Problèmes d'authentification RADIUS dans ONS 15454 version 6.0

Contenu

Introduction

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

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ONS 15454
- Serveur de RAYON

Composants utilisés

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

- Version 6.0 du Cisco ONS 15454

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Informations générales

Le RAYON est un système de la Sécurité distribuée qui sécurise l'Accès à distance aux réseaux et aux services réseau contre l'accès non autorisé. Le RAYON comporte ces trois composants :

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

Un noeud d'ONS 15454 fonctionne en tant que client du RAYON. Le client passe les informations utilisateur aux serveurs indiqués de RAYON, et puis agit sur la réponse. Les serveurs de RAYON 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 des transactions entre le client RADIUS et le serveur. Le secret partagé n'est jamais envoyé au-dessus du réseau. En outre, tous les mots de passe utilisateur sont chiffrés une fois permutés entre le client et le serveur de RAYON. Le procédé de cryptage élimine la possibilité de quelqu'un qui surveille un réseau non sécurisé pour 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 de RAYON. Terminez-vous ces étapes afin de créer un secret partagé :

1. Log dans le contrôleur de transport de Cisco (CTC).
2. Allez à la vue du réseau.
3. Sélectionnez ONS spécifique 15454 afin d'aller à la vue de module.
4. **Ravitaillement de** clic **> Sécurité > serveur de RAYON**.
5. Tapez l'adresse IP du serveur de RAYON dans le champ IP Address (voir la flèche A sur le schéma 1).
6. Tapez un secret partagé dans le domaine secret partagé. Un secret partagé est une chaîne de texte qui des servir de mot de passe entre un client RADIUS et un serveur de RAYON (voir la flèche B sur le schéma 1).
7. Tapez le numéro de port d'authentification de RAYON dans le domaine de port d'authentification (voir le C de flèche sur le schéma 1).Le numéro de port d'authentification par défaut est 1812. Si le noeud est un ÈNE, placez le port d'authentification à un nombre dans la marge de 1860 et de 1869.
8. Tapez le nombre de port de traçabilité de RAYON dans le domaine de port de traçabilité (voir la flèche D sur le schéma 1).Le nombre par défaut de port de traçabilité est 1813. Si le noeud est un ÈNE, placez le port de traçabilité à un nombre dans la marge de 1870 et de 1879.**Figure 1 – Sécurité : Serveur de RAYON**

Employez les secrets partagés pour s'assurer qu'un périphérique Rayon-activé que vous avez

configuré avec le même secret partagé envoie tous les messages de RAYON excepté le message d'Access-demande.

Les secrets partagés s'assurent que le message de RAYON n'obtient pas modifié en transit. En d'autres termes, les secrets partagés mettent à jour l'intégrité des messages. Les secrets partagés chiffrent également quelques attributs RADIUS, par exemple, mot de passe utilisateur et Tunnel-mot de passe.

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

Supports secrets partagés de groupe de caractère :

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

Mappage de groupe de sécurité d'utilisateur

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

« shell : priv-lvl=X » où X peut être valeur de 0 à 3 :

- 0 représente RTRV.
- 1 représente PROV.
- 2 représente la MAINTENANCE.
- 3 représente SUPERBE.

Mot de passe

Le serveur et le client de RAYON ne limitent pas les caractères que vous utilisez pour un mot de passe. Cependant, le CTC a une limite. Pour la version 6.0 ONS 15454, voici les caractères que le CTC prend en charge :

- Lettres (majuscules et minuscules), par exemple, A, B, a et B.
- Chiffres, par exemple, 1, 2 et 3.
- Seulement #, %, et + symboles spéciaux.

Cisco prévoit d'enlever la limite de symboles spéciaux dans les versions ultérieures d'ONS 15454. Référez-vous au pour en savoir plus de l'ID de bogue Cisco CSCsc16604 (clients enregistrés seulement).

Informations connexes

- Support et documentation techniques - Cisco Systems