RADIUS-verificatieproblemen in ONS 15454 versie 6.0

Inhoud

Inleiding

Dit document beschrijft een aantal bekende problemen met de verificatie van de RADIUS-server (Dial-In User Service) op afstand in ONS 15454 versie 6.0 in een Cisco ONS 15454-omgeving.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ONS 15454 kaart
- RADIUS-server

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ONS 15454 versie 6.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

RADIUS is een systeem van gedistribueerde beveiliging dat toegang op afstand tot netwerken en netwerkservices garandeert tegen toegang door onbevoegden. RADIUS bestaat uit deze drie componenten:

- Een protocol met een beeldformaat waarin User Datagram Protocol (UDP)/IP wordt gebruikt
- Een server
- Een client

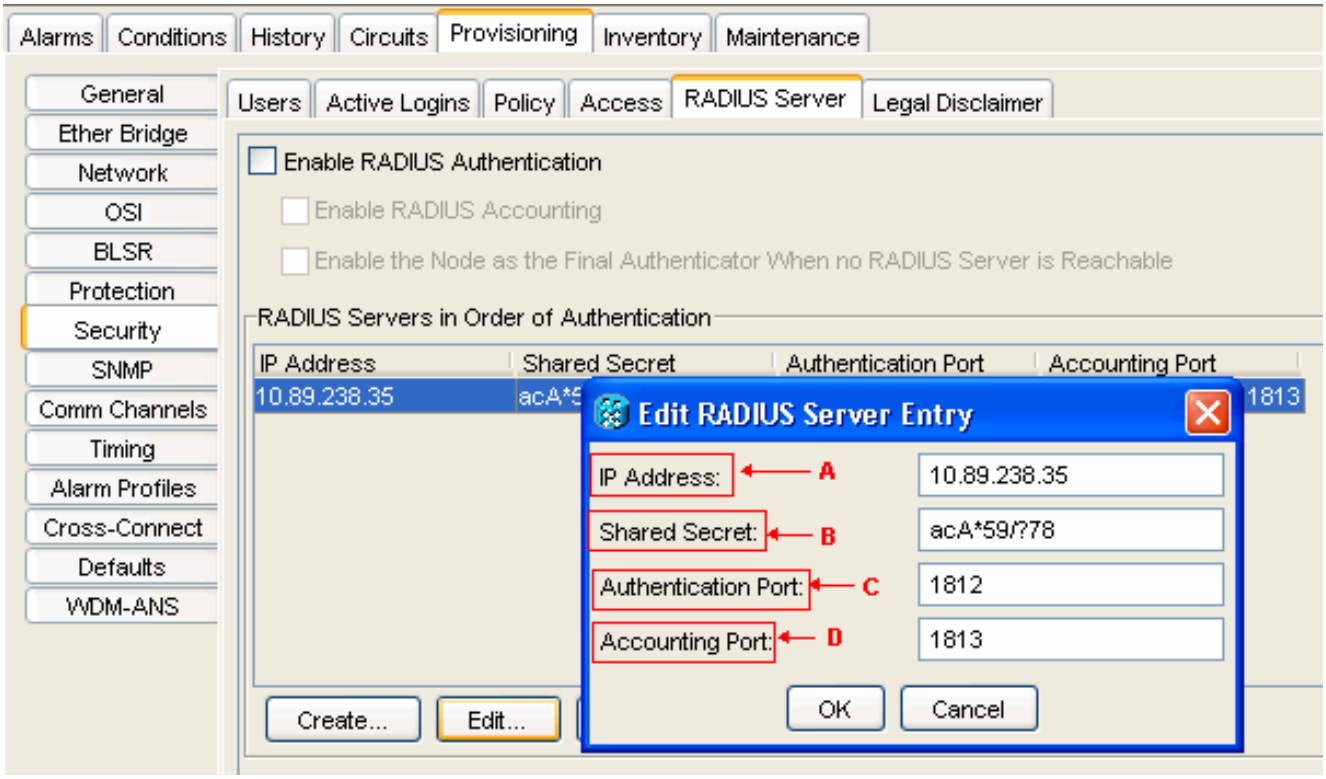
Een ONS 15454 knooppunt werkt als een client voor RADIUS. De client geeft gebruikersinformatie door aan aangewezen RADIUS-servers en werkt vervolgens in op de respons. RADIUS-servers ontvangen gebruikersverbindingsverzoeken, authentiek de gebruiker en retourneren alle configuratieinformatie die nodig is voor de client om de service aan de gebruiker te leveren.

Een gedeeld geheim bevestig transacties tussen de RADIUS-client en de server. Het gedeelde geheim wordt nooit via het netwerk verstuurd. Daarnaast worden alle wachtwoorden versleuteld wanneer deze worden uitgewisseld tussen de client en de RADIUS-server. Het encryptieproces heft de mogelijkheid op van iemand die een onbeveiligd netwerk controleert om het wachtwoord van een gebruiker te bepalen.

Gedeeld geheim

Een gedeeld geheim is een tekststring die fungeert als een wachtwoord tussen de ONS15454 RADIUS-client en de RADIUS-server. Voltooi deze stappen om een gedeeld geheim te maken:

1. Log in op Cisco Transport Controller (CTC).
2. Ga naar de netwerkweergave.
3. Selecteer een specifieke ONS 15454 om naar de shelf-weergave te gaan.
4. Klik op **Provisioning > Security > RADIUS-server**.
5. Typ het IP-adres van de RADIUS-server in het veld IP-adres (zie pijl A in afbeelding 1).
6. Typ een gedeeld geheim in het veld Gedeeld geheim. Een gedeeld geheim is een tekststring die fungeert als een wachtwoord tussen een RADIUS-client en een RADIUS-server (zie pijl B in afbeelding 1).
7. Typ het RADIUS-verificatiepoortnummer in het veld Verificatiepoort (zie pijl C in afbeelding 1).Het standaard authenticatiepoortnummer is 1812. Als het knooppunt een ENE is, stelt u de verificatiepoort in op een nummer binnen het bereik van 1860 en 1869.
8. Typ het RADIUS-accounting poortnummer in het veld Accounting Port (zie pijl D in afbeelding 1).Het standaard accounting poortnummer is 1813. Als het knooppunt een ENE is, stelt u de accounting poort in op een getal binnen het bereik van 1870 en 1879.**Afbeelding 1 - Beveiliging: RADIUS-server**



Gebruik gedeelde geheimen om ervoor te zorgen dat een RADIUS-enabled apparaat dat u met hetzelfde gedeelde geheim hebt ingesteld alle RADIUS-berichten behalve het Access-Application-bericht verstuurt.

Gedeelde geheimen zorgen dat het RADIUS-bericht niet wordt gewijzigd tijdens het transport. Met andere woorden, gedeelde geheimen houden de berichtintegriteit in stand. De gedeelde geheimen versleutelen ook bepaalde RADIUS-eigenschappen, bijvoorbeeld User-Password en Tunnel-Password.

ONS 15454 versie 6.0 beperkt de lengte van een gedeeld geheim tot 16 tekens. Vanaf ONS 15454 versie 6.2 is Cisco echter van plan de maximale lengte tot 128 tekens te verhogen. Raadpleeg Cisco bug-ID CSCsc16614 (alleen geregistreerde klanten) voor meer informatie.

Gedeeld geheime tekengroep ondersteunt:

- Brieven (hoofdletters en kleine letters), bijvoorbeeld A, B, a en b.
- De getallen bijvoorbeeld 1, 2 en 3.
- Symbolen, die alle tekens vertegenwoordigen die niet zijn gedefinieerd als letters of cijfers, bijvoorbeeld >, (en *.

Toewijzing van gebruikersbeveiligingsgroepen

Een eigenschap-waarde (AV) paar vertegenwoordigt een variabele en een van de mogelijke waarden die de variabele kan houden. Binnen ONS 15454 worden gebruikers in kaart gebracht aan verschillende beveiligingsgroepen op basis van Cisco AV-paar. Hierna volgt een voorbeeld:

"shell:priv-lvl=X" waarbij X waarde van 0 tot 3 kan zijn:

- 0 staat voor RTRV.
- 1 staat voor PROV.
- 2 staat voor MAINT.

- 3 staat voor SUPER.

Wachtwoord

De RADIUS-server en -client beperken de tekens die u voor een wachtwoord gebruikt niet. CTC heeft echter een beperking. Voor ONS 15454 versie 6.0 zijn hier de tekens die CTC ondersteunt:

- Brieven (hoofdletters en kleine letters), bijvoorbeeld A, B, a en b.
- De getallen bijvoorbeeld 1, 2 en 3.
- Alleen de #, % en + speciale symbolen.

Cisco is van plan de beperking van speciale symbolen in latere versies van ONS 15454 te verwijderen. Raadpleeg Cisco bug-ID CSCsc16604 (alleen geregistreerde klanten) voor meer informatie.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems