Problèmes d'authentification RADIUS dans ONS 15454 version 6.0

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Conventions](#)
[Informations générales](#)
[Secret partagé](#)
[Mappage de groupe de sécurité utilisateur](#)
[Mot de passe](#)
[Informations connexes](#)

Introduction

Ce document décrit quelques problèmes connus avec l'authentification du serveur RADIUS (Remote Authentication Dial-In User Service) dans ONS 15454 version 6.0 dans un environnement ONS 15454 de Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ONS 15454
- serveur RADIUS

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ONS 15454 version 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

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

RADIUS est un système de sécurité distribuée qui sécurise l'accès distant aux réseaux et aux services réseau contre les accès non autorisés. RADIUS comprend les trois composants suivants :

- Un protocole avec un format de trame qui utilise le protocole User Datagram Protocol (UDP)/IP
- Un serveur
- Un client

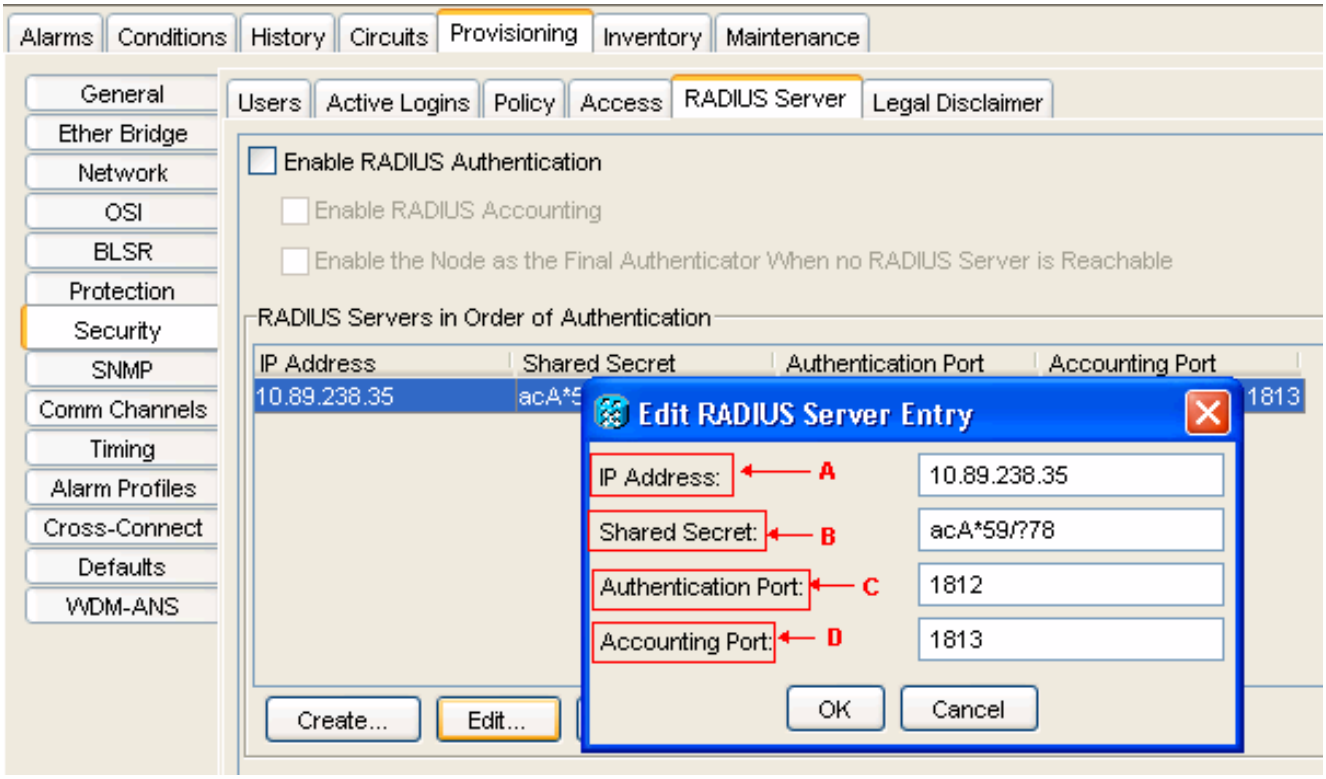
Un noeud ONS 15454 fonctionne en tant que client de RADIUS. Le client transmet les informations utilisateur aux serveurs RADIUS désignés, puis agit sur la réponse. Les serveurs RADIUS reçoivent des demandes de connexion utilisateur, authentifient l'utilisateur et renvoient toutes les informations de configuration nécessaires pour que le client fournisse le service à l'utilisateur.

Un secret partagé authentifie les transactions entre le client et le serveur RADIUS. Le secret partagé n'est jamais envoyé sur le réseau. En outre, tous les mots de passe utilisateur sont chiffrés lorsqu'ils sont échangés entre le client et le serveur RADIUS. Le processus de cryptage élimine la possibilité pour une personne qui surveille un réseau non sécurisé de déterminer le mot de passe d'un utilisateur.

Secret partagé

Un secret partagé est une chaîne de texte qui sert de mot de passe entre le client RADIUS ONS15454 et le serveur RADIUS. Complétez ces étapes afin de créer un secret partagé :

1. Connectez-vous à Cisco Transport Controller (CTC).
2. Accédez à la vue Réseau.
3. Sélectionnez un ONS spécifique 15454 afin d'accéder à la vue Étagère.
4. Cliquez sur **Provisioning > Security > RADIUS Server**.
5. Tapez l'adresse IP du serveur RADIUS dans le champ IP Address (Adresse IP) (voir la flèche A à la Figure 1).
6. Tapez un secret partagé dans le champ Secret partagé. Un secret partagé est une chaîne de texte qui sert de mot de passe entre un client RADIUS et un serveur RADIUS (voir la flèche B à la Figure 1).
7. Tapez le numéro du port d'authentification RADIUS dans le champ Authentication Port (Port d'authentification) (voir la flèche C dans la Figure 1).Le numéro de port d'authentification par défaut est 1812. Si le noeud est un ENE, définissez le port d'authentification sur un nombre compris entre 1860 et 1869.
8. Tapez le numéro du port de comptabilité RADIUS dans le champ Port de comptabilité (voir la flèche D à la Figure 1).Le numéro de port de comptabilité par défaut est 1813. Si le noeud est un ENE, définissez le port de comptabilité sur un nombre compris entre 1870 et 1879.**Figure 1 - Sécurité : Serveur RADIUS**



Utilisez des secrets partagés pour vous assurer qu'un périphérique RADIUS que vous avez configuré avec le même secret partagé envoie tous les messages RADIUS à l'exception du message de demande d'accès.

Les secrets partagés s'assurent que le message RADIUS n'est pas modifié en transit. En d'autres termes, les secrets partagés préservent l'intégrité des messages. Les secrets partagés chiffrent également certains attributs RADIUS, par exemple User-Password et Tunnel-Password.

ONS 15454 version 6.0 limite la longueur d'un secret partagé à 16 caractères. Cependant, à partir de la version 6.2 de l'ONS 15454, Cisco prévoit d'augmenter la longueur maximale à 128 caractères. Référez-vous à l'ID de bogue Cisco CSCsc16614 (clients enregistrés uniquement) pour plus d'informations.

Le groupe de caractères secrets partagés prend en charge :

- Lettres (majuscules et minuscules), par exemple A, B, a et b.
- Numéros, par exemple, 1, 2 et 3.
- Symboles, qui représentent tous les caractères qui ne sont pas définis comme des lettres ou des chiffres, par exemple >, (et *.

Mappage de groupe de sécurité utilisateur

Une paire attribut-valeur (AV) représente une variable et l'une des valeurs possibles que la variable peut contenir. Dans ONS 15454, les utilisateurs sont mappés à différents groupes de sécurité basés sur la paire AV Cisco. Voici un exemple :

«shell : priv-lvl=X » où X peut avoir une valeur comprise entre 0 et 3 :

- 0 représente RTRV.
- 1 représente le PROV.
- 2 représente MAINT.

- 3 représente SUPER.

Mot de passe

Le serveur et le client RADIUS ne limitent pas les caractères que vous utilisez pour un mot de passe. Toutefois, la CCT a des limites. Pour ONS 15454 version 6.0, voici les caractères pris en charge par CTC :

- Lettres (majuscules et minuscules), par exemple A, B, a et b.
- Numéros, par exemple, 1, 2 et 3.
- Seuls les symboles spéciaux #, % et +.

Cisco prévoit de supprimer la limitation des symboles spéciaux dans les versions ultérieures de ONS 15454. Référez-vous à l'ID de bogue Cisco CSCsc16604 (clients enregistrés uniquement) pour plus d'informations.

Informations connexes

- Support et documentation techniques - Cisco Systems