ACS 5.x und höher - Fehlerbehebung für sichere ACS

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Problem: "Fehler: Die aktuelle Konfiguration wurde erfolgreich in die Startdatei gespeichert % Manifestdatei nicht im Paket gefunden" auf ACS-Appliance während Appliance-Upgrade
Lösung
Problem: ACS Server 5.x kann nicht über die Benutzeroberfläche neu gestartet werden
Lösung
Problem: Probleme beim Einrichten der Active Directory-Authentifizierung mit ACS 5.2
Lösung
Problem: Es können nicht mehr als 100 Seiten im Buchführungsbericht angezeigt werden.
Lösung
Problem: Der Authentifizierungsbericht für eine Gruppe von Geräten kann nicht erstellt werden.
Lösung
Problem: Die Datenbank für Überwachung und Berichte ist derzeit nicht verfügbar. Versuchen Sie, die Verbindung in 5 Sekunden wiederherzustellen.
Lösung
Problem: 22056 Betreff nicht im/den entsprechenden Identitätsspeicher(en) gefunden
Lösung
Problem: ACS kann nicht mit Active Directory integriert werden.
Lösung
Problem: ACS kann nicht mit LDAP integriert werden.
Lösung
Problem: "csco acs_internal_operations_diagnostics-Fehler: Kann nicht in die lokale Speicherdatei schreiben" Fehlermeldung
Lösung
Problem: ACS 5.1 kann nicht mit Active Directory integriert werden.
Lösung
Problem: ACS 5.x kann nicht so konfiguriert werden, dass reguläre Ausdrücke in den Service-Auswahlregeln erkannt werden.
Lösung
Problem: Die SFTP-Sicherung funktioniert nicht, wenn Cisco Works als SFTP-Server verwendet wird.
Lösung
Problem: "Ungültige EAP-Payload verworfen"

Lösung
Problem: "Der ACS-Laufzeitprozess wird derzeit für diese Instanz nicht ausgeführt."
Lösung
Problem: Benutzer mit dem Kennwort konnten nicht exportiert werden.
Lösung
Problem: Interne ACS-Benutzer sind gelegentlich deaktiviert.
Lösung
Problem: "Die TACACS+-Authentifizierungsanfrage endete mit Fehler."
Lösung
Problem: "Radius-Authentifizierungsanfrage aufgrund eines kritischen Protokollierungsfehlers abgelehnt"
Lösung
Problem: Die ACS View-Schnittstelle zeigt oben auf der Seite "Data Upgrade Failed" (Datenaktualisierung fehlgeschlagen) an, wenn ACS von 5.2 auf 5.3 aktualisiert wird.
Lösung
Problem: Problem mit "Change password on next login acs" (Kennwort für nächste Anmeldung ändern) in Cisco ACS 5.0
Lösung
Problem: "% Anwendungsaktualisierung fehlgeschlagen, Fehler - -999. Bitte prüfen Sie die ADE-Protokolle auf Details, oder führen Sie sie erneut mit - Installation der Debuganwendung - aktiviert" auf der ACS-Appliance während des Upgrades aus.
Lösung
Problem: Fehler "Authentifizierung fehlgeschlagen: 12308 Client gesendet Ergebnis TLV zeigt Fehler an"
Lösung
Problem: Fehler "24495 Active Directory-Server sind nicht verfügbar"
Lösung
Problem: Fehler "Zeitüberschreitung der EAP-Sitzung 5411"
Lösung
Problem: Die 802.1x-Authentifizierung funktioniert nicht, wenn Anmeldungsbeschränkungen auf dem Active Directory konfiguriert sind.
Lösung
Problem: Fehler: "Sie sind nicht berechtigt, die angeforderte Seite anzuzeigen", wenn ACS 5.x Admin mit der Rolle ChangeUserPassword das Kennwort ändert
Lösung
Problem: Fehlermeldung für ACS 5.x bei fehlgeschlagener Authentifizierung "24495 Active Directory-Server sind nicht verfügbar."
Lösung
Problem: Verbindung zur ACS-Appliance mit BMC nicht möglich
Lösung
Problem: Im Monitor wird ein Warnalarm "Löschen 20.000 Sitzungen" mit der Ursache "Aktive Sitzungen sind überbegrenzt" angezeigt, und das allgemeine Dashboard wird angezeigt.
Lösung
Problem: ACS 5.x-Fehler "11013 RADIUS-Paket ist bereits im Prozess"
Lösung
Problem: Fehler bei der RADIUS-Authentifizierung mit dem Fehler "11012 RADIUS-Paket enthält ungültigen Header"

Lösung
Problem: Die RADIUS/TACACS+-Authentifizierung ist fehlgeschlagen mit dem Fehler "11007 Konnte kein Netzwerkgerät oder AAA-Client suchen".
Lösung
Problem: Die RADIUS-Authentifizierung ist fehlgeschlagen mit dem Fehler "11050 RADIUS-Anfrage aufgrund von Systemüberlastung verworfen".
Lösung
Problem: Die RADIUS-Authentifizierung ist fehlgeschlagen mit dem Fehler "11309 Falsches RADIUS MS-CHAP v2-Attribut".
Lösung
Problem: ACS meldet eine Speichernutzung von über 90 %. Alarm
Lösung
Problem: Fehler:com.cisco.nm.acs.mgmt.msgbus.FatalBusException: Verknüpfung von Knoten fehlgeschlagen
Lösung
Problem: Fehler:com.cisco.nm.acs.mgmt.msgbus.FatalBusException: Verknüpfung von Knoten fehlgeschlagen
Lösung
Problem: Fehler 11026 Die angeforderte dACL wurde nicht gefunden.
Lösung
Problem: error 11025 Der Access-Request für die angeforderte dACL fehlt ein cisco-av-pair-Attribut mit dem Wert aaa:event=acl-download. Der Antrag wird abgelehnt.
Lösung
Problem: Fehler 11023 Die angeforderte dACL wurde nicht gefunden. Dies ist ein unbekannter dACL-Name.
Lösung
Problem: Administratorauthentifizierung fehlgeschlagen mit Fehler 10001 Interner Fehler. Falsche Konfigurationsversion
Lösung
Problem: Administratorauthentifizierung fehlgeschlagen mit Fehler 10002 Interner Fehler: Keine geeigneten Services geladen
Lösung
Problem: Administratorauthentifizierung fehlgeschlagen mit Fehler 10003 Interner Fehler: Administratorauthentifizierung erhalten leeren Administratornamen
Lösung
Problem: Fehlergrund: 24428 Verbindungsfehler in LRPC, LDAP oder KERBEROS
Lösung
Problem: Die TACACS+-Auth-Proxy-Authentifizierung funktioniert nicht auf einem Router, auf dem IOS 15.x vom ACS 5.x-Server ausgeführt wird.
Lösung
Problem: Abrufen von Fehlermeldung Store Failure (acs-xxx, TACACSAccounting) von ACS 5.x
Lösung
Problem: Die Benutzerauthentifizierung ist fehlgeschlagen mit dem Fehler "11036 Das RADIUS-Attribut der Nachrichtenauthentifizierung ist ungültig."
Lösung
Problem: RADIUS Accounting ist fehlgeschlagen mit dem Fehler "11037 Dropped accounting request received via unsupported port".

Lösung
Problem: RADIUS Accounting ist fehlgeschlagen mit dem Fehler "11038 RADIUS Accounting-Request Header enthält ungültiges Authentifiziererfeld."
Fehler: "24493 ACS hat Probleme bei der Kommunikation mit Active Directory mithilfe seiner Anmeldeinformationen für das System."
Lösung
Problem: "Beim Erstellen von Shell-Profilnamen mit Sonderzeichen wie "ê" kann der ACS abstürzen."
Lösung
Problem: Abrufen von "Analysefehler in Zeile 2: nicht wohlgeformt (ungültiges Token)" bei Ausführung von "show run" in der ACS 5.x-CLI.
Lösung
Problem: ACS 5.x /opt-Partition füllt sehr schnell aus
Lösung
Problem: Abfragen der gewünschten Domäne
Lösung
Problem: Gleichzeitige Übergeordnete und untergeordnete Domänen
Lösung
Problem: Anmelden bei einer Remotedatenbank
Lösung
Problem: VMWare-Unterstützung
Lösung
Problem: Speicherplatzanforderungen
Lösung
Problem: "24401 Konnte keine Verbindung zum ACS Active Directory-Agenten herstellen."
Lösung
Problem: Der Laufzeitprozess zeigt den Status "Ausführung fehlgeschlagen" an.
Lösung
Problem: Fehlgeschlagene ACS-Authentifizierung, wenn das UCS eine erneute Authentifizierung erzwingt
Lösung
Problem: "2444 Active Directory-Vorgang ist aufgrund eines nicht angegebenen Fehlers im ACS fehlgeschlagen."
Lösung
Problem: ACS 5.1-Benutzer mit AD 2008 R2-Server können nicht authentifiziert werden
Lösung
Fehler: 2056 Betreff nicht im/den entsprechenden Identitätsspeicher(en) gefunden.
Lösung
Problem: ipt_connlimit: Hopfen: Ungültiger ct-Status?
Lösung
Problem:ACs 5.x/ISE sehen in einer RADIUS-Anfrage von Cisco IOS Software Release 15.x NAS kein RADIUS-Attribut für die Anrufer-ID des RADIUS-Servers
Lösung
Problem: Benutzerkonten werden bei der ersten Instanz falscher Anmeldeinformationen gesperrt, selbst wenn sie für 3 Versuche konfiguriert wurden.
Lösung

[Problem: Backup von ACS kann nicht gespeichert werden](#)
[Lösung](#)
[Zugehörige Informationen](#)

Einleitung

Dieses Dokument enthält Informationen zur Fehlerbehebung im Cisco Secure Access Control System (ACS) und zur Behebung von Fehlermeldungen.

Weitere Informationen zur Fehlerbehebung für Cisco Secure ACS 3.x und 4.x finden Sie unter Sicherer Zugriffskontrollserver (ACS 3.x und 4.x) - Fehlerbehebung.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco Secure Access Control System, Version 5.x und höher.

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).

Problem: "Fehler: Die aktuelle Konfiguration wurde erfolgreich in die Startdatei gespeichert % Manifestdatei nicht im Paket gefunden" auf ACS-Appliance während Appliance-Upgrade

Der `Fehler: Die aktuelle Konfiguration wurde erfolgreich in die Startdatei gespeichert % Manifest-Datei, die im Paketfehler nicht gefunden wurde,` wird angezeigt, wenn versucht wird, ACS Express von 5.0 auf 5.0.1 zu aktualisieren.

Lösung

Führen Sie die folgenden Schritte aus, um die ACS-Appliance problemlos zu aktualisieren:

1. Laden Sie Patch 9 (5-0-0-21-9.tar.gpg) und ADE-OS

(ACS_5.0.0.21_ADE_OS_1.2_upgrade.tar.gpg) von folgender Seite herunter: **Cisco.com > Support > Software herunterladen > Sicherheit > Cisco Secure Access Control System 5.0 > Secure Access Control System Software > 5.0.0.21**

2. Installieren Sie nach der Installation der beiden Dateien das ACS 5.1-Upgrade ACS_5.1.0.44.tar.gz. Diese ist im gleichen Pfad wie im vorherigen Schritt verfügbar.
3. Verwenden Sie diesen Befehl, um das Upgrade zu installieren:

```
application upgrade
```

Damit ist der Aktualisierungsvorgang abgeschlossen.

Unter Aktualisieren eines ACS-Servers von 5.0 auf 5.1 finden Sie weitere Informationen zum Aktualisieren der ACS-Appliance.

Problem: ACS Server 5.x kann nicht über die Benutzeroberfläche neu gestartet werden

In diesem Abschnitt wird erläutert, warum Sie den ACS-Server Version 5.x nicht über die Benutzeroberfläche neu starten können.

Lösung

Es ist keine Option verfügbar, den ACS 5.x-Server über die Benutzeroberfläche neu zu starten. Der ACS kann nur über die CLI neu gestartet werden.

Problem: Probleme beim Einrichten der Active Directory-Authentifizierung mit ACS 5.2

Beim Einrichten der Active Directory (AD)-Authentifizierung für einen neuen 5.2 ACS-Dienst wird folgende Fehlermeldung angezeigt:

```
Unerwarteter RPC-Fehler: Zugriff aufgrund unerwarteter Konfigurations- oder Netzwerkfehler
verweigert. Bitte probieren Sie die –verbose Option aus oder führen Sie "adinfo –diag" aus.
```

Lösung

Der ACS muss Berechtigungen schreiben, um sich beim AD zu authentifizieren. Stellen Sie dem Dienstkonto temporäre Schreibberechtigungen zur Verfügung, um dieses Problem zu beheben.

Problem: Es können nicht mehr als 100 Seiten im Buchführungsbericht angezeigt werden.

Beim Versuch, einen benutzerdefinierten AAA-Abrechnungsbericht mit ACS Version 5.1 zu generieren, können nicht mehr als 100 Seiten angezeigt werden. Dies gilt nicht für mehrere ältere Berichte. Wie ändern Sie diese Einstellung, um alle Seiten anzuzeigen?

Lösung

Sie können die Anzahl der Seiten im ACS nicht ändern, da die maximale Anzahl der angezeigten Seiten standardmäßig nur 100 beträgt. Um diese Einschränkung zu überwinden und ältere Statistiken anzuzeigen, müssen Sie die Filteroptionen so ändern, dass spezifischere Übereinstimmungen möglich sind. Wenn Sie beispielsweise versuchen, den Bericht für die letzten dreißig Tage zu generieren, enthält er ein großes Volumen, und die letzten 100 Seiten können die Aktivität nur für die letzte Stunde anzeigen. Es wird empfohlen, die Filteroptionen hier zu verwenden. Wenn Sie die Filteroption als Benutzer-ID verwenden und den Zeitraum angeben, werden viel ältere Berichte ausgegeben.

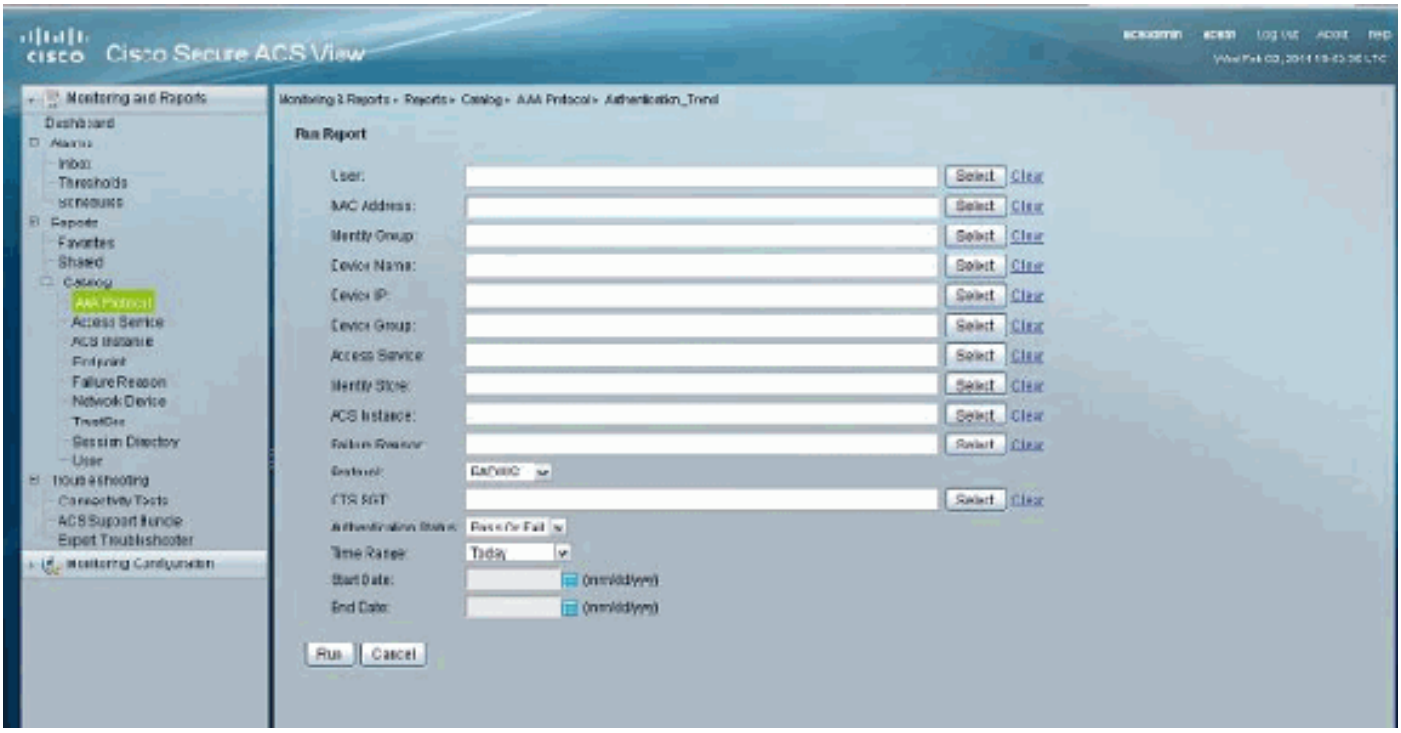
Problem: Der Authentifizierungsbericht für eine Gruppe von Geräten kann nicht erstellt werden.

Dieses Problem tritt auf, wenn versucht wird, den Authentifizierungsbericht nur für eine Gruppe von sechs Routern/Switches und nicht für alle Geräte zu erstellen. ACS Version 4.x wird verwendet.

Lösung

Mit ACS 4.x ist dies nicht möglich. Sie müssen auf ACS 5.x migrieren, da diese Funktion in dieser Version verfügbar ist. Sie können Berichte für die spezifische Gerätegruppe extrahieren, indem Sie die Katalogberichte generieren.

Weitere Informationen finden Sie in diesem Bild:



Problem: Die Datenbank für Überwachung und Berichte ist derzeit nicht verfügbar. Versuchen Sie, die Verbindung in 5 Sekunden wiederherzustellen.

Wenn Sie in ACS 5.x auf die Launch Monitoring and Report Viewer (Überwachung und

Berichtsanzeige starten) klicken, wird diese Fehlermeldung angezeigt: `Die Datenbank für Überwachung und Berichte ist derzeit nicht verfügbar. Versuchen Sie, die Verbindung in 5 Sekunden wiederherzustellen. Wenn das Problem weiterhin besteht, wenden Sie sich an Ihren ACS-Administrator.`

Lösung

Führen Sie eine der folgenden Workarounds aus, um dieses Problem zu beheben:

- Starten Sie die ACS-Dienste über die CLI neu, indem Sie die folgenden Befehle eingeben:
  ```
  application stop acs
  application start acs
  ```
- Aktualisieren Sie auf den neuesten verfügbaren Patch. Weitere Informationen hierzu finden Sie unter Anwenden von Upgrade-Patches.

Problem: 22056 Betreff nicht im/den entsprechenden Identitätsspeicher(en) gefunden

AD-Benutzer werden nicht mit ACS Version 5.x authentifiziert und erhalten die folgende Fehlermeldung: `2056 Betreff nicht im/den entsprechenden Identitätsspeicher(en) gefunden.`

Lösung

Diese Fehlermeldung wird angezeigt, wenn der ACS den Benutzer in der ersten in der Identitätsspeichersequenz konfigurierten Datenbank nicht finden konnte. Dies ist eine Informationsmeldung, die sich nicht auf die Leistung des ACS auswirkt. Die Art, wie ACS 5.x die Authentifizierung für interne oder externe Benutzer durchführt, unterscheidet sich von der vorherigen Version 4.x. Bei der Version 5.x gibt es eine Option namens Identity Store Sequence, um die Sequenz der zu authentifizierenden Benutzerdatenbanken zu definieren. Weitere Informationen finden Sie unter Konfigurieren von Identitätsspeichersequenzen.

Wenn Sie diesen Fehler erhalten, wenn Sie mit dem ACS Anfragen für eine untergeordnete Domäne authentifizieren, müssen Sie dem Benutzernamen ein UPN-Suffix oder ein NETBIOS-Präfix hinzufügen. Weitere Informationen finden Sie in den Hinweisen im Abschnitt Microsoft AD.

Problem: ACS kann nicht mit Active Directory integriert werden.

Benutzer können ACS nicht in Active Directory integrieren, und die Fehlermeldung "`Samba Port Status`" (`Samba-Portstatus-Fehler)` wird ausgegeben.

Lösung

Um dieses Problem zu beheben, stellen Sie sicher, dass diese Ports offen sind, um die Active Directory-Funktionalität zu unterstützen:

- Samba-Port - TCP 445
- LDAP - TCP 389
- LDAP - UDP 389
- KDC - TCP 88

- kpasswd - TCP 464
- NTP - UDP 123
- Globaler Katalog - TCP - 3268
- DNS - UDP 53

Der ACS muss alle Rechenzentren in der Domäne erreichen, damit die ACS-AD-Integration abgeschlossen werden kann. Auch wenn eines der Rechenzentren nicht über das ACS erreichbar ist, findet die Integration nicht statt. Weitere Informationen finden Sie unter Cisco Bug ID CSCte92062 (nur registrierte Kunden).

Problem: ACS kann nicht mit LDAP integriert werden.

In diesem Dokument wird ACS 5.2 als AAA-RADIUS-Server für die 802.1X-Implementierung verwendet. 802.1X kann mit dem ACS über den internen Benutzerspeicher erfolgreich verwendet werden, bei der Integration von ACS und LDAP treten jedoch Probleme auf. Diese Fehlermeldung wird angezeigt:

```
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
```

Lösung

In diesem Fall wird LDAP mit dem PEAP verwendet, und die interne Authentifizierungsmethode ist eap-mschap v2. Dies schlägt fehl, da LDAP für PEAP (eap-mschap v2) nicht unterstützt wird. Es wird empfohlen, eap-tls oder das AD zu verwenden.

Problem: "csco acs_internal_operations_diagnostics-Fehler: Kann nicht in die lokale Speicherdatei schreiben" Fehlermeldung

Während der Replikation des ACS repliziert der primäre ACS nicht ordnungsgemäß und zeigt folgende Fehlermeldung an:

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

Lösung

Starten Sie die ACS-Dienste neu, und stellen Sie sicher, dass die kritische Protokollierung deaktiviert ist. Weitere Informationen finden Sie unter Cisco Bug ID CSCth66302 (nur registrierte Kunden). Falls dies nicht hilft, wenden Sie sich an das Cisco TAC, um den neuesten ACS-Patch zu erhalten, der zur Lösung dieses Problems geeignet ist.

Problem: ACS 5.1 kann nicht mit Active Directory integriert werden.

Bei der Implementierung der AD-Integration wird folgende Fehlermeldung angezeigt:

```
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.
```

Lösung

Schließen Sie diese Problemumgehung ab, um dieses Problem zu beheben:

1. Löschen Sie das vorhandene Systemkonto auf AD.
2. Erstellen Sie eine neue Einheit.
3. Gehen Sie zu Eigenschaften der OU, und deaktivieren Sie **Berechtigungen erben**.
4. Erstellen Sie ein neues Systemkonto für den ACS in der neuen Einheit.
5. Lassen Sie das AD replizieren.
6. Versuchen Sie, über die ACS-GUI dem AD beizutreten.

In einigen Fällen ist es auch hilfreich, wenn Sie sich an Microsoft wenden und die Hot Fix anwenden.

Problem: ACS 5.x kann nicht so konfiguriert werden, dass reguläre Ausdrücke in den Service-Auswahlregeln erkannt werden.

Lösung

Dies ist nicht möglich, da es in ACS 5.x noch nicht unterstützt wird.

Problem: Die SFTP-Sicherung funktioniert nicht, wenn Cisco Works als SFTP-Server verwendet wird.

Wenn sich die Netzwerkressource auf dem CiscoWorks-Server befindet, funktioniert der Backup-Scheduler problemlos mit anderen SFTP-Clients, nicht jedoch mit ACS 5.2. Insbesondere bei der Verbindungsversuche vom ACS zum SFTP-Server wird die Fehlermeldung `konnte keine Schlüsselaustauschmethode aushandeln` angezeigt.

Lösung

In diesem Fall ist der SFTP-Server kein FIPS-kompatibles Gerät, das die DH 14-Gruppe verwendet. ACS unterstützt nur Server mit DH 14-Unterstützung, da sie FIPS-konform sind. Weitere Informationen zu diesem Problem finden Sie unter Known Limitations in ACS 5.2.

Problem: "Ungültige EAP-Payload verworfen"

Der `Fehler: Beim` Authentifizieren der Wireless-Benutzer mit dem ACS 5.0-Patch 7 wird eine `ungültige` Fehlermeldung `für den` Ausfall der `EAP-Payload` empfangen.

Lösung

Dies ist ein beobachtetes Verhalten, das in den Cisco Bug-IDs CSCsz54975 (nur registrierte Kunden) und CSCsy46036 (nur registrierte Kunden) behandelt wird.

Um dieses Problem zu beheben, aktualisieren Sie auf ACS 5.0 Patch 9, der als Teil des Upgrades auf 5.1 oder 5.2 erforderlich ist. Ausführliche Informationen finden Sie unter Aktualisieren der Datenbank. Dies beinhaltet auch Informationen zum Upgrade auf Patch 9.

Problem: "Der ACS-Laufzeitprozess wird derzeit für diese Instanz nicht ausgeführt."

Benutzer können sich nicht bei der ACS-GUI anmelden, und diese Fehlermeldung wird ausgegeben:

```
"Der ACS-Laufzeitprozess wird derzeit für diese Instanz nicht ausgeführt. Änderungen können an der ACS-Konfiguration vorgenommen werden (diese werden in der Datenbank gespeichert), Änderungen werden jedoch erst wirksam, wenn der Laufzeitprozess neu gestartet wird."
```

Lösung

Durch manuelles Neustarten des Laufzeitprozesses über die CLI und Neustarten der Appliance wird dieses Problem behoben. Hierbei handelt es sich um ein geringfügiges Problem, das keine Leistungsprobleme für den ACS verursacht. Es gibt zwei kleinere Fehler, die dieses Verhalten nicht beobachten konnten. Weitere Informationen finden Sie unter Cisco Bug IDs CSCtb99448 (nur registrierte Kunden) und CSCtc75323 (nur registrierte Kunden).

Führen Sie folgende Befehle aus der ACS-CLI aus, um die Laufzeitprozesse manuell neu zu starten:

- **ACS Stopp Runtime**
- **ACS Start Runtime**

Problem: Benutzer mit dem Kennwort konnten nicht exportiert werden.

Sie können die Benutzerdatenbank mit einer CSV-Datei in einen anderen ACS 5.x exportieren und importieren. Das Feld für das Benutzerkennwort ist jedoch nicht enthalten (das Feld für das Benutzerkennwort ist leer). Wie verschiebt man einen lokalen Benutzeridentitätsspeicher von einem ACS zu einem anderen, der die Kennwortinformationen enthält?

Lösung

Dies ist nicht möglich, da dies zu einer Sicherheitslücke wird. In diesem Fall besteht eine Lösung darin, ein Sicherungs- und Wiederherstellungsverfahren durchzuführen. Die Einschränkung dieser Problemumgehung besteht jedoch darin, dass die Sicherung und Wiederherstellung nur für einen anderen ACS mit ähnlicher Konfiguration funktioniert.

Problem: Interne ACS-Benutzer sind gelegentlich deaktiviert.

ACS-Benutzer werden gelegentlich deaktiviert, wenn die Meldung "`Kennwort abgelaufen`" angezeigt wird. Die Kennwortablaufrichtlinie ist für 60 Tage festgelegt, diese Benutzer müssen jedoch manuell aktiviert werden, damit sie darauf zugreifen können.

Lösung

Dieses Verhalten wird in der Cisco Bug-ID CSCtf06311 beobachtet und abgelegt (nur registrierte Kunden). Dieses Problem kann durch Anwendung von Patch 3 auf ACS 5.1 gelöst werden. Um alle gelösten Probleme unter Patch 3 anzuzeigen, lesen Sie die Informationen Behoben Probleme in Cumulative Patch ACS 5.1.0.44.3. Weitere Informationen zum Aktualisieren des Patches finden Sie unter Anwenden von Upgrade-Patches.

Problem: "Die TACACS+-Authentifizierungsanfrage endete mit Fehler."

Der ACS-Authentifizierungsbericht zeigt die `TACACS+-Authentifizierungsanfrage, die mit einer` Fehlermeldung `beendet wurde`.

Lösung

Dies tritt auf, wenn für die TACACS-Authentifizierung der Servicetyp auf PPP festgelegt ist. Weitere Informationen finden Sie unter Cisco Bug ID CSCte16911 (nur registrierte Kunden).

Problem: "Radius-Authentifizierungsanfrage aufgrund eines kritischen Protokollierungsfehlers abgelehnt"

Die RADIUS-Authentifizierung wird mit der `RADIUS-Authentifizierungsanforderung aufgrund einer kritischen` Fehlermeldung `abgelehnt`.

Lösung

Dieser Fehler wird im Cisco Bug ID CSCth66302 detailliert beschrieben (nur registrierte Kunden).

Problem: Die ACS View-Schnittstelle zeigt oben auf der Seite "Data Upgrade Failed" (Datenaktualisierung fehlgeschlagen) an, wenn ACS von 5.2 auf 5.3 aktualisiert wird.

Die ACS View-Schnittstelle zeigt oben auf der Seite `Data Upgrade Failed (Datenaktualisierung fehlgeschlagen)` an, wenn der ACS von 5.2 auf 5.3 aktualisiert wird.

Lösung

Dieser Fehler wird in der Cisco Bug-ID CSCtu15651 detailliert beschrieben (nur registrierte Kunden).

Problem: Problem mit "Change password on next login acs" (Kennwort für nächste Anmeldung ändern) in Cisco ACS 5.0

Lösung

In ACS 5.0 kann die Kennwortablauffunktion (der Benutzer muss das Kennwort bei der nächsten Anmeldung ändern) im lokalen Benutzer-ID-Store ausgewählt werden, funktioniert aber nicht. Das Problem mit der Erweiterungsanfrage CSCtc31598 in ACS Version 5.1 wird behoben.

Problem: "% Anwendungsaktualisierung fehlgeschlagen, Fehler - -999. Bitte prüfen Sie die ADE-Protokolle auf Details, oder führen Sie sie erneut mit - Installation der Debuganwendung - aktiviert" auf der ACS-Appliance während des Upgrades aus.

Das `%-Anwendungs-Upgrade ist fehlgeschlagen, Fehler - -999. Bitte überprüfen Sie die ADE-Protokolle auf Details, oder` es wird `ein` Fehler `mit aktivierter Debuganwendung` angezeigt`, wenn` versucht wird, ein ACS Express von 5.0 auf 5.0.1 zu aktualisieren.

Lösung

Dieser Fehler tritt auf, wenn das verwendete Repository TFTP ist und die Dateigröße größer als 32 MB ist. ACS Express kann Dateien mit einer Größe von mehr als 32 MB nicht verarbeiten. Verwenden Sie FTP als Repository, um dieses Problem zu beheben, selbst wenn die Dateigröße mehr als 32 MB beträgt.

Problem: Fehler "Authentifizierung fehlgeschlagen: 12308 Client gesendet Ergebnis TLV zeigt Fehler an"

Die `Authentifizierung ist fehlgeschlagen: 12308 Client gesendet Ergebnis TLV zeigt einen Fehler` auf dem ACS an, wenn Sie versuchen, sich zum ersten Mal zu authentifizieren. Beim zweiten Mal funktioniert die Authentifizierung einwandfrei.

Lösung

Dieser Fehler kann behoben werden, wenn Sie die **schnelle Wiederverbindung** deaktivieren. Ein Upgrade auf **Patch 2 von ACS Version 5.2** hilft, das Problem zu beheben, ohne dass die Fast Reconnect-Funktion deaktiviert wird.

Dieser Fehler kann auch behoben werden, wenn Sie die **erzwungene Kryptobindung** der Komponente deaktivieren. Weitere Informationen finden Sie unter Cisco Bug ID CSCtj31281 (nur registrierte Kunden).

Problem: Fehler "24495 Active Directory-Server sind nicht verfügbar"

Die Authentifizierung beginnt mit dem Fehler: `24495 Active Directory-Server sind nicht verfügbar.` in den ACS 5.3-Protokollen.

Lösung

In der Datei ACSADAgent.log über die CLI des ACS 5.x finden Sie Meldungen wie:`11.03.06:06 xlpacs01 adclient[30401]: INFO <bg:bindingRefresh> base.bind.healing Verlorene Verbindung zu xxxxxxxx. Wird im nicht verbundenen Modus ausgeführt: entriegeln`. Wenn der `Modus Wird getrennt ausgeführt angezeigt:` Fehlermeldung `entriegeln`, d. h. der ACS 5.3 kann keine stabile Verbindung mit Active Directory aufrechterhalten. Die Lösung besteht darin, entweder zu LDAP zu wechseln oder den ACS auf Version 5.2 herabzusetzen. Weitere Informationen finden Sie unter Cisco Bug ID CSCtx71254 (nur registrierte Kunden).

Problem: Fehler "Zeitüberschreitung der EAP-Sitzung 5411"

`5411` Fehlermeldungen `zur Zeitüberschreitung bei EAP-Sitzungen` werden auf ACS 5.x empfangen.

Lösung

EAP-Sitzungs-Timeouts treten häufig bei PEAP auf, bei dem die Komponente die Authentifizierung neu startet, nachdem das ursprüngliche Paket an den RADIUS-Server gesendet wurde, und in den meisten Fällen kein Hinweis auf ein Problem darstellt.

Der gewöhnlich angezeigte Fluss ist:

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

Am Ende ist die Authentifizierung erfolgreich. Allerdings ist im ACS ein Thread aufgrund des plötzlichen Neustarts der EAP-Sitzung vom Supplicant geöffnet, der eine erfolgreiche Authentifizierung und anschließend die EAP-Sitzungs-Timeout-Meldung bewirkt. Das liegt oft an der Treiberebene der Maschine. Stellen Sie sicher, dass die NIC/Wireless-Treiber auf dem Client-Computer auf dem neuesten Stand sind. Sie können auf dem Client erfassen und EAP filtern. | EAPOL, um zu sehen, was der Client bei der Verbindung empfängt oder sendet.

Problem: Die 802.1x-Authentifizierung funktioniert nicht, wenn Anmeldungsbeschränkungen auf dem Active Directory konfiguriert sind.

Die 802.1x-Authentifizierung funktioniert nicht, wenn für die Benutzer im Active Directory Anmeldeeinschränkungen konfiguriert sind.

Lösung

Wenn Sie Anmeldebeschränkungen haben, legen Sie Active Directory für einen einzelnen Computer fest und versuchen Sie, eine 802.1x-Authentifizierung durchzuführen. Die Authentifizierung schlägt fehl, da aus der Sicht von Active Directory die Authentifizierung vom ACS erfolgt und nicht vom Computer, auf dem die Anmeldebeschränkung festgelegt ist. Damit die Authentifizierung erfolgreich ist, können die Anmeldebeschränkungen so festgelegt werden, dass sie die ACS-Computerkonten enthalten.

Problem: Fehler: "Sie sind nicht berechtigt, die angeforderte Seite anzuzeigen", wenn ACS 5.x Admin mit der Rolle ChangeUserPassword das Kennwort ändert

Der Administrator-Benutzer der ACS 5.x-Benutzeroberfläche mit der **ChangeUserPassword-**Rolle kann das Kennwort des in der internen Datenbank gespeicherten AAA-Benutzers nicht ändern. Nach dem Ändern des Kennworts erhält der Benutzer die folgende Popup-Fehlermeldung: `Sie sind nicht berechtigt, die angeforderte Seite anzuzeigen.`

Lösung

Dies kann auftreten, wenn die ACS 5.x-Datenbank von ACS 4.x migriert wird. Verwenden Sie die **SuperAdmin-**Berechtigung, um das Benutzerkennwort zu ändern. Weitere Informationen finden Sie unter Cisco Bug ID CSCty91045 (nur registrierte Kunden).

Problem: Fehlermeldung für ACS 5.x bei fehlgeschlagener Authentifizierung "24495 Active Directory-Server sind nicht verfügbar."

Lösung

Sie müssen die Active Directory-Integration mit ACS 5.x überprüfen. Wenn es sich um eine verteilte Konfiguration handelt, stellen Sie sicher, dass sowohl der primäre als auch der sekundäre ACS 5.x in der Konfiguration ordnungsgemäß in Active Directory integriert sind.

Problem: Verbindung zur ACS-Appliance mit BMC nicht möglich

Wenn der BMC Client (ein Hardware-Level-Tool) zum Einstieg in die ACS 1121 IBM Server verwendet wird, wird festgestellt, dass der BMC Client über zwei IP-Adressen verfügt.

Lösung

Dieses Verhalten wurde identifiziert und in der Cisco Bug-ID CSCtj81255 protokolliert (nur registrierte Kunden). Um dies zu beheben, müssen Sie den BMC DHCP-Client auf dem ACS 1121 deaktivieren.

Problem: Im Monitor wird ein Warnalarm "Löschen 20.000 Sitzungen" mit der Ursache "Aktive Sitzungen sind überbegrenzt"

angezeigt, und das allgemeine Dashboard wird angezeigt.

Die Anzahl der Datensätze, die in einem Sitzungsverzeichnis gespeichert werden können, ist begrenzt. Da die Anfragen des Kunden sehr umfangreich sind, wird die Obergrenze schnell erreicht. Nach Erreichen des Grenzwerts löscht ACS-View eine bestimmte Anzahl von Datensätzen (z. B. 20.000) aus dem Sitzungsverzeichnis und sendet eine Warnmeldung. Sie können diese Grenze erhöhen, aber es ist nicht viel hilfreich, außer die Warnungen zu verlängern.

Lösung

Führen Sie folgende Schritte aus, um dieses Problem zu beheben:

- Es wird empfohlen, die Protokollierung zu deaktivieren, um die Datenbank anzuzeigen.Gehen Sie zu **Cisco Secure ACS > System Administration > Configuration > Log Configuration > Logging Categories > Global > "Passed Authentications" > Remote Syslog Target**, und entfernen Sie **LogCollector** aus Selected Targets.Gehen Sie zu **Cisco Secure ACS > System Administration > Configuration > Log Configuration > Logging Categories > Global > "Failed Attempts" (Ausgefallene Versuche) > Remote Syslog Target (Remote-Syslog-Ziel),** und entfernen Sie **LogCollector** aus Selected Targets.Gehen Sie zu **Cisco Secure ACS > Systemverwaltung > Konfiguration > Protokollkonfiguration > Protokollierungskategorien > Global > Bearbeiten: "RADIUS Accounting" > Remote Syslog Target** und entfernen **LogCollector** aus ausgewählten Zielen.
- Sie können die Authentifizierungsanforderungen für die Prüfung ignorieren, da es sich hierbei nicht um echte Authentifizierungsanforderungen handelt. Führen Sie folgende Schritte aus:Gehen Sie zu **Cisco Secure ACS > Monitoring Configuration > System Configuration > Add Filter**, und erstellen Sie den Filter. Das Erstellen des Filters auf der Grundlage des *Benutzernamens* ist geeigneter, da die Nachfrageanforderungen als mit einem Scheinbenutzernamen gesendet werden können. Wenn Sie im ACS eine separate Zugriffsrichtlinie erstellen, um diese Anfragen zu bearbeiten, können auch Filter basierend auf dem *Access Service* erstellt werden.

Problem: ACS 5.x-Fehler "11013 RADIUS-Paket ist bereits im Prozess"

Bei einer ACS 5.3-Bereitstellung scheitern Benutzer mit der 802.1x-Authentifizierung. Die verwendete Datenbank ist ein Active Directory. Der RADIUS-Fehlercode wird hier angezeigt:

```
RADIUS-Anfrage verworfen: 11013 RADIUS-Paket wird bereits verarbeitet
```

Lösung

Der ACS hat diese Anforderung ignoriert, da es sich um ein Duplikat eines anderen Pakets handelt, das derzeit verarbeitet wird. Dies kann aus folgenden Gründen auftreten:

- Die Durchschnittslatenzstatistik für RADIUS-Anfragen liegt nahe oder übersteigt das Timeout für Client-RADIUS-Anfragen vom Client.
- Ein externer Identitätsdatenspeicher kann sehr langsam sein.

- Der ACS wurde überladen.

Führen Sie die folgenden Schritte aus, um Folgendes zu beheben:

1. Erhöhen Sie das Client-RADIUS-Anforderungs-Timeout des Clients.
2. Verwenden Sie einen schnelleren oder zusätzlichen externen Identitätsdatenspeicher.
3. Folgen Sie den Anweisungen, um die Überlastung des ACS zu reduzieren.

Problem: Fehler bei der RADIUS-Authentifizierung mit dem Fehler "11012 RADIUS-Paket enthält ungültigen Header"

Lösung

Der Header des eingehenden RADIUS-Pakets wurde nicht richtig analysiert. Um dieses Problem zu beheben, überprüfen Sie Folgendes:

- Überprüfen Sie das Netzwerkgerät oder den AAA-Client auf Hardwareprobleme.
- Überprüfen Sie das Netzwerk, das das Gerät mit dem ACS verbindet, auf Hardwareprobleme.
- Überprüfen Sie, ob das Netzwerkgerät oder der AAA-Client bekannte RADIUS-Kompatibilitätsprobleme hat.

Problem: Die RADIUS/TACACS+-Authentifizierung ist fehlgeschlagen mit dem Fehler "11007 Konnte kein Netzwerkgerät oder AAA-Client suchen".

Diese Fehlermeldung wird auf dem ACS angezeigt, wenn eine ASA eine RADIUS-Zugriffsanforderungsmeldung sendet:

```
11007 Konnte kein Netzwerkgerät oder AAA-Client finden
```

Lösung

Dies liegt daran, dass eine Diskrepanz zwischen der IP-Adresse des ACS-Clients und der IP-Schnittstelle besteht, die die Anfrage tatsächlich sendet. Manchmal führt die Firewall eine Adressumwandlung zu diesem AAA-Client durch. Überprüfen Sie, ob der AAA-Client auf diesem Pfad mit der richtigen übersetzten IP-Adresse konfiguriert ist:

Netzwerkressourcen > Netzwerkgeräte und AAA-Clients

Problem: Die RADIUS-Authentifizierung ist fehlgeschlagen mit dem Fehler "11050 RADIUS-Anfrage aufgrund von Systemüberlastung verworfen".

Benutzer können aufgrund der fehlgeschlagenen Authentifizierung nicht auf das Netzwerk zugreifen. Diese Fehlermeldung vom ACS wird empfangen:

```
11050 RADIUS-Anfrage aufgrund von Systemüberlastung abgebrochen
```

Lösung

Cisco ACS verwirft diese Authentifizierungsanforderungen aufgrund von Überlastung. Dies kann durch die Replikation vieler paralleler Authentifizierungsanforderungen verursacht werden. Führen Sie folgende Schritte aus, um dies zu vermeiden:

- Ändern Sie die Einstellungen für **Netzwerkgerät/AAA-Client**, sodass die Option **Unterstützung für** die **veraltete TACACS+-Einzelverbindung** verwendet wird. Dadurch verwendet der Client dieselbe Sitzung für alle Anfragen, anstatt mehrere Sitzungen zu erstellen.
- Unterlassen Sie die Benutzer, zu einem bestimmten Zeitpunkt neue Authentifizierungsanforderungen zu erstellen.
- Starten Sie den ACS-Server neu.

Problem: Die RADIUS-Authentifizierung ist fehlgeschlagen mit dem Fehler "11309 Falsches RADIUS MS-CHAP v2-Attribut".

Lösung

Dieser Fehler ist auf die ungültige Länge oder den falschen Wert eines der MSCHAP v2-Attribute (MS-CHAP-Challenge, MS-CHAP-Response, MS-CHAP-CPW-2 oder MS-CHAP-NT-Enc-PW) im empfangenen RADIUS Access-Request-Paket zurückzuführen.

Problem: ACS meldet eine Speichernutzung von über 90 %. Alarm

ACS meldet eine Speichernutzung von mehr als 90 %.Alarm: `Cisco Secure ACS - AlarmbenachrichtigungSchweregrad: Critical Alarm Name ACS - Systemstatusverursachungs-/Trigger-Alarm ausgelöst durch ACS - SystemstatusschwelleAlarm Details ACS Instance CPU Utilization (%) Speicherauslastung (%) Festplatten-E/A-Auslastung (%) genutzter Speicherplatz /opt (%) genutzter Speicherplatz /localdisk: (%) Verwendeter Festplattenspeicher / (%) KOM-AAA02 0,41 90,14 0,02 9,57 5,21 25,51`

Lösung

Dieses Problem tritt in der Regel bei ACS 5.2 auf. Um dieses Problem zu beheben, laden Sie den ACS neu, um den Speicher freizugeben, oder aktualisieren Sie auf ACS 5.2 Patch 7 oder höher. Weitere Informationen finden Sie unter Cisco Bug ID CSCtk52607 (nur registrierte Kunden).

Problem: Fehler:com.cisco.nm.acs.mgmt.msgbus.FatalBusException: Verknüpfung von Knoten fehlgeschlagen

In einer verteilten Konfiguration nach einer Wartungsaufgabe (Beitritt zu einer primären, erzwungenen vollständigen Replikation, Patching) meldet die ACS-Instanz A im Bildschirm der verteilten Bereitstellung die ACS-Instanz B als offline, während B tatsächlich online ist und Instanz A als online meldet. In den Verwaltungsprotokollen sehen Sie `error:com.cisco.nm.acs.mgmt.msgbus.FileBusException: Verknüpfung von Knoten fehlgeschlagen.`

Lösung

Dies kann auftreten, wenn eine vorherige Instanz des Replikationsmanagement-Service nach dem Einsetzen der neuen Instanz immer noch an Port 2030 gebunden ist und versucht, eine Bindung an diesen Port herzustellen. Führen Sie in der CLI von ACS Instanz B die Datei ACS:sho acs-logs ACSManagement aus. `Protokoll | i Replication Service`. Sie sehen Meldungen wie `Replication Service fehlgeschlagen.:Port bereits in Gebrauch: 2030.` Gegenwärtig besteht die Problemumgehung darin, die ACS-Instanz B neu zu starten (die Instanz B, die die andere als online meldet). Weitere Informationen finden Sie unter Cisco Bug ID CSCtx56129 (nur registrierte Kunden).

Problem: Fehler:com.cisco.nm.acs.mgmt.msgbus.FatalBusException: Verknüpfung von Knoten fehlgeschlagen

In einer verteilten Konfiguration nach einer Wartungsaufgabe (Beitritt zu einer primären, erzwungenen vollständigen Replikation, Patching) meldet die ACS-Instanz A im Bildschirm der verteilten Bereitstellung die ACS-Instanz B als offline, während B tatsächlich online ist und Instanz A als online meldet. In den Verwaltungsprotokollen sehen Sie `error:com.cisco.nm.acs.mgmt.msgbus.FileBusException: Verknüpfung von Knoten fehlgeschlagen.`

Lösung

Aktualisieren Sie auf ACS 5.2 Patch 6 oder höher, um dieses Problem zu beheben. Weitere Informationen finden Sie unter Cisco Bug ID CSCto47203 (nur registrierte Kunden).

Hinweis: Die viewDB-Sicherung schlägt fehl, sobald die ""/opt"-Nutzung 30 % überschreitet. Es ist erforderlich, NFS-Staging so zu konfigurieren, dass eine Sicherung durchgeführt wird, wenn ""/opt" die Auslastung von 30 % überschreitet.

Problem: Fehler 11026 Die angeforderte dACL wurde nicht gefunden.

Die RADIUS-Authentifizierung schlägt mit der folgenden Fehlermeldung fehl: `11026 Die angeforderte dACL wurde nicht gefunden.`

Lösung

Die Anfrage wird abgelehnt, da die in der RADIUS Access-Request angeforderte Version der herunterladbaren Zugriffskontrollliste nicht gefunden wurde. Die Anfrage für die herunterladbare ACL erfolgte lange nach der ursprünglichen Zugriffsanfrage. Daher war die Version der herunterladbaren ACL nicht mehr verfügbar. Die Ursache für diese Verzögerung finden Sie in der Anfrage für die herunterladbare ACL vom RADIUS-Client.

Problem: error 11025 Der Access-Request für die angeforderte dACL fehlt ein cisco-av-pair-Attribut mit dem Wert aaa:event=acl-

download. Der Antrag wird abgelehnt.

Die RADIUS-Authentifizierung schlägt mit der folgenden Fehlermeldung fehl: `11025 Bei der Zugriffsanforderung für die angeforderte dACL fehlt ein cisco-av-pair-Attribut mit dem Wert aaa:event=acl-download. Der Antrag wird abgelehnt.`

Lösung

Jede Zugriffsanfrage für die herunterladbare ACL muss ein `cisco-av-pair-Attribut` mit dem Wert `aaa:event=acl-download` aufweisen. In diesem Fall fehlt dem Attribut die Anforderung, und der ACS hat die Anforderung nicht erfüllt. Überprüfen Sie, ob das Netzwerkgerät oder der AAA-Client bekannte RADIUS-Kompatibilitätsprobleme hat.

Problem: Fehler 11023 Die angeforderte dACL wurde nicht gefunden. Dies ist ein unbekannter dACL-Name.

Die RADIUS-Authentifizierung schlägt mit der folgenden Fehlermeldung fehl: `11023 Die angeforderte dACL wurde nicht gefunden. Dies ist ein unbekannter dACL-Name.`

Lösung

Überprüfen Sie die ACS-Konfiguration, um sicherzustellen, dass die im Authorization Profile (Autorisierungsprofil) angegebene herunterladbare ACL in der Liste der herunterladbaren ACLs vorhanden ist. Dies ist eine Fehlkonfiguration auf der ACS-Seite.

Problem: Administratorauthentifizierung fehlgeschlagen mit Fehler 10001 Interner Fehler. Falsche Konfigurationsversion

Die Administratorauthentifizierung schlägt mit diesem Fehler fehl: `10001 Interner Fehler. Falsche Konfigurationsversion.`

Lösung

Dieser Fehler kann durch eine beschädigte ACS-Datenbank oder ein Problem in den zugrunde liegenden Konfigurationsdaten verursacht werden. Wenden Sie sich an Cisco TAC (nur registrierte Kunden), um weitere Informationen zu erhalten.

Problem: Administratorauthentifizierung fehlgeschlagen mit Fehler 10002 Interner Fehler: Keine geeigneten Services geladen

Die Administratorauthentifizierung schlägt mit diesem Fehler fehl: `10002 Interner Fehler: Nicht geeigneter Service geladen.`

Lösung

ACS 5.x kann den AAC-Konfigurationsservice nicht laden. Dies kann durch eine beschädigte

ACS-Datenbank oder durch ein Problem in den zugrunde liegenden Konfigurationsdaten verursacht werden. Sie kann auch auftreten, wenn die Systemressourcen erschöpft sind. Wenden Sie sich an Cisco TAC (nur registrierte Kunden), um weitere Informationen zu erhalten.

Problem: Administratorauthentifizierung fehlgeschlagen mit Fehler 10003 Interner Fehler: Administratorauthentifizierung erhalten leeren Administratornamen

Die Administratorauthentifizierung schlägt mit diesem Fehler fehl: `10003 Interner Fehler: Die Administratorauthentifizierung erhielt einen leeren Administratornamen.`

Lösung

Beim Zugriff auf die Benutzeroberfläche von ACS 5.x erhält der ACS einen leeren Benutzernamen. Überprüfen Sie die Gültigkeit des Benutzernamens, der an das ACS übertragen wurde. Falls gültig, wenden Sie sich an Cisco TAC (nur registrierte Kunden), um weitere Informationen zu erhalten.

Problem: Fehlergrund: 24428 Verbindungsfehler in LRPC, LDAP oder KERBEROS

Diese Fehlermeldung wird auf dem ACS angezeigt:

```
Fehlergrund: 24428 Verbindungsfehler in LRPC, LDAP oder KERBEROS Dieser RPC-Verbindungsproblem kann darauf zurückzuführen sein, dass das Stub falsche Daten erhalten hat
```

Lösung

Um dieses Problem zu beheben, aktualisieren Sie den ACS auf Version 5.2.

Problem: Die TACACS+-Auth-Proxy-Authentifizierung funktioniert nicht auf einem Router, auf dem IOS 15.x vom ACS 5.x-Server ausgeführt wird.

Die TACACS+-Auth-Proxy-Authentifizierung funktioniert nicht auf einem Router, auf dem die Cisco IOS-Softwareversion 15.x von einem ACS 5.x-Server ausgeführt wird.

Lösung

TACACS+ Auth-Proxy wird nur nach ACS 5.3 Patch 5 unterstützt. Aktualisieren Sie Ihr ACS 5.x, oder verwenden Sie RADIUS für Auth-Proxy.

Problem: Abrufen von Fehlermeldung Store Failure (acs-xxx, TACACSAccounting) von ACS 5.x

Lösung

Der ACS 5.1 TACACS-Accounting-Bericht übersieht einige Attribute wie Benutzername, Berechtigungsebene und Anforderungstyp, wenn er ein fehlerhaftes Accounting-Paket vom Client empfängt. In einigen Fällen führt dies zur Generierung eines "Store Failure (acs-xxx, TACACSAccounting)"-Alarms in View. Um dieses Problem zu beheben, überprüfen Sie Folgendes:

- Das vom Client gesendete Accounting-Paket weist ein fehlerhaftes TACACS-Argument auf (z. B. eine Abweichung in der Länge und dem Wert eines Arguments, das vom AAA-Client gesendet wurde).
- Stellen Sie sicher, dass der Client ein gültiges Accounting-Paket mit der richtigen Länge und dem Wert der Argumente sendet.

Weitere Informationen finden Sie unter Cisco Bug ID CSCte88357 (nur registrierte Kunden).

Problem: Die Benutzerauthentifizierung ist fehlgeschlagen mit dem Fehler "11036 Das RADIUS-Attribut der Nachrichtenauthentifizierung ist ungültig."

Lösung

Überprüfen Sie Folgendes:

- Überprüfen Sie, ob die Shared Secrets auf dem AAA-Client und dem ACS-Server übereinstimmen.
- Stellen Sie sicher, dass der AAA-Client und das Netzwerkgerät keine Hardwareprobleme oder Probleme mit der RADIUS-Kompatibilität haben.
- Stellen Sie sicher, dass das Netzwerk, das das Gerät mit dem ACS verbindet, keine Hardwareprobleme aufweist.

Problem: RADIUS Accounting ist fehlgeschlagen mit dem Fehler "11037 Dropped accounting request received via unsupported port".

Lösung

Die Buchhaltungsanfrage wurde verworfen, weil sie über eine nicht unterstützte UDP-Portnummer empfangen wurde. Überprüfen Sie Folgendes:

- Stellen Sie sicher, dass die Konfiguration der Accounting-Port-Nummer auf dem AAA-Client und dem ACS-Server übereinstimmt.
- Stellen Sie sicher, dass der AAA-Client keine Hardwareprobleme oder Probleme mit der RADIUS-Kompatibilität hat.

Problem: RADIUS Accounting ist fehlgeschlagen mit dem Fehler

"11038 RADIUS Accounting-Request Header enthält ungültiges Authentifiziererfeld."

Der ACS kann das Feld "Authenticator" im Header des RADIUS Accounting-Request-Pakets nicht validieren. Das Feld "Authenticator" darf nicht mit dem RADIUS-Attribut "Message-Authenticator" verwechselt werden. Stellen Sie sicher, dass der auf dem AAA-Client konfigurierte RADIUS Shared Secret mit dem für das ausgewählte Netzwerkgerät auf dem ACS-Server konfigurierten Wert übereinstimmt. Stellen Sie außerdem sicher, dass der AAA-Client keine Hardwareprobleme oder Probleme mit der RADIUS-Kompatibilität hat.

Fehler: "24493 ACS hat Probleme bei der Kommunikation mit Active Directory mithilfe seiner Anmeldeinformationen für das System."

Lösung

Überprüfen Sie den ACS auf AD-Konnektivität, und stellen Sie sicher, dass das ACS-Systemkonto im AD noch vorhanden ist.

Problem: "Beim Erstellen von Shell-Profilnamen mit Sonderzeichen wie "ê" kann der ACS abstürzen."

Lösung

Dieses Verhalten wurde identifiziert und in Cisco Bug ID CSCts17763 protokolliert (nur registrierte Kunden). Sie müssen ein Upgrade auf 5.3.40 Patch 1 oder 5.2.26 Patch 7 durchführen.

Problem: Abrufen von "Analysefehler in Zeile 2: nicht wohlgeformt (ungültiges Token)" bei Ausführung von "show run" in der ACS 5.x-CLI.

Lösung

Stellen Sie sicher, dass die auf dem ACS konfigurierte SNMP-Community gültige Zeichen enthält. Im Community-Namen dürfen nur alphanumerische Zeichen (nur Buchstaben und Zahlen) verwendet werden.

Problem: ACS 5.x /opt-Partition füllt sehr schnell aus

Lösung

ACS 5.x bietet aufgrund des unzureichenden Speicherplatzes in der */opt*-Partition keinen Speicherplatz mehr. Dies ist auf die hohe Anzahl von Protokolldaten zurückzuführen, die die ACS-Ansicht überfluten. Als Problemumgehung müssen Sie die View-Datenbank häufig ersetzen. Da

ACS View nicht jeden Tag Gigabyte an Daten verarbeiten kann, müssen Sie die Protokollierungsdaten organisieren. Wenn Sie alle Protokolle benötigen, verwenden Sie einen externen Syslog-Server anstelle der ACS-Ansicht. Wenn Sie nur einen Teil der Protokollierungsdaten verwenden müssen, verwenden Sie *Systemverwaltung > Konfiguration > Protokollkonfiguration > Protokollierungskategorien > Global,* um nur die erforderlichen Protokolle an den Protokollsammler für die ACS View zu senden.

Problem: Abfragen der gewünschten Domäne

Kann ACS 5.x beim Beitritt zu einer Active Directory-Domäne die gewünschten Domänen-Controller (DCs) abfragen?

Lösung

Nein. Zurzeit fragt der ACS den DNS mit der Domäne ab, um eine Liste aller Rechenzentren in der Domäne abzurufen. Dann versucht es, mit allen zu kommunizieren. Wenn die Verbindung zu einem einzigen Rechenzentrum fehlschlägt, wird die ACS-Verbindung zur Domäne als fehlerhaft deklariert.

Problem: Gleichzeitige Übergeordnete und untergeordnete Domänen

Besteht die Möglichkeit, ACS 5.x sowohl in der übergeordneten als auch in der untergeordneten Domäne gleichzeitig einzurichten?

Lösung

Nein. Zurzeit kann ACS 5.x nur Teil einer Domäne sein. ACS 5.x kann Benutzer/Systeme jedoch von mehreren vertrauenswürdigen Domänen aus authentifizieren.

Problem: Anmelden bei einer Remotedatenbank

Kann ich die ACS 5.x View-Daten in einer Remote-Datenbank speichern?

Lösung

Ja, mit ACS 5.x können Sie die ACS View-Daten auf Microsoft SQL-Servern und Oracle SQL-Servern protokollieren.

Problem: VMWare-Unterstützung

Lösung

ACS 5.x kann auf einem virtuellen System installiert werden. Die neueste Version, ACS 5.3, kann auf den folgenden VMWare-Versionen installiert werden:

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

Problem: Speicherplatzanforderungen

Welche Festplattenspeicherplatzanforderungen bestehen für die ACS 5.x-Testversion?

Lösung

Für die Testversion ist mindestens 60 GB Festplattenspeicher erforderlich. Für die Produktionsinstallation werden 500 GB benötigt.

Problem: "24401 Konnte keine Verbindung zum ACS Active Directory-Agenten herstellen."

Lösung

Um diesen Fehler zu beheben, überprüfen Sie Folgendes:

- Überprüfen Sie, ob der ACS-Computer der Active Directory-Domäne angeschlossen ist.
- Überprüfen Sie den Verbindungsstatus zwischen dem ACS-Computer und dem Active Directory-Server.
- Überprüfen Sie, ob der ACS Active Directory-Agent ausgeführt wird.

Weitere Informationen finden Sie unter Cisco Bug ID CSCtx71254 (nur registrierte Kunden).

Problem: Der Laufzeitprozess zeigt den Status "Ausführung fehlgeschlagen" an.

Beim Aktualisieren des Cisco ACS mit einem Patch wird der Laufzeitprozess im Status "Ausführung fehlgeschlagen" festgehalten, und diese Meldung wird protokolliert:

```
"local0 err err 83 2012-06-12T12:11:08+0200 192.168.150.74 ACS-Logforward-FEHLER:
/opt/CSCOacs/runtime/bin/run-logforward.sh: Zeile 18: 7097 Segmentierungsfehler (Core-gedumpt)
./$daemon -b -f $logfile"
```

Lösung

Dies kann ein Problem mit dem MD5-Patch des letzten Patches sein. Überprüfen Sie die MD5-Prüfsumme des letzten auf das Cisco ACS angewendeten Patches. Laden Sie das Programm erneut herunter, und wenden Sie es dann ordnungsgemäß an.

Problem: Fehlgeschlagene ACS-Authentifizierung, wenn das UCS eine erneute Authentifizierung erzwingt

Der UCS-Server ist so konfiguriert, dass er einen Java-Client vom Cisco ACS authentifiziert. Der Authentifizierungsprozess umfasst die Verwendung des RSA Token-Servers. Die erste Authentifizierung verläuft erfolgreich. Wenn das UCS aktualisiert und den Java-Client zur erneuten Authentifizierung zwingt, schlägt es jedoch fehl, da RSA die Wiederverwendung von Token nicht zulässt. Daher schlägt die Authentifizierung fehl.

Lösung

Dies ist eine Einschränkung aus Sicht des UCS-Servers, nicht aber aus Sicht des Cisco ACS. Der UCS-Server führt eine Zwei-Faktor-Authentifizierung durch, die für Cisco ACS bei Verwendung mit RSA-Token nicht unterstützt wird. Derzeit wird es nicht unterstützt. Als Problemumgehung wird empfohlen, alle Datenbankserver, z. B. AD oder LDAP, außer dem RSA Token-Server zu verwenden.

Problem: "2444 Active Directory-Vorgang ist aufgrund eines nicht angegebenen Fehlers im ACS fehlgeschlagen."

Lösung

Bei einem AD-bezogenen Vorgang ist ein nicht zugeordneter Fehler aufgetreten. Siehe ACS 5.x-Integration in Microsoft AD-Konfigurationsbeispiel und konfigurieren Sie die AD-Integration mit dem ACS ordnungsgemäß. Wenn alle Elemente gemäß Dokument richtig konfiguriert sind, wenden Sie sich für weitere Fehlerbehebung an das Cisco TAC.

Problem: ACS 5.1-Benutzer mit AD 2008 R2-Server können nicht authentifiziert werden

Lösung

Dies ist auf Kompatibilitätsprobleme zurückzuführen. Die AD 2008 R2-Integration wird nur von der ACS 5.2-Version unterstützt. Aktualisieren Sie Ihr ACS auf 5.2 oder höher. Weitere Informationen finden Sie unter Cisco Bug ID CSCtg12399 (nur registrierte Kunden).

Fehler: 2056 Betreff nicht im/den entsprechenden Identitätsspeicher(en) gefunden.

Wenn die SSL VPN-Benutzer versuchen, von einer RSA-Appliance authentifiziert zu werden, wird diese Fehlermeldung vom Cisco ACS Server empfangen:

```
Fehlergrund: 2056 Betreff nicht im/den entsprechenden Identitätsspeicher(en) gefunden.
```

Lösung

Überprüfen Sie, ob der Benutzer in der Datenbank vorhanden ist, in der der ACS gesucht wird. Stellen Sie bei RSA und RADIUS Identity Store sicher, dass die Option **Treat Reject** als **fehlgeschlagene Authentifizierung** ausgewählt ist. Dies ist unter der Registerkarte Erweitert der Konfiguration des Identity Store möglich.

Problem: ipt_connlimit: Hopfen: Ungültiger ct-Status?

Die `ipt_connlimit: Hopfen: Ungültiger ct-Status?` wird auf der Konsole angezeigt, wenn ACS 5.x unter VMWare ausgeführt wird.

Lösung

Dies ist eine kosmetische Botschaft. Weitere Informationen finden Sie unter Cisco Bug ID CSCth25712 (nur registrierte Kunden).

Problem:ACs 5.x/ISE sehen in einer RADIUS-Anfrage von Cisco IOS Software Release 15.x NAS kein RADIUS-Attribut für die Anrufer-ID des RADIUS-Servers

ACs 5.x/ISE sehen kein `RADIUS-Attribut für RADIUS-Anfragen von Cisco IOS Software Release 15.x NAS.`

Lösung

Verwenden Sie den Befehl radius-server-Attribut 31 Send nas-port-detail **in Cisco IOS Software Release 15.x, um das Senden des Attributs zu ermöglichen.**

Problem: Benutzerkonten werden bei der ersten Instanz falscher Anmeldeinformationen gesperrt, selbst wenn sie für 3 Versuche konfiguriert wurden.

Wenn ACS 5.3 in Active Directory auf einer funktionalen Ebene von Windows 2008 R2 integriert ist, werden Benutzerkonten, die mit Sperrparametern (3 falsche Versuche) eingerichtet wurden, vorzeitig gesperrt, nachdem der Benutzer die falschen Anmeldeinformationen nur einmal eingegeben hat.

Lösung

Weitere Informationen finden Sie unter Cisco Bug ID CSCtz03211 (nur registrierte Kunden).

Problem: Backup von ACS kann nicht gespeichert werden

Beim Versuch, eine Sicherung vom ACS zu speichern, `liegt` die `Ursache darin: Zuwachssicherung nicht konfiguriert - Details: Die inkrementelle Sicherung ist nicht konfiguriert.Die Konfiguration der inkrementellen Sicherung ist erforderlich, damit die Bereinigung der Datenbank erfolgreich durchgeführt werden kann. Dadurch können Probleme mit dem Speicherplatz auf der Festplatte vermieden werden. Die Größe der View-Datenbank beträgt 0,08 GB, und die Größe der Festplatte beträgt 0,08 GB,` wird angezeigt.

Lösung

Sie können keine inkrementelle Sicherung, vollständige Sicherung und Datenlöschung gleichzeitig ausführen. Wenn eine dieser Jobs ausgeführt wird, müssen Sie 90 Minuten warten, bevor Sie mit dem nächsten Job beginnen können.

Zugehörige Informationen

- Support-Seite für das Cisco Secure Access Control System
- Cisco Secure Access Control System - Benutzerhandbücher
- Technischer Support und Dokumentation für Cisco Systeme