Secure Access Control System 5.x en latere FAQ

Inhoud

Inleiding

Dit document bevat antwoorden op de meest frequent gestelde vragen (FAQ) met betrekking tot Cisco Secure Access Control System (ACS) 5.x en hoger.

Verificatiegerelateerde problemen

Q. Kan een paar gebruikers/groepen van de interne ACS 5.x-gegevensbank worden uitgesloten van het beleid van het gebruikerswachtwoord (Systeembeheer > Gebruikers > Verificatieinstellingen)?

A. Standaard moet elke interne gebruiker van een database voldoen aan het wachtwoordbeleid van de gebruiker. Momenteel kunnen geen gebruikers/groepen van de interne ACS 5.x-gegevensbank worden uitgesloten.

Q. Kan een paar GUI beheerders van ACS 5.x worden uitgesloten van het beleid van het administratieve gebruikerswachtwoord (systeembeheer > beheerders > Instellingen > Verificatie)?

A. Standaard moet elke GUI-beheergebruiker voldoen aan het wachtwoordbeleid van de administratieve gebruiker. Momenteel kan geen enkel administratief gebruik van ACS 5.x worden uitgesloten.

V. biedt ACS 5.x ondersteuning voor VMWare-tools?

A. Nee. Op dit moment worden VMWare-gereedschappen niet ondersteund met ACS versie 5.x. Raadpleeg Cisco bug-ID CSCtg50048 (alleen geregistreerde klanten) voor meer informatie.

Q. Wat zijn de ondersteunde MAP-verificatieprotocollen voor ACS 5.x wanneer LDAP als identiteitswinkel is ingesteld?

A. Wanneer LDAP als identiteitswinkel wordt gebruikt, steunt ACS 5.2 alleen PEAP-GTC-, EAP-FAST-GTC- en EAP-TLS-protocollen. Het ondersteunt EAP-FAST MSCHAPv2, PEAP-

MSCHAPv2 en EAP-MD5 niet. Raadpleeg voor meer informatie het verificatieprotocol en de compatibiliteit van de gebruikersdatabase.

Q. Waarom is de authenticatie voor WLC met de gebruikstraal voor ACS mislukt, en waarom heeft ACS geen mislukte pogingen getoond?

A. Er is een probleem met **ACS 5.0- en WLC-interoperabiliteit** vóór pleister 4. Download de pleister 8 en breng de pleister aan op de CLI. Gebruik TFTP niet om dit probleem op te lossen.

Q. Waarom kan ik geen tar.gz-bestanden herstellen die met de opdracht back-up-log in ACS 5.2 werden gemaakt?

A. U kunt logbestanden die van een back-up zijn gemaakt, niet herstellen met de opdracht **reservekopie**. U kunt alleen de bestanden herstellen waarvan een back-up is gemaakt voor de ACS-configuratie en ADE-OS. Raadpleeg de **opdrachten back-up** en **back--bestanden** in de CLI **Referentiegids voor het Cisco Secure Access Control System 5.1 voor meer informatie.**

Kan ik het aantal onsuccesvolle wachtwoordpogingen voor ACS 5.2 beperken?

A. Nee. Deze optie is niet beschikbaar voor ACS 5.2, maar wordt verwacht te worden geïntegreerd in ACS 5.3. Raadpleeg het gedeelte Functies Niet ondersteund in de Releaseopmerkingen voor Cisco Secure Access Control System 5.2 voor meer informatie.

Q. Ik kan de optie niet gebruiken om het wachtwoord te wijzigen bij volgende inloggen voor interne gebruikers in ACS 5.0. Hoe los ik dit probleem op?

A. De optie om het wachtwoord te wijzigen bij volgende inloggen wordt niet ondersteund in ACS 5.0. Ondersteuning voor deze optie is beschikbaar in ACS 5.1 en latere versies.

Wat betekent dit alarm op ACS?

```
Cisco Secure ACS - Alarm Notification
Severity: Warning
Alarm Name delete 20000 sessions
Cause/Trigger active sessions are over limit
Alarm Details session is over 250000
```

A. Deze fout betekent dat wanneer de ACS-weergave een limiet van 250.000 sessies bereikt, het alarm gooit om 20.000 sessies te verwijderen. De ACS-Viewgegevensbank slaat alle vorige authenticatiesessies op en wanneer het 250.000 bereikt, geeft het een alarm om de cache op te ruimen en 20.000 sessies te verwijderen.

V. Hoe pak ik deze foutmelding op: `Verificatie mislukt: 24407 Gebruikersverificatie tegen actieve map mislukt, omdat de gebruiker zijn wachtwoord moet wijzigen`?

A. Deze foutmelding wordt weergegeven wanneer er een probleem is met het wachtwoordbeheer tijdens de SDI-verificatie. ACS 5.x wordt gebruikt als een Radius-proxy en de gebruikers moeten zijn gewaarmerkt door een RSA-server. De Radius-proxy naar RSA zal alleen werken zonder wachtwoordbeheer. De reden is dat de OTP-waarde moet worden hersteld door de Radius-server om de wachtwoordwaarde aan de RSA-server te bepalen. Wanneer het wachtwoordbeheer in de tunnelgroep is ingeschakeld, wordt het verzoek om Radius verstuurd met de eigenschappen MS-

CHAPv2. RSA ondersteunt MS-0CHAPv2 niet; zij ondersteunt alleen PAP.

Schakel wachtwoordbeheer uit om dit probleem op te lossen. Raadpleeg voor meer informatie Cisco bug-ID CSCsx47423 (alleen geregistreerde klanten).

V. Is het mogelijk ACS-admin te beperken om alleen bepaalde hulpmiddelen binnen ACS 5.1 te beheren?

A. Neen, het is niet mogelijk ACS-admin te beperken om alleen bepaalde hulpmiddelen binnen ACS 5.1 te beheren.

Q. Ondersteunt ACS QoS bij authenticatie zodat RADIUS voorrang kan krijgen boven TACACS?

A. Neen, ACS ondersteunt QoS niet op het gebied van authenticatie. ACS geeft geen prioriteit aan RADIUS-verificatieverzoeken boven TACACS- of TACACS-verzoeken boven RADIUS.

Q. Kan ACS 5.x-proxy-TACACS- en RADIUS-authenticaties voor andere TACACS- of RADIUS-servers?

A. Ja, alle ACS 5.x versies kunnen de RADIUS-authenticaties aan andere RADIUS-servers proxy uitvoeren. ACS 5.3 en later kunnen de TACACS-authenticaties aan andere TACACS-servers volstaan.

Q. Kan ACS 5.x de inbeleigenschappen van een actieve gebruiker controleren om toegang te verlenen?

A. Ja, in ACS 5.3 en later kunt u de toegang tot de inbelrechten van een gebruiker toestaan, ontkennen en controleren. De permissies worden gecontroleerd tijdens authenticaties of vragen van Actieve Map. Het wordt ingesteld in het woordenboekje Active Directory.

V. ondersteunen ACS 5.x het CHAP of de MSCHAP-verificatietypen voor TACACS+?

A. Ja, de verificatietypen TACACS+ CHAP en MSCHAP worden ondersteund in ACS versies 5.3 en later.

Q. Kan ik het wachtwoordtype van een ACS interne gebruiker op een externe databank instellen?

A. Ja, in ACS 5.3 en later kunt u het wachtwoordtype van een ACS interne gebruiker instellen. Deze optie was beschikbaar in ACS 4.x.

Q. Kan ik een authenticatie doorgeven of nalaten op basis van het tijdstip waarop de gebruiker in de ACS Interne Identity Store is gemaakt?

A. Ja, in ACS 5.3 en later kunt u het **aantal uren** gebruiken **sinds de Creatie van de Gebruiker** om uw beleid te creëren. Deze eigenschap bevat het aantal uren sinds de gebruiker in de Interne

Identity Store werd aangemaakt tot het tijdstip van de huidige verificatieaanvraag.

Q. Kan ik wildkaarten gebruiken om een nieuwe host in de ACS interne database toe te voegen?

A. Ja, ACS 5.3 en laat u later toe om wildcards te gebruiken wanneer u nieuwe hosts in de interne identiteitswinkel toevoegt. Het stelt u ook in staat om alle kaarten in te voeren (nadat u de eerste drie octetten hebt ingevoerd) om alle apparaten van de geïdentificeerde fabrikant te specificeren.

Q. Kan ik IP adresgroepen op ACS 5.x configureren en ze van ACS toewijzen?

A. Nee, het is momenteel niet mogelijk IP-adresgroepen te maken op ACS 5.x.

Q. Kan ik het IP-adres van de AAA-cliënt zien waar het verzoek in het FAILED AUTHENTICATION-rapport kwam?

A. Nee, het is niet mogelijk om het IP-adres van de AAA-cliënt te zien vanaf waar het verzoek binnenkwam.

V. Wat is de weergave van het herstel van de logberichten in ACS 5.3?

A. ACS 5.3 biedt een nieuwe functie om alle logbestanden te herstellen die gemist worden wanneer de weergave omlaag is. ACS verzamelt deze gemiste loggen en slaat ze op in zijn database. Met deze functie kunt u de gemiste logbestanden uit de ACS-database terughalen naar de weergave-database nadat er een back-up is gemaakt van de weergave. Om deze functie te kunnen gebruiken, moet u de configuratie van het logbericht voor het herstellen van het **wachtwoord** instellen. Raadpleeg voor meer informatie over het configureren van het logberichtherstel, systeembewerkingen van het monitorvenster en het melden van meldingen.

Q. Kan ik de ACS 5.x database comprimeren door de database-compress opdracht van de Solution Engine CLI uit te geven? Deze optie was beschikbaar in ACS 4.x.

A. Ja, in ACS 5.3 en later, vermindert de **database-compress** opdracht de ACS-databases met een optie om de ACS-transactietabel te verwijderen. De beheerders van ACS kunnen deze opdracht uitgeven om de omvang van de database te beperken. Dit helpt de grootte van de database en de tijd die nodig is voor back-ups en volledige synchronisatie te beperken.

Kan ik een AAA-client doorzoeken op basis van zijn IP-adres?

A. Ja, ACS 5.3 en staat u later toe om een netwerkapparaat te zoeken met zijn IP adres. U kunt ook kaarten en het bereik gebruiken om een specifieke set netwerkapparaten te doorzoeken.

Q. Kan ik een voorwaarde creëren gebaseerd op het tijdstip waarop de gebruiker werd opgericht in de ACS Interne Identity Store?

A. Ja, in ACS 5.3 en later kunt u het **aantal uren** gebruiken **sinds de** attributie **van de Creatie van de Gebruiker** die u in staat stelt om de voorwaarden van de beleidsregel te configureren, gebaseerd op het tijdstip waarop de gebruiker in ACS Interne Identity Store werd gemaakt. Bijvoorbeeld: ALS **groep=HelpDesk&numberUrenByUserCreation>48** dan afwijzen. Deze

eigenschap bevat het aantal uren sinds de gebruiker in de Interne Identity Store werd gemaakt tot het tijdstip van de huidige authenticatieaanvraag.

Q. Kan ik controleren in welke Identity Store de gebruiker is geauthentiseerd in de autorisatie sectie van een servicebeleid?

A. Ja, in ACS 5.3 en later kunt u de eigenschap **Verificatie Identity Store** gebruiken, die u in staat stelt om de beleidsregelvoorwaarden te configureren op basis van de Verificatiewinkel. Bijvoorbeeld: ALS **VerificatieIdentityStore=LDAP_NY** dan afwijzen. Deze eigenschap bevat de naam van de gebruikte Identity Store en wordt met de naam van de betrokken Identity Store bijgewerkt na een geslaagde verificatie.

Q. Wanneer gaat ACS naar de volgende Identity Store gedefinieerd in de Identity Store sequentie?

A. Het ACS gaat naar de volgende Identity Store die in deze scenario's is gedefinieerd:

- Een gebruiker is niet in de eerste Identity Store gevonden
- Er is geen Identity Store beschikbaar in de volgorde

Wat is het beleid inzake accountantsbeperking in ACS 5.3?

A. Met het beleid voor accountbeperking kunt u de gebruikers van Interne Identity Store uitschakelen wanneer de ingestelde datum niet langer is dan de toegestane datum, het ingestelde aantal dagen groter is dan de toegestane dagen of het aantal opeenvolgende onsuccesvolle inlogpogingen de drempel overschrijdt. De standaardwaarde voor date is meer dan 30 dagen vanaf de huidige datum. De standaardwaarde voor dagen mag niet meer dan 60 dagen vanaf de huidige dag zijn. De standaardwaarde voor mislukte pogingen is 5.

Q. Kan ik het wachtwoord van een interne gebruiker van ACS via telnet wijzigen?

A. Ja, u mag het wachtwoord van een interne gebruiker van de gegevensbank wijzigen met behulp van TACACS+ via telnet. U moet het **Wachtwoord voor wijziging inschakelen** voor **TELNET inschakelen** bij **Wachtwoordwijziging** op ACS 5.x.

Q. Kan de primaire ACS 5.x-instantie de reservekopieën automatisch periodiek bijwerken of zou het slechts moeten gebeuren wanneer een configuratie is gewijzigd?

A. ACS 5.x zal onmiddellijk worden herhaald in de Secundaire ACS wanneer u wijzigingen aanbrengt op het Primaire ACS. Als u bovendien geen wijzigingen in het Primaire ACS aanbrengt, zal het elke 15 minuten een kracht-replicatie uitvoeren. Op dit punt is er geen optie om de timer te controleren zodat ACS de informatie na een specifieke tijd kan repliceren.

Q. Kan ik een rapport over ACS 5.x van alle gebruikers bekijken/exporteren die momenteel geregistreerd en geauthentiseerd zijn van ACS op verschillende NAS-klanten?

A. Ja, het is mogelijk. Er zijn twee afzonderlijke rapporten voor RADIUS en TACACS+. U kunt ze

vinden onder **Monitoring & Reports > Rapporten > Catalyst > Session Directory > RADIUS actieve sessies en TACACS actieve sessies.** Beide rapporten zijn gebaseerd op de boekhoudkundige informatie van de NAS-klanten aangezien deze u in staat stelt te volgen wanneer de gebruiker zich aansluit en uitlogt. De sessiegeschiedenis stelt u zelfs in staat om informatie van het begin te krijgen en tijdens een bepaalde dag te stoppen.

Gerelateerde informatie

- Ondersteuning voor Cisco Secure Access Control System
- Technische ondersteuning en documentatie – Cisco Systems