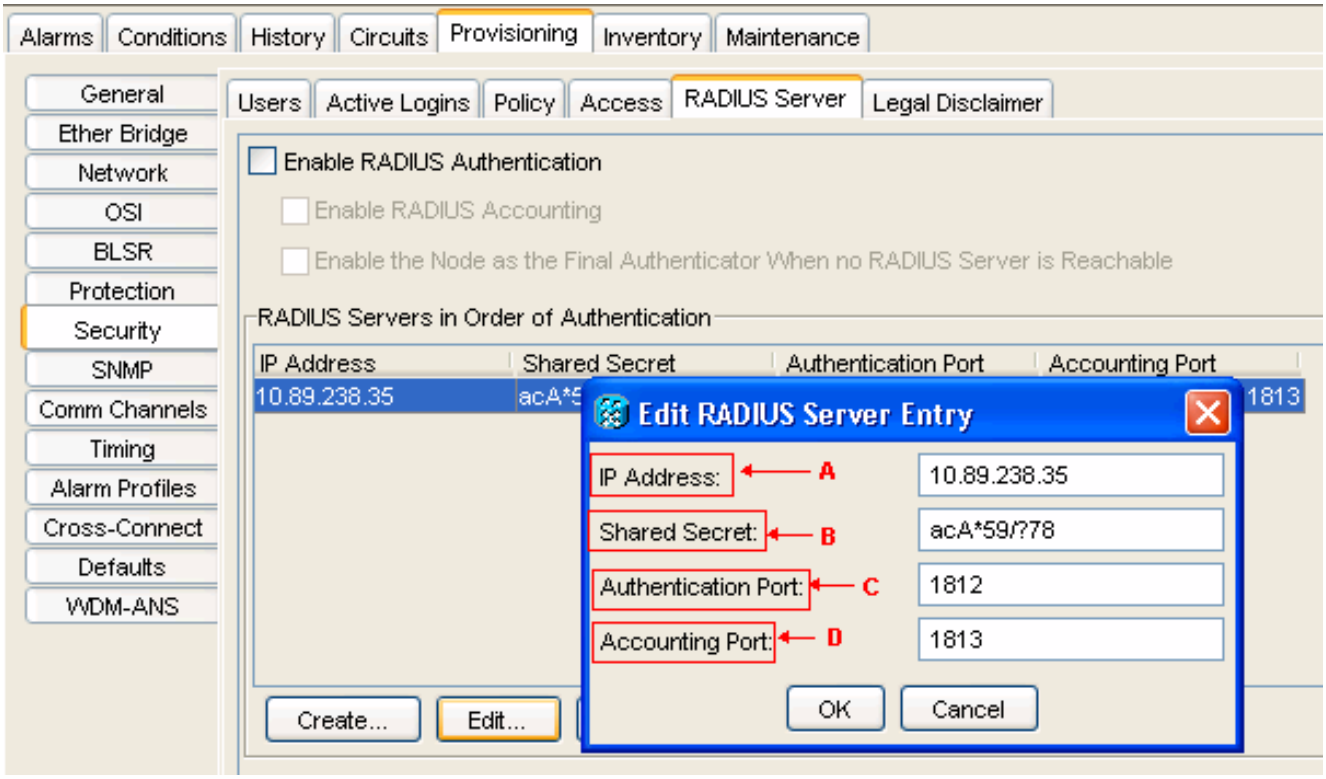
Un nodo ONS15454 actúa como cliente de RADIUS. El cliente pasa la información del usuario a los servidores RADIUS designados, y después actúa en la respuesta. Los servidores de RADIUS reciben las peticiones de conexión del usuario, autentican al usuario, y devuelven toda la información de la configuración 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 sobre la red. Además, se cifra cualquier contraseña del usuario cuando está intercambiada entre el cliente y el servidor de RADIUS. El proceso del cifrado elimina la posibilidad alguien que monitorea una red insegura para determinar 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 de RADIUS. Complete estos pasos para crear un secreto compartido:

1. Registro en el Cisco Transport Controller (CTC).
2. Vaya a la vista de la red.
3. Seleccione un ONS15454 específico para ir a la opinión del estante.
4. Haga clic el **> Security (Seguridad) > al servidor de RADIUS del aprovisionamiento**.
5. Teclee la dirección IP del servidor de RADIUS en el campo de la dirección IP (véase la flecha A en el cuadro 1).
6. Teclee un secreto compartido en el campo del secreto compartido. Un secreto compartido es una cadena de texto que los servicios como contraseña entre un cliente RADIUS y un servidor de RADIUS (véase la flecha B en el cuadro 1).
7. Teclee el número del puerto de la autenticación de RADIUS en el campo de puerto de autenticación (véase el C de la flecha en el cuadro 1).El número del puerto de la autenticación predeterminada es 1812. Si el nodo es un ENE, fije el puerto de autenticación a un número dentro del rango de 1860 y 1869.
8. Teclee el número del puerto de contabilidad RADIUS en el campo de puerto de contabilidad (véase la flecha D en el cuadro 1).El número predeterminado del puerto de contabilidad es 1813. Si el nodo es un ENE, fije el puerto de contabilidad a un número dentro del rango de 1870 y 1879.**Cuadro 1 – Seguridad: Servidor de RADIUS**



Utilice los secretos compartidos para asegurarse de que un dispositivo habilitado para RADIUS que usted ha configurado con el mismo secreto compartido envía todos los mensajes de RADIUS excepto el mensaje del pedido de acceso.

Los secretos compartidos se aseeguran que el mensaje de RADIUS no consigue modificado adentro transita. Es decir los secretos compartidos mantienen la Integridad del mensaje. Los secretos compartidos también cifran algunos atributos de RADIUS, por ejemplo, la Contraseña del Usuario y la Túnel-contraseña.

La versión 6.0 ONS15454 limita la longitud de un secreto compartido a 16 caracteres. Sin embargo, de la versión 6.2 ONS15454 hacia adelante, Cisco planea aumentar el Largo máximo a los caracteres 128. Refiera al Id. de bug Cisco CSCsc16614 (clientes registrados solamente) para más información.

Soportes del grupo del carácter del secreto compartido:

- Cartas (mayúsculas y minúsculas), por ejemplo, A, B, a y B.
- Números, por ejemplo, 1, 2 y 3.
- Símbolos, que representan todos los caracteres que no se definan como las cartas o números, por ejemplo, >, (, y *.

Asignación del grupo de seguridad del usuario

Un par del valor de atributo (AV) representa una variable y la que está de los valores posibles que la variable puede sostener. Dentro del ONS15454, asocian a los usuarios a diversos grupos de seguridad basados en los pares del Cisco AV. Aquí tiene un ejemplo:

“shell: priv-lvl=X” donde X puede ser valor de 0 a 3:

- 0 representa el RTRV.
- 1 representa PROV.

- 2 representa el MAINT.
- 3 representa ESTUPENDO.

Contraseña

El servidor de RADIUS y el cliente no limitan los caracteres que usted utiliza para una contraseña. Sin embargo, el CTC tiene una limitación. Para la versión 6.0 ONS15454, aquí están los caracteres que el CTC soporta:

- Cartas (mayúsculas y minúsculas), por ejemplo, A, B, a y B.
- Números, por ejemplo, 1, 2 y 3.
- Solamente #, %, y + símbolos especiales.

Planes de Cisco para quitar el límite de símbolos especiales en versiones posteriores del ONS15454. Refiera al Id. de bug Cisco CSCsc16604 (clientes registrados solamente) para más información.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems