ACS 5.x en later - probleemoplossing voor beveiligde ACS

Inhoud

Inleiding

Dit document bevat informatie over de manier waarop u Cisco Secure Access Control System (ACS) kunt oplossen en over de oplossing van foutmeldingen.

Raadpleeg voor informatie over de oplossing van Cisco Secure ACS 3.x en 4.x voor problemen

met Secure Access Control Server (ACS 3.x en 4.x) bij de probleemoplossing.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op versie 5.x van het Cisco Secure Access Control System en hoger.

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.

Probleem: "Fout: Opslaan van de actieve configuratie naar opstartbeeld %.Kennis niet gevonden in de bundel" op ACS-apparaat tijdens upgrade

De `fout: Opslaan van de actieve configuratie naar startup met succes %` Kennis `niet gevonden in de bundelfout` verschijnt als een poging wordt gedaan om de ACS Express te verbeteren van 5.0 naar 5.0.1.

Oplossing

Voltooi deze stappen om het ACS-apparaat zonder problemen te upgraden:

1. Download patch 9 (5-0-0-21-9.tar.gpg) en ADE-OS (ACS_5.0.0.21_ADE_OS_1.2_upgrade.tar.gpg) van: **Cisco.com > Ondersteuning > Download software > Security > Cisco Secure Access Control System 5.0 > Secure Access Control System-software > 5.0.21**
2. Nadat u de twee bestanden hebt geïnstalleerd, installeert u de ACS 5.1 upgrade ACS_5.1.0.44.tar.gz. Dit is beschikbaar vanaf hetzelfde pad vanaf de vorige stap.
3. Gebruik deze opdracht om de upgrade te installeren:

```
application upgrade
```

Dit voltooit de upgradeprocedure.

Raadpleeg het gedeelte Besturing van een ACS-server van 5.0 tot 5.1 voor meer informatie over het upgraden van het ACS-apparaat.

Probleem: Kan ACS Server 5.x niet opnieuw starten vanuit GUI

In deze sectie wordt uitgelegd waarom u de ACS-serverversie 5.x niet uit de GUI kunt hervatten.

Oplossing

Er is geen optie beschikbaar om de ACS 5.x-server vanuit de GUI opnieuw te starten. De ACS kan alleen vanaf de CLI worden herstart.

Probleem: Instellen van actieve redexverificatie met ACS 5.2

Bij het opzetten van Active Directory (AD) authenticatie voor een nieuwe 5.2 ACS-service, wordt deze foutmelding ontvangen:

```
Onverwachte RPC-fout: Toegang geweigerd wegens onverwachte configuratie of netwerkfout. Probeer
de –breedgedragen optie of voer "adinfo –diag" uit.
```

Oplossing

De ACS moet vergunningen schrijven om te authentiseren met de AD. Om deze kwestie op te lossen, geef tijdelijk schrijfrecht aan de dienstrekening.

Probleem: Kan niet meer dan 100 pagina's in het accounting rapport weergeven

Wanneer u probeert een aangepast AAA-accounting rapport te genereren met ACS versie 5.1, kunt u niet meer dan 100 pagina's bekijken. Dit geldt niet voor meerdere oudere rapporten. Hoe verandert u deze instelling om alle pagina's te zien?

Oplossing

U kunt het aantal pagina's in de ACS niet wijzigen omdat het maximale aantal weergegeven pagina's standaard slechts 100 is. Om deze beperking te overwinnen en oudere statistieken te bekijken, moet u de filteropties wijzigen zodat er specifiekere overeenkomsten kunnen worden gemaakt. Als u bijvoorbeeld probeert het rapport de afgelopen dertig dagen te genereren, bevat het een groot volume en tonen de laatste 100 pagina's de activiteit wellicht slechts gedurende het laatste uur. Hier is het gebruik van de filteropties aanbevolen. Het filteren optie als gebruiker-ID gebruiken en het tijdbereik instellen levert veel oudere rapporten op.

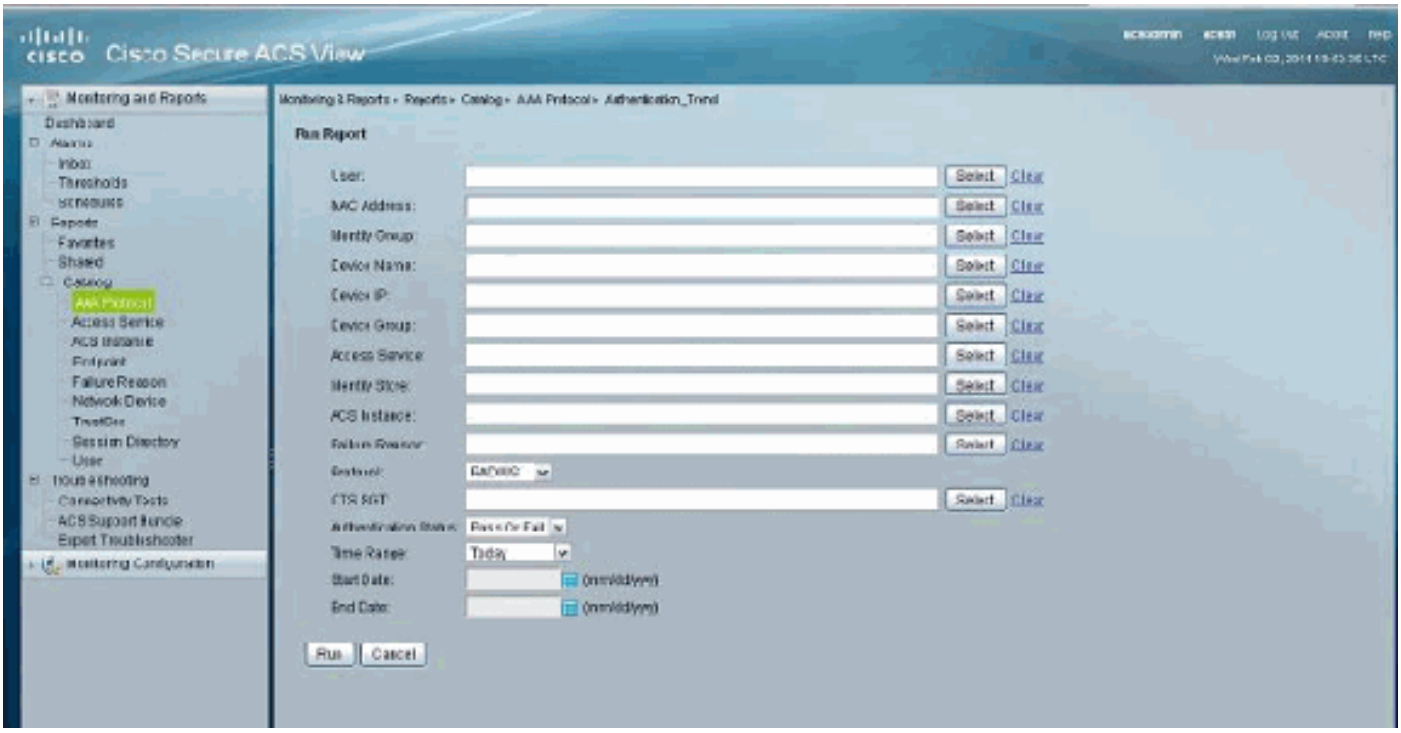
Probleem: Kan geen rapport voor een groep apparaten opleveren voor een goede/een defecte authenticatie

Dit probleem doet zich voor wanneer u het authenticatierapport alleen voor een groep van zes routers/switches probeert te genereren, niet voor alle apparaten. ACS versie 4.x wordt gebruikt.

Oplossing

Dit is niet mogelijk bij ACS 4.x. U moet naar ACS 5.x migreren omdat deze optie beschikbaar is bij die versie. U kunt rapporten extraheren voor de specifieke groep apparaten door de Catalaanse rapporten te genereren.

Raadpleeg deze afbeelding voor een beter begrip:



Probleem: De databank voor toezicht en rapportage is momenteel niet beschikbaar. Proberen opnieuw te verbinden in 5 seconden.

Wanneer u op het venster Start Monitoring and Report van ACS 5.x klikt, wordt deze foutmelding ontvangen: `De databank voor toezicht en rapportage is momenteel niet beschikbaar. Proberen opnieuw te verbinden in 5 seconden. Als het probleem blijft bestaan, kunt u contact opnemen met de ACS-beheerder.`

Oplossing

Voer een van deze tijdelijke oplossingen uit om dit probleem op te lossen:

- Start de ACS-services van CLI opnieuw door deze opdrachten uit te geven:
  ```
  application stop acs
  application start acs
  ```
- upgrade naar het laatste beschikbare pleister. Raadpleeg Upgradepatches toepassen voor meer informatie hierover.

Probleem: 22056 Onderwerp niet in het (de) daarop van toepassing zijnde identiteitsbewijs(s)

AD-gebruikers worden niet geauthentiseerd met ACS versie 5.x en ontvangen deze foutmelding: `22056 Onderwerp niet in het (de) desbetreffende identiteitsbewijs(s).`

Oplossing

Deze foutmelding doet zich voor wanneer ACS er niet in geslaagd is om de gebruiker in de eerste genoemde database te vinden die in de reeks Identity Store is ingesteld. Dit is een informatief bericht en heeft geen invloed op de prestaties van het ACS. De manier waarop ACS 5.x de authenticatie voor interne of externe gebruikers uitvoert is anders dan de vorige 4.x versie. Met de versie 5.x wordt een optie genoemd Identity Store Sequence om de sequentie te definiëren van gebruikersdatabases die echt geauthentiseerd moeten worden. Raadpleeg voor meer informatie de Oplossingen voor Identity Store configureren.

Als u deze fout ontvangt wanneer u de ACS gebruikt om verzoeken tegen een Child Domain te authentiseren, dan moet u een UPN achtervoegsel of het prefix van NETPDN aan de gebruikersnaam toevoegen. Raadpleeg voor meer informatie de opmerkingen in het gedeelte Microsoft AD.

Probleem: Kan ACS niet met actieve map integreren

De gebruikers kunnen ACS met Actieve Map niet integreren en de foutmelding `Samba Port Status` wordt ontvangen.

Oplossing

Om dit probleem op te lossen, moet u ervoor zorgen dat deze poorten open zijn om de functionaliteit van de actieve map te ondersteunen:

- Samba-poort - TCP 445
- LDAP - TCP 389
- LDAP - UDP 389
- KDC - TCP 88
- kpasswd - TCP 464
- NTP- UDP 12.3
- Wereldwijde catalogus - TCP 3268
- DNS - UDP 53

De ACS moet alle DC's in het domein bereiken om de ACS-AD-integratie compleet te maken. Zelfs als één van de DC's niet bereikbaar is vanuit het ACS-systeem gebeurt de integratie niet. Raadpleeg Cisco bug-ID CSCte92062 (alleen geregistreerde klanten) voor meer informatie.

Probleem: Kan ACS niet integreren met LDAP

In dit document wordt ACS 5.2 gebruikt als een AAA RADIUS-server voor 802.1X-implementatie. 802.1X kan met succes worden gebruikt met ACS met behulp van de interne gebruikerswinkel, maar er zijn kwesties die ACS en LDAP integreren. Deze foutmelding wordt weergegeven:

```
Radius authentication failed for USER: example MAC:
UU-VV-WW-XX-YY-ZZ AUTHTYPE: PEAP(EAP-MSCHAPv2)
EAP session timed out : 5411 EAP session timed out
```

Oplossing

In dit geval wordt bij het PEAP gebruik gemaakt van LDAP en de gebruikte interne echtheidsmethode is een zwak punt v2. Dit zal mislukken omdat LDAP niet wordt ondersteund voor PEAP (PEAP-mschap v2). Aanbevolen wordt gebruik te maken van e-toetsen of de AD.

Probleem: "Cisco acs_interne_Operations_diagnostische fout: Kan niet naar lokaal opslagbestand schrijven" Fout-bericht

Tijdens de replicatie van het ACS-systeem wordt het primaire ACS niet correct herhaald en toont deze foutmelding:

```
csco acs_internal_operations_diagnostics error: could
 not write to local storage file
```

Oplossing

Start de ACS-services opnieuw en controleer of de kritisch registreren is uitgeschakeld. Raadpleeg voor meer informatie Cisco bug-ID CSCth6302 (alleen geregistreerde klanten). Als dit niet helpt, neemt u contact op met Cisco TAC om het laatste ACS-pleister geschikt te maken om dit probleem op te lossen.

Probleem: Kan ACS 5.1 niet integreren met Active Directory

Bij het implementeren van AD-integratie wordt deze foutmelding ontvangen:

```
Error while configuring Active Directory:Using writable
 domain controller:test1.test.pvt Authentication error due unexpect
 configuration or network error. Please try the --verbose option or run 'adinfo
 -diag' to diagnose the problem. Join to domain 'test.pvt', zone 'null'
 failed.
```

Oplossing

Voltooi dit tijdelijke oplossing voor dit probleem:

1. Verwijdert de bestaande computeraccount op AD.
2. Maak een nieuwe OU.
3. Ga naar Eigenschappen van de OU en maak **erfrechten** los.
4. Maak een nieuwe computeraccount voor de ACS in de nieuwe OU.
5. Laat de AD kopiëren.
6. Probeer mee te doen met de AD vanaf de ACS GUI.

In bepaalde gevallen is het ook handig als u contact opneemt met Microsoft en de Hot Fix toepast.

Probleem: Kan ACS 5.x niet configureren om reguliere expressies in de service selectieregels te herkennen

Oplossing

Dit is niet mogelijk omdat het nog niet wordt ondersteund in ACS 5.x.

Probleem: SFTP-back-up werkt niet wanneer Cisco Works als SFTP-server wordt gebruikt

Wanneer de netwerkbron op de CiscoWorks server staat, werkt de reserveplanner prima met andere SFTP-clients maar niet ACS 5.2. In het bijzonder, wanneer u probeert verbinding te maken met de SFTP-server vanuit de ACS, `kan de` foutmelding `niet onderhandelen over een belangrijke` wisselkoersfout.

Oplossing

In dit geval is de SFTP-server geen FIPS-compatibel apparaat met behulp van de DH 14-groep. ACS ondersteunt alleen servers met DH 14-ondersteuning omdat deze FIPS-compatibel is. Raadpleeg voor meer informatie over dit onderwerp de bekende beperkingen in ACS 5.2.

Probleem: "Ongeldige EAP lading gedropt"

De `fout: Ongeldige MAP-lading verloren` foutmelding wordt ontvangen terwijl de draadloze gebruikers worden geauthentiseerd op ACS 5.0-pleister 7.

Oplossing

Dit is een waargenomen gedrag en wordt aangepakt in Cisco bug IDs CSCsz54975 (alleen geregistreerde klanten) en CSCsy46036 (alleen geregistreerde klanten).

Om dit probleem op te lossen, moet u overgaan op ACS 5.0-patch 9, dat als onderdeel van de upgrade naar 5.1 of 5.2 vereist is. Raadpleeg Upgradeversie van de databank voor volledige informatie. Dit bevat ook informatie over het upgraden naar pleister 9.

Probleem: "ACS-uitvoering proces loopt op dit moment niet."

Gebruikers kunnen niet inloggen op de ACS-GUI en deze foutmelding wordt ontvangen.

```
"De ACS-uitvoering-procedure loopt op dit moment niet. Veranderingen kunnen in de ACS-
configuratie worden aangebracht (deze zullen in de database worden opgeslagen) maar de
wijzigingen zullen niet van kracht worden totdat het run-proces opnieuw is gestart."
```

Oplossing

Het uitvoeren van het programma vanuit de CLI-indeling wordt handmatig hergestart en het apparaat wordt opnieuw opgestart. Dit is een ondergeschikt probleem en creëert geen enkele prestatiekwestie voor de ACS. Er zijn twee kleine insecten gedeponeerd om dit gedrag te observeren. Raadpleeg voor meer informatie Cisco bug-ID's CSCtb9448 (alleen geregistreerde klanten) en CSCtc75323 (alleen geregistreerde klanten).

Om de baanbrekende processen handmatig te hervatten, geeft u deze opdrachten uit van de ACS CLI:

- acs - stop
- acs - start

Probleem: Kan de gebruikers met het wachtwoord niet exporteren

U kunt de gebruikersdatabase naar een ander ACS 5.x met een CSV-bestand exporteren en importeren, maar het veld gebruikerswachtwoord is niet beschikbaar (weergegeven blanco). Hoe verplaats je de lokale identiteitswinkel van een ACS naar een andere die de wachtwoordinformatie bevat?

Oplossing

Dit is niet mogelijk, aangezien dit een inbreuk op de beveiliging wordt. In dit geval is het uitvoeren van een back-up- en herstelprocedure een tijdelijke oplossing. Maar de beperking tot deze tijdelijke oplossing is dat de back-up en het herstel alleen werken voor een ander ACS met een vergelijkbare configuratie.

Probleem: ACS-interne gebruikers worden met tussenpozen uitgeschakeld

ACS-gebruikers worden met tussenpozen uitgeschakeld met een `Wachtwoord verlopen` bericht. Het wachtwoordverloopbeleid is voor 60 dagen ingesteld, maar deze gebruikers moeten handmatig in- en uitschakelen om toegang te verkrijgen.

Oplossing

Dit gedrag wordt waargenomen en gedeponeerd in Cisco bug-ID CSCtf06311 (alleen geregistreerde klanten). Dit probleem kan worden opgelost door pleister 3 op ACS 5.1 toe te passen. Om alle opgeloste kwesties onder pleister 3 te bekijken, zie Opgeloste kwesties in Cumulatieve Patch ACS 5.1.0.44.3. Raadpleeg voor gerelateerde informatie over hoe de pleister te verbeteren de toepassing van upgrade-patches.

Probleem: "TACACS+ verificatieaanvraag beëindigd met fout"

Het ACS-verificatierapport toont de `TACACS+-verificatieaanvraag die is afgesloten met een foutmelding`.

Oplossing

Dit gebeurt wanneer de TACACS-verificatie het servicetype op PPP heeft ingesteld. Raadpleeg Cisco bug-ID CSCte16911 (alleen geregistreerde klanten) voor meer informatie.

Probleem: "Radius-verificatieaanvraag verworpen vanwege een kritische logfout"

Radius-verificatie wordt verworpen omdat het `verzoek` om `Radius-verificatie is verworpen omdat de` foutmelding `kritisch registreren` is.

Oplossing

Deze fout is gedetailleerd in Cisco bug-ID CSCth6302 (alleen geregistreerde klanten).

Probleem: ACS-weergaveinterface toont "Data Upgrade Down" bovenaan de pagina wanneer ACS van 5.2 tot 5.3 is bijgewerkt

De interface ACS-weergave toont een `upgrade van gegevens mislukt` boven op de pagina wanneer de ACS-upgrade van 5.2 naar 5.3 wordt uitgevoerd.

Oplossing

Deze fout is in Cisco bug-id CSCtu15651 gedetailleerd (alleen geregistreerde klanten).

Probleem: Uitgeven met "Wachtwoord wijzigen bij volgende inlogoptie" op Cisco ACS 5.0

Oplossing

In ACS 5.0 kan de wachtwoordverloopfunctie (de gebruiker moet het wachtwoord wijzigen bij de volgende aanmelding) in de lokale gebruiker ID Store worden geselecteerd maar werkt niet. Een verzoek om verbetering CSCtc31598 stelt de kwestie in ACS versie 5.1 vast.

Probleem: "% Aangepaste upgrade mislukt, fout - 999. Controleer ADE-logbestanden op details, of herstart met - debug-toepassing geïnstalleerd - ingeschakeld" op ACS-apparaat tijdens upgrade

De `% applicatie is mislukt, fout -999. Controleer ADE-logbestanden op details, of herrun met - debug-applicatie geïnstalleerd -` deze fout verschijnt toen er een poging werd gedaan om een ACS Express te verbeteren van 5.0 naar 5.0.1.

Oplossing

Deze fout doet zich voor wanneer de gebruikte opslagplaats TFTP is en de bestandsgrootte groter is dan 32 MB. ACS Express kan bestanden van meer dan 32 MB niet verwerken. Gebruik FTP als opslagplaats om dit probleem op te lossen, zelfs als de bestandsgrootte meer dan 32 MB bedraagt.

Probleem: Fout: "Verificatie mislukt: 12308 Cliënt verzonden Resultaat TLV met melding van storing"

De `verificatie is mislukt: 12308 Client verzonden Resultaat TLV die op een fout wijst`, treedt op

op in het ACS wanneer u voor het eerst probeert te authenticeren. Verificatie werkt voor de tweede keer.

Oplossing

Deze fout kan worden opgelost wanneer u **Fast Ethernet** uitschakelt. Een upgrade naar **parkeren 2 van ACS versie 5.2** helpt u het probleem op te lossen zonder dat de Fast Reconconnect wordt uitgeschakeld.

Deze fout kan ook worden opgelost wanneer u **Gedwongen cryptobinding** op de aanvrager uitschakelt. Raadpleeg Cisco bug-ID CSCtj31281 (alleen geregistreerde klanten) voor meer informatie.

Probleem: Fout "2495 Active Directory servers is niet beschikbaar"

Verificatie start bij fout: `2495 actieve servers zijn niet beschikbaar.` in de ACS 5.3-stammen.

Oplossing

Controleer het bestand ACSADAgent.log via de CLI van de ACS 5.x voor berichten zoals:`Mar 11 00:06:06 xlpacs01 adclient[30401]: INFO <bg:bindingRefresh> base.bind.healing Verloren verbinding met xxxxxxx. Invoerend in ontkoppelde modus: losmaken.` Als u de `modus Actief` ziet `in de ontkoppelde modus:` Dit betekent dat ACS 5.3 geen stabiele verbinding met Active Directory kan onderhouden. De tijdelijke versie is switch naar LDAP of een lagere ACS-versie naar 5.2. Raadpleeg Cisco bug-ID CSCtx71254 (alleen geregistreerde klanten) voor meer informatie.

Probleem: Fout "5411 EAP sessie geplaatst"

`5411 Met de MAP overeengekomen` foutmeldingen worden op ACS 5.x ontvangen.

Oplossing

EAP sessie-onderbrekingen zijn vrij gebruikelijk bij PEAP waar de veeleisende herstart-authenticatie na het eerste pakket naar de RADIUS-server gaat en meestal geen indicatie van een probleem zijn.

De stroom die vaak wordt gezien is:

```
Supplicant ------------- Authenticator -------------- ACS
Connect
<------------------Request for Identity
----------------------> Response Identity ------------->
<--------------   EAP Challenge <-----------------
EAPOL-Start ------------->
normal flow ending in successful authentication.......
```

Uiteindelijk is de echtheidscontrole succesvol. Er blijft echter een draad open op het ACS als gevolg van de abrupte herstart van de MAP-sessie door de aanvrager, die leidt tot een

succesvolle authenticatie gevolgd door het MAP-bericht voor de tijdelijke versie van de sessie. Dit is vaak te wijten aan het bestuurdersniveau van de machine. Zorg ervoor dat de NIC/Wireless-stuurprogramma's op de clientmachine zijn bijgewerkt. U kunt de client en het filter opnemen op EAP || EAPOL om te zien wat de cliënt ontvangt of verstuurt bij de verbinding.

Probleem: 802.1x-verificatie werkt niet als meldingsbeperkingen op de actieve map zijn ingesteld

802.1x-verificatie werkt niet als de gebruikers beperkingen voor aanmelding hebben ingesteld in de actieve map.

Oplossing

Als u openings beperkingen hebt ingesteld Actieve Map voor één machine en probeert u een 802.1x verificatie te maken. De authenticatie faalt omdat in het perspectief van Actieve Map de authenticatie van het ACS komt, niet de machine waarop de openings- beperkingen zijn ingesteld. Om de authenticatie succesvol te laten verlopen, kunnen de openings-beperkingen worden ingesteld om de ACS-machineverklaring op te nemen.

Probleem: Fout: "U bent niet geautoriseerd om de gevraagde pagina te bekijken" wanneer ACS 5.x admin met ChangeUserPassword rol het wachtwoord wijzigt

ACS 5.x GUI beheerder met de rol **ChangeUserPassword** kan het wachtwoord van de AAA-gebruiker niet wijzigen dat in de interne database is opgeslagen. Nadat u het wachtwoord hebt gewijzigd, ontvangt de gebruiker deze pop-up foutmelding: `U bent niet geautoriseerd om de gevraagde pagina te bekijken.`

Oplossing

Dit kan voorkomen wanneer de ACS 5.x-database wordt gemigreerd van ACS 4.x. Gebruik het **SuperAdmin-**voorrecht om het gebruikerswachtwoord te wijzigen. Raadpleeg Cisco bug-ID CSCty91045 (alleen geregistreerde klanten) voor meer informatie.

Probleem: Het verkrijgen van een fout op ACS 5.x voor mislukte verificatie zijn "24495 Active Directory servers niet beschikbaar."

Oplossing

U moet de integratie van de Actieve Map met ACS 5.x controleren. Als het een gedistribueerde instelling is, zorg er dan voor dat zowel het primaire als het secundaire ACS 5.x in de instelling correct geïntegreerd zijn met Active Directory.

Probleem: Kan geen verbinding met het ACS-apparaat maken met BMC

Wanneer de BMC-client (een hardware level-tool) wordt gebruikt om in de ACS 1121 IBM-servers te komen, wordt opgemerkt dat de BMC-client twee IP-adressen heeft.

Oplossing

Dit gedrag is geïdentificeerd en aangemeld in Cisco bug-id CSCtj81255 (alleen geregistreerde klanten). Om dit op te lossen, moet u de BMC DHCP-client op ACS 1121 uitschakelen.

Probleem: Een waarschuwingsalarm "verwijder 20000 sessies" met oorzaak "actieve sessies zijn te lang", verschijnt in de monitor en rapporteert het algemene dashboard.

Er is een limiet aan het aantal records dat een sessieleiding kan aanhouden. Omdat de waarschijnlijke verzoeken zwaar zijn in de instellingen van de klant, wordt de grenswaarde snel bereikt. Na het bereiken van de limiet verwijdert ACS-View door middel van een ontwerp een bepaald aantal records (bijvoorbeeld 20k) uit de sessiemap en stuurt hij een waarschuwing. U kunt deze limiet verhogen, maar dit helpt niet veel, behalve het verlengen van de waarschuwing.

Oplossing

Voer de volgende handelingen uit om dit op te lossen:

- Aanbevolen wordt om houtkap uit te schakelen om de database te bekijken.Ga naar **Cisco Secure ACS > System-beheer > Configuration > Log Configuration > Logging Categorieën > Global > "Passed Authentications" > Remote SYS-doel** en verwijder **LogCollector** van geselecteerde doelen.Ga naar **Cisco Secure ACS > System-beheer > Configuration > Log Configuration > Logging Categorieën > Global > "Failpogingen" > Remote SLUG-doel** en verwijder **LogCollector** van geselecteerde doelen.Ga naar **Cisco Secure ACS > Systeembeheer > Configuratie > Logconfiguratie > Vastlegging categorieën > Global > Bewerken: "RADIUS-accounting" > afstandsbediening om LogCollector** te verwijderen uit geselecteerde doelen.
- U kunt de proefverzoeken om verificatie negeren omdat dit geen echte echtheidsverzoeken zijn. Voer de volgende handelingen uit:Ga naar **Cisco Secure ACS > Configuratie controleren > Systeemconfiguratie > Filter toevoegen** en maak het filter. Het maken van het filter op basis van de *gebruikersnaam* is passender omdat de proefaanvragen worden verzonden onder de naam van een dummy. Als u een afzonderlijk toegangsbeleid in ACS maakt om deze proefverzoeken te verwerken, dan kunnen filters ook op basis van *toegangsservice* worden gemaakt.

Probleem: ACS 5.x fout "1013 RADIUS-pakket al in het proces"

In een ACS 5.3 plaatsing, mislukken gebruikers dot1x authenticatie. De gebruikte database is een actieve map. De RADIUS-mislukkingscode wordt hier weergegeven:

```
RADIUS-aanvraag ingetrokken: 11013 RADIUS-pakket dat al in het proces zit
```

Oplossing

ACS heeft dit verzoek genegeerd omdat het een duplicaat is van een ander pakket dat momenteel wordt verwerkt. Dit kan voorkomen vanwege een van deze factoren:

- De statistische gegevens over de gemiddelde RADIUS-aanvraag liggen dicht bij of hoger dan de RADIUS-aanvraagtijd van de client.
- Externe identiteitswinkel kan erg langzaam zijn.
- De ACS is overbelast.

Voer deze stappen uit om een oplossing te vinden:

1. Verhoog de client-RADIUS-aanvraagtijd van de client.
2. Gebruik een sneller of extra extern identiteitsbewijs.
3. Volg de manieren om de overbelasting op ACS te verminderen.

Probleem: RADIUS-verificatie mislukt met fout "11012 RADIUS-pakket bevat ongeldige header"

Oplossing

De header van het inkomende RADIUS-pakket is niet correct geparseerd. Controleer om dit op te lossen het volgende:

- Controleer het netwerkapparaat of AAA-client op hardwareproblemen.
- Controleer het netwerk dat het apparaat met de ACS verbindt voor hardwareproblemen.
- Controleer of het netwerkapparaat of de AAA-client bekend is met de RADIUS-compatibiliteit.

Probleem: RADIUS/TACACS+ verificatie mislukt met fout "1007 Kan netwerkapparaat of AAA-client niet vinden"

Deze foutmelding wordt op ACS ontvangen wanneer een ASA een bericht met boogtoegang verstuurt:

```
1007 kan geen netwerkapparaat of AAA-client lokaliseren
```

Oplossing

Dit komt voor omdat er een mismatch is tussen de IP van de ACS-client en de interface IP die het verzoek daadwerkelijk verstuurt. Soms voert de firewall een adresvertaling uit naar deze AAA-client. Controleer of de AAA-client correct is geconfigureerd met het juiste vertaalde IP-adres in dit pad:

Netwerkbronnen > Netwerkapparaten en AAA-clients

Probleem: RADIUS-verificatie faalde bij fout "11050 RADIUS-verzoek gedaald als gevolg van systeemoverbelasting".

De gebruikers hebben geen toegang tot het netwerk vanwege de authenticatiefouten. Deze foutmelding van de ACS wordt ontvangen:

`11050 RADIUS-verzoek ingetrokken door systeemoverbelasting`

Oplossing

Cisco ACS laat deze authenticatieverzoeken vanwege overbelasting vallen. Dit kan worden veroorzaakt door het reproduceren van vele parallelle aanhoudingsverzoeken. Voer een van de volgende handelingen uit om dit te voorkomen:

- Wijzig de instellingen **van** de **client/AAA-client** zodat deze de optie **Verouderde TACACS+ single Connection** gebruikt. Hierdoor zal de client dezelfde sessie voor alle verzoeken opnieuw gebruiken in plaats van veel sessies te maken.
- Weiger de gebruikers enige tijd nieuwe authenticatieverzoeken in te dienen.
- Start de ACS-server opnieuw.

Probleem: RADIUS-verificatie faalde bij fout "11309 Onjuiste RADIUS MS-CHAP v2, eigenschap."

Oplossing

Deze fout komt voor door de ongeldige lengte of onjuiste waarde van één van de MSCHAP v2 eigenschappen (MS-CHAP-Challenge, MS-CHAP-Response, MS-CHAP-CPW-2, of MS-CHAP-NT-Enc-PW) in het ontvangen toegangspakket van de RADIUS.

Probleem: ACS meldt geheugengebruik meer dan 90%. Alarm

ACS rapporteert geheugen gebruik meer dan 90%.Alarm zoals het volgende: `Cisco beveiligde ACS - AlarmmeldingErnst: Kritische alarmnaam ACS - Alarmalarm voor systeemziekte/trigger veroorzaakt door ACS - systeemgezondheidsdrempelAlarmdetails ACS-instel-gebruik (%) Geheugenbenutting (%) Schijf I/O-gebruik (%) Disc-gebruikte ruimte/opt (%) Disc-gebruikte schijfruimte/localschijf: (%) gebruikte schijfruimte / (%) KOM-AAA02 0,41 90,14 0,02 9,57 5,21 25,51`

Oplossing

Dit probleem wordt meestal gezien op ACS 5.2. Om dit probleem op te lossen, moet u de ACS opnieuw laden om het geheugen te bevrijden of de ACS 5.2-pleister 7 of later te verbeteren. Raadpleeg Cisco bug-ID CSCtk52607 (alleen geregistreerde klanten) voor meer informatie.

Probleem: fout:com.cisco.nm.acs.mgmt.msgbus.FatalBusException: Knipperen mislukt

In een gedistribueerde opstelling na een onderhoudstaak (die zich bij een primaire, krachtige volledige replicatie, patching) aansluit, ACS A instantie B rapporteert ACS instantie B als offline in het gedistribueerde inzetscherm, terwijl B echt online is en instantie A als online meldt. In de beheerlogbestanden ziet u `fout:com.cisco.nm.acs.mgmt.msgbus.FatalBusException: Kan knooppunten niet koppelen.`

Oplossing

Dit kan voorkomen als een vorige instantie van de dienst van het replicatiebeheer nog aan haven 2030 is gebonden wanneer de nieuwe instantie komt en aan die haven probeert te binden. Uit CLI van ACS instantie B, run:sho acs-logs bestand ACSM-beheer. `logboek | i replicatiedienst`. U zult berichten zoals de `replicatieservice` zien.`:Port reeds in gebruik: 2030.` Op dit moment is de tijdelijke oplossing het opnieuw opstarten van ACS-instantie B (de instantie die de andere als online meldt). Raadpleeg Cisco bug-ID CSCtx56129 (alleen geregistreerde klanten) voor meer informatie.

Probleem: fout:com.cisco.nm.acs.mgmt.msgbus.FatalBusException: Knipperen mislukt

In een gedistribueerde opstelling na een onderhoudstaak (die zich bij een primaire, krachtige volledige replicatie, patching) aansluit, ACS A instantie B rapporteert ACS instantie B als offline in het gedistribueerde inzetscherm, terwijl B echt online is en instantie A als online meldt. In de beheerlogbestanden ziet u `fout:com.cisco.nm.acs.mgmt.msgbus.FatalBusException: Kan knooppunten niet koppelen.`

Oplossing

upgrade naar ACS 5.2-pleister 6 of later om dit probleem op te lossen. Raadpleeg Cisco bug-ID CSCto47203 (alleen geregistreerde klanten) voor meer informatie.

Opmerking: de viewDB back-up zal mislukken als het gebruik "/optie" meer dan 30% bedraagt. Het is vereist om NFS-stappen te configureren om een back-up uit te voeren wanneer ""/"opt" meer dan 30% gebruik bevat.

Probleem: fout 11026 De gevraagde dACL is niet gevonden

RADIUS-verificatie faalt bij deze foutmelding: `11026 De gevraagde dACL is niet gevonden.`

Oplossing

Het verzoek wordt afgewezen omdat de versie van de downloadbare ACL die in het RADIUS-toegangsverzoek wordt aangevraagd, niet wordt gevonden. Het verzoek om de downloadbare ACL is lang na de oorspronkelijke toegangsaanvraag ingediend. Daarom was de versie van de downloadbare ACL niet langer beschikbaar. Vind de reden voor deze vertraging in het verzoek om de Downloadbare ACL van de RADIUS-client.

Probleem: fout 11025 Het verzoek om toegang tot de gevraagde dACL te ontvangen is een cisco-av-paar eigenschap met de waarde a:event=acl-download. Het verzoek wordt afgewezen

RADIUS-verificatie faalt bij deze foutmelding: `11025 Het verzoek om toegang tot de gevraagde dACL is bij gebrek aan een cisco-av-paareigenschap met de waarde a:event=acl-download. Het verzoek wordt afgewezen.`

Oplossing

Elk toegangsverzoek voor de downloadbare ACL moet een `cisco-av-paar eigenschap` hebben met de waarde `aaa:event=acl-download`. In dit geval ontbreekt deze eigenschap het verzoek en heeft de ACS het verzoek niet ingewilligd. Controleer of het netwerkapparaat of de AAA-client bekend is met de RADIUS-compatibiliteit.

Probleem: fout 11023 De gevraagde dACL is niet gevonden. Dit is een onbekende dACL-naam

RADIUS-verificatie faalt bij deze foutmelding: `11023 De gevraagde dACL is niet gevonden. Dit is een onbekende dACL-naam.`

Oplossing

Controleer de ACS-configuratie om te controleren of de downloadbare ACL die in het machtigingsprofiel is gespecificeerd, in de lijst van downloadbare ACL's bestaat. Dit is een ACS-zijmisconfiguratie.

Probleem: Verificatie van beheerder mislukt met fout 10001 Interne fout. Onjuiste configuratie

Verificatie beheerder faalt bij deze fout: `10001 Interne fout. Onjuiste configuratie.`

Oplossing

Deze fout kan worden veroorzaakt door een beschadigde ACS-database of door een probleem in de onderliggende configuratiegegevens. Neem contact op met Cisco TAC (alleen geregistreerde klanten) voor meer informatie.

Probleem: Verificatie beheerder mislukt met fout 10002 Interne fout: Geen geschikte service laden

Verificatie beheerder faalt bij deze fout: `10002 Interne fout: Geen geschikte service laden.`

Oplossing

ACS 5.x kan de AAC-configuratieservice niet laden. Dit kan worden veroorzaakt door een beschadigde ACS-database, of door een probleem in de onderliggende configuratiegegevens. Het kan ook gebeuren wanneer de systeemmiddelen zijn uitgeput. Neem contact op met Cisco TAC (alleen geregistreerde klanten) voor meer informatie.

Probleem: Verificatie beheerder mislukt met fout 1003 Interne fout: Verificatie door beheerder met lege beheerdersnaam

Verificatie beheerder faalt bij deze fout: `10003 Interne fout: Administrator-verificatie heeft de lege Administrator-naam ontvangen.`

Oplossing

Wanneer ACS toegang heeft tot de GUI van ACS 5.x, ontvangt ACS een lege gebruikersnaam. Controleer de geldigheid van de aan het ACS doorgegeven gebruiksnaam. Als dit geldig is, neemt u contact op met Cisco TAC (alleen geregistreerde klanten) voor meer informatie.

Probleem: Reden van fout: 2428 Er is een fout opgetreden in verband met de verbinding in LRPC, LDAP of KERBEROS

Deze foutmelding wordt op de ACS ontvangen:

```
Reden van fout: 2428 vergissing die verband houdt met de verbinding is opgetreden bij LRPC, LDAP of KERBEROS Dit RPC-verbindingsprobleem kan zijn doordat de stub onjuiste gegevens heeft ontvangen
```

Oplossing

Om dit probleem op te lossen, upgrade van het ACS naar versie 5.2.

Probleem: De verificatie van TACACS+ proxy werkt niet op een router die IOS 15.x van ACS 5.x-server uitvoert

De verificatie van TACACS+ proxy werkt niet op een router die Cisco IOS-softwarerelease 15.x van een ACS 5.x-server uitvoert.

Oplossing

TACACS+ auth-Proxy wordt alleen ondersteund na ACS 5.3-pleister 5. upgrade van uw ACS 5.x of gebruik RADIUS voor auth-Proxy.

Probleem: Het krijgen van foutmelding Store fail (acs-xxx, TacacsAccounting) van ACS 5.x

Oplossing

Het TACACS 5.1 boekhoudingsrapport mist een paar eigenschappen zoals gebruikersnaam, bevoorrechtingsniveau, en aanvraagtype wanneer het een misvormd boekhoudpakket van de cliënt ontvangt. In sommige gevallen leidt dit tot het aanmaken van het "Store fail (acs-xxx, TacacsAccounting)" alarm in View. Controleer om dit op te lossen het volgende:

- Het rekeningspakket dat door de client wordt verzonden heeft een misvormd TACACS-argument (bijvoorbeeld een verkeerde match in lengte en waarde van een argument dat door AAA-client wordt verzonden).
- Zorg ervoor dat de klant een geldig rekeningspakket met de juiste lengte en waarde voor de argumenten verstuurt.

Raadpleeg Cisco bug-ID CSCte8357 (alleen geregistreerde klanten) voor meer informatie.

Probleem: Verificatie door gebruiker mislukt met fout "11036 De RADIUS-kenmerk van de Message-Authenticator is ongeldig."

Oplossing

Controleer het volgende:

- Controleer of de gedeelde geheimen op de AAA client en ACS server match zijn.
- Zorg ervoor dat de AAA-client en het netwerkapparaat geen hardwareproblemen of problemen met RADIUS-compatibiliteit hebben.
- Zorg ervoor dat het netwerk dat het apparaat met ACS verbindt geen hardwareproblemen heeft.

Probleem: RADIUS-accounting is mislukt met fout "11037 Dropped accounting request ontvangen via niet-ondersteunde poort."

Oplossing

Een boekhoudkundige aanvraag werd ingetrokken omdat ze werd ontvangen via een niet-ondersteund UDP-poortnummer. Controleer het volgende:

- Zorg ervoor dat de configuratie van het boekhoudpoortnummer op de AAA-client en op de ACS-serverwedstrijd.
- Zorg ervoor dat de AAA-client geen hardwareproblemen of problemen met RADIUS-compatibiliteit heeft.

Probleem: RADIUS-accounting is mislukt met fout "11038 RADIUS-accounting-aanvraag header bevat ongeldige authenticator veld."

ACS kan het veld Verificator in de header van het pakket RADIUS-accounting-aanvraag niet valideren. Het veld Authenticator mag niet worden verward met de RADIUS-eigenschap van Berichtverificatie. Zorg ervoor dat het RADIUS gedeelde geheim dat op de AAA-client is geconfigureerd voor het geselecteerde netwerkapparaat op de ACS-server. Zorg er ook voor dat de AAA-client geen hardwareproblemen of problemen met RADIUS-compatibiliteit heeft.

Fout: "2493 ACS heeft problemen die met Actieve Map communiceren met zijn machinegeloofsbrieven."

Oplossing

Controleer de ACS voor AD-connectiviteit en zorg ervoor dat de ACS-machineaccount nog in de AD aanwezig is.

Probleem: "Wanneer u Shell Profile namen maakt met speciale tekens zoals "ê", kan ACS crashen."

Oplossing

Dit gedrag is geïdentificeerd en aangemeld in Cisco bug-ID CSCts17763 (alleen geregistreerde klanten). U moet overgaan naar een pleister van 5.3.40 1 of 5.2.26 7.

Probleem: "Parse error op regel 2: niet goed gevormd (ongeldig token)" terwijl "Show run" op de ACS 5.x CLI wordt uitgevoerd.

Oplossing

Zorg dat de SNMP-gemeenschap die op de ACS is ingesteld, geldige tekens heeft. Alleen alfanumerieke tekens (alleen letters en cijfers) mogen in de gemeenschapsnaam worden gebruikt.

Probleem: ACS 5.x/opt-verdeling vult zeer snel op

Oplossing

ACS 5.x heeft geen schijfruimte meer door ontoereikende ruimte in de */opt*-indeling. Dit komt voor vanwege het hoge aantal loggegevens dat de ACS-weergave overstroomt. Als een tijdelijke oplossing moet u de View database vaak vervangen. Omdat ACS View niet met gigabyte aan gegevens per dag kan omgaan, moet je de loggegevens organiseren. Wanneer u alle logbestanden nodig hebt, gebruikt u een externe syslogserver in plaats van de ACS-weergave. Wanneer u slechts een deel van de loggegevens hoeft te gebruiken, gebruikt u *Systeembeheer > Configuratie > Log configuratie > Logging Categorieën > Wereldwijd* om alleen de vereiste logbestanden naar de ACS-weergave-verzamelaar te sturen.

Probleem: Het gewenste domein zoeken

Kan ACS 5.x query Adverse Domain Controllers (DC's) als u zich bij een Active Directory Domain aansluit?

Oplossing

Nee. Op dit moment vraagt ACS de DNS met het domein om een lijst te krijgen van alle DC's in het domein. Dan probeert het met hen allemaal te communiceren. Als de verbinding met zelfs één DC mislukt, wordt de ACS verbinding met het domein verklaard als mislukt.

Probleem: Parent- en kinderdomeinen tegelijkertijd

Is er een manier om ACS 5.x in zowel ouder- als kinderdomeinen tegelijk op te zetten?

Oplossing

Neen. Op dit moment kan ACS 5.x slechts een deel van één domein zijn. ACS 5.x kan echter gebruikers/machines van meerdere vertrouwde domeinen voor authenticatie behoeden.

Probleem: Vastlegging aan externe database

Kan ik de ACS 5.x Beeld gegevens aan een ver gegevensbestand registreren?

Oplossing

Ja, ACS 5.x staat u toe om de ACS View gegevens te registreren aan Microsoft SQL servers en Oracle SQL servers.

Probleem: Ondersteuning van VMWare

Oplossing

ACS 5.x kan op een virtuele machine worden geïnstalleerd. De meest recente versie, ACS 5.3, kan op deze VMW-versies worden geïnstalleerd:

- VMWare ESX 3.5
- VMWare ESX 4.0
- VMWare ESX i4.1
- VMWare ESX 5.0

Probleem: Vereisten voor schijfruimte

Wat zijn de vereisten voor de schijfruimte voor de ACS 5.x-versie van de evaluatie?

Oplossing

Voor de evaluatieversie is een minimale schijfruimte van 60 GB vereist. 500 GB is vereist voor de productie-installatie.

Probleem: "24401 kon geen verbinding met ACS Actieve Map agent opzetten."

Oplossing

Controleer het volgende om deze fout op te lossen:

- Controleer of de ACS-machine is aangesloten op het Active Directory-domein.
- Controleer de aansluitingsstatus tussen de ACS-machine en de Active Directory-server.
- Controleer of de ACS Active Directory Agent actief is.

Raadpleeg Cisco bug-ID CSCtx71254 (alleen geregistreerde klanten) voor meer informatie.

Probleem: Runtime" proces toont "executie mislukt" toestand

Wanneer u Cisco ACS met een patch uploadt, wordt het Runtime-proces vastgehouden in de status "Executie mislukt" en wordt dit bericht gelogd:

```
"Local0 err 83 2012-06-12T12:11:08+0200 192.168.150.74 ACS-logvoorwaartse fout:
/opt/CSCOacs/runtime/bin/run-logforward.sh: regel 18: 7097 Segmentation-fout (kern gedumpt)
./$daemon -b -f $logfile"
```

Oplossing

Dit kan een probleem zijn met het MD5-pleister van de laatste pleister. Controleer de MD5 checksum van de laatste pleister die op Cisco ACS is toegepast. Download dat opnieuw en pas het vervolgens op de juiste manier toe.

Probleem: Ontbrekende ACS-verificatie bij herauthenticatie UCS-eenheden

De UCS-server is ingesteld om een Java-client voor het Cisco ACS te authentiseren. De authenticatieprocedure omvat het gebruik van RSA Token server. De eerste authenticatie passeert. Echter, wanneer UCS verfrist en de client van Java dwingt om opnieuw te authentiseren, faalt het omdat RSA niet toestaat om een token opnieuw te gebruiken. Daarom faalt de authenticatie.

Oplossing

Dit is een beperking van de aansprakelijkheid van de UCS Server, maar niet van Cisco ACS. De UCS Server volgt een twee-factor authenticatie die een niet-ondersteunde optie is voor Cisco ACS bij gebruik met RSA Tokens. Op dit moment wordt het niet ondersteund. Als tijdelijke oplossing is het raadzaam om alle databases te gebruiken, zoals AD of LDAP, anders dan de RSA Token server.

Probleem: "2444 Active Directory operation heeft gefaald vanwege een niet-gespecificeerde fout in ACS"

Oplossing

Een niet in kaart gebrachte fout is opgetreden in een AD-gerelateerde bewerking. Raadpleeg de ACS 5.x-integratie met Microsoft AD Configuration Voorbeeld en stel de AD-integratie met de ACS correct in. Als alles overeenkomstig het document goed is geconfigureerd, neemt u contact op met Cisco TAC voor meer probleemoplossing.

Probleem: Kan ACS 5.1-gebruikers niet echt maken met AD 2008 R2-server

Oplossing

Dit gebeurt vanwege onverenigbaarheden. AD 2008 R2-integratie wordt alleen ondersteund door ACS 5.2-versie. upgrade uw ACS naar 5.2 of hoger. Raadpleeg Cisco bug-ID CSCtg12399 (alleen geregistreerde klanten) voor meer informatie.

Fout: 22056 Onderwerp niet in het (de) desbetreffende identiteitsbewijs(s).

Wanneer de SSL VPN-gebruikers proberen geauthentiseerd te krijgen van een RSA-apparaat, wordt deze foutmelding ontvangen van de Cisco ACS-server:

```
Redelijkheid fout: 22056 Onderwerp niet in het (de) desbetreffende identiteitsbewijs(s).
```

Oplossing

Controleer of de gebruiker aanwezig is in de gegevensbank waar de ACS naar op zoek is. Zorg er bij RSA en RADIUS Identity Store voor dat de optie **Afwijzen behandelen** is geselecteerd omdat de **verificatie** is **mislukt**. Dit staat onder het tabblad Geavanceerd van de configuratie van Identity Store.

Probleem: ipt_connlimit: Oeps: Ongeldige staat van Ct?

De `ipt_conlimiet: Oeps: Ongeldige staat van Ct?` Er verschijnt een foutbericht op de console wanneer ACS 5.x bij VMWare draait.

Oplossing

Dit is een cosmetische boodschap. Raadpleeg Cisco bug-ID CSCth25712 (alleen geregistreerde klanten) voor meer informatie.

Probleem:ACs 5.x/ISE ziet geen attribuut van het oproepstation-id in een RADIUS-verzoek van Cisco IOS-softwarerelease 15.x NAS

ACs 5.x / ISE ziet geen `Straal die roepen-station-id` attribuut in een RADIUS-verzoek van Cisco IOS-softwarerelease 15.x NAS.

Oplossing

Gebruik de eigenschap **straal-server** 31 om **het** verzenden van de opdracht nas-poort-detail op Cisco IOS softwarerelease 15.x toe te staan om het verzenden van de eigenschap toe te laten.

Probleem: Gebruikersrekeningen worden vergrendeld in eerste instantie van verkeerde aanmeldingsgegevens, zelfs als dit voor 3 pogingen is ingesteld

Wanneer ACS 5.3 met Actieve Map op een functioneel niveau van Windows 2008 R2 wordt geïntegreerd, worden de gebruikersaccounts die zijn ingesteld met uitsluitingsparameters (3 onjuiste pogingen) voortijdig afgesloten nadat de gebruiker de verkeerde aanmeldingsgegevens slechts eenmaal heeft ingevoerd.

Oplossing

Raadpleeg Cisco bug-ID CSCtz03211 (alleen geregistreerde klanten) voor meer informatie.

Probleem: Niet in staat om back-up van ACS op te slaan

Tijdens een poging om een back-up op te slaan van het ACS, `veroorzaakt` het `volgende: Meer back-up niet ingesteld - Details: Een stapsgewijze back-up is niet ingesteld.Het configureren van stapsgewijze back-up is nodig om de gegevensverwijdering succesvol te maken. Dit helpt problemen met schijfruimte te voorkomen. De grootte van de View database is 0,08GB en de grootte die deze op de vaste schijf inneemt, is` een waarschuwing `van 0,08GB`.

Oplossing

U kunt niet tegelijkertijd een stapsgewijze back-up, volledige back-up en gegevensverwijdering uitvoeren. Als een van deze banen wordt uitgevoerd, moet je 90 minuten wachten voordat je met de volgende baan kunt beginnen.

Gerelateerde informatie

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