

ACS 5.x以降 : Secure ACSのトラブルシューティング

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[問題 : 「Error:Saved the running configuration to startup successfully % Manifest file not found in the bundle」が表示される \(アプライアンスのアップグレード中に ACS アプライアンスで\)](#)

[解決方法](#)

[問題 : ACS サーバ 5.x を GUI から再起動できない](#)

[解決方法](#)

[問題 : ACS 5.2 で Active Directory 認証の設定に問題がある](#)

[解決方法](#)

[問題 : アカウンティング レポートを 100 ページを超えて表示できない](#)

[解決方法](#)

[問題 : デバイスのグループについて合格または不合格の認証レポートを生成できない](#)

[解決方法](#)

[問題 : 「The monitoring and reports database is currently unavailable.Attempting to reconnect in 5 seconds.」](#)

[解決方法](#)

[問題 : 「22056 Subject not found in the applicable identity store\(s\)」](#)

[解決方法](#)

[問題 : ACS と Active Directory を統合できない](#)

[解決方法](#)

[問題 : ACS と LDAP を統合できない](#)

[解決方法](#)

[問題 : 「cisco acs internal operations diagnostics error:could not write to local storage file」エラーメッセージ](#)

[解決方法](#)

[問題 : ACS 5.1 と Active Directory を統合できない](#)

[解決方法](#)

[問題 : サービス セレクション ルールの正規表現を認識できるように ACS 5.x を構成できない](#)

[解決方法](#)

[問題 : Cisco Works を SFTP サーバとして使用しているとき SFTP バックアップが動作しない](#)

[解決方法](#)

[問題 : 「Invalid EAP payload dropped」](#)

[解決方法](#)

[問題：「ACS runtime process is not running on this instance at this time.」](#)

[解決方法](#)

[問題：パスワード付きでユーザをエクスポートできない](#)

[解決方法](#)

[問題：ACS 内部ユーザが断続的に無効になる](#)

[解決方法](#)

[問題：「TACACS+ authentication request ended with error」](#)

[解決方法](#)

[問題：「RADIUS authentication request rejected due to critical logging error」](#)

[解決方法](#)

[問題：ACS を 5.2 から 5.3 にアップグレードしたとき、ACS ビュー インターフェイスのページ上部に「Data Upgrade Failed」と表示される](#)

[解決方法](#)

[問題：Cisco ACS 5.0 の「change password on next login acs」に関する問題](#)

[解決方法](#)

[問題：「% Application upgrade failed, Error - -999. Please check ADE logs for details, or re-run with - debug application install - enabled」をチェックします。](#)

[解決方法](#)

[問題：エラー「Authentication failed:12308 Client sent Result TLV indicating failure」](#)

[解決方法](#)

[問題：エラー「24495 Active Directory servers are not available」](#)

[解決方法](#)

[問題：エラー「5411 EAP session timed out」](#)

[解決方法](#)

[問題：ログオン制限が Active Directory に設定された場合、802.1x 認証が機能しない](#)

[解決方法](#)

[問題：エラー:ChangeUserPassword ロールを持つ ACS 5.x 管理者がパスワードを変更すると「You are not authorized to view the requested page」と表示される](#)

[解決方法](#)

[問題：ACS 5.x で認証の失敗エラー「24495 Active Directory servers are not available.」が表示される](#)

[解決方法](#)

[問題：BMC を使用して ACS アプライアンスに接続できない](#)

[解決方法](#)

[問題：警告アラーム「delete 20000 sessions」が理由「active sessions are over limit」でモニタおよびレポート一般ダッシュボードに表示される](#)

[解決方法](#)

[問題：ACS 5.x エラー「11013 RADIUS packet already in the process」](#)

[解決方法](#)

[問題：RADIUS 認証がエラー「11012 RADIUS packet contains invalid header」で失敗する](#)

[解決方法](#)

[問題：RADIUS/TACACS+ 認証がエラー「11007 Could not locate Network Device or AAA Client」で失敗する](#)

[解決方法](#)

[問題：RADIUS 認証がエラー「11050 RADIUS request dropped due to system overload」で失敗する](#)

解決方法

問題：RADIUS 認証がエラー「11309 Incorrect RADIUS MS-CHAP v2 attribute.」で失敗する

解決方法

問題：ACS でメモリ使用量が 90 % を超えたことが報告されるアラーム

解決方法

問題：「error:com.cisco.nm.acs.mgmt.msgbus.FatalBusException:Failed to link nodes」

解決方法

問題：「error:com.cisco.nm.acs.mgmt.msgbus.FatalBusException:Failed to link nodes」

解決方法

問題：エラー「11026 The requested dACL is not found」

解決方法

問題：エラー「11025 The Access-Request for the requested dACL is missing a cisco-av-pair attribute with the value aaa:event=acl-download,The request is rejected」

解決方法

問題：エラー「11023 The requested dACL is not foundThis is an unknown dACL name」

解決方法

問題：管理者認証がエラー「10001 Internal error:Incorrect configuration version」で失敗する

解決方法

問題：管理者認証がエラー「10002 Internal error:Failure to load appropriate service」で失敗する

解決方法

問題：管理者認証がエラー「10003 Internal error:Administrator authentication received blank Administrator name」で失敗する

解決方法

問題：Failure reason:24428 Connection related error has occurred in either LRPC, LDAP or KERBEROS」

解決方法

問題：IOS 15.x を実行中のルータ上で、ACS 5.x サーバからの TACACS+ 認証プロキシ認証が機能しない

解決方法

問題：ACS 5.x から「Store failure (acs-xxx, TacacsAccounting)」エラーメッセージが表示される

解決方法

問題：ユーザ認証がエラー「11036 The Message-Authenticator RADIUS attribute is invalid.」で失敗する

解決方法

問題：RADIUS アカウンティングがエラー「11037 Dropped accounting request received via unsupported port.」で失敗する

解決方法

問題：RADIUS アカウンティングがエラー「11038 RADIUS Accounting-Request header contains invalid Authenticator field.」で失敗する

エラー：「24493 ACS has problems communicating with Active Directory using its machine credentials.」

解決方法

問題：「When creating Shell Profile names with special characters like "ê", ACS may crash.」

解決方法

問題：「show run」を ACS 5.x CLI で実行中に「Parse error at line 2:not well-formed (invalid token)」を受け取る。

[解決方法](#)

[問題：ACS 5.x /opt パーティションがすぐにいっぱいになる](#)

[解決方法](#)

[問題：目的のドメインの照会](#)

[解決方法](#)

[問題：親ドメインと子ドメインの同時設定](#)

[解決方法](#)

[問題：リモート データベースへのロギング](#)

[解決方法](#)

[問題：VMware サポート](#)

[解決方法](#)

[問題：ディスク スペースに関する要件](#)

[解決方法](#)

[問題：「24401 Could not establish connection with ACS Active Directory agent.」](#)

[解決方法](#)

[問題：「ランタイム」プロセスが「Execution Failed」状態を表示する](#)

[解決方法](#)

[問題：UCS が再認証を強制するときに ACS 認証に失敗する](#)

[解決方法](#)

[問題：「24444 Active Directory operation has failed because of an unspecified error in the ACS」](#)

[解決方法](#)

[問題：ACS 5.1 ユーザを AD 2008 R2 Server で認証できない](#)

[解決方法](#)

[エラー：「22056 Subject not found in the applicable identity store\(s\)」。](#)

[解決方法](#)

[問題：ipt_connlimit:Oops:Invalid ct state ?](#)

[解決方法](#)

[問題：ACs 5.x / ISE は Cisco IOS ソフトウェア リリース 15.x NAS からの RADIUS 要求の RADIUS calling-station-id 属性を表示できません](#)

[解決方法](#)

[問題：3 回の試行を設定していても、間違ったクレデンシャルの最初のインスタンスでユーザ アカウントがロックされる](#)

[解決方法](#)

[問題：ACS からのバックアップを保存できない](#)

[解決方法](#)

[関連情報](#)

[概要](#)

このドキュメントでは、Cisco Secure Access Control System (ACS) のトラブルシューティング方法およびエラー メッセージの解決方法について説明します。

Cisco Secure ACS 3.x および 4.x のトラブルシューティング方法については、「[Secure Access Control Server \(ACS 3.x and 4.x\) Troubleshooting](#)」を参照してください。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Secure Access Control System バージョン 5.x 以降に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

問題：「Error:Saved the running configuration to startup successfully % Manifest file not found in the bundle」が表示される（アプライアンスのアップグレード中に ACS アプライアンスで）

```
Error: Saved the running configuration to startup successfully % Manifest file not found in the bundleACS Express 5.0 5.0.1
```

解決方法

ACS アプライアンスを正常にアップグレードするには、次の手順を実行します。

1. 次の場所から、パッチ 9 ([5-0-0-21-9.tar.gpg](#)) および ADE-OS ([ACS_5.0.0.21_ADE_OS_1.2_upgrade.tar.gpg](#)) をダウンロードします。[Cisco.com] > [support] > [download software] > [Security] > [Cisco Secure Access Control System 5.0] > [Secure Access Control System Software] > [5.0.0.21]
2. 2 つのファイルをインストールしたら、ACS 5.1 アップグレード [ACS 5.1.0.44.tar.gz](#) をインストールします。これは、前述の手順の同じパスから使用できます。
3. 次のコマンドを使用して、アップグレードをインストールします。

[application upgrade](#)

これで、アップグレード手順は完了です。

ACS アプライアンスのアップグレード方法の詳細については、『[Upgrading an ACS Server from 5.0 to 5.1](#)』を参照してください。

問題：ACS サーバ 5.x を GUI から再起動できない

ここでは、ACS サーババージョン 5.x を GUI から再起動できない理由について説明します。

解決方法

ACS 5.x サーバを GUI から再起動するオプションはありません。ACS アドレスは、CLI からのみ再起動できます。

問題：ACS 5.2 で Active Directory 認証の設定に問題がある

Active Directory (AD) 認証を新しい 5.2 ACS サービスで設定すると、次のエラー メッセージが表示されます。

```
Unexpected RPC Error:Access Denied due to unexpected configuration or network error.Please try the --verbose option or run "adinfo --diag".
```

解決方法

ACS では、AD で認証を行う場合、書き込み許可が必要です。この問題を解決するには、サービスアカウントへの一時的な書き込み許可を提供します。

問題：アカウントング レポートを 100 ページを超えて表示できない

ACS バージョン 5.1 でカスタム AAA アカウンティング レポートを生成しようとする、100 ページを超えて表示できません。いくつかの古いレポートは含まれません。すべてのページを表示できるように、この設定を変更する必要があります。

解決方法

表示できる最大ページ数はデフォルトで 100 ページなので、ACS で表示されるページ数は変更できません。このページ数制限を増やし、古い統計情報を表示するには、フィルタリング オプションを変更して、一致条件を絞り込む必要があります。たとえば、最新の 30 日間のレポートを生成する場合、情報が多いため、最後の 100 ページには、最新の 1 時間のアクティビティだけしか含まれない場合があります。次に、フィルタリング オプションについて説明します。フィルタリング オプションにユーザ ID を使用し、時間範囲を指定することで、古いレポートも含まれるようになります。

問題：デバイスのグループについて合格または不合格の認証レポートを生成できない

この問題は、すべてのデバイスではなく、6 つのルータとスイッチのグループだけの認証レポートを生成しようとするときに発生します。使用している ACS バージョンは 4.x です。

解決方法

このレポート生成は、ACS 4.x では実行できません。この機能を使用するには、ACS 5.x に移行する必要があります。特定のデバイス グループのレポートを作成するには、[カタログ レポート](#)を

生成します。

詳細については、次の画像を参照してください。



問題：「The monitoring and reports database is currently unavailable. Attempting to reconnect in 5 seconds.」

[Launch Monitoring and Report Viewer from ACS 5.x] をクリックすると、このエラーメッセージが表示されます。The monitoring and reports database is currently unavailable. Attempting to reconnect in 5 seconds.ACS

解決方法

この問題を解決するには、次のいずれかの回避策を実行します。

- 次のコマンドを実行して、CLI から ACS サービスを再起動します。
application stop acs
application start acs
- 使用できる最新のパッチにアップグレードします。詳細については、『[Applying Upgrade Patches](#)』を参照してください。

問題：「22056 Subject not found in the applicable identity store(s)」

AD ユーザが ACS バージョン 5.x で認証できず、次のエラーメッセージが表示されます。22056 Subject not found in the applicable identity store(s)

解決方法

このエラーメッセージは、ID ストア シーケンスで設定される最初のデータベース リストで ACS

がユーザを検出できない場合に発生します。これは、情報メッセージで、ACSのパフォーマンスに影響はありません。内部または外部ユーザの認証方法は、ACS 5.x と 4.x よりも前のバージョンとは異なります。5.x バージョンでは、認証されるユーザ データベースのシーケンスを定義する ID ストア シーケンスと呼ばれるオプションがあります。詳細については、『[Configuring Identity Store Sequences](#)』を参照してください。

ACS を使用して Child ドメインに対する要求を認証するときこのエラーが発生する場合、UPN サフィクスまたは NETBIOS プレフィクスをユーザ名に追加する必要があります。詳細については、『[Microsoft AD」セクションの注意事項を参照してください。](#)』

問題 : ACS と Active Directory を統合できない

ユーザが ACS と Active Directory を統合できず、「Samba Port Status Error」エラー メッセージが表示されます。

解決方法

この問題を解決するには、次のポートが Active Directory 機能をサポートするようにオープンになっていることを確認します。

- Samba ポート - TCP 445
- LDAP - TCP 389
- LDAP - UDP 389
- KDC - TCP 88
- kpasswd - TCP 464
- NTP- UDP 123
- グローバル カタログ - TCP - 3268
- DNS - UDP 53

ACS-AD 統合を完了するには、ACS は、ドメインのすべての DC に到達できる必要があります。ACS から到達できない DC が 1 つあるだけでも、統合は行われません。詳細については、Cisco Bug ID [CSCte92062](#) ([登録ユーザ専用](#)) を参照してください。

問題 : ACS と LDAP を統合できない

このドキュメントでは、ACS 5.2 は、802.1X 実装の AAA RADIUS サーバとして使用されます。802.1X は、内部ユーザ ストアを使用する ACS で正常に使用できますが、ACS と LDAP の統合問題が発生します。次のエラー メッセージが表示されます。

```
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
```

解決方法

この例では、LDAPはPEAPで使用され、使用される内部認証方式はeap-mschap v2です。LDAPはPEAP(eap-mschap v2)でサポートされていないため、これは失敗します。eap-tls または AD を使用することを推奨します。

問題 : 「cisco acs internal operations diagnostics error:could

not write to local storage file」エラー メッセージ

ACS 複製中、プライマリ ACS が正しく複製を行わず、次のエラー メッセージが表示されます。

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

解決方法

ACS サービスを再起動して、重要なログが無効にされているか確認します。詳細については、Cisco Bug ID [CSCth66302](#) ([登録ユーザ専用](#)) を参照してください。表示されていない場合、[Cisco TAC](#) に問い合わせ、この問題を解決するための最新の ACS パッチを取得してください。

問題 : ACS 5.1 と Active Directory を統合できない

AD 統合を実装しようとする、次のエラー メッセージが表示されます。

```
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
-dia' to diagnose the problem. Join to domain 'test.pvt', zone 'null'
failed.
```

解決方法

この問題を解決するには、次の回避策を実行します。

1. AD で既存のマシン アカウントを削除します。
2. 新規 OU を作成します。
3. OU の [Properties] に移動し、[inherit permissions] チェックボックスをオフにします。
4. 新しい OU で ACS の新しいマシン アカウントを作成します。
5. AD の複製を許可します。
6. ACS GUI から AD に接続します。

場合によっては、Microsoft に問い合わせ、[ホットフィックス](#) を適用してください。

問題 : サービス セレクション ルールの正規表現を認識できるように ACS 5.x を構成できない

解決方法

ACS 5.x ではまだサポートされていないので、これは実行できません。

問題 : Cisco Works を SFTP サーバとして使用しているとき SFTP バックアップが動作しない

ネットワークリソースがCiscoWorksサーバにある場合、バックアップスケジューラは他のSFTPクライアントでは正常に動作しますが、ACS 5.2では動作しません。具体的には、ACSから

SFTPサーバに接続しようとする時、「Unable to negotiate a key exchange method」エラーメッセージが表示されます。

解決方法

この場合、SFTP サーバは、DH 14 グループを使用する FIPS 対応デバイスではありません。ACS でサポートされるサーバは、DH 14 をサポートする FIPS 対応のサーバだけです。この問題の詳細については、『[Known Limitations in ACS 5.2](#)』を参照してください。

問題：「Invalid EAP payload dropped」

Error: Invalid EAP payload dropped ACS 5.0 7

解決方法

これは予期された動作で、Cisco Bug ID [CSCsz54975](#) ([登録ユーザ専用](#)) および [CSCsy46036](#) ([登録ユーザ専用](#)) で対応されます。

この問題を解決するには、ACS 5.0パッチ9にアップグレードします。このパッチは5.1または5.2へのアップグレードの一部として必要です。詳細については、「[データベースのアップグレード](#)」を参照してください。また、パッチ9へのアップグレード方法について説明しています。

問題：「ACS runtime process is not running on this instance at this time.」

ユーザが ACS GUI にログインできず、次のエラーメッセージが表示されます。

The ACS runtime process is not running on this instance at this time.Changes can be made to the ACS configuration (these will be saved in the database), but changes will not take effect until the runtime process is restarted.

解決方法

この問題を解決するには、CLI からランタイム プロセスを手動で再起動して、アプライアンスを再起動します。これは小さな問題で、ACS のパフォーマンスには影響はありません。この動作に関しては2つのマイナーバグが報告されています。詳細については、Cisco Bug ID [CSCtb99448](#) ([登録ユーザ専用](#)) および [CSCtc75323](#) ([登録ユーザ専用](#)) を参照してください。

ランタイム プロセスを手動で再起動するには、ACS CLI から次のコマンドを実行します。

- `acs stop runtime`
- `acs start runtime`

問題：パスワード付きでユーザをエクスポートできない

CSV ファイルでユーザ データベースを別の ACS 5.x にエクスポートおよびインポートできますが、ユーザ パスワード フィールドは含まれません (空白になります)。パスワードを含むローカルユーザの ID ストアを ACS 間で移動するにはどのようにすればよいのですか。

解決方法

これは、セキュリティ違反になるため実行できません。この場合の回避策としては、バックアップを実行して、復元します。ただし、バックアップと復元を別の ACS で実行できるのは、設定が同様な場合だけです。

問題 : ACS 内部ユーザが断続的に無効になる

ACS ユーザが断続的に無効になり、「Password expired」メッセージが表示されます。パスワード失効ポリシーは 60 日間に設定されていますが、これらのユーザは、アクセスを取得するために手動で有効にする必要があります。

解決方法

これは予期された動作で、Cisco Bug ID [CSCtf06311](#) ([登録ユーザ専用](#)) に記載されています。この問題は、パッチ3をACS 5.1に適用することで解決できます。パッチ3で解決されたすべての問題を表示するには、『[Resolved Issues in Cumulative Patch ACS 5.1.0.44.3](#)』を参照してください。パッチのアップグレード方法に関する[情報](#)。

問題 : 「TACACS+ authentication request ended with error」

ACS 認証レポートに「TACACS+ authentication request ended with error」エラー メッセージが表示されます。

解決方法

これは、TACACS 認証のサービス タイプが PPP に設定されている場合に発生します。詳細については、Cisco Bug ID [CSCte16911](#) ([登録ユーザ専用](#)) を参照してください。

問題 : 「RADIUS authentication request rejected due to critical logging error」

RADIUS 認証が拒否され、「Radius Authentication Request Rejected due to critical logging error」エラー メッセージが表示されます。

解決方法

このエラーは Cisco Bug ID [CSCth66302](#) ([登録ユーザ専用](#)) で詳しく説明されています。

問題 : ACS を 5.2 から 5.3 にアップグレードしたとき、ACS ビュー インターフェイスのページ上部に「Data Upgrade Failed」と表示される

ACS を 5.2 から 5.3 にアップグレードしたとき、ACS ビュー インターフェイスのページ上部に「Data Upgrade Failed」と表示されます。

解決方法

このエラーは Cisco Bug ID [CSCtu15651](#) ([登録ユーザ専用](#)) で詳しく説明されています。

問題 : Cisco ACS 5.0 の「change password on next login acs」に関する問題

解決方法

ACS 5.0 で、ローカル ユーザ ID ストアのパスワード失効機能 (ユーザは次のログイン時にパスワードを変更する必要があります) を選択できますが、機能しません。拡張機能の要求 [CSCtc31598](#) により、ACS バージョン 5.1 でのこの問題は解決されます。

問題 : 「% Application upgrade failed, Error - -999. Please check ADE logs for details, or re-run with - debug application install - enabled」をチェックします。

% Application upgrade failed, Error - -999. Please check ADE logs for details, or re-run with - debug application install - enabledは、ACS Expressを5.0から5.0.1にアップグレードしようとすると表示されます。

解決方法

このエラーは、使用するリポジトリが TFTP で、ファイル サイズが 32 MB を超える場合に発生します。ACS Express は、32 MB を超えるファイルを処理できません。ファイル サイズが 32 MB を超える場合でもこの問題を解決するには、リポジトリとして FTP を使用します。

問題 : エラー「Authentication failed:12308 Client sent Result TLV indicating failure」

「Authentication failed: 12308 Client sent Result TLV indicating failure ACS 2 回目の認証は正常に機能します。

解決方法

このエラーは、[Fast Reconnect] を無効にすることで解決できます。ACS バージョン 5.2 のパッチ 2 にアップグレードすることで、[Fast Reconnect] を無効にせずにこの問題を解決できます。

このエラーは、サブリカントで [Forced cryptobinding] を無効にしても解決できます。詳細については、Cisco Bug ID [CSCtj31281](#) ([登録ユーザ専用](#)) を参照してください。

問題 : エラー「24495 Active Directory servers are not available」

認証が失敗し、「24495 Active Directory servers are not available.」エラーが ACS 5.3 ログに記

録されます。

解決方法

ACS 5.x の CLI で ACSADAgent.log ファイルを参照し、次のようなメッセージがないか確認します。「Mar 11 00:06:06 xlpacs01 adclient[30401]: INFO <bg:bindingRefresh> base.bind.healing Lost connection to xxxxxxxx.Running in disconnected mode:unlatch」
「Running in disconnected mode: unlatch ACS 5.3 Active Directory」
解決策として、LDAP に切り替えるか、ACS を 5.2 バージョンにダウングレードします。詳細については、Cisco Bug ID [CSCtx71254](#) ([登録ユーザ専用](#)) を参照してください。

問題：エラー「5411 EAP session timed out」

5411 EAP session timed out ACS 5.x

解決方法

EAP セッション タイムアウトは、最初のパケットが RADIUS サーバから送信された後でサブリカントが認証を再開する PEAP で一般的ですが、ほとんどの場合、問題の兆候ではありません。

通常のフローは次のとおりです。

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

最終的に認証は成功します。ただし、サブリカントから EAP セッションが突然再起動されるため、ACS で問題が残ります。これにより、認証が成功した後で EAP セッション タイムアウト メッセージが表示されます。これは、マシンのドライバレベルの問題であることが多いです。NIC/ワイヤレスドライバがクライアント マシンで最新であるか確認します。クライアントでキャプチャし、EAP || EAPOLを使用して、クライアントが接続時に送受信する内容を確認します。

問題：ログオン制限が Active Directory に設定された場合、802.1x 認証が機能しない

ログオン制限が Active Directory に設定された場合、802.1x 認証が機能しません。

解決方法

ログオン制限が Active Directory でシングル マシンに設定されている場合、802.1x を認証しようとすると、認証は失敗します。これは、ログオン制限が設定されるマシンではなく、ACS から認証される Active Directory で失敗します。認証を正常に行うには、ACS マシン アカウントを含めるようにログオン制限を設定します。

問題：エラー:ChangeUserPassword ロールを持つ ACS 5.x 管理

者がパスワードを変更すると「You are not authorized to view the requested page」と表示される

ChangeUserPassword ロールを持つ ACS 5.x GUI admin ユーザが、内部データベースに保存されている AAA ユーザのパスワードを変更できません。パスワードの変更後、ユーザに次のエラーメッセージが表示されます。You are not authorized to view the requested page

解決方法

これは、ACS 5.x データベースを ACS 4.x から移行するときに発生します。ユーザパスワードを変更するには、SuperAdmin 特権を使用します。詳細については、Cisco Bug ID [CSCty91045](#) (登録ユーザ専用) を参照してください。

問題：ACS 5.x で認証の失敗エラー「24495 Active Directory servers are not available.」が表示される

解決方法

Active Directory と ACS 5.x との統合を確認する必要があります。分散設定の場合、設定のプライマリおよびセカンダリの両方の ACS 5.x が Active Directory と正しく統合されているか確認します。

問題：BMC を使用して ACS アプライアンスに接続できない

BMC クライアント (ハードウェア レベル ツール) が ACS 1121 IBM サーバとのアクセスに使用される場合、BMC クライアントの IP アドレスが 2 つあることが確認されます。

解決方法

この動作は確認済みで、Cisco Bug ID [CSCtj81255](#) (登録ユーザ専用) に記載されています。この問題を解決するには、ACS 1121 の BMC DHCP クライアントを無効にする必要があります。

問題：警告アラーム「delete 20000 sessions」が理由「active sessions are over limit」でモニタおよびレポート一般ダッシュボードに表示される

セッション ディレクトリが保持できるレコード数には制限があります。ユーザの設定でプロンプト要求が頻繁にある場合、すぐに制限に到達します。制限に到達すると、設計上では、ACS-View はセッション ディレクトリから一定数のレコード (たとえば、20K) を削除し、アラートを送信します。この制限を増やすことができますが、アラートが長くなるので、あまり推奨しません。

解決方法

この問題を解決するには、次の手順を実行します。

- ログを無効にして、データベースを表示することを推奨します。[Cisco Secure ACS] > [System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] > [Global] > ["Passed Authentications"] > [Remote Syslog Target] に移動して、[Selected Targets] から [LogCollector] を削除します。[Cisco Secure ACS] > [System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] > [Global] > ["Failed Attempts"] > [Remote Syslog Target] に移動して、[Selected Targets] から [LogCollector] を削除します。[Cisco Secure ACS] > [System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] > [Global] > [Edit: "RADIUS Accounting"] > [Remote Syslog Target] に移動して、[Selected Targets] から [LogCollector] を削除します。
- プローブ認証要求は、実際の認証要求ではないので、これは無視できます。次の作業を実行してください。[Cisco Secure ACS] > [Monitoring Configuration] > [System Configuration] > [Add Filter] に移動して、フィルタを作成します。プローブ要求はダミーユーザ名で送信されると見なされるので、ユーザ名に基づいたフィルタを作成することが適しています。ACSで個別のアクセスポリシーを作成して、これらのプローブ要求を処理する場合、アクセスサーバに基づいてフィルタを作成できます。

問題 : ACS 5.x エラー「11013 RADIUS packet already in the process」

ACS 5.3 導入で、ユーザの dot1x 認証が失敗します。使用されるデータベースは Active Directory です。次の RADIUS 障害コードが表示されます。

```
RADIUS Request dropped: 11013 RADIUS packet already in the process
```

解決方法

この要求は、現在処理中の別のパケットの複製なので、ACS で無視されます。これは、次のいずれかの場合に発生します。

- Average RADIUS Request Latency 統計情報が、クライアントのクライアント RADIUS 要求タイムアウトに近いか、これを超過している。
- 外部 ID ストアが非常に遅い。
- ACS に過負荷が発生している。

この問題を解決するには、次の手順を実行します。

1. クライアントのクライアント RADIUS 要求タイムアウトを増やします。
2. 高速または追加の外部 ID ストアを使用します。
3. ACS で過負荷を削減します。

問題 : RADIUS 認証がエラー「11012 RADIUS packet contains invalid header」で失敗する

解決方法

着信 RADIUS パケットのヘッダーが正しく解析されていません。これを解決するには、次のことを確認します。

- ネットワーク デバイスまたは AAA クライアントにハードウェア問題が発生していないか確認します。
- デバイスを ACS に接続するネットワークでハードウェア問題がないか確認します。
- ネットワーク デバイスまたは AAA クライアントで既知の RADIUS 互換性問題が発生していないか確認します。

問題 : RADIUS/TACACS+ 認証がエラー「11007 Could not locate Network Device or AAA Client」で失敗する

ASA が RADIUS アクセス要求メッセージを送信するときに、次のエラー メッセージが ACS で表示されます。

```
11007 Could not locate Network Device or AAA Client
```

解決方法

これは、ACS クライアントの IP と実際に要求を送信するインターフェイス IP が一致していないため発生します。ファイアウォールにより、この AAA クライアントへのアドレス変換が実行されることがあります。次のパスで正しく変換された IP アドレスで AAA クライアントが正しく設定されていることを確認します。

[Network Resources] > [Network Devices and AAA Clients]

問題 : RADIUS 認証がエラー「11050 RADIUS request dropped due to system overload」で失敗する

ユーザは、認証障害のためにネットワークにアクセスできません。ACS から次のエラー メッセージが表示されます。

```
11050 RADIUS request dropped due to system overload
```

解決方法

Cisco ACS は、過負荷のため、これらの認証要求をドロップします。これは、多くのパラレル認証要求の複製により発生します。この問題を回避するには、次のいずれかの手順を実行します。

- [Legacy TACACS+ Single Connection Support] オプションを使用するように、[Network Device/AAA Client] 設定を変更します。この場合、クライアントは、多くのセッションを作成せずに、すべての要求で同じセッションを再利用します。
- 一定期間、ユーザが新しい認証要求をできないようにします。
- ACS サーバを再起動します。

問題 : RADIUS 認証がエラー「11309 Incorrect RADIUS MS-CHAP v2 attribute。」で失敗する

解決方法

このエラーは、受信した RADIUS アクセス要求パケットのいずれかの MSCHAP v2 属性 (MS-CHAP-Challenge、MS-CHAP-Response、MS-CHAP-CPW-2 または MS-CHAP-NT-Enc-PW) で長さが無効か、値が不正なため発生します。

問題 : ACS でメモリ使用量が 90 % を超えたことが報告されるアラーム

ACS により、次のようなメモリ使用量が 90 % を超えたことを報告するアラームが表示されます

```
o Cisco Secure ACS - Alarm NotificationSeverity: Critical Alarm Name ACS - System
HealthCause/Trigger Alarm caused by ACS - System Health thresholdAlarm Details ACS Instance CPU
Utilization (%) Memory Utilization (%) Disk I/O Utilization (%) Disk Space Used /opt (%) Disk
Space Used /localdisk:(%) Disk Space Used / (%) KOM-AAA02 0.41 90.14 0.02 9.57 5.21 25.51
```

解決方法

この問題は通常、ACS 5.2で発生します。この問題を解決するには、ACSをリロードしてメモリを解放するか、ACS 5.2パッチ7以降にアップグレードします。詳細については、Cisco Bug ID [CSCtk52607](#) ([登録ユーザ専用](#)) を参照してください。

問題 : 「error:com.cisco.nm.acs.mgmt.msgbus.FatalBusException:Failed to link nodes」

メンテナンス タスク後の分散設定で (プライマリへの参加、完全な複製の強制実行、パッチ適用)、ACS インスタンス A は ACS インスタンス B を分散導入画面でオフラインと報告するが、B は実際はオンラインでインスタンス A をオンラインと報告します。管理ログで、「
error:com.cisco.nm.acs.mgmt.msgbus.FatalBusException: Failed to link nodes

解決方法

これは、新しいインスタンスがアップし、ポート 2030 にバインドしようとしたときに、複製管理サービスの以前のインスタンスがそのポートにまだバインドされている場合に発生します。ACS インスタンス B の CLI から、run:sho acs-logs ファイル ACSManagement.log | i。次のようなメッセージが示されます。「Replication service failed.:Port already in use: 2030.」。現在の回避策としては、ACS インスタンス B (他方をオンラインとして報告するインスタンス) を再起動することです。詳細については、Cisco Bug ID [CSCtx56129](#) ([登録ユーザ専用](#)) を参照してください。

問題 : 「error:com.cisco.nm.acs.mgmt.msgbus.FatalBusException:Failed to link nodes」

メンテナンス タスク後の分散設定で (プライマリへの参加、完全な複製の強制実行、パッチ適用)、ACS インスタンス A は ACS インスタンス B を分散導入画面でオフラインと報告するが、B は実際はオンラインでインスタンス A をオンラインと報告します。管理ログで、「
error:com.cisco.nm.acs.mgmt.msgbus.FatalBusException: Failed to link nodes

解決方法

ACS 5.2 パッチ 6 以降にアップグレードして、この問題を解決します。詳細については、Cisco Bug ID [CSCto47203](#) ([登録ユーザ専用](#)) を参照してください。

注: "/opt"の使用率が30%を超えると、viewDBのバックアップは失敗します。"/opt"使用率が30%を超えたらバックアップを実行するように NFS ステージングを設定する必要があります。

問題: エラー「11026 The requested dACL is not found」

次のエラーメッセージが表示されて、RADIUS 認証が失敗します。11026 The requested dACL is not found

解決方法

RADIUS アクセス要求で要求されるダウンロード可能な ACL のバージョンが見つからないため、要求は拒否されます。ダウンロード可能な ACL の要求は、元のアクセス要求の後で発生しました。このため、ダウンロード可能な ACL のバージョンを使用できませんでした。RADIUS クライアントからダウンロード可能な ACL の要求でこの遅延の理由を探します。

問題: エラー「11025 The Access-Request for the requested dACL is missing a cisco-av-pair attribute with the value aaa:event=acl-download,The request is rejected」

次のエラーメッセージが表示されて、RADIUS 認証が失敗します。11025 The Access-Request for the requested dACL is missing a cisco-av-pair attribute with the value aaa:event=acl-download.The request is rejected

解決方法

ダウンロード可能な ACL のすべてのアクセス要求には、値 aaa:event=acl-download の cisco-av-pair attribute があります。この場合、この属性には要求が欠落していて、ACS は要求を失敗します。ネットワーク デバイスまたは AAA クライアントで既知の RADIUS 互換性問題が発生していないか確認します。

問題: エラー「11023 The requested dACL is not foundThis is an unknown dACL name」

次のエラーメッセージが表示されて、RADIUS 認証が失敗します。11023 The requested dACL is not found.This is an unknown dACL name

解決方法

許可プロファイルで指定されたダウンロード可能な ACL が、ダウンロード可能 ACL のリストに存在するか、ACS 設定を確認します。これは、ACS 側の設定問題です。

問題: 管理者認証がエラー「10001 Internal error:Incorrect

configuration version」で失敗する

管理者認証が次のエラーで失敗します。10001 Internal error: Incorrect configuration version

解決方法

このエラーは、ACS データベースが壊れている、または基礎となる設定データの問題により発生します。詳細については、[Cisco TAC](#) ([登録ユーザ専用](#)) を参照してください。

問題：管理者認証がエラー「10002 Internal error:Failure to load appropriate service」で失敗する

管理者認証が次のエラーで失敗します。10002 Internal error: Failure to load appropriate service

解決方法

ACS 5.x は、AAC 設定サービスをロードできません。このエラーは、ACS データベースが壊れている、または基礎となる設定データの問題により発生します。また、システム リソースが不足している場合でも発生します。詳細については、[Cisco TAC](#) ([登録ユーザ専用](#)) を参照してください。

問題：管理者認証がエラー「10003 Internal error:Administrator authentication received blank Administrator name」で失敗する

管理者認証が次のエラーで失敗します。10003 Internal error:Administrator authentication received blank Administrator name

解決方法

ACS 5.x の GUI にアクセスすると、ACS は空のユーザ名を受け取ります。ACS に転送されるユーザ名の有効性を確認してください。有効な場合、[Cisco TAC](#) ([登録ユーザ専用](#)) で詳細について問い合わせてください。

問題：Failure reason:24428 Connection related error has occurred in either LRPC, LDAP or KERBEROS」

次のエラー メッセージが ACS で受信されます。

Failure reason:24428 Connection related error has occurred in either LRPC, LDAP or KERBEROS This RPC connection problem may be because the stub received incorrect data

解決方法

この問題を解決するには、ACS をバージョン 5.2 にアップグレードしてください。

問題：IOS 15.x を実行中のルータ上で、ACS 5.x サーバからの TACACS+ 認証プロキシ認証が機能しない

TACACS+ Auth-Proxy 認証が、ACS 5.x サーバから Cisco IOS ソフトウェア リリース 15.x を実行するルータ上で機能しません。

解決方法

TACACS+ Auth-Proxy は ACS 5.3 パッチ 5 以降のみでサポートされます。ACS 5.x をアップグレードするか、Auth-Proxy RADIUS を使用します。

問題：ACS 5.x から「Store failure (acs-xxx, TacacsAccounting)」エラーメッセージが表示される

解決方法

ACS 5.1 TACACS アカウンティング レポートで、不正なアカウンティング パケットをクライアントから受信するときに、ユーザ名、特権レベルおよび要求タイプなどのいくつかの属性が欠落します。この場合、ビューで「Store failure (acs-xxx, TacacsAccounting)」アラームが生成されます。これを解決するには、次のことを確認します。

- クライアントにより送信されるアカウンティング パケットの TACACS 引数が不正です（たとえば、AAA クライアントにより送信される引数の長さおよび値が一致しません）。
- クライアントが引数の長さおよび値が正しい有効なアカウンティング パケットを送信していることを確認します。

詳細については、Cisco Bug ID [CSCte88357](#) ([登録ユーザ専用](#)) を参照してください。

問題：ユーザ認証がエラー「11036 The Message-Authenticator RADIUS attribute is invalid.」で失敗する

解決方法

次の項目を確認してください。

- AAA クライアントと ACS サーバの共有秘密が一致している。
- AAA クライアントとネットワーク デバイスでハードウェア問題または RADIUS 互換性問題がない。
- デバイスと ACS を接続するネットワークにハードウェア問題がない。

問題：RADIUS アカウンティングがエラー「11037 Dropped accounting request received via unsupported port.」で失敗する

解決方法

サポートされていない UDP ポート番号を介して受信されたため、アカウンティング要求はドロ

アップされます。次の項目を確認してください。

- AAA クライアントおよび ACS サーバのアカウントング ポート番号設定が一致する。
- AAA クライアントにハードウェア問題または RADIUS 互換性問題がない。

問題：RADIUS アカウンティングがエラー「11038 RADIUS Accounting-Request header contains invalid Authenticator field.」で失敗する

ACS が RADIUS アカウンティング要求パケットのヘッダーの Authenticator フィールドを検証できません。Authenticator フィールドは Message-Authenticator RADIUS 属性と混合しないでください。AAA クライアントで設定される RADIUS 共有秘密が、選択された ACS サーバのネットワーク デバイスの共有秘密と一致することを確認します。また、AAA クライアントにハードウェア問題または RADIUS 互換性問題がないことも確認します。

エラー:「24493 ACS has problems communicating with Active Directory using its machine credentials.」

解決方法

ACS で AD 接続を確認し、ACS マシン アカウントが AD に存在するか確認します。

問題：「When creating Shell Profile names with special characters like "ê", ACS may crash.」

解決方法

この動作は確認済みで、Cisco Bug ID [CSCts17763](#) ([登録ユーザ専用](#)) に記載されています。5.3.40 パッチ 1 または 5.2.26 パッチ 7 にアップグレードする必要があります。

問題：「show run」を ACS 5.x CLI で実行中に「Parse error at line 2:not well-formed (invalid token)」を受け取る。

解決方法

ACS で設定されている SNMP コミュニティに有効な文字があることを確認します。コミュニティ名に使用できるのは英数字 (文字および数字) だけです。

問題：ACS 5.x /opt パーティションがすぐにいっぱいになる

解決方法

/opt パーティションの容量が不十分なため、ACS 5.x のディスク領域が不足しています。これは、ACS View のログ データが大量にあるため発生します。解決策として、View データベースを頻

繁に交換する必要があります。ACS View は GB 単位のデータに毎日対応できないので、ログデータを整理する必要があります。すべてのログが必要な場合、ACS View ではなく、外部 syslog サーバを使用します。ログデータの一部だけを使用する必要がある場合、[System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] > [Global] を使用して、必要なログだけを ACS View ログ コレクタに送信します。

問題：目的のドメインの照会

Active Directory ドメインに参加する場合、ACS 5.x は必要なドメイン コントローラ (DC) をクエリーできますか。

解決方法

いいえ。現在、ACSはドメインを使用してDNSを照会し、ドメイン内のすべてのDCのリストを取得します。次に、これらすべてとの通信を試行します。接続に失敗した DC が 1 つでもあると、そのドメインとの ACS 接続は失敗します。

問題：親ドメインと子ドメインの同時設定

親子両方のドメインで同時に ACS 5.x を設定する方法はありますか。

解決方法

いいえ。現在、ACS 5.xは1つのドメインにのみ含めることができます。ただし、ACS 5.x は、複数の信頼できるドメインのユーザまたはマシンを認証できます。

問題：リモート データベースへのロギング

ACS 5.x View データをリモート データベースに記録できますか？

解決方法

できます。ACS 5.x では、ACS View データを Microsoft SQL サーバや Oracle SQL サーバに記録できます。

問題：VMware サポート

解決方法

ACS 5.x は仮想マシンにインストールできます。最新バージョンの ACS 5.3 は、次の VMware バージョンにインストールできます。

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

問題：ディスクスペースに関する要件

ACS 5.x 評価版のディスク領域要件は何ですか。

解決方法

評価版では、60 GB 以上のディスク領域が必要です。本稼働インストールでは 500 GB が必要です。

問題：「24401 Could not establish connection with ACS Active Directory agent.」

解決方法

このエラーを解決するには、次のことを確認します。

- ACS マシンが Active Directory ドメインに参加している。
- ACS マシンと Active Directory サーバ間の接続ステータス。
- ACS Active Directory エージェントが実行している。

詳細については、Cisco Bug ID [CSCtx71254](#) ([登録ユーザ専用](#)) を参照してください。

問題：「ランタイム」プロセスが「Execution Failed」状態を表示する

パッチで Cisco ACS を更新しようとする、Runtime プロセスが「Execution Failed」状態になり、次のメッセージが記録されます。

```
local0 err err 83 2012-06-12T12:11:08+0200 192.168.150.74 ACS ACS logforward ERROR:  
/opt/CSCOacs/runtime/bin/run-logforward.sh:line 18:7097 Segmentation fault (core dumped)  
./$daemon -b -f $logfile
```

解決方法

これは、最新パッチの MD5 パッチで発生します。Cisco ACS に適用される最新パッチの MD5 チェックサムを確認します。再びダウンロードして、正しく適用します。

問題：UCS が再認証を強制するときに ACS 認証に失敗する

UCS サーバが Java クライアントを Cisco ACS から認証するように設定されています。この認証プロセスでは、RSA トークン サーバを使用します。最初の認証には成功します。しかし、UCS がリフレッシュし、Java クライアントの再認証を矯正すると、RSA でトークンの再利用が許可されていないため失敗します。そのため、認証が失敗します。

解決方法

これは、Cisco ACS ではなく、UCS サーバ上の制限です。UCS サーバでは、RSA トークンを使

用するとき Cisco ACS ではサポートされていない機能である 2 要素認証が実行されます。現在、これはサポートされていません。解決策として、AD または LDAP など、RSA Token サーバ以外のデータベースサーバを使用することを推奨します。

[問題 : 「24444 Active Directory operation has failed because of an unspecified error in the ACS」](#)

[解決方法](#)

AD 関連操作でアンマッピングエラーが発生しています。『[ACS 5.x と Microsoft AD の統合の設定例](#)』を参照して、[ACS との AD 統合を正しく設定します](#)。ドキュメントに従いすべてが正しく設定されている場合、さらなるトラブルシューティングについては Cisco TAC を参照してください。

[問題 : ACS 5.1 ユーザを AD 2008 R2 Server で認証できない](#)

[解決方法](#)

互換性問題が原因です。AD 2008 R2 統合は ACS 5.2 バージョンのみでサポートされています。ACS を 5.2 以降にアップグレードします。詳細については、Cisco Bug ID [CSCtg12399](#) ([登録ユーザ専用](#)) を参照してください。

[エラー: 「22056 Subject not found in the applicable identity store\(s\)」。](#)

SSL VPN ユーザが RSA アプライアンスから認証しようとする、Cisco ACS サーバから次のエラーメッセージが表示されます。

```
Failure reason:22056 Subject not found in the applicable identity store(s)
```

[解決方法](#)

ACS が参照するように指定されているデータベースにユーザが存在するか確認します。RSA および RADIUS ID ストアの場合、[Treat Reject] オプションで [authentication failed] が選択されていることを確認します。これは、ID ストア設定の [Advanced] タブ下にあります。

[問題 : ipt_connlimit:Oops:Invalid ct state ?](#)

「`ipt_connlimit: Oops:Invalid ct state ?`」エラーメッセージがコンソールに表示されます (ACS 5.x が VMware で実行している場合)。

[解決方法](#)

これは表面的なメッセージです。詳細については、Cisco Bug ID [CSCth25712](#) ([登録ユーザ専用](#)) を参照してください。

問題 : ACs 5.x / ISE は Cisco IOS ソフトウェア リリース 15.x NAS からの RADIUS 要求の RADIUS calling-station-id 属性を表示できません

問題 : ACs 5.x / ISE は Cisco IOS ソフトウェア リリース 15.x NAS からの RADIUS 要求の RADIUS calling-station-id 属性を表示できません。

解決方法

[radius-server attribute 31 send nas-port-detail](#) コマンドを Cisco IOS ソフトウェア リリース 15.x で使用して、属性の送信を有効にします。

問題 : 3 回の試行を設定していても、間違っただけのクレデンシャルの最初のインスタンスでユーザ アカウントがロックされる

ACS 5.3 が Active Directory と Windows 2008 R2 機能レベルで統合される場合、ロックアウト パラメータ (3 回の失敗) が設定されているユーザ アカウントは、ユーザがクレデンシャル入力を一度間違っただけでロックされます。

解決方法

詳細については、Cisco Bug ID [CSCtz03211](#) ([登録ユーザ専用](#)) を参照してください。

問題 : ACS からのバックアップを保存できない

ACS からのバックアップの保存中に、「Cause: Incremental Backup Not Configured-Details: Incremental backup is not configured. Configuring incremental backup is necessary to make the database purge successful. This will help to avoid disk space issues. View database Size is 0.08GB and size it occupies on the harddisk is 0.08GB

解決方法

増分バックアップ、完全バックアップおよびデータの削除を同時に実行することはできません。これらのジョブのいずれかが実行中の場合は、次のジョブを開始するまでに 90 分間待機する必要があります。

関連情報

- [Cisco Secure Access Control System のサポート ページ](#)
- [Cisco Secure Access Control System のエンドユーザ ガイド](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)