Secure Access Control System 5.x und neuere FAQ

Inhalt

Einführung

Dieses Dokument enthält Antworten auf die am häufigsten gestellten Fragen (FAQs) zum Cisco Secure Access Control System (ACS) 5.x und höher.

Authentifizierungsbezogene Probleme

F. Können einige Benutzer/Gruppen der internen ACS 5.x-Datenbank von der Richtlinie für das Benutzerpasswort ausgeschlossen werden (Systemverwaltung > Benutzer > Authentifizierungseinstellungen)?

Antwort: Standardmäßig muss jeder interne Datenbankbenutzer die Kennwortrichtlinie für den Benutzer einhalten. Derzeit können keine Benutzer/Gruppen der internen ACS 5.x-Datenbank ausgeschlossen werden.

F. Können einige GUI-Administratoren von ACS 5.x von der Richtlinie für das Administratorkennwort ausgeschlossen werden (Systemverwaltung > Administratoren > Einstellungen > Authentifizierung)?

Antwort: Standardmäßig muss jeder GUI-Administrator-Benutzer die Richtlinien für Administratorkennwörter erfüllen. Derzeit kann kein administrativer Benutzer von ACS 5.x ausgeschlossen werden.

F. Bietet ACS 5.x Unterstützung für VMWare-Tools?

Antwort: Nein. Derzeit werden die VMWare-Tools nicht von ACS Version 5.x unterstützt. Weitere Informationen finden Sie unter Cisco Bug ID CSCtg50048 (nur registrierte Kunden).

F. Welche EAP-Authentifizierungsprotokolle werden für ACS 5.x unterstützt, wenn LDAP als Identitätsspeicher konfiguriert ist?

Antwort: Wenn LDAP als Identitätsspeicher verwendet wird, unterstützt ACS 5.2 nur die Protokolle PEAP-GTC, EAP-FAST-GTC und EAP-TLS. EAP-FAST MSCHAPv2, PEAP EAP-MSCHAPv2 und

EAP-MD5 werden nicht unterstützt. Weitere Informationen finden Sie unter Authentifizierungsprotokoll und Benutzerdatenbankkompatibilität.

F. Warum ist die Authentifizierung für WLC mit dem Verwendungsradius bei ACS fehlgeschlagen, und warum hat ACS keine fehlgeschlagenen Versuche gezeigt?

Antwort: Es besteht ein Problem mit der **ACS 5.0- und WLC-Interoperabilität** vor Patch 4. Laden Sie Patch 8 herunter, und wenden Sie den Patch auf die CLI an. Verwenden Sie TFTP nicht, um dieses Problem zu beheben.

F. Warum kann ich keine tar.gz-Dateien wiederherstellen, die mit dem backup-log-Befehl in ACS 5.2 gesichert wurden?

Antwort: Protokolldateien, die mit dem Befehl **backup-log** gesichert werden, können nicht wiederhergestellt werden. Sie können nur die für die ACS-Konfiguration und ADE-OS gesicherten Dateien wiederherstellen. Weitere Informationen finden Sie in den Befehlen **für Backups** und **Backupprotokolle** im CLI-Referenzhandbuch für das Cisco Secure Access Control System 5.1.

F. Kann ich die Anzahl der fehlgeschlagenen Kennwortversuche auf ACS 5.2 begrenzen?

Antwort: Nein. Diese Funktion ist für ACS 5.2 nicht verfügbar, soll aber in ACS 5.3 integriert werden. Weitere Informationen finden Sie im Abschnitt Funktionen, die nicht unterstützt werden, der Versionshinweise für das Cisco Secure Access Control System 5.2.

F. Ich kann die Option zum Ändern des Kennworts bei der nächsten Anmeldung für interne Benutzer in ACS 5.0 nicht verwenden. Wie kann ich dieses Problem beheben?

Antwort: Die Option zum Ändern des Kennworts bei der nächsten Anmeldung wird in ACS 5.0 nicht unterstützt. Diese Funktion wird ab ACS 5.1 unterstützt.

F. Was bedeutet dieser Alarm auf ACS?

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

Antwort: Dieser Fehler bedeutet, dass die ACS-Ansicht, wenn sie eine Grenze von 250.000 Sitzungen erreicht, einen Alarm auslöst, um 20.000 Sitzungen zu löschen. In der ACS View-Datenbank werden alle vorherigen Authentifizierungssitzungen gespeichert. Wenn sie 250.000 erreicht haben, wird ein Alarm ausgegeben, um den Cache zu löschen und 20.000 Sitzungen zu löschen.

F. Wie kann ich diese Fehlermeldung beheben? `Authentifizierung fehlgeschlagen: 24407 Benutzerauthentifizierung mit Active Directory fehlgeschlagen, da der Benutzer sein Kennwort ändern muss`?

Antwort: Diese Fehlermeldung wird angezeigt, wenn bei der SDI-Authentifizierung ein Problem mit

der Kennwortverwaltung auftritt. ACS 5.x wird als Radius-Proxy verwendet und die Benutzer müssen von einem RSA-Server authentifiziert werden. Der Radius-Proxy zu RSA funktioniert nur ohne Kennwortverwaltung. Der Grund hierfür ist, dass der OTP-Wert vom Radius-Server wiederhergestellt werden kann, um den Kennwortwert auf den RSA-Server zu verteilen. Wenn die Kennwortverwaltung in der Tunnelgruppe aktiviert ist, wird die Radius-Anforderung mit MS-CHAPv2-Attributen gesendet. RSA unterstützt MS-0CHAPv2 nicht. Es unterstützt nur PAP.

Um dieses Problem zu beheben, deaktivieren Sie die Kennwortverwaltung. Weitere Informationen finden Sie unter Cisco Bug ID CSCsx47423 (nur registrierte Kunden).

F. Kann der ACS-Administrator festlegen, dass nur bestimmte Geräte in ACS 5.1 verwaltet werden?

Antwort: Nein, es ist nicht möglich, den ACS-Administrator zu beschränken, nur bestimmte Geräte innerhalb von ACS 5.1 zu verwalten.

F. Unterstützt der ACS QoS bei der Authentifizierung, damit RADIUS gegenüber TACACS priorisiert werden kann?

Antwort: Nein, der ACS unterstützt QoS bei der Authentifizierung nicht. ACS priorisiert RADIUS-Authentifizierungsanforderungen nicht gegenüber TACACS- oder TACACS-Anfragen gegenüber RADIUS.

F. Können ACS 5.x TACACS- und RADIUS-Authentifizierungen für andere TACACS- oder RADIUS-Server proxylieren?

Antwort: Ja, alle ACS 5.x-Versionen können die RADIUS-Authentifizierungen auf andere RADIUS-Server verweisen. ACS 5.3 und höher können die TACACS-Authentifizierungen auf andere TACACS-Server verweisen.

F. Kann ACS 5.x die Einwahlattribute eines Active Directory-Benutzers überprüfen, um Zugriff zu gewähren?

Antwort: Ja, in ACS 5.3 und höher können Sie den Zugriff auf die Einwahlberechtigungen eines Benutzers zulassen, verweigern und steuern. Die Berechtigungen werden bei Authentifizierungen oder Abfragen von Active Directory überprüft. Es wird auf dem dedizierten Active Directory-Wörterbuch festgelegt.

F. Unterstützt ACS 5.x die Authentifizierungstypen CHAP oder MSCHAP für TACACS+?

Antwort: Ja, die Authentifizierungstypen TACACS+ CHAP und MSCHAP werden in ACS 5.3 und höher unterstützt.

F. Kann ich den Kennworttyp eines internen ACS-Benutzers auf eine externe Datenbank festlegen?

Antwort: Ja, in ACS 5.3 und höher können Sie den Kennworttyp eines internen ACS-Benutzers festlegen. Diese Funktion war in ACS 4.x verfügbar.

F. Kann ich eine Authentifizierung basierend auf dem Zeitpunkt, zu dem der Benutzer im internen ACS-Identitätsspeicher erstellt wurde, bestehen bzw. scheitern?

Antwort: Ja, in ACS 5.3 und höher können Sie das Attribut **Number of Hours Since User Creation (Anzahl der Stunden seit Benutzererstellung)** verwenden, um Ihre Richtlinien zu erstellen. Dieses Attribut enthält die Anzahl der Stunden, die seit der Erstellung des Benutzers im internen Identitätsspeicher zum Zeitpunkt der aktuellen Authentifizierungsanforderung vergangen sind.

F. Kann ich Platzhalter verwenden, um einen neuen Hosteintrag in die interne ACS-Datenbank hinzuzufügen?

Antwort: Ja, mit ACS 5.3 und höher können Sie Platzhalter verwenden, wenn Sie dem internen Identity Store neue Hosts hinzufügen. Außerdem können Sie Platzhalter eingeben (nachdem Sie die ersten drei Oktette eingegeben haben), um alle Geräte des angegebenen Herstellers anzugeben.

F. Kann ich IP-Adresspools auf dem ACS 5.x konfigurieren und von ACS zuweisen?

Antwort: Nein, derzeit ist es nicht möglich, IP-Adresspools auf ACS 5.x zu erstellen.

F. Kann ich die IP-Adresse des AAA-Clients sehen, von dem die Anfrage im FAILED AUTHENTICATION-Bericht einging?

Antwort: Nein, es ist nicht möglich, die IP-Adresse des AAA-Clients anzuzeigen, von der aus die Anfrage einging.

F. Was ist die Protokollwiederherstellung in ACS 5.3?

Antwort: ACS 5.3 bietet eine neue Funktion zum Wiederherstellen von Protokollen, die bei einem Ausfall der Ansicht verpasst wurden. ACS sammelt diese verpassten Protokolle und speichert sie in seiner Datenbank. Mit dieser Funktion können Sie die verpassten Protokolle aus der ACS-Datenbank in die Ansichtsdatenbank abrufen, nachdem die Ansicht gesichert wurde. Um diese Funktion verwenden zu können, müssen Sie die Konfiguration zur Wiederherstellung von Protokollnachrichten auf **ein** setzen. Weitere Informationen zum Konfigurieren der Wiederherstellung von Protokollnachrichten finden Sie unter Überwachung und Berichtsanzeige-Systemvorgänge.

F. Kann ich die ACS 5.x-Datenbank komprimieren, indem ich den Befehl database-compress in der Solution Engine-CLI ausgebe? Diese Funktion war in ACS 4.x verfügbar.

Antwort: Ja, in ACS 5.3 und höher reduziert der Befehl **database-compress** die ACS-Datenbankgröße mit der Option, die ACS-Transaktionstabelle zu löschen.ACS-Administratoren können diesen Befehl ausführen, um die Datenbankgröße zu reduzieren. Dies trägt dazu bei, die Datenbankgröße und den Zeitaufwand für Backups sowie die vollständige Synchronisierung zu reduzieren, die für die Wartung erforderlich ist.

F. Kann ich einen AAA-Client-Eintrag anhand seiner IP-Adresse suchen?

Antwort: Ja, mit ACS 5.3 und höher können Sie ein Netzwerkgerät mit seiner IP-Adresse suchen. Sie können auch Platzhalter und den Bereich verwenden, um eine bestimmte Gruppe von Netzwerkgeräten zu durchsuchen.

F. Kann ich eine Bedingung erstellen, die auf dem Zeitpunkt basiert, zu dem der Benutzer im internen ACS-Identitätsspeicher erstellt wurde?

Antwort: Ja, in ACS 5.3 und höher können Sie das Attribut **Number of Hours Since User Creation** (**Anzahl der Stunden seit Benutzererstellung)** verwenden, mit dem Sie die Bedingungen für Richtlinienregeln konfigurieren können, basierend auf dem Zeitpunkt, zu dem der Benutzer im internen ACS-Identitätsspeicher erstellt wurde. Beispiel: IF **group=HelpDesk&NumberofHoursSinceUserCreation>48** dann Ablehnen. Dieses Attribut enthält die Anzahl der Stunden, die seit der Erstellung des Benutzers im internen Identity Store zum Zeitpunkt der aktuellen Authentifizierungsanforderung vergangen sind.

F. Kann ich überprüfen, welcher Identitätsspeicher der Benutzer im Abschnitt Autorisierung einer Service-Richtlinie authentifiziert wurde?

Antwort: Ja, in ACS 5.3 und höher können Sie das **Authentication Identity Store-**Attribut verwenden, mit dem Sie die Richtlinienregelbedingungen auf Basis des Authentifizierungs-Identity-Store konfigurieren können. Beispiel: IF **AuthenticationIdentityStore=LDAP_NY** dann ablehnen. Dieses Attribut enthält den Namen des verwendeten Identity Store und wird nach erfolgreicher Authentifizierung mit dem entsprechenden Identity Store-Namen aktualisiert.

F. Wann wird der ACS zum nächsten in der Identity Store-Sequenz definierten Identitätsspeicher wechseln?

Antwort: Der ACS wird zum nächsten in der Identity Store-Sequenz definierten Identitätsspeicher in den folgenden Szenarien:

- Ein Benutzer wird im ersten Identitätsspeicher nicht gefunden.
- Ein Identity Store ist in der Sequenz nicht verfügbar.

F. Was ist die Account Disablement-Richtlinie in ACS 5.3?

Antwort: Mit der Richtlinie zur Kontodeaktivierung können Sie die Benutzer des internen Identitätsspeichers deaktivieren, wenn das konfigurierte Datum das zulässige Datum überschreitet, die konfigurierte Anzahl von Tagen die zulässigen Tage überschreitet oder die Anzahl aufeinander folgender fehlgeschlagener Anmeldeversuche den Schwellenwert überschreitet. Der Standardwert für das Datum überschreitet 30 Tage ab dem aktuellen Datum. Der Standardwert für Tage sollte nicht mehr als 60 Tage ab dem aktuellen Tag betragen. Der Standardwert für fehlgeschlagene Versuche ist 5.

F. Kann ich das Kennwort eines internen Datenbankbenutzers von ACS über Telnet ändern?

Antwort: Ja, Sie können das Kennwort eines internen Datenbankbenutzers mithilfe von TACACS+ über Telnet ändern. Sie müssen **TELNET Change Password** unter **Password Change Control (Kennwortänderungskontrolle)** auf ACS 5.x **aktivieren**.

F. Aktualisiert die primäre ACS 5.x-Instanz die Sicherungsinstanzen automatisch regelmäßig oder sollte dies nur geschehen, wenn eine Konfiguration geändert wurde?

Antwort: ACS 5.x repliziert sofort auf den sekundären ACS, wenn Sie Änderungen am primären ACS vornehmen. Wenn Sie anschließend keine Änderungen am primären ACS vornehmen, wird alle 15 Minuten eine Replikation durchgeführt. Zu diesem Zeitpunkt gibt es keine Möglichkeit, den Timer zu steuern, sodass ACS die Informationen nach einer bestimmten Zeit replizieren kann.

F. Kann ich einen Bericht auf ACS 5.x aller Benutzer anzeigen/exportieren, die derzeit über ACS auf verschiedenen NAS-Clients angemeldet und authentifiziert sind?

Antwort: Ja, es ist möglich. Es gibt zwei separate Berichte für RADIUS und TACACS+. Sie finden sie unter **Monitoring & Reports > Reports > Catalog > Session Directory > RADIUS Active Sessions and TACACS Active Sessions.** Beide Berichte basieren auf den Accounting-Informationen der NAS-Clients, da Sie nachverfolgen können, wann der Benutzer eine Verbindung herstellt und sich abmeldet. Der Sitzungsverlauf ermöglicht es Ihnen sogar, Informationen von Anfang an und von Ende der Nachrichten an einem bestimmten Tag abzurufen.

Zugehörige Informationen

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