RADIUS-Authentifizierungsprobleme in ONS 15454 Version 6.0

Inhalt

Einführung

In diesem Dokument werden einige bekannte Probleme mit der Remote Authentication Dial-In User Service (RADIUS)-Serverauthentifizierung in der ONS 15454 Version 6.0 in einer Cisco ONS 15454-Umgebung beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco ONS 15454
- RADIUS-Server

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ONS 15454 Version 6.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

RADIUS ist ein System für verteilte Sicherheit, das den Remote-Zugriff auf Netzwerke und Netzwerkservices gegen unbefugten Zugriff schützt. RADIUS umfasst die folgenden drei Komponenten:

- Ein Protokoll mit einem Frame-Format, das User Datagram Protocol (UDP)/IP verwendet
- Ein Server
- Ein Client

Ein ONS 15454-Knoten agiert als Client von RADIUS. Der Client leitet Benutzerinformationen an bestimmte RADIUS-Server weiter und bearbeitet anschließend die Antwort. RADIUS-Server empfangen Benutzerverbindungsanforderungen, authentifizieren den Benutzer und geben alle Konfigurationsdaten zurück, die der Client für die Bereitstellung des Dienstes an den Benutzer benötigt.

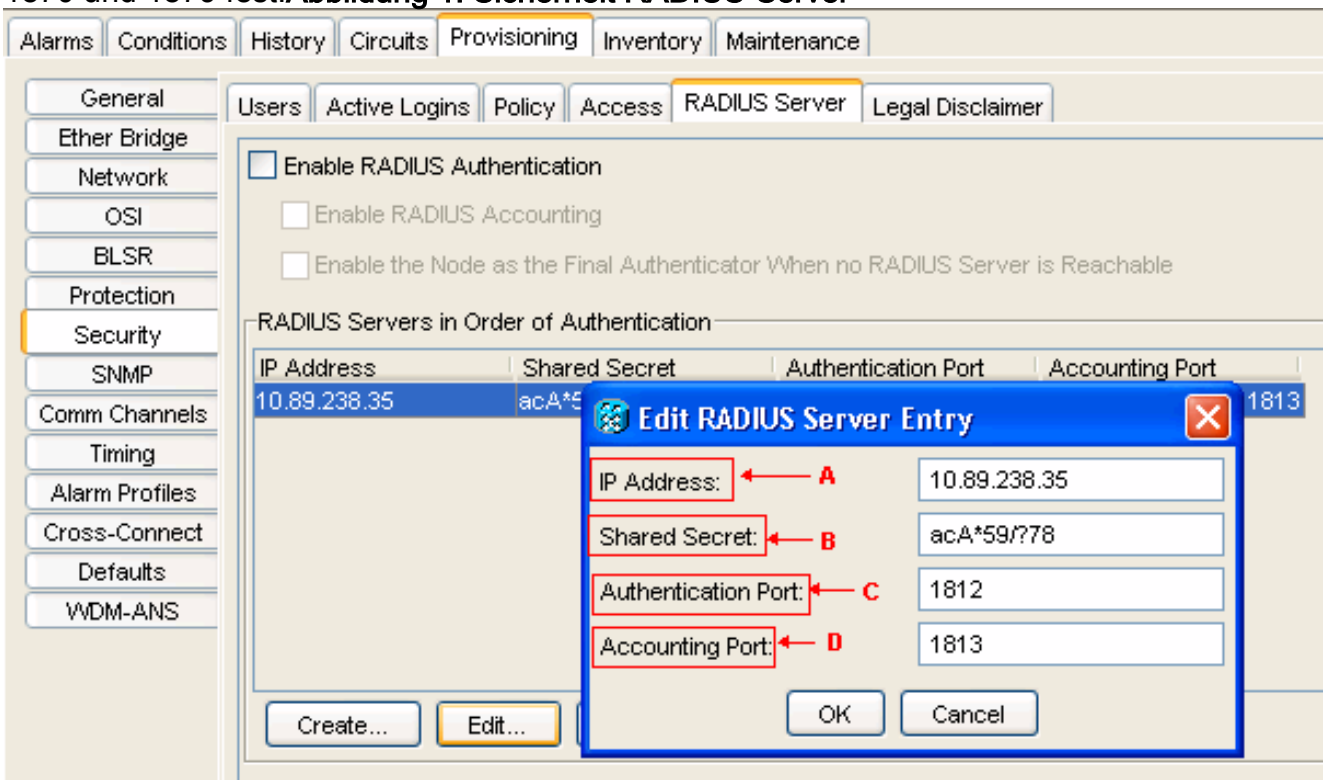
Ein gemeinsamer geheimer Schlüssel authentifiziert Transaktionen zwischen dem RADIUS-Client und dem -Server. Das gemeinsam genutzte Geheimnis wird niemals über das Netzwerk übertragen. Darüber hinaus werden alle Benutzerkennwörter verschlüsselt, wenn sie zwischen dem Client und dem RADIUS-Server ausgetauscht werden. Der Verschlüsselungsprozess verhindert, dass jemand, der ein ungesichertes Netzwerk überwacht, das Kennwort eines Benutzers festlegt.

Gemeinsamer geheimer Schlüssel

Ein gemeinsamer geheimer Schlüssel ist eine Textzeichenfolge, die als Kennwort zwischen dem ONS15454 RADIUS-Client und dem RADIUS-Server dient. Gehen Sie wie folgt vor, um einen gemeinsamen geheimen Schlüssel zu erstellen:

1. Melden Sie sich beim Cisco Transport Controller (CTC) an.
2. Gehen Sie zur Netzwerkansicht.
3. Wählen Sie eine bestimmte ONS 15454 aus, um zur Gehäuseansicht zu wechseln.
4. Klicken Sie auf **Provisioning > Security > RADIUS Server**.
5. Geben Sie die IP-Adresse des RADIUS-Servers in das Feld IP-Adresse ein (siehe Pfeil A in Abbildung 1).
6. Geben Sie im Feld "Freier geheimer Schlüssel" einen freigegebenen geheimen Schlüssel ein. Ein gemeinsamer geheimer Schlüssel ist eine Textzeichenfolge, die als Kennwort zwischen einem RADIUS-Client und einem RADIUS-Server dient (siehe Pfeil B in Abbildung 1).
7. Geben Sie die RADIUS-Authentifizierungsportnummer in das Feld Authentifizierungsport ein (siehe Pfeil C in Abbildung 1).Die Standard-Authentifizierungsportnummer lautet 1812. Wenn es sich bei dem Knoten um eine ENE handelt, legen Sie für den Authentifizierungsport eine Zahl im Bereich von 1860 und 1869 fest.
8. Geben Sie die RADIUS Accounting-Portnummer in das Feld Accounting Port ein (siehe Pfeil

D in Abbildung 1).Die Standard-Accounting-Portnummer lautet 1813. Wenn es sich bei dem Knoten um eine ENE handelt, legen Sie für den Buchhaltungsport eine Zahl im Bereich von 1870 und 1879 fest.**Abbildung 1: Sicherheit RADIUS-Server**



Verwenden Sie freigegebene Geheimnisse, um sicherzustellen, dass ein RADIUS-aktiviertes Gerät, das mit demselben gemeinsamen geheimen Schlüssel konfiguriert wurde, alle RADIUS-Nachrichten außer der Access-Request-Nachricht sendet.

Gemeinsam genutzte Geheimnisse stellen sicher, dass die RADIUS-Nachricht bei der Übertragung nicht geändert wird. Mit anderen Worten, gemeinsame Geheimnisse wahren die Integrität der Nachrichten. Gemeinsam genutzte Geheimnisse verschlüsseln auch einige RADIUS-Attribute, z. B. User-Password und Tunnel-Password.

ONS 15454, Version 6.0, begrenzt die Länge eines gemeinsam genutzten Geheimhaltungsgrades auf 16 Zeichen. Ab ONS 15454 Version 6.2 plant Cisco jedoch, die maximale Länge auf 128 Zeichen zu erhöhen. Weitere Informationen finden Sie unter Cisco Bug ID CSCsc16614 (nur registrierte Kunden).

Die Gruppe für gemeinsam genutzte geheime Zeichen unterstützt:

- Buchstaben (Groß- und Kleinbuchstaben), z. B. A, B, a und b.
- Zahlen, z. B. 1, 2 und 3.
- Symbole, die alle Zeichen darstellen, die nicht als Buchstaben oder Ziffern definiert sind, z. B. >, (und *.

Zuordnung von Benutzergruppen

Ein Attributwert-Paar (AV) stellt eine Variable und einen der möglichen Werte dar, die die Variable enthalten kann. Innerhalb der ONS 15454 werden die Benutzer verschiedenen Sicherheitsgruppen zugeordnet, die auf dem Cisco AV-Paar basieren. Hier ein Beispiel:

"shell:priv-lvl=X", wobei X den Wert 0 bis 3 haben kann:

- 0 steht für RTRV.
- 1 steht für PROV.
- 2 steht für MAINT.
- 3 steht für SUPER.

Kennwort

Der RADIUS-Server und -Client schränkt die für ein Kennwort verwendeten Zeichen nicht ein. Der Ausschuss zur Bekämpfung des Terrorismus hat jedoch eine Einschränkung. Für ONS 15454, Version 6.0, gibt es folgende Zeichen, die von CTC unterstützt werden:

- Buchstaben (Groß- und Kleinbuchstaben), z. B. A, B, a und b.
- Zahlen, z. B. 1, 2 und 3.
- Nur die Sonderzeichen #, % und +.

Cisco plant, in späteren Versionen der ONS 15454 die Beschränkung auf Sonderzeichen aufzuheben. Weitere Informationen finden Sie unter Cisco Bug ID CSCsc16604 (nur registrierte Kunden).

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme