目次

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ユーザやグループの一部をパスワード ポリシーから除外することはできますか（[System Administration] > [Users] > [Authentication Settings]）。

A. 内部データベースの各ユーザは、ユーザ パスワード ポリシーにデフォルトで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 GUI 管理者の一部を管理ユーザ パスワード ポリシーから除外することはできますか（[System Administration] > [Administrators] > [Settings] > [Authentication]）。

A. 各 GUI 管理ユーザはデフォルトで管理ユーザ 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 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。 現時点では、VMWare ツールは ACS バージョン 5.x でサポートされていません。 詳細は、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 ID ストアとして使用する場合、ACS 5.2 がサポートするプロトコルは PEAP-GTC、EAP-FAST-GTC、EAP-TLS のみです。 EAP-FAST MSCHAPv2、PEAP EAP-MSCHAPv2、EAP-MD5 はサポートされません。 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. WLC での認証に ACS RADIUS を使用すると失敗するのはなぜですか。また、失敗したことが ACS に表示されないのはなぜですか。

A. パッチ 4 より前の **ACS 5.0 と WLC との相互運用性**に問題があります。パッチ 8 をダウンロー

ドし、CLI で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 の backup-log コマンドで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 ファイルを復元することはできません。 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 では、パスワード入力失敗の回数を制限できますか。

A. いいえ。 ACS 5.2 では使用できませんが、ACS 5.3 で機能の統合が予定されています。 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の項を参照してください。

Q. ACS 5.0 で、内部ユーザの次回ログイン時にパスワードを変更するというオプションが使用できません。 この問題を解決するにはどうすればよいですか。

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

Q. ACS のこのアラームはどういう意味ですか。

A. このエラーは、ACS View が制限の 250,000 セッションに達した場合に、ACS が 20,000 セッション削除するよう促すアラームです。 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で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 管理を制限することは可能ですか。

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 管理を制限することはでき

ません。

Q. ACS は、RADIUS を TACACS より優先させるために認証で QoS をサポートしますか。

A. いいえ、ACS は認証で QoS をサポートしません。 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 サーバに対して TACACS および RADIUS 認証をプロキシできますか。

A. はい、ACS 5.x バージョンはすべて 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 では、アクセス権を付与するために、Active Directory ユーザのダイヤルイン属性を確認できますか。

A. はい、ACS 5.3 以降では、ユーザのダイヤルイン アクセス権によるアクセスを許可、拒否、コントロールできます。 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 は、TACACS+ の CHAP または MSCHAP 認証タイプをサポートしますか。

A. はい、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 ストア内でユーザが作成された時間に基づいて認証を成功、または失敗させることができますか。

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規ホスト エントリを追加する際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 ストアに新規ホストを追加する際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 プールを設定して、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 レポートに、要求が送信された AAA クライアントの IP アドレスを表示することはできますか。

A. 要求が送信された AAA クライアントの IP アドレスを表示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 は、ビューがダウンしている場合に失われたログを復元する新しい機能を提供しています。 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 の 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 Transaction 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削減できます。ACS 管理者は、データベース サイズを削減するためにこのコマンドを発行できます。 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 アドレスで AAA クライアントの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 デバイスを検索することができます。 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 ストア内でユーザが作成された時間に基づいて条件を作成することができますか。

A. はい、ACS 5.3 以降で Number of Hours Since User Creation 属性を使用できます。この属性を使えば、ACS 内部 ID ストアでユーザが作成された時間に基づいてポリシー ルールの条件を設定できます。 次に、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、どの ID ストアでユーザが認証されたかを確認できますか。

A. はい、ACS 5.3 以降で Authentication Identity Store 属性を使用できます。この属性を使用して、認証 ID ストアに基づいたポリシー ルールの条件を設定できます。 次に、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 は、ID ストア シーケンスで定義されている次の ID ストアにいつ移動しま

すか。

A. ACS は、次の場合に 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 のアカウントの無効化ポリシーはどんなものですか。

A. アカウント無効化ポリシーを使用すると、次の場合に内部 ID ストアのユーザを無効にできます。設定された日付を超過した、設定された日数を超えた、連続してログインに失敗した回数がしきい値を超えた場合、です。 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. ACS の内部データベースのユーザのパスワードを telnet を使用して変更できますか。

A. はい、telnet から TACACS+ を使用して内部データベースの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 インスタンスはバックアップ インスタンスを一定の間隔で自動的に更新しますか、それとも設定が変更された場合だけですか。

A. ACS 5.x では、プライマリ ACS で変更を行うたびに即座にセカンダリ 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. ACS 5.x で、別の NAS クライアントの ACS に現在ログインし認証されたすべてのユーザのレポートを表示したり、エクスポートしたりすることはできますか。

A. はい、できます。 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