Secure Access Control System 5.x 以降に関する FAQ

内容

[概要](#)
[認証に関する問題](#)
[関連情報](#)

概要

このドキュメントでは、Cisco Secure Access Control System（ACS）5.x 以降に関するよくある質問（FAQ）に回答しています。

認証に関する問題

Q. ACS 5.x内部データベースの一部のユーザ/グループをユーザパスワードポリシー([System Administration] > [Users] > [Authentication Settings])から除外できますか。

A.デフォルトでは、すべての内部データベースユーザがユーザパスワードポリシーに準拠する必要があります。現時点では、ACS 5.x 内部データベースのユーザ、グループは除外できません。

Q. ACS 5.xの一部のGUI管理者を管理ユーザパスワードポリシー([System Administration] > [Administrators] > [Settings] > [Authentication])から除外できますか。

A.デフォルトでは、すべてのGUI管理ユーザが管理ユーザパスワードポリシーに準拠している必要があります。現時点では、ACS 5.x の管理ユーザは除外できません。

Q. ACS 5.xはVMWareツールをサポートしていますか。

A.いいえ。現在、VMWareツールはACSバージョン5.xではサポートされていません。詳細については、Cisco Bug ID CSCtg50048（登録ユーザ専用）を参照してください。

Q. LDAPがIDストアとして設定されている場合、ACS 5.xでサポートされるEAP認証プロトコルは何ですか。

A. LDAPをアイデンティティストアとして使用する場合、ACS 5.2はPEAP-GTC、EAP-FAST-GTC、およびEAP-TLSプロトコルのみをサポートします。EAP-FAST MSCHAPv2、PEAP EAP-MSCHAPv2、およびEAP-MD5はサポートされていません。詳細については、『認証プロトコルとユーザデータベースの互換性』を参照してください。

Q. ACSでradiusを使用するWLCの認証が失敗したのはなぜですか。また、失敗した試行がACSに表示されないのはなぜですか。

A.パッチ4の前にACS 5.0とWLCの相互運用性に問題があります。パッチ8をダウンロードし、CLIにパッチを適用してください。この問題を修正するために TFTP を使用しないでください。

Q. ACS 5.2でbackup-logコマンドを使用してバックアップされたtar.gzファイルを復元できないのはなぜですか。

A. backup-logコマンドでバックアップされたログファイルは復元**でき**ません。復元できるのは ACS 設定と ADE-OS のバックアップ ファイルだけです。詳細については、Cisco Secure Access Control System 5.1 の CLI リファレンス ガイドの backup **および backup-logs コマンドを参照してください。**

Q. ACS 5.2で失敗したパスワードの試行回数を制限できますか。

A.いいえ。この機能はACS 5.2では使用できませんが、ACS 5.3で統合される予定です。詳細については、『Cisco Secure Access Control System 5.2リリースノート』の「サポートされない機能」セクションを参照してください。

Q. ACS 5.0の内部ユーザの次回ログイン時にパスワードを変更するオプションを使用できません。この問題を解決するにはどうすればよいのですか。

A. ACS 5.0では、次回ログイン時にパスワードを変更するオプションはサポートされていません。この機能のサポートは、ACS 5.1以降のバージョンで利用可能です。

Q. ACSのこのアラームは何を意味しますか。

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

A.このエラーは、ACS Viewが250,000セッションの制限に達すると、20,000セッションを削除するアラームをスローすることを意味します。ACS View データベースはそれまでの認証セッションをすべて保存しており、セッション数が 250,000 に到達すると、キャッシュをクリアして 20,000 セッションを削除するよう促すアラームが発生します。

Q.次のエラーメッセージを解決するにはどうすればよいのですか。`Authentication failed:24407 User authentication against Active Directory failed since user is required to change his password?`

A.このエラーメッセージは、SDI認証中にパスワード管理に問題がある場合に表示されます。ACS 5.x を RADIUS プロキシとして使用し、ユーザを RSA サーバで認証する必要があります。RSA への RADIUS プロキシは、パスワードを管理しない場合にだけ機能します。パスワードの値を RSA サーバにプロキシするために、RADIUS サーバが OTP 値を復元できる必要があるためです。パスワード管理がトンネル グループで有効になっていると RADIUS 要求が MS-CHAPv2 属性で送信されます。RSA は MS-0CHAPv2 をサポートしていません。サポートしているのは PAP のみです。

この問題を解決するには、パスワード管理を無効にします。詳細については、Cisco Bug ID

CSCsx47423（登録ユーザ専用）を参照してください。

Q. ACS 5.1内の特定のデバイスだけを管理するようにACS管理者を制限することはできますか。

A.いいえ。ACS 5.1内の特定のデバイスだけを管理するようにACS管理者を制限することはできません。

Q. ACSは、RADIUSをTACACSよりも優先できるように、認証でQoSをサポートしていますか。

A.いいえ。ACSは認証でQoSをサポートしていません。ACS では TACACS より RADIUS 認証要求を優先させることも、RADIUS より TACACS 要求を優先させることもありません。

Q. ACS 5.xは他のTACACSまたはRADIUSサーバにTACACSおよびRADIUS認証をプロキシできますか。

A.あります。すべてのACS 5.xバージョンで、RADIUS認証を他のRADIUSサーバにプロキシできます。ACS 5.3 以降では、TACACS 認証を他の TACACS サーバにプロキシできます。

Q. ACS 5.xは、Active Directoryユーザのダイヤルイン属性をチェックしてアクセスを許可できますか。

A.はい。ACS 5.3以降では、ユーザのダイヤルイン権限のアクセスを許可、拒否、および制御できます。ダイヤルイン アクセス権は、認証中、または Active Directory からのクエリでチェックされます。これは Active Directory 専用のディクショナリに設定されます。

Q. ACS 5.xでは、TACACS+?のCHAPまたはMSCHAP認証タイプがサポートされていますか。

A.あります。TACACS+ CHAPおよびMSCHAP認証タイプは、ACSバージョン5.3以降でサポートされています。

Q. ACS内部ユーザのパスワードタイプを外部データベースに設定できますか。

A.はい。ACS 5.3以降では、ACS内部ユーザのパスワードタイプを設定できます。この機能は ACS 4.x で使用できました。

Q. ACS内部IDストアでユーザが作成された時刻に基づいて認証を通過/失敗できますか。

A.はい。ACS 5.3以降では、[Number of Hours **Since User Creation]属性を使用してポリシーを作成**できます。この属性には、ユーザが内部 ID ストア内で作成されてから、現在の認証要求までの時間数が含まれます。

Q. ACS内部データベースに新しいホストエントリを追加するためにワイルドカードを使用できますか。

A.はい。ACS 5.3以降では、内部IDストアに新しいホストを追加するときにワイルドカードを使用できます。また、製造元が特定されたすべてのデバイスを指定するため、最初の 3 オクテットの後にワイルドカードを入力できるようになっています。

Q. ACS 5.xでIPアドレスプールを設定し、ACSから割り当てることはできますか。

A.いいえ。現在、ACS 5.xでIPアドレスプールを作成することはできません。

Q. FAILED AUTHENTICATIONレポートで要求が発生したAAAクライアントのIPアドレスを確認できますか。

A.いいえ。要求の送信元であるAAAクライアントのIPアドレスを確認することはできません。

Q. ACS 5.3のView Log Message Recoveryとは何ですか。

A. ACS 5.3には、ビューがダウンしたときに失われたログを回復する新機能が搭載されています。ACS は失われたログを収集し、データベース内に保存します。この機能を使用すると、失われたログを ACS データベースから取得して、ビューが稼動を再開した後にビュー データベースに戻すことができます。この機能を使用するには、Log Message Recovery Configuration を **on** に設定する必要があります。View Log Message Recovery の設定の詳細については、モニタリング、レポート ビューア システムの運用を参照してください。

Q. Solution Engine CLIからdatabase-compressコマンドを発行してACS 5.xデータベースを圧縮することはできますか。この機能は ACS 4.x で使用できました。

A.はい。ACS 5.3以降では、**database-compressコマンドでACSトランザクションテーブルを削除するオプションを使用してACSデータベースのサイズを縮小できます。ACS管理者は、このコマンドを発行してデータベースのサイズを縮小できます。**このコマンドは、データベース サイズを削減し、保守に必要なバックアップや完全同期にかかる時間を短縮するのに役立ちます。

Q. IPアドレスに基づいてAAAクライアントエントリを検索できますか。

A.はい、ACS 5.3以降では、IPアドレスを使用してネットワークデバイスを検索できます。また、特定のネットワーク デバイスのセットを検索するためにワイルドカードや範囲指定を使用することも可能です。

Q. ACS内部IDストアでユーザが作成された時刻に基づいて条件を作成できますか。

A.はい。ACS 5.3以降では、[Number of Hours Since User Creation]属性を使用できます。この属性を使用すると、ACS内部IDストアでユーザが作成された時刻に基づいてポリシールール条件を設定できます。以下に、いくつかの例を示します。IF **group=HelpDesk&NumberofHoursSinceUserCreation>48 then reject.**この属性には、ユーザが内部 ID ストアで作成されてから、現在の認証要求までの時間数が含まれます。

Q.サービスポリシーの[Authorization]セクションでユーザが認証されたIDストアを確認できますか。

A. Yes, in ACS 5.3以降では**Authentication Identity Store属性を使用できます。**これにより、認証

IDストアに基づいてポリシールール条件を設定できます。以下に、いくつかの例を示します。IF **AuthenticationIdentityStore=LDAP_NY then reject.**この属性には使用される ID ストアの名前が含まれ、認証が成功した後に、関連する ID ストア名で更新されます。

Q. ACSがIDストアシーケンスで定義された次のIDストアに移動するのはいつですか。

A. ACSは、次のシナリオでIDストアシーケンスで定義されている次のIDストアに移動します。

- 最初の ID ストアでユーザが検出されない
- ID ストアがシーケンスで使用できない

Q. ACS 5.3のアカウント無効化ポリシーとは何ですか。

A. Account Disablement Policyを使用すると、設定した日付が許可された日付を超えている、設定した日数が許可された日数を超えている、または連続して失敗したログイン試行の数がしきい値を超えている場合に、内部IDストアをを無効できます。日付超過のデフォルト値は、現在の日付から 30 日です。日数のデフォルト値は現在の日付から 60 日以下です。失敗した回数のデフォルト値は 5 です。

Q. Telnet経由でACSの内部データベースユーザのパスワードを変更できますか。

A.はい。Telnet経由でTACACS+を使用して、内部データベースユーザのパスワードを変更できます。ACS 5.x で [Password Change Control] の [Enable TELNET Change Password] を選択する必要があります。

Q.プライマリACS 5.xインスタンスは定期的にバックアップインスタンスを自動的に更新しますか。それとも、設定が変更されたときにだけ更新されますか。

A. ACS 5.xは、プライマリACSで変更を行うと、ただちにセカンダリACSに複製されます。また、プライマリ ACS に変更がない場合、15 分ごとに強制的に複製します。現時点では、タイマーを制御して ACS が特定の時間の後に情報を複製できるようなオプションはありません。

Q.現在ログインしていて、異なるNASクライアントのACSから認証されているすべてのユーザのACS 5.xのレポートを表示/エクスポートできますか。

A.はい、可能です。RADIUS 用と TACACS+ 用の 2 つの別々のレポートがあります。[Monitoring & Reports] **> [Reports]** > [Catalog] **> [Session Directory] の [RADIUS Active Sessions] および [TACACS Active Sessions]** で確認できます。いずれのレポートも NAS クライアントからのアカウンティング情報に基づいており、ユーザがいつ接続し、ログアウトしたかをトラッキングできます。セッションの履歴を使用すると、最初から情報を取得し、特定の日にメッセージを停止することもできます。

関連情報

- Cisco Secure Access Control System のサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems