Cisco Active Directory Agent インストレーション / セットアップ ガイド、リリース 1.0

2011 年 12 月 13 日

Text Part Number: OL-25134-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

CONTENTS

はじめに

このマニュアルでは、Cisco Active Directory Agent のインストールと設定の手順を説明します。このマニュアルでは、Cisco Active Directory Agent を指す用語として AD Agent を使用します。

ここでは、次の内容について説明します。

対象読者

このマニュアルは、導入時に Active Directory Agent を使用するネットワーク管理者を対象としています。このマニュアルでは、読者がネットワーキングの原理と応用についての実用的な知識を持ち、ネットワーク システム管理者としての経験があることを前提としています。

マニュアルの編成

このマニュアルのトピックは次のように編成されています。

- はじめに
- Cisco Active Directory Agent の概要
- Active Directory Agent のインストールと設定
- Active Directory Agent コマンド リファレンス
- 「カスタマー ログ メッセージ」
- 「Windows アプリケーション イベント ログ」
- 「Active Directory Agent の問題のトラブルシューティング」

表記法

このマニュアルで使用する表記法では、^ 記号は *Ctrl* キーを表します。たとえば、^**z** というキーの組み合わせは、**Ctrl** キーを押しながら **z** キーを押すことを意味します。

コマンドの説明では、次の表記法を使用しています。

- システム プロンプトが含まれている例は、ユーザがプロンプトに対してコマンドを入力する、対話型セッションを表します。システム プロンプトは、現在の EXEC コマンド インタープリタのレベルを示しています。たとえば、プロンプト `Router>` はユーザ レベル、プロンプト `Router#` は*特権*レベルであることを表しています。通常、特権レベルにアクセスするにはパスワードが必要です。
- コマンドおよびキーワードは、**太字**で示しています。
- ユーザが値を指定する引数は、*イタリック体*で示しています。
- 角カッコ（[ ]）の中の要素は、省略可能です。
- 必ずいずれか 1 つを選択しなければならないキーワードは、波カッコ（{}）で囲み、縦棒（|）で区切って示しています。

例を挙げて説明する場合は、次の表記法を使用しています。

- 端末セッションおよびコンソール画面例は、`screen` フォントで示しています。
- ユーザが入力する情報は、**太字の `screen` フォント**で示しています。
- パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。
- システム プロンプトに対するデフォルトの応答は、角カッコ（[]）で囲んで示しています。
- 行の先頭に感嘆符（!）がある場合には、コメント行であることを示します。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイントアドバイス 「*時間節約*」の意味です。ここに紹介している方法で作業を行うと、時間を短縮できます。

（注） 「*注釈*」です。次に進む前に検討する必要がある重要情報、役に立つ情報、このマニュアル以外の参照資料などを紹介しています。

マニュアルの最新情報

表 1　『Active Directory Agent インストレーション/セットアップ ガイド』の最新情報

日付	説明
2011/06/23	第 2 章に 国際化はサポートされていません。という注を追加。
2011/06/13	Cisco AD Agent Release 1.0

関連資料

このリリースのマニュアル

表 2 に、入手可能な AD Agent Release 1.0 の製品マニュアルの一覧を示します。

表 2　このリリースのマニュアル

参照先	URL
『Installation and Setup Guide for the Cisco Active Directory Agent, Release 1.0』	http://www.cisco.com/en/US/docs/security/ibf/setup_guide/ad_agent_setup_guide.html
『Release Notes for the Cisco Active Directory Agent, Release 1.0』	http://www.cisco.com/en/US/docs/security/ibf/release_notes/ibf10_rn.html
『Open Source Used in Cisco Active Directory Agent 1.0』	http://www.cisco.com/en/US/docs/security/ibf/open_source_license_document/ipcentral.pdf

その他の関連マニュアル

適応型セキュリティ アプライアンス（ASA）5500 シリーズ、リリース 8.4.2 のマニュアルと Cisco IronPort Web セキュリティ アプライアンス（WSA）のマニュアルへのリンクは、Cisco.com の以下の場所に記載されています。

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスのページ
  http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html
- Cisco IronPort Web セキュリティ アプライアンスのページ
  http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html

通告

Active Directory Agent Release 1.0 で使用されているすべてのオープン ソース ライセンスについては、http://www.cisco.com/en/US/docs/security/ibf/open_source_license_document/ipcentral.pdf を参照してください。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

Cisco Active Directory Agent の概要

Cisco Active Directory Agent（AD Agent）は、Windows マシン上で実行され、Active Directory ドメイン コントローラ（DC）マシンの集合をリアルタイムにモニタし、一般にユーザ ログインを示す認証関連イベントを確認し、データベース内の IP アドレスとユーザ ID のマッピングを認識、分析、キャッシュし、クライアント デバイスに対して最新のマッピングを使用可能にするコンポーネントです。

クライアント デバイス（Cisco 適応型セキュリティ アプライアンス（ASA）や Cisco IronPort Web セキュリティ アプライアンス（WSA）など）は、最新の IP-to-user-identity マッピング セットを次のいずれかの方法で取得するため、RADIUS プロトコルを使用して AD Agent と通信します。

- オンデマンド：AD Agent は、特定のマッピングに対するクライアント デバイスからの On-Demand クエリーに応答できます。
- バルク ダウンロード：AD Agent は、現在キャッシュ内にあるマッピング セット全体を求めるクライアント デバイスからの要求に応答できます。

オンデマンド方式とバルク ダウンロード方式の両方で、クライアント デバイスからの要求に、後続の更新に関連する通知の要求も含んでいることを示すタグを特別に付けることができます。

たとえば、クライアント デバイスが基本的な On-Demand クエリーを要求すると、AD Agent は応答してそのキャッシュ内で検出される特定のマッピングを提供しますが、そのマッピングに関するそれ以降の更新は送信しません。ただし、On-Demand クエリーに通知要求が含まれている場合、AD Agent からの最初の応答は前述と同様ですが、後でこの特定のマッピングが変更される場合、AD Agent は要求元のクライアント デバイス（および通知登録しているその他のすべてのクライアント デバイス）に対し、この特定のマッピングの変更について事前に通知します。

同様に、クライアント デバイスが基本的なバルク ダウンロードを要求する場合、AD Agent は現在キャッシュ内にあるすべてのマッピングを含むセッション データのスナップショットを転送しますが、それ以降の更新は送信しません。一方、レプリケーション登録要求の場合、AD Agent からの最初の応答は前述の場合と同様ですが、後でマッピング セットに対して何らかの変更（新規マッピングの追加、特定のマッピングの変更など）が行われると、AD Agent は要求元のクライアント デバイス（およびレプリケーション登録しているその他のすべてのクライアント デバイス）に対し、以前に送信されたスナップショットと比較して、それらの変更について事前に通知します。

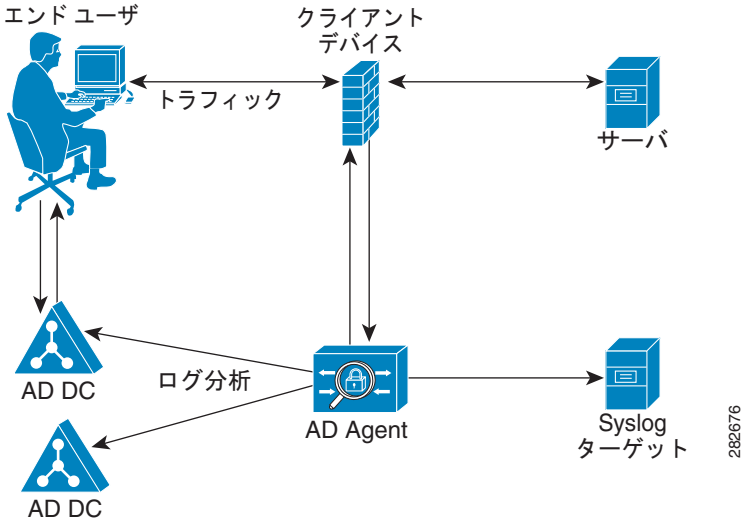
AD Agent により検出、管理、提供される IP-to-user-identity マッピングには、IPv4 アドレスの他に IPv6 アドレスを含めることができます。

AD Agent は 1 つ以上の Syslog サーバにログを送信できます。

いずれかの AD ドメイン コントローラまたはクライアント デバイスで障害が発生しても、AD Agent は引き続き機能します。AD Agent は他のドメイン コントローラから情報を取得します。ただし、AD Agent のフェールオーバーは行われません。Cisco AD Agent 内蔵の「ウォッチドッグ」機能は、AD Agent 内部の Windows プロセスを継続的にモニタし、プロセスがクラッシュしたことを検出すると自動的にそのプロセスを再起動します。

図 1-1 に、サンプル シナリオでの AD Agent の役割を示します。

図 1-1　　ソリューションにおける AD Agent



この例では、ユーザがコンピュータからログインしてサーバへのアクセスを要求し、これにより Web トラフィックが生成されます。クライアント デバイスは Web トラフィックをインターセプトし、コンピュータにログインしたユーザに関して尋ねる RADIUS 要求を AD Agent に送信します。AD Agent は最新の IP-to-user-identity マッピング セットを管理しており、ユーザ情報をクライアント デバイスに送信します。クライアント デバイスはユーザ ID 情報を使用して、エンド ユーザにアクセス権を付与するかどうかを決定します。

AD Agent はネットワーク内の以下のコンポーネントと通信します。

- クライアント デバイス
- Active Directory ドメイン コントローラ マシン
- Syslog サーバ

（注）　AD Agent は最大 100 のクライアント デバイスと最大 30 のドメイン コントローラ マシンに対応でき、また最大 64,000 の IP-to-user-identity マッピングを内部にキャッシュできます。

クライアント デバイス

クライアント デバイスは AD Agent から最新の IP-to-user-identity マッピングをアクティブに取得（およびパッシブに受信）します。

クライアント デバイスは次の方法で AD Agent からマッピングを取得できます。

- AD Agent に対して新しい各 IP に対するクエリーを実行する
- ユーザ ID および IP アドレスのデータベース全体のローカル コピーを維持する

クライアント デバイスは、最新の IP-to-user-identity マッピング セットを AD Agent から受信し、また他のメカニズムによって学習したマッピングの更新を AD Agent に送信します。たとえば ASA デバイスは次の内容で AD Agent を更新します。

- （AD Agent がユーザ ID にマップできなかった IP アドレスの）Web 認証フォールバック中に学習された新しいマッピング

- VPN セッションから学習した新しいマッピング
- VPN/カットスルー プロキシ、NetBIOS プローブ、MAC チェックから学習したログオフまたは切断に伴うマッピング削除

これらの更新は RADIUS Accounting-Request メッセージとして送信されます。

（注）　AD Agent に通知を送信するように ASA デバイスを設定する方法については、ASA エンドユーザ マニュアルを参照してください。

Active Directory ドメイン コントローラ マシン

Active Directory はこのソリューションの一部ですが、Active Directory 管理者により管理されます。データの信頼性と正確さは、Active Directory ドメイン コントロールのデータによって決まります。AD Agent は Active Directory ドメイン コントローラからのイベントをモニタし、学習し、読み取ります。

AD Agent は、ユーザ認証に Kerberos を使用する認証イベントのみをモニタします。

AD Agent がモニタするイベントは通常ログインによって引き起こされますが、以下のアクティビティによって引き起こされることもあります。

- Windows の「runas」コマンドの使用
- Windows の「net user」コマンドの使用

AD Agent は、次に示すサポートされている Windows Server バージョンで実行されている Active Directory ドメイン コントローラ マシンを最大 30 までモニタできます。

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

（注）　Windows Server 2003 R2 はサポートされていません。

Windows Server 2008 または Windows Server 2008 R2 が実行されているすべての Active Directory ドメイン コントローラ マシンに、適切な Microsoft ホットフィックスがインストールされていることを確認することが重要です（「Active Directory の要件」（P.2-5）を参照）。AD Agent がドメイン コントローラ マシンに直接インストールされているか、またはドメイン コントローラ マシンをリモート操作でモニタしているかどうかに関係なく、ホットフィックスを適用する必要があります。

同様に、各 Active Directory ドメイン コントローラ マシン上の監査ポリシーで、正常に完了した認証試行操作の監査が許可されていることを確認することが重要です（「AD Agent での AD ドメイン コントローラからの情報取得の設定」（P.2-9）を参照）。

AD Agent は、AD Agent マシンが参加しているドメインとの信頼関係が設定されているドメインをモニタできます。AD Agent では次に示す Active Directory 構造がサポートされています。

- シングル フォレスト、シングル ドメイン
- シングル フォレスト、マルチ ドメイン
- マルチ フォレスト

Syslog サーバ

AD Agent は、管理とトラブルシューティングに関する情報が含まれているログを 1 つ以上の Syslog サーバに転送できます。これらのログの内容は、AD Agent マシンの C:¥IBF¥radiusServer¥runtime¥logs¥localStore¥ ディレクトリにあるカスタマー ログと同一です。Syslog メカニズムにより、Syslog サーバが実行されており、Syslog メッセージを受信できるターゲット マシンにこの情報がリモート配信されます。

CHAPTER 2

Active Directory Agent のインストールと設定

Active Directory Agent は、Windows インストーラとしてパッケージングされているソフトウェア アプリケーションです。Windows マシンにインストールし、クライアント デバイスおよび AD ドメイン コントローラを設定する必要があります。

この章は次のトピックで構成されています。

（注） ASA デバイスに関連する設定については、ASA エンドユーザ マニュアルを参照してください。

要件

ここでは、次の項目について説明します。

ハードウェア要件

Active Directory Agent をインストールするには、次のいずれかが必要です。

- Windows 2003 マシン
- Windows 2008 マシン
- Windows 2008 R2 マシン

（注） Windows 2003 R2 はサポートされていません。

（注） 国際化はサポートされていません。

この AD Agent マシンは、モニタ対象の Active Directory ドメイン コントローラであるか、または個別の専用 Windows マシンです。

ソリューションで複数の AD Agent マシンをインストールする必要がある場合は、以下の点に注意してください。

- ドメイン コントローラ マシンではない AD Agent マシンの数に制限はありません。
- 特定の AD ドメインでは 1 つのドメイン コントローラ マシンにのみ AD Agent を直接インストールできます。

いずれの場合でも、AD Agent マシンは表 2-1 に示すハードウェアの最小仕様要件を満たしている必要があります。

表 2-1　AD Agent マシンの最小ハードウェア仕様要件

コンポーネント	仕様
CPU	Intel Xeon 2.66 GHz Q9400（クアッド コア）
システム メモリ	4 GB の SDRAM
ハード ディスクの空き容量	500 GB

接続要件

AD Agent が適切に機能するためには、この AD Agent で設定されているすべてのクライアントデバイス、Active Directory ドメイン コントローラ マシン、ターゲット Syslog サーバと自由に通信できる必要があります。Windows Firewall（またはその他の互換サードパーティ ファイアウォール ソフトウェア）が AD Agent マシンまたは Active Directory ドメイン コントローラ マシンで実行されている場合、各エンドポイントのファイアウォール ソフトウェアで、自由な通信のために必要な例外を設定する必要があります。

このセクションでは、Windows Firewall を例に、Windows Firewall を実行するすべてのエンドポイントで定義する必要がある例外について詳しく説明します。

- 「AD Agent マシンで設定する必要がある Windows Firewall 例外」（P.2-3）
- 「個別の Active Directory ドメイン コントローラ マシンで設定する必要がある Windows Firewall 例外」（P.2-4）

その他の互換サードパーティ ファイアウォール ソフトウェアについては、ベンダーのマニュアルで該当する例外の設定方法を参照してください。

AD Agent マシンで設定する必要がある Windows Firewall 例外

AD Agent マシンで Windows Firewall が有効に設定されている場合は、次の操作を実行する必要があります。

a. 次のプログラムについて Windows Firewall 例外を明示的に定義してください。

- C:¥IBF¥adObserver¥ADObserver.exe
- C:¥IBF¥radiusServer¥runtime¥win32¥bin.build¥rt_daemon.exe

AD Agent マシンで Windows Server 2008 または Windows Server 2008 R2 が実行されている場合は、以下の Windows コマンド ラインを使用してこれらの例外を定義します（それぞれのコマンドは 1 行に入力します）。

- **netsh advfirewall firewall add rule name="Cisco AD Agent (AD Observer)" dir=in action=allow program="C:¥IBF¥adObserver¥ADObserver.exe" enable=yes**
- **netsh advfirewall firewall add rule name="Cisco AD Agent (RADIUS Server)" dir=in action=allow program="C:¥IBF¥radiusServer¥runtime¥win32¥bin.build¥rt_daemon.exe" enable=yes**

AD Agent マシンで Windows Server 2003（SP1 以上インストール済）が実行されている場合、以下の Windows コマンド ラインを使用してこれらの例外を定義します（それぞれのコマンドは 1 行に入力します）。

- **netsh firewall add allowedprogram C:¥IBF¥adObserver¥ADObserver.exe "Cisco AD Agent (AD Observer)" ENABLE**
- **netsh firewall add allowedprogram C:¥IBF¥radiusServer¥runtime¥win32¥bin.build¥rt_daemon.exe "Cisco AD Agent (RADIUS Server)" ENABLE**

（注）　元の Windows Server 2003 では Windows Firewall はサポートされていません。Windows Server 2003 SP1 で Windows Firewall に対応しましたが、デフォルトでは Windows Firewall は無効に設定されています。Windows Server 2003 SP2 では Windows Firewall はデフォルトで有効に設定されています。

1. **adacfg dc create** コマンドを使用して AD Agent マシンとは別の Active Directory ドメイン コントローラ マシンを設定する場合は、AD Agent マシンで、必要な WMI 関連通信を許可する Windows Firewall 例外も定義する必要があります。

（注）　AD Agent マシンと、このマシンとは別のドメイン コントローラ マシンで Windows Firewall が有効に設定されており、AD Agent が AD ドメイン コントローラ マシンと通信する必要がある場合は常に、各マシンで WMI の例外を設定する必要があります。いずれかのマシンで Windows Firewall が実行されていない場合、そのマシンでは WMI 例外は必要ありません。AD ドメイン コントローラが 1 つであり、AD Agent がこのドメイン コントローラと同じマシンで実行されている場合も、WMI 例外は不要です。

AD Agent マシンで Windows Server 2008 または Windows Server 2008 R2 が実行されている場合は、以下の Windows コマンド ラインを使用してこの WMI 関連の例外を定義します（それぞれのコマンドは 1 行に入力します）。

```
netsh advfirewall firewall set rule group="Windows Management Instrumentation (WMI)"
new enable=yes
```

AD Agent マシンで Windows Server 2003（SP1 以上インストール済）が実行されている場合は、以下の Windows コマンド ラインを使用してこの WMI 関連の例外を定義します（それぞれのコマンドは 1 行に入力します）。

- `netsh firewall add portopening protocol=tcp port=135 name="Cisco AD Agent (WMI_DCOM_TCP135)"`
- `netsh firewall add allowedprogram program=%windir%¥system32¥wbem¥unsecapp.exe name="Cisco AD Agent (WMI_UNSECAPP)"`

個別の Active Directory ドメイン コントローラ マシンで設定する必要がある Windows Firewall 例外

AD Agent マシンで **adacfg client create** コマンドを使用して設定した個別の Active Directory ドメイン コントローラ マシンで、Windows Firewall が有効な場合は、そのドメイン コントローラ マシンで必要な WMI 関連の通信を許可する Windows Firewall 例外を定義する必要があります。

このドメイン コントローラ マシンで Windows Server 2008 または Windows Server 2008 R2 が実行されている場合は、以下の Windows コマンド ラインを使用してこの WMI 関連の例外を設定できます（コマンドは 1 行に入力します）。

```
netsh advfirewall firewall set rule group="Windows Management Instrumentation (WMI)" new
enable=yes
```

このドメイン コントローラ マシンで Windows Server 2003（SP1 以降インストール済）が実行されている場合は、以下の Windows コマンド ラインを使用してこの WMI 関連の例外を設定できます（コマンドは 1 行に入力します）。

```
netsh firewall set service RemoteAdmin enable
```

オープン ポートのリスト

表 2-2 に、AD Agent がクライアント デバイスおよび Active Directory ドメイン コントローラとの通信に使用する伝送制御プロトコル（TCP）ポートとユーザ データグラム プロトコル（UDP）ポートの一部を示します。AD Agent ではこれらのポートがオープンでなければなりません。

（注）　このリストには、WMI により使用される動的割り振り（ランダム）ポート番号は含まれていません。

表 2-2　AD Agent のオープン ポートのリスト

ポート番号	プロトコル	サービス
8888 （ローカル ホスト）	TCP	設定変更
514	UDP	Syslog
すべてのインターフェイスで 1645	UDP	レガシー RADIUS

表 2-2　AD Agent のオープン ポートのリスト（続き）

ポート番号	プロトコル	サービス
すべてのインターフェイスで 1646	UDP	レガシー RADIUS Accounting
すべてのインターフェイスで 1812	UDP	RADIUS
すべてのインターフェイスで 1813	UDP	RADIUS Accounting

設定変更および RADIUS 用のポート番号はハードコーディングされており変更できません。AD Agent マシンでこれらのポート番号を使用する他のソフトウェア アプリケーションを実行しないでください。たとえば、AD Agent マシンで別の RADIUS サーバが実行されていてはなりません。

Active Directory の要件

AD Agent がドメイン コントローラと通信するためには、以下の前提条件を満たしている必要があります。

- ユーザがログイン中に認証を実行し、セキュリティ ログが AD Agent によりモニタされる個々の各 AD ドメイン コントローラでは、次のサポートされている Windows Server バージョンのいずれかが実行されている必要があります。
  - Windows Server 2003
  - Windows Server 2008
  - Windows Server 2008 R2

（注）　Windows Server 2003 R2 はサポートされていません。

（注）　国際化はサポートされていません。

- また、Windows Server 2008 または Windows Server 2008 R2 が実行されている各ドメイン コントローラ マシンでは、該当する Microsoft ホットフィックスがインストールされている必要があります。AD Agent がドメイン コントローラ マシンに直接インストールされているか、またはドメイン コントローラ マシンをリモート操作でモニタしているかどうかに関係なく、ホットフィックスをインストールする必要があります。

  Windows Server 2008 が実行されているドメイン コントローラには、以下の 2 つの Microsoft ホットフィックスをインストールする必要があります。

  a. http://support.microsoft.com/kb/958124

     このパッチは、Microsoft の WMI でのメモリ リークを修正します。このメモリ リークを修正しないと、AD Agent がドメイン コントローラに接続して「アップ」ステータスになることができません。

  b. http://support.microsoft.com/kb/973995

     このパッチは、Microsoft の WMI でのメモリ リークを修正します。このメモリ リークを修正しないと、Active Directory が必要な認証関連イベントをドメイン コントローラのセキュリティ ログに書き込めない状況が散発的に発生します。この場合、AD Agent はそのドメイン コントローラを介して認証されるユーザ ログインの一部に対応するマッピングを学習できません。

Windows Server 2008 R2 が実行されているドメイン コントローラ マシンでは、以下の Microsoft ホットフィックスをインストールする必要があります（SP1 がインストールされていない場合）。

http://support.microsoft.com/kb/981314

このパッチは、Microsoft の WMI でのメモリ リークを修正します。このメモリ リークを修正しないと、Active Directory が必要な認証関連イベントをドメイン コントローラのセキュリティ ログに書き込めない状況が散発的に発生します。この場合、AD Agent はそのドメイン コントローラを介して認証されるユーザ ログインの一部に対応するマッピングを学習できません。

- 同様に、ユーザがログイン中に認証を実行し、セキュリティ ログが AD Agent によりモニタされる個別の AD ドメイン コントローラでは、「監査ポリシー」（[Group Policy Management] の設定の一部）で正常なログオンによってその AD ドメイン コントローラ マシンの Windows セキュリティ ログに必要なイベントが生成されるように設定されている必要があります。「AD Agent での AD ドメイン コントローラからの情報取得の設定」（P.2-9）を参照してください。
- **adacfg dc create** コマンドを使用して単一ドメイン コントローラ マシンを設定する前にも、（AD Agent マシンで設定するドメイン コントローラ マシンを介した）ユーザ認証をモニタするすべてのドメイン（例：ドメイン *D[i]*）との間に信頼関係が設定されているドメイン（例：ドメイン *J*）に、AD Agent が最初に参加していることを確認してください。

  Active Directory ドメインの構造に応じて可能なシナリオを以下に示します。

  1. シングル フォレスト、シングル ドメイン：すべてのドメイン コントローラ マシンに対するドメインが 1 つのみ（*D[i]*）であり、これはドメイン *J* と同一です。AD Agent マシンは最初にこのシングル ドメインに参加する必要があります。その他のドメインは使用されないため、その他のドメインとの間に信頼関係を設定する必要はありません。
  2. シングル フォレスト、マルチ ドメイン：シングル フォレスト内のすべてのドメイン間で、すでに固有の双方向の信頼関係が設定されています。したがって、AD Agent は最初にこのフォレスト内の 1 つのドメイン *J* に参加します。このドメイン *J* は、ドメイン コントローラ マシンに対応するドメイン *D[i]* のいずれとも同一である必要はありません。ドメイン *J* と各 *D[i]* ドメインとの間には固有の信頼関係が設定されているため、信頼関係を明示的に設定する必要はありません。
  3. マルチ フォレスト、マルチ ドメイン：ドメイン *J* が属するフォレストが、ドメイン コントローラ マシンに対応する *D[i]* の 1 つ以上のドメインが属するフォレストとは異なることがあります。この場合、各 *D[i]* ドメインとドメイン *J* の間に、次のいずれかまたは両方の方法で有効な信頼関係が設定されていることを明示的に確認する必要があります。

  a. 2 つのドメイン（*D[i]* と *J*）の間には双方向の外部信頼関係を設定できます。

  b. ドメイン *D[i]* に対応するフォレストとドメイン *J* に対応するフォレストの間に、双方向のフォレスト信頼関係を設定できます。

  信頼関係を設定するには、[Start] > [All Programs] > [Administrative Tools] > [Active Directory Domains and Trusts] を選択します。

（注）　この要件に対応せず、特定の DC マシンに関連付けられているドメインとの間に必要な信頼関係が設定されているドメインに AD Agent マシンが参加していない場合、**adacfg dc create** コマンドを使用してその DC マシンを設定する操作を実行すると、正常に完了したように見えます。しかし、その DC マシンでは非常に高い CPU 負荷などのさまざまな問題が発生し始めることがあります。

Active Directory Agent のインストール

Active Directory Agent をインストールするには、次の手順を実行します。

ステップ 1　Active Directory Agent をインストールする Windows マシンに、Active Directory Agent インストーラ実行ファイルをコピーします。

ステップ 2　**AD_Agent-v1.0.0.32-build-539.Installer.exe** ファイルを実行します。

[Cisco AD Agent Setup] ダイアログボックスが表示されます。

ステップ 3　[Yes] をクリックし、インストールを続行します。

インストーラにより AD Agent が Windows マシンの C:¥IBF¥ ディレクトリにインストールされます。インストール処理の進行状況を確認できます。インストールが正常に完了すると、[Completed] メッセージが表示されます。

ステップ 4　[Close] をクリックして、インストーラを終了します。

インストールされた Active Directory Agent の確認

インストール後に Active Directory Agent が実行されているかどうかを確認するには、次の手順を実行します。

ステップ 1　Windows Command Line Prompt に移動します（[Start] > [All Programs] > [Accessories] > [Command Prompt]）。

ステップ 2　**cd C:¥IBF¥CLI** と入力します。

ステップ 3　**adactrl.exe show running** と入力します。

次のような出力が表示されます。

```
running C:¥¥IBF¥¥watchdog¥¥radiusServer.bat since 2010-12-27 T15:32:31
running C:¥¥IBF¥¥watchdog¥¥adObserver.bat since 2010-12-27 T15:32:38
```

この出力には、AD Agent 内部プロセスがこのマシンで実行開始した日時に関する情報が示されます。

Active Directory Agent のアンインストール

Active Directory Agent をアンインストールするには、次の手順を実行します。

ステップ 1　C:¥IBF¥ フォルダに移動します。

デフォルトでは、Active Directory Agent は Windows マシンの C:¥IBF¥ ディレクトリにインストールされています。

ステップ 2　**AD_Agent.Uninstaller.exe** ファイルを実行します。

AD Agent がアンインストールされます。

Active Directory Agent の設定

AD Agent のインストール後に、Windows Firewall などのファイアウォールが AD Agent マシンで実行されている場合には AD Agent マシンで必要な例外が設定されていることを最初に確認してください（「AD Agent マシンで設定する必要がある Windows Firewall 例外」（P.2-3）を参照）。その後、AD Agent で以下を設定する必要があります。

- ユーザがログイン中に認証を実行する個別の Active Directory ドメイン コントローラ。このドメイン コントローラから新しいマッピングを学習するため、このコントローラのセキュリティ ログが AD Agent によりモニタされます。

（注）　また、導入するバックアップ ドメイン コントローラをすべて含める必要があります。

- AD Agent マシンから IP-to-user-identity マッピングを取得するように設定されているクライアント デバイス（ASA デバイスなど）。

Syslog サーバにログを送信するように AD Agent を設定することもできます。

（注）　AD ドメイン コントローラとクライアント デバイスの設定前にまず AD Agent で Syslog サーバを設定すると、トラブルシューティング情報が localStore に加え Syslog サーバでも使用できるようになります。このトラブルシューティング情報を Syslog サーバで保持しておくと、セットアップ中に問題が発生した場合に役立ちます。

AD Agent のインストール後、adacfg コマンドを実行する前に、AD Agent が適切に初期化されるまでしばらく（約 30 秒）お待ちください。

- AD Agent が実行されていないときにいずれかの adacfg コマンドを実行すると、次のメッセージが表示されます。

```
Error: HTTP request sending failed with error "Couldn't connect to server"! For
further syntax information, use adacfg help.
```

- AD Agent が完全に初期化される前にいずれかの adacfg コマンドを実行すると、次のメッセージが表示されます。

```
Caught exception: Module PipConfigurator not initialized!
```

ここでは、次の項目について説明します。

- 「AD Agent での Syslog サーバへのログ送信の設定」（P.2-9）
- 「AD Agent での AD ドメイン コントローラからの情報取得の設定」（P.2-9）
- 「AD Agent でクライアント デバイスによる AD Agent からの情報取得を許可する設定」（P.2-12）

（注）　このセクションでは、AD Agent で行う必要がある設定についてのみ説明します。ソリューションが適切に機能するためには、クライアント デバイスで AD Agent と AD ドメイン コントローラを設定する必要もあります。詳細については、*ASA のエンドユーザ マニュアル*を参照してください。

AD Agent での Syslog サーバへのログ送信の設定

管理上の目的と、トラブルシューティング情報の入手のために、Syslog サーバへログを送信するように AD Agent を設定できます。

Syslog サーバへログを送信するように AD Agent を設定するには、次の手順を実行します。

ステップ 1　AD Agent Windows マシンにログインします。

ステップ 2　コマンド ライン プロンプトで cd **C:¥IBF¥CLI** と入力します。

ステップ 3　次のコマンドを入力します。

adacfg syslog create -name <*syslog-target-nickname*> **-ip** <*IP-address*> [**-facility** <*syslog-facility*>]

説明：

- *syslog-target-nickname* は、Syslog サーバに割り当てるフレンドリ名です。
- *IP-address* は Syslog サーバの IP アドレスです。
- *syslog-facility* の値は LOCAL0 ～ LOCAL7 です。デフォルトは LOCAL6 です。

次のメッセージが表示されます。

```
Reply: Command completed successfully.
```

AD Agent での AD ドメイン コントローラからの情報取得の設定

ユーザがログイン中に認証を実行する個別 Active Directory ドメイン コントローラは AD Agent 上で個別に設定する必要があります。これにより、AD Agent はその特定のドメイン コントローラのセキュリティ ログをモニタし、そのドメイン コントローラから新しい IP-to-user-identity マッピングを学習できます。

（注）　導入するバックアップ ドメイン コントローラ マシンをすべて含める必要があります。

特定の AD ドメイン コントローラ マシンから情報を取得するように AD Agent を設定するには、次の手順を実行します。

ステップ 1　AD ドメイン コントローラ マシンで実行されている Windows Server オペレーティング システムのバージョンが、サポートされているバージョンであることを確認します。（「Active Directory の要件」（P.2-5）を参照）。

ステップ 2　AD ドメイン コントローラ マシンで Windows Server 2008 または Windows Server 2008 R2 が実行されている場合は、該当する Microsoft ホットフィックスがマシンにインストールされていることを確認します（「Active Directory の要件」（P.2-5）を参照）。指定されているホットフィックスが適用されていない Windows Server 2008 または 2008 R2 が実行されている AD ドメイン コントローラを使用してはなりません。

ステップ 3　Windows Firewall などのファイアウォール ソフトウェアが AD ドメイン コントローラ マシンで有効になっている場合は、AD ドメイン コントローラ マシンで必要なファイアウォール例外が定義されていることを確認します（「個別の Active Directory ドメイン コントローラ マシンで設定する必要がある Windows Firewall 例外」（P.2-4）を参照）。

ステップ 4　ドメイン コントローラ マシンに関連付けられているドメインに、AD Agent マシンが参加するドメインとの適切な信頼関係が設定されていることを確認します。

ステップ 5　「監査ポリシー」（[Group Policy Management] の設定の一部）で、正常なログオンによってその AD ドメイン コントローラ マシンの Windows セキュリティ ログに必要なイベントが生成されるように設定されていることを確認します（通常これは Windows のデフォルト設定ですが、この設定が正しいことを明示的に確認する必要があります）。これを確認するには、[Start] > [Programs] > [Administrative Tools] > [Group Policy Management] を選択します。[Group Policy Management] の左側のナビゲーション ペインで次の操作を実行します。

a. [Domains] の下で該当するドメインに移動します。

b. ナビゲーション ツリーを展開します。

c. [Default Domain Policy] を右クリックします。

d. [Edit] メニュー項目を選択します。これにより [Group Policy Management Editor] が開きます。

e. [Group Policy Management Editor] の左側のナビゲーションペインで次の操作を実行します。

f. [Default Domain Policy] > [Computer Configuration] > [Policies] > [Windows Settings] > [Security Settings] を選択します。

- Windows Server 2003 または Windows Server 2008（R2 以外）の場合は [Local Policies] > [Audit Policy] を選択します。2 つのポリシー項目（[Audit Account Logon Events] と [Audit Logon Events]）で、対応する [Policy Setting] に [Success] 状態が直接的または間接的に含まれていることを確認します。[Success] 状況を間接的に含めるには、[Policy Setting] に [Not Defined] を設定します。この場合、上位ドメインから有効値が継承されるため、[Success] 状態を明示的に含めるようにその上位ドメインの [Policy Setting] を設定する必要があります。
- Windows Server 2008 R2 の場合は [Advanced Audit Policy Configuration] > [Audit Policies] > [Account Logon] を選択します。2 つのポリシー項目（[Audit Kerberos Authentication Service] と [Audit Kerberos Service Ticket Operations]）に対応する [Policy Setting] に、前述のように [Success] 状態が直接または間接的に含まれていることを確認します。

g. [Audit Policy] の項目設定が変更されている場合は、「**gpupdate /force**」を実行して新しい設定を強制的に有効にする必要があります。

ステップ 6　AD Agent Windows マシンにログインします。

ステップ 7　コマンド ライン プロンプトで cd **C:¥IBF¥CLI** と入力します。

ステップ 8　次のコマンドを入力します。

adacfg dc create -name <*DC-nickname*> **-host** <*DC-hostname-or-FQDN*> **-domain** <*full-DNS-name-of-AD-domain*> **-user** <*username-member-of-Domain-Admins-group*> **-password** <*password-of-user*>

説明：

- *DC-nickname* は、ドメイン コントローラに割り当てるフレンドリ名です。
- *DC-hostname-or-FQDN* は、AD Agent によりモニタされる AD ドメイン コントローラ マシンのホスト名または完全修飾ドメイン名です。
- *full-DNS-name-of-AD-domain* は、AD ドメインの完全 DNS 名です。
- *username-member-of-Domain-Admins-group* は、ドメイン コントローラ マシンのセキュリティ ログのモニタに使用される既存のアカウントのユーザ名です。

  このアカウントにはドメイン コントローラ マシンのセキュリティ ログを読み取るために必要な権限が付与されている必要があります。「-domain」オプションに指定したドメインの AD グループ「Domain Admins」に属するアカウントを指定することで、容易かつ確実にこの操作を実行できます。

あるいは、以下のすべての要件に対応していれば、「Domain Admins」グループに属さないメンバーでも必要な権限を取得できます。

- アカウントが AD グループ「Distributed COM Users」に属している。
- アカウントに、ドメイン コントローラ マシンの WMI 名前空間（特に「CIMV2」名前空間）へのアクセス権限が付与されている。この権限を設定するには、「wmimgmt.msc」スナップインを使用するか、またはグループ ポリシーを使用します（すべてのドメイン コントローラ マシンに反映する場合）。詳しくは、http://blogs.msdn.com/b/spatdsg/archive/2007/11/21/set-wmi-namespace-security-via-gpo-script.aspx を参照してください。
- ドメイン コントローラ マシンのセキュリティ イベント ログを読み取る権限がアカウントに付与されている。この権限を設定するには、レジストリの CustomSD キーを使用するか、または Group Policy を使用します（すべてのドメイン コントローラ マシンに反映する場合）。詳しくは、http://msdn.microsoft.com/en-us/library/aa363648%28v=vs.85%29.aspx を参照してください。

- *password-of-user* は、指定したユーザ名に対応するパスワードです。

次のメッセージが表示されます。

```
Reply: Command completed successfully.
```

現在設定されている AD ドメイン コントローラ マシンとそのアップまたはダウン ステータスのリストを表示するには、**adacfg dc list** コマンドを使用します。このコマンドを定期的に実行し、AD ドメイン コントローラ マシンのステータスを再確認できます。

特定の AD ドメイン コントローラを作成する **adacfg dc create** コマンドを実行した後で、その AD ドメイン コントローラのステータスが初期設定の「down」から「up」または「down(no-retry)」になるまでしばらく（約 1 分）お待ちください。

- 「up」状態は、その AD ドメイン コントローラへの接続が確立されたことを示します。場合によっては、特定の AD ドメイン コントローラ マシンが初めて「up」状態になった時点から、以前のマッピングがそのマシンから取得され、**adacfg cache list** コマンドで表示できるようになるまで、さらに数分（またはこれよりも長い期間）待つ必要があります。
- 「down(no-retry)」状態は、（クレデンシャルが誤っていることなどが原因で）接続を確立できず、AD Agent が接続確立を再試行しないことを示します。
- 「down」状態は、現在 AD Agent はその AD ドメイン コントローラ マシンと接続していないが、接続確立を定期的に再試行することを示します。

また、**adacfg dc erase** コマンドを使用して AD Agent から任意のドメイン コントローラ設定を削除することもできます。

これらのコマンドについて詳しくは、「adacfg dc list」（P.A-8）、「adacfg cache list」（P.A-9）、および「adacfg dc erase」（P.A-8）を参照してください。

AD Agent でクライアント デバイスによる AD Agent からの情報取得を許可する設定

AD Agent がクライアント デバイスからの要求（この AD Agent からのマッピング情報を受信する要求）に応答するように、AD Agent で各クライアント デバイス（ASA など）を設定する必要があります。

（注）　1 つの AD Agent では最大 100 のクライアント デバイス（ASA デバイスなど）がサポートされています。

特定のクライアント デバイスと通信するように AD Agent を設定するには、次の手順を実行します。

ステップ 1　AD Agent Windows マシンにログインします。

ステップ 2　コマンド ライン プロンプトで cd **C:¥IBF¥CLI** と入力します。

ステップ 3　次のコマンドを入力します。

adacfg client create -name <*client-nickname*> **-ip** <*IP-address*>*[/*<*prefix-length-for-IP-range*>*]* **-secret** <*RADIUS-shared-secret*>

説明：

- *client-nickname* は、特定のクライアントデバイスに割り当てるフレンドリ名です。
- *IP-address/*<*prefix-length-for-IP-range*> は、特定のクライアント デバイスの IP アドレスを指定します。オプションでサブネット範囲を定義できます。
- *RADIUS-shared-secret* は、RADIUS プロトコルが通信に使用する共有秘密です。この *secret* は、そのクライアント デバイスで設定される鍵です。

（注）　正しい RADIUS-shared-secret を入力したことを確認してください。このようにしないと、そのクライアント デバイスからの要求が無視されます。

次のメッセージが表示されます。

```
Reply: Command completed successfully!
```

現在設定されているクライアントデバイスのリストを表示するには **adacfg client list** コマンドを使用し、AD Agent から任意のクライアント デバイス設定を削除するには **adacfg client erase** コマンドを使用します。これらのコマンドについて詳しくは、「adacfg client list」（P.A-5）および「adacfg client erase」（P.A-5）を参照してください。

ステップ 4　特定のクライアント デバイスに関する手順に従い、この AD Agent マシンを認識するようにクライアント デバイスを設定します。

APPENDIX A

Active Directory Agent コマンド リファレンス

この付録には、Active Directory Agent 固有のコマンドがアルファベット順に記載されています。コマンドには、次のモードがあります。

- adactrl：AD Agent の開始、停止、再起動と AD Agent の実行ステータスのモニタリングに使用されます。
- adacfg：Active Directory Agent でクライアント デバイス、Active Directory ドメイン コントローラ、および Syslog サーバと設定するために使用されます。

この付録では、コマンドごとに、その使用方法の簡単な説明、コマンドの構文、使用上のガイドライン、および使用例を示します。

この付録の構成は、次のとおりです。

AD Agent 制御コマンド

ここでは、次のコマンドについて説明します。

- **adactrl help**
- **adactrl restart**
- **adactrl show running**
- **adactrl start**
- **adactrl stop**
- **adactrl version**

（注） すべての adactrl コマンドでは大文字と小文字が区別されます。

adactrl help

adactrl コマンドとその構文のリストを表示します。

構文
adactrl help

例
```
C:¥IBF¥CLI>adactrl help
Cisco AD Agent adctrl -- version 1.0.0.32, build 539
    Usage: adactrl COMMAND
    where COMMAND can be:
        start        - to start the AD Agent
        stop         - to stop the AD Agent
        restart      - to restart the AD Agent
        show running - to show the running status of the AD Agent
        version      - to view info on AD Agent version currently installed
        help         - to view this help
```

adactrl restart

AD Agent を停止して再起動します。

構文
adactrl restart

例
```
C:¥IBF¥CLI>adactrl restart
OK
```

adactrl show running

AD Agent の内部コンポーネント（radiusServer および adObserver）のステータスを表示します。

構文
adactrl show running

例
```
C:¥IBF¥CLI>adactrl show running
running C:¥¥IBF¥¥watchdog¥¥radiusServer.bat since 2011- 1- 5 T10:25:44
running C:¥¥IBF¥¥watchdog¥¥adObserver.bat since 2011- 1- 5 T10:25:44
```

adactrl start

AD Agent を開始します。

構文
adactrl start

例

```
C:¥IBF¥CLI>adactrl start
OK
```

adactrl stop

AD Agent を停止します。

構文

adactrl stop

例

```
C:¥IBF¥CLI>adactrl stop
OK
```

adactrl version

Windows マシンにインストールされている AD Agent のバージョンを表示します。

構文

adactrl version

例

```
C:¥IBF¥CLI>adactrl version
Cisco AD Agent adactrl -- version 1.0.0.32, build 539
(Built from sources last modified 2011-04-21 12:20:17 +0300)
```

AD Agent コンフィギュレーション コマンド

ここでは、次のコマンドについて説明します。

- **adacfg help**
- **adacfg help client**
- **adacfg client create**
- **adacfg client erase**
- **adacfg client list**
- **adacfg client status**
- **adacfg help dc**
- **adacfg dc create**
- **adacfg dc erase**
- **adacfg dc list**
- **adacfg help cache**
- **adacfg cache list**
- **adacfg cache clear**

- adacfg help options
- adacfg options list
- adacfg options set
- adacfg help syslog
- adacfg syslog create
- adacfg syslog erase
- adacfg syslog list
- adacfg version

（注）　adacfg コマンドでは大文字と小文字が区別されません。

adacfg help

adacfg コマンド構文の概要情報を表示します。

構文
adacfg help

例
```
C:¥IBF¥CLI>adacfg help
Cisco AD Agent adacfg -- version 1.0.0.32, build 539
    Usage: adacfg [COMMAND]
    where COMMAND can be:
        client       - to manage client-devices of AD Agent
        dc           - to manage AD domain-controller machines monitored by AD Agent
        syslog       - to manage syslog-targets of AD Agent
        options      - to manage configurable settings for AD Agent
        cache        - to manage cache of identity-mappings maintained by AD Agent
        version      - to view info on AD Agent version currently installed
        help         - to view this help
        help COMMAND - to view the help for specified COMMAND
```

adacfg help client

クライアント関連 **adacfg** コマンドの詳細な構文の要約を表示します。

構文
adacfg help client

例
```
C:¥IBF¥CLI>adacfg help client
Cisco AD Agent adacfg -- version 1.0.0.32, build 539
    Usage:  adacfg client [SUBCOMMAND] [ARGS]
    where SUBCOMMAND can be:
            create  - to configure a new client
            list    - to list all previously configured clients
            erase   - to erase a previously configured client
            status  - to view status of clients subscribed for notification
```

```
        help    - to view this help
detailed syntax (write command on a single line!):
        adacfg client create -name <client-nickname>
                             -ip <IP-address>[/<prefix-length-for-IP-range>]
                             -secret <RADIUS-shared-secret>
        adacfg client list
        adacfg client erase -name <client-nickname>
        adacfg client status
```

adacfg client create

新しいクライアント デバイスを設定します。

構文

adacfg client create -name <*client-nickname*> **-ip** <*IP-address*>*[/*<*prefix-length-for-IP-range*>*]* **-secret** <*RADIUS-shared-secret*>

説明：

- *client-nickname*：クライアント デバイスに割り当てることができるフレンドリ名。
- *IP-address*：クライアント デバイスの IP アドレス。
- *prefix-length-for-IP-range*：オプションで IP サブネット範囲を定義できます。
- *RADIUS-shared-secret*：RADIUS プロトコルによりクライアント デバイスとの通信に使用される RADIUS 共有秘密。この *secret* は、クライアント デバイスで設定される鍵です。

例

```
C:¥IBF¥CLI>adacfg client create -name asa1 -ip 10.77.202.1/32 -secret cisco123
Reply: Command completed successfully!
```

adacfg client erase

以前に設定したクライアントを消去します。

構文

adacfg client erase -name <*client-nickname*>

client-nickname は、クライアント デバイスの名前です。

例

```
C:¥IBF¥CLI>adacfg client erase -name asa1
Reply: Command completed successfully!
```

adacfg client list

これまでに設定されたすべてのクライアント デバイスをリストします。

構文

adacfg client list

例

```
C:¥IBF¥CLI>adacfg client list
Name  IP/Range
----  ---------
asa1  10.77.204.2
asa2  10.77.101.3
asa3  10.77.101.4
```

adacfg client status

通知（通知要求も含む On-Demand クエリー、またはレプリケーション登録要求）登録されているクライアントの同期ステータスを表示します。

構文

adacfg client status

例

```
C:¥IBF¥CLI>adacfg client status
Subscribed-IP  Sync Status
-------------  ------------
10.77.101.2    In-Sync
10.77.101.3    Out-Of-Sync
10.77.101.4    Out-Of-Sync
10.77.101.5    In-Sync
```

adacfg help dc

DC 関連 **adacfg** コマンドの詳細な構文の要約を表示します。

構文

adacfg help dc

例

```
C:¥IBF¥CLI>adacfg help dc
Cisco AD Agent adacfg -- version 1.0.0.32, build 539
    Usage:  adacfg dc [SUBCOMMAND] [ARGS]
    where SUBCOMMAND can be:
            create  - to configure a new AD domain-controller machine
            list    - to list all previously configured AD domain-controller machines
            erase   - to erase a previously configured AD domain-controller machine
            help    - to view this help
    detailed syntax (write command on a single line!):
            adacfg dc create -name <DC-nickname>
                             -host <DC-hostname-or-FQDN>
                             -domain <full-DNS-name-of-AD-domain>
                             -user <username-member-of-Domain-Admins-group>
                             -password <password-of-user>
            adacfg dc list
            adacfg dc erase -name <DC-nickname>
```

adacfg dc create

新しい AD ドメイン コントローラ マシンを設定します。

構文

adacfg dc create -name <*DC-nickname*> **-host** <*DC-hostname-or-FQDN*> **-domain** <*full-DNS-name-of-AD-domain*> **-user** <*username-member-of-Domain-Admins-group*> **-password** <*password-of-user*>

説明：

- *DC-nickname*：Active Directory ドメイン コントローラの名前。
- *DC-hostname-or-FQDN*：AD ドメイン コントローラのホスト名、または Active Directory ドメイン コントローラの完全修飾ドメイン名（FQDN）。
- *full-DNS-name-of-AD-domain*：AD ドメインの完全 DNS 名。
- *username-member-of-Domain-Admins-group*：ドメイン コントローラ マシンのセキュリティ ログのモニタリングに使用される既存のアカウントのユーザ名。

  このアカウントにはドメイン コントローラ マシンのセキュリティ ログを読み取るために必要な権限が付与されている必要があります。「-domain」オプションに指定したドメインの AD グループ「Domain Admins」に属するアカウントを指定することで、容易かつ確実にこの操作を実行できます。

  あるいは、以下のすべての要件に対応していれば、「Domain Admins」グループに属さないメンバーでも必要な権限を取得できます。

  - アカウントが AD グループ「Distributed COM Users」に属している。
  - アカウントに、ドメイン コントローラ マシンの WMI 名前空間（特に「CIMV2」名前空間）へのアクセス権限が付与されている。この権限を設定するには、「wmimgmt.msc」スナップインを使用するか、またはグループ ポリシーを使用します（すべてのドメイン コントローラ マシンに反映する場合）。詳しくは、http://blogs.msdn.com/b/spatdsg/archive/2007/11/21/set-wmi-namespace-security-via-gpo-script.aspx を参照してください。
  - ドメイン コントローラ マシンのセキュリティ イベント ログを読み取る権限がアカウントに付与されている。この権限を設定するには、レジストリの CustomSD キーを使用するか、または Group Policy を使用します（すべてのドメイン コントローラ マシンに反映する場合）。詳しくは、http://msdn.microsoft.com/en-us/library/aa363648%28v=vs.85%29.aspx を参照してください。
- *password-of-user*：前述のユーザ名に対応するパスワード。

例

```
C:¥IBF¥CLI>adacfg dc create -name abc-dc1 -host amer.acs.com -domain acs.com -user xyz
-password axbycz
Warning: please make sure that this DC machine has:
  [1] all necessary patches installed, and
  [2] a properly configured Audit Policy.
  For more details, visit:
  http://www.cisco.com/en/US/docs/security/asa/asa84/release/notes/README_FIRST.html

Command completed successfully!
```

adacfg dc erase

以前に設定された AD ドメイン コントローラ マシンを消去します。

構文
adacfg dc erase -name <*DC-nickname*>

例
```
C:¥IBF¥CLI>adacfg dc erase -name abc-dc1
Reply: Command completed successfully!
```

adacfg dc list

これまでに設定されたすべての AD ドメイン コントローラ マシンをリストします。

構文
adacfg dc list

例
```
C:¥IBF¥CLI>adacfg dc list
C:¥IBF¥CLI>adacfg dc list
Name     Host/IP       Username     Domain-Name   Latest Status
----     -------       --------     -----------   -------------
abc-dc1  amer.acs.com  domainAdmin  ACS           up
abc-dc2  amer2.acs.com domainAdmin                down
abc-dc3  amer3.acs.com domainAdmin                down(no-retry)
```

adacfg help cache

キャッシュ関連 **adacfg** コマンドの詳細な構文の要約を表示します。

構文
adacfg help cache

例
```
C:¥IBF¥CLI>adacfg help cache
Cisco AD Agent adacfg -- version 1.0.0.32, build 539
    Usage:  adacfg cache [SUBCOMMAND]
    where SUBCOMMAND can be:
            list  - to view the currently cached mappings
            clear - to clear the currently cached mappings
            help  - to view this help
    detailed syntax:
            adacfg cache list
            adacfg cache clear
```

adacfg cache list

現在キャッシュされているマッピングを表示します。

構文
adacfg cache list

例

```
C:¥IBF¥CLI>adacfg cache list
IP           User-Name Domain Response-to-Probe Mapping-Type Mapping-Origin Create-Time
--           --------- ------ ----------------- ------------ -------------- -----------
10.77.100.1  User1     AD1    true              DC           AD1  2011-01-05T09:37:17Z
10.77.100.2  User2     AD1    true              DC           AD1  2011-01-05T09:37:21Z
```

adacfg cache clear

現在キャッシュされているマッピングをクリアします。

構文
adacfg cache clear

例

```
C:¥IBF¥CLI>adacfg cache clear
Removed 10 records.
```

（注） キャッシュ内部が完全にクリアされるまでお待ちください。キャッシュのクリアにかかる時間は、現在キャッシュされているマッピングの数によって異なります。

キャッシュ内のマッピングの数が非常に多い場合、完全にクリアするまでに約 1 分かかります。また、この処理の実行中に **adacfg cache list** コマンドを呼び出すと、マッピングがまだ存在していることが示される場合や、「データベースがロックされている」ことを示す SQL エラーが返される場合がありますが、このような結果は安全に無視できます。キャッシュ クリア操作が内部で完了した後で **adacfg cache list** コマンドを実行すると、「Total mappings count」が 0 として返されます。

adacfg help options

オプション関連 **adacfg** コマンドの詳細な構文の要約を表示します。

構文
adacfg help options

例

```
C:¥IBF¥CLI>adacfg help options
Cisco AD Agent adacfg -- version 1.0.0.32, build 539
    Usage:  adacfg options [SUBCOMMAND] [ARGS]
    where SUBCOMMAND can be:
            list - to view the current settings of the configurable options
            set  - to configure one or more of the configurable options
```

```
        help - to view this help
detailed syntax:
        adacfg options list
        adacfg options set [-<optionName> <optionValue>] [...]

      an <optionName>/<optionValue> pair can be:

        [-userLogonTTL <number-of-minutes>]
          Time duration after which logged-in user is marked as being logged-out.

        [-dcStatusTime <number-of-seconds>]
          Time span between consecutive monitorings of DC-machine up/down status.

        [-dcHistoryTime <number-of-seconds>]
          Amount of time before the present from which to start reading
          the security logs of DC-machines that are configured
          (via 'adacfg dc create') for the first time ever.

        [-notifyAttributes <text>]
          Comma-separated list of attributes to be sent in notifications to
          subscribed client-devices.

          Fully expanded list:
            domain,time-stamp,responds-to-probe,mapping-type,mapping-origin

          Wildcard equivalent to the fully expanded list:
            *

        [-logLevel <level>]
          Logging level for the customer logs (localStore and syslogs).

          Valid values: FATAL, ERROR, WARN, INFO, or DEBUG

          Default value: INFO
```

adacfg options list

設定オプションの現行設定値を表示します。

構文

adacfg options list

例

```
C:¥IBF¥CLI>adacfg options list
Option           Value
---------------  -----
userLogonTTL     1440
dcHistoryTime    86400
dcStatusTime     60
notifyAttributes *
logLevel         INFO
```

adacfg options set

1 つ以上の設定オプションを設定します。

構文

adacfg options set [-<optionName> <optionValue>] [...]

optionName と optionValue のペアには、次のいずれかまたはすべてを指定できます。

- **[userLogonTTL** <*number-of-minutes*>**]**：ログイン ユーザがログアウトしたものとしてマークされるまでの期間。
- **[dcStatusTime** <*number-of-seconds*>**]**：連続して行われる DC マシンのアップまたはダウン ステータスのモニタリングの間隔。
- **[dcHistoryTime** <*number-of-seconds*>**]**：「adacfg dc create」を使用して設定された DC マシンのセキュリティ ログを初めて読み取り開始する時点までの時間。
- **[notifyAttributes** <*text*>**]**：登録されているクライアント デバイスに送信される通知に指定される属性のコンマ区切りリスト。以下のいずれかまたはすべての属性を指定できます。
  - **domain、time-stamp、responds-to-probe、mapping-type、mapping-origin**
  - *（すべての属性に相当するワイルドカード）
- **[logLevel** <*level*>**]**：カスタマー ログ（localStore および Syslog）のログ レベル。有効な値は FATAL、ERROR、WARN、INFO、および DEBUG です。デフォルトのレベルは INFO です。

（注） AD Agent は、「NOTICE」ログ レベル（「INFO」と「WARN」の間のレベル）を使用して一部のカスタマー ログ メッセージを生成しますが、**adacfg options set -logLevel** コマンドを使用して「logLevel」の設定値として「NOTICE」を明示的に選択することはできません。詳細については、付録 B「カスタマー ログ メッセージ」を参照してください。

adacfg help syslog

Syslog 関連 **adacfg** コマンドの詳細な構文の要約を表示します。

構文

adacfg help syslog

例

```
C:¥IBF¥CLI>adacfg help syslog

Cisco AD Agent adacfg -- version 1.0.0.32, build 539
    Usage:  adacfg syslog [SUBCOMMAND] [ARGS]
    where SUBCOMMAND can be:
            create  - to configure a new syslog-target
            list    - to list all previously configured syslog-targets
            erase   - to erase a previously configured syslog-target
            help    - to view this help
    detailed syntax (write command on a single line!):
            adacfg syslog create -name <syslog-target-nickname>
                                 -ip <IP-address>
                                [-facility <syslog-facility>]
              valid syslog facility values:  LOCAL0 - LOCAL7
              default syslog facility value: LOCAL6
            adacfg syslog list
            adacfg syslog erase -name <syslog-target-nickname>
```

adacfg syslog create

新しい Syslog ターゲットを設定します。

構文

adacfg syslog create -name <*syslog-target-nickname*> **-ip** <*IP-address*> [**-facility** <*syslog-facility*>]

説明：

- *syslog-target-nickname*：Syslog サーバの名前。
- *IP-address*：Syslog サーバの IP アドレス。
- *syslog-facility*：ファシリティ値（LOCAL0 ～ LOCAL7）。デフォルトは LOCAL6 です。

例

```
C:¥IBF¥CLI>adacfg syslog create -name mysyslog -ip 10.77.202.1 -facility LOCAL6
Reply: Command completed successfully!
```

adacfg syslog erase

以前に設定された Syslog ターゲットを消去します。

構文

adacfg syslog erase -name <*syslog-target-nickname*>

syslog-target-nickname は AD Agent に接続している Syslog ターゲットの名前です。

例

```
C:¥IBF¥CLI>adacfg syslog erase -name mysyslog
Reply: Command completed successfully.
```

adacfg syslog list

これまでに設定されたすべての Syslog ターゲットをリストします。

構文

adacfg syslog list

例

```
C:¥IBF¥CLI>adacfg syslog list
Name      IP           Facility
-----     ---          ---------
mysyslog  10.77.202.4  LOCAL6
```

adacfg version

Windows マシンにインストールされている AD Agent のバージョンを表示します。

構文

adacfg version

例

```
C:¥IBF¥CLI>adacfg version
Cisco AD Agent adacfg -- version 1.0.0.32, build 539
<Built from sources last modified 2011-04-21 12:20:17 +0300>
```

APPENDIX **B**

カスタマー ログ メッセージ

この付録では、AD Agent により（「logLevel」設定オプションの現行値に基づいて）生成されるさまざまなカスタマー ログ メッセージを機能カテゴリ別に示します。

「logLevel」設定を変更するには、**adacfg options set –logLevel** コマンドを使用します。

（注） 一部のログ メッセージは「NOTICE」ログ レベル（「INFO」と「WARN」の間のレベル）に関連付けられていますが、前述の adacfg コマンドを使用して「logLevel」を設定する場合には「NOTICE」を選択できません。

次のスケールに、詳細度が低いものから順にログ レベルの範囲を示します。イタリック体で示されている「NOTICE」は「logLevel」で設定できるオプションではありません。太字で示されている「INFO」は、「logLevel」のデフォルト設定です。

FATAL < ERROR < WARN < *NOTICE* < **INFO** < DEBUG

（注） 問題のトラブルシューティングを行う際には、デフォルト設定値の「INFO」を詳細度が最も高い「DEBUG」に変更すると役立つことがよくあります。ただしこの設定では、AD Agent のパフォーマンスに悪影響を及ぼす可能性があります。問題が解決したら「logLevel」の設定を元に戻しておくことをお勧めします。

同様に、「logLevel」をデフォルト設定値の「INFO」を詳細度が最も低い「WARN」に変更すると、AD Agent のパフォーマンスに良い影響を及ぼすことがあります。ただしこの設定では「INFO」または「NOTICE」レベルのメッセージ（管理や監査の目的で重要である可能性があるメッセージ）が出力されません。

これまでのカスタマー ログ メッセージのローカル アーカイブは「C:¥IBF¥radiusServer¥runtime¥logs¥localStore」ディレクトリに保持されています。これらのログ メッセージは、**adacfg syslog create** コマンドを使用して設定されている任意のリモート Syslog ターゲットにも転送されます。

表 B-1 に、カスタマー ログに記録される AD Agent 固有のメッセージのメッセージ コード、ログ レベル、メッセージ クラス、メッセージ テキスト、説明を示します。このリストは生成されるすべてのメッセージが収録されているわけではありません。たとえば、汎用の RADIUS 関連メッセージなどのその他のメッセージは含まれていません。

表 B-1　AD Agent のログ メッセージ

メッセージ コード	ロギング レベル	メッセージ クラス	メッセージ テキスト	説明
AD Agent の開始と停止 （より広範囲な一連のメッセージが Windows Application Event Log に記録されています）。詳細については、付録 C「Windows アプリケーション イベント ログ」を参照してください。				
31502	INFO	STARTUP-SHUTDOWN	Started Runtime	AD Agent の「RADIUS サーバ」サブコンポーネントが開始されました。
設定変更				
68000	NOTICE	IBF_CONFIG_CHANGE	Created DC configuration	AD Agent で **adacfg dc create** コマンドを使用してドメイン コントローラ マシンが設定されました。
68001	NOTICE	IBF_CONFIG_CHANGE	Deleted DC configuration	AD Agent から **adacfg dc erase** コマンドを使用してドメイン コントローラ マシン設定が削除されました。
68002	NOTICE	IBF_CONFIG_CHANGE	Created RADIUS-client configuration	AD Agent で **adacfg client create** コマンドを使用してクライアント デバイスが設定されました。
68003	NOTICE	IBF_CONFIG_CHANGE	Deleted RADIUS-client configuration	**adacfg client erase** コマンドを使用してクライアント デバイス設定が AD Agent から削除されました。
マッピングの更新				
12862	INFO	IBF_RADIUS_SERVER	Updated mapping in Identity Cache	AD Agent の内部キャッシュで IP-address-to-user-identity マッピングが追加または更新されました。
12855	INFO	IBF_RADIUS_SERVER	Dropped Identity Cache mapping-update due to userLogonTTL	ログオン時刻が（「userLogonTTL」設定オプションを基準にして）かなり前であるため、着信 IP-address-to-user-identity マッピング更新が AD Agent により無視されました。
12856	INFO	IBF_RADIUS_SERVER	Dropped Identity Cache mapping-update: older than existing mapping	着信 IP-address-to-user-identity マッピング更新が AD Agent により無視されました。これは、関連付けられているログオン時刻が、AD Agent により現在キャッシュされている同じ IP アドレスのマッピングのものよりも古いためです。

表 B-1　AD Agent のログ メッセージ（続き）

メッセージ コード	ロギング レベル	メッセージ クラス	メッセージ テキスト	説明
12859	INFO	IBF_RADIUS_SERVER	Dropped Identity Cache mapping-update having timestamp in future	着信 IP-address-to-user-identity マッピング更新が AD Agent により無視されました。これは、関連付けられているログオン時刻が将来の時刻であるためです。
12861	INFO	IBF_RADIUS_SERVER	Dropped Identity Cache mapping-update: same time as existing mapping	着信 IP-address-to-user-identity マッピング更新が AD Agent により無視されました。これは、関連付けられているログオン時刻が、AD Agent により現在キャッシュされている同じ IP アドレスおよびユーザ名のマッピングのものと同一であるためです。
12867	WARN	IBF_RADIUS_SERVER	Approaching stress limit on Identity Cache mapping-updates	AD Agent で、キャッシュされているマッピングの数が最大収容制限数に近づいています。 現在 100,000 を超えるマッピングがキャッシュされています。キャッシュに入れられているマッピングの数が 200,000 に達すると、AD Agent は後続の着信マッピング更新を無視します。
12868	ERROR	IBF_RADIUS_SERVER	Dropped Identity Cache mapping-updates: stress limit exceeded	AD Agent のマッピングの最大収容制限数（200,000 マッピング）に達したため、新たな着信マッピング更新はすべて無視されます。
12893	INFO	IBF_RADIUS_SERVER	Deleted mapping in Identity Cache	AD Agent の内部キャッシュから IP-address-to-user-identity マッピングが削除されました。
同期要求				
12869	INFO	IBF_RADIUS_SERVER	Detected Synch request with registration for notifications	AD Agent のキャッシュに現在含まれているすべてのマッピングのセッション データ スナップショットを受信することをクライアント デバイスが要求しました。 クライアントは AD Agent へのレプリケーションのための登録を要求しています。
12860	INFO	IBF_RADIUS_SERVER	Detected Synch request with no registration for notifications	AD Agent のキャッシュに現在含まれているすべてのマッピングのセッション データ スナップショットを受信することをクライアント デバイスが要求しました。 クライアントは AD Agent へのレプリケーションのための登録を要求していません。

表 B-1　AD Agent のログ メッセージ（続き）

メッセージ コード	ロギング レベル	メッセージ クラス	メッセージ テキスト	説明
12870	INFO	IBF_RADIUS_SERVER	Detected Synch request without change to registration state	AD Agent のキャッシュに現在含まれているすべてのマッピングのセッション データ スナップショットを受信することをクライアント デバイスが要求しました。 クライアントは AD Agent でレプリケーション関連の状態を変更しません。
12871	INFO	IBF_RADIUS_SERVER	Detected deregistration Request	クライアント デバイスが AD Agent からのレプリケーション登録解除を要求しました。
12872	WARN	IBF_RADIUS_SERVER	Approaching capacity limit on max registrations	AD Agent で、一度に通知登録可能なユニーク クライアント デバイスの数の最大制限に近づいています。 現在 100 を超えるユニーク クライアント デバイスが通知登録されている可能性があります。ユニーク クライアント デバイスの数が 120 に達すると、AD Agent はそれ以降着信する通知登録要求を無視します。
12873	ERROR	IBF_RADIUS_SERVER	Dropped registrations: capacity limit exceeded	AD Agent で、一度に通知登録可能なユニーク クライアント デバイスの数が最大制限数である 120 に達したため、AD Agent は着信する新たな通知登録要求をすべて無視します。
CoA-Based トラフィック				
12884	INFO	IBF_RADIUS_SERVER	Sent RADIUS CoA-Request with Notification to PEP	AD Agent は、クライアント デバイスに提供された時点以降に変更されたマッピングについてクライアント デバイスに事前に通知します。 クライアント デバイスへのこの通知更新は、RADIUS CoA-Request パケットを使用して送信されました。
11223	INFO	Dynamic-Authorization	Received CoA ACK response	AD Agent が、クライアント デバイスから送信された RADIUS CoA-ACK パケットを受信しました。クライアント デバイスは、AD Agent によって送信された CoA-Request パケットの受信を確認しました。
11224	INFO	Dynamic-Authorization	Received CoA NAK response	AD Agent が、クライアント デバイスから送信された RADIUS CoA-NAK パケットを受信しました。クライアント デバイスは、AD Agent により送信された CoA-Request パケットに関する問題を確認しました。

表 B-1　AD Agent のログ メッセージ（続き）

メッセージ コード	ロギング レベル	メッセージ クラス	メッセージ テキスト	説明
セッション データ スナップショットの転送				
12878	INFO	IBF_RADIUS_SERVER	Stopping current transfer of session data snapshot	現在進行中のクライアント デバイスへのセッション データ スナップショットの転送を停止しています。
12881	INFO	IBF_RADIUS_SERVER	Started transfer of session data snapshot	クライアント デバイスへのセッション データ スナップショットの転送が新たに開始されました。 **（注）** このログ項目は、2 つ以上の RADIUS パケットを使用するスナップショット転送のみに使用されます。1 番目のパケットは #12881 でマーキングされます。最後のパケットは #12883 でマーキングされます。この間のパケットはすべて #12882 でマーキングされます。
12882	INFO	IBF_RADIUS_SERVER	Continued transfer of session data snapshot	現在進行中のクライアント デバイスへのセッション データ スナップショットの転送が続行します。 **（注）** このログ項目は、3 つ以上の RADIUS パケットを使用する大規模スナップショット転送のみに使用されます。1 番目のパケットは #12881 でマーキングされ、最後のパケットは #12883 でマーキングされます。この間のすべてのパケットは #12882 でマーキングされます。
12883	INFO	IBF_RADIUS_SERVER	Finished transfer of session data snapshot	クライアント デバイスへのセッション データ スナップショットの転送が正常に完了しました。 1 つの RADIUS パケットに収まる非常に小規模なスナップショット転送はこのログ項目のみでマーキングされますが、#12881 または #12882 ログ項目はマーキングされません。
On-Demand クエリー				
12864	INFO	IBF_RADIUS_SERVER	Detected On-Demand Entity-Request from PEP	クライアント デバイスが特定の IP アドレスのマッピングの受信を要求しました（後続通知要求を含んでいる場合と含んでいない場合があります）。

表 B-1　AD Agent のログ メッセージ（続き）

メッセージ コード	ロギング レベル	メッセージ クラス	メッセージ テキスト	説明
12866	INFO	IBF_RADIUS_SERVER	Could not find identity in Identity Cache	AD Agent が、要求された IP アドレスが含まれているマッピングをキャッシュで見つけることができませんでした。
キープアライブ要求				
12885	INFO	IBF_RADIUS_SERVER	Detected Keepalive Request from PEP	クライアント デバイスがキープアライブ要求を AD Agent に送信しました。
ドメイン ステータス クエリー				
12890	INFO	IBF_RADIUS_SERVER	Prepared Domain Status Query-Response	AD Agent の準備が完了し、特定の Active Directory ドメインに関する AD Agent の接続ステータスを要求したクライアント デバイスに対して応答を送信できる状態にあります。
ドメイン コントローラ ステータスのトラッキング				
12892	INFO	IBF_AD_MONITOR	ActiveDirectory domain controller status changed	AD Agent がドメイン コントローラ マシンのアップまたはダウン ステータスの変更を検出しました。
その他				
12888	WARN	IBF_RADIUS_SERVER	Internal Warning	AD Agent で内部の問題が発生しました。
12889	ERROR	IBF_RADIUS_SERVER	Internal Error	AD Agent で内部の問題が発生しました。
汎用 Pass/Fail ステータス （このような各ログ エントリは、関連付けられている [IbfSessionID] 属性の値が同一である対応エントリを示します）				
5200	NOTICE	Passed-Attempt	IBF request succeeded	AD Agent は、クライアント デバイスから以前に受信した要求（同期要求、オンデマンド クエリー、キープアライブ要求、ドメイン ステータス クエリー）を正常に処理できました。
5400	NOTICE	Failed-Attempt	IBF request failed	AD Agent クライアント デバイスから以前に受信した要求（同期要求、オンデマンド クエリー、キープアライブ要求、ドメイン ステータス クエリー）を正常に処理できませんでした。これは、[FailureReason] 属性の値に示されている理由が原因です。 この [Failed-Attempt] ログ エントリまたはその他の同様の（汎用）[Failed-Attempt] ログ エントリの [FailureReason] のコードを、この表の次のサブセクションに示します。

表 B-1　AD Agent のログ メッセージ（続き）

メッセージ コード	ロギング レベル	メッセージ クラス	メッセージ テキスト	説明
5405	NOTICE	Failed-Attempt	RADIUS Request dropped	AD Agent は RADIUS パケットを受信しましたが、[FailureReason] 属性の値に示されている理由が原因で、このパケットをサイレントにドロップしました。 この [Failed-Attempt] ログ エントリまたはその他の同様の（汎用）[Failed-Attempt] ログ エントリの [FailureReason] のコードを、この表の次のサブセクションに示します。
5413	NOTICE	Failed-Attempt	RADIUS Accounting-Request dropped	AD Agent は RADIUS Accounting-Request パケットを受信しましたが、[FailureReason] 属性の値に示されている理由が原因で、このパケットをサイレントにドロップしました。 この [Failed-Attempt] ログ エントリまたはその他の同様の（汎用）[Failed-Attempt] ログ エントリの [FailureReason] のコードを、この表の次のサブセクションに示します。

[FailureReason] のメッセージ

（[Failed-Attempt] ログ エントリに示されているがこの表のこのサブセクションにない [FailureReason] コードは、AD Agent 内部エラーとして扱ってください）

11007	DEBUG	RADIUS	Could not locate Network Device or AAA Client	現在設定されているどのクライアント デバイスにも関連付けられていない IP アドレスから RADIUS パケットを受信しました。「adacfg client create」を使用してこのデバイスが設定されていることを確認してください。
11011	WARN	RADIUS	RADIUS listener failed	RADIUS 要求の受信に使用する 1 つ以上の UDP ポートを開くことができませんでした。AD Agent マシンでその他のプロセスがポート 1812、1813、1645、または 1646 を使用していないことを確認してください。
11012	ERROR	RADIUS	RADIUS packet contains invalid header	無効なヘッダーが含まれている RADIUS パケットを受信しました。クライアント デバイスに AD Agent との互換性があり、適切に機能していることを確認してください。
11013	INFO	RADIUS	RADIUS packet already in the process	着信 RADIUS 要求が AD Agent により無視されました。これは、この要求が、以前受信して現在処理中の別のパケットと重複しているためです。

表 B-1　AD Agent のログ メッセージ（続き）

メッセージ コード	ロギング レベル	メッセージ クラス	メッセージ テキスト	説明
11014	ERROR	RADIUS	RADIUS packet contains invalid attribute(s)	無効な属性が含まれている RADIUS パケットを受信しました。クライアント デバイスに AD Agent との互換性があり、適切に設定されており、適切に機能していることを確認してください。
11021	ERROR	RADIUS	RADIUS could not decipher password.packet missing necessary attributes	暗号化できないパスワードが含まれている RADIUS パケットを受信しました。クライアント デバイスに AD Agent との互換性があり、適切に設定されており、適切に機能していることを確認してください。クライアント デバイスと AD Agent の両方で同じ RADIUS 共有秘密が適切に設定されていることを確認してください。
11029	WARN	RADIUS	Unsupported RADIUS packet type	無効なパケット タイプが含まれている RADIUS パケットを受信しました。クライアント デバイスに AD Agent との互換性があり、適切に設定されており、適切に機能していることを確認してください。
11030	WARN	RADIUS	Pre-parsing of the RADIUS packet failed	無効な RADIUS パケットを受信しました。クライアント デバイスに AD Agent との互換性があり、適切に設定されており、適切に機能していることを確認してください。
11031	WARN	RADIUS	RADIUS packet type is not a valid Request	RADIUS 要求パケットが予期されているときに RADIUS 応答パケットを受信しました。クライアント デバイスに AD Agent との互換性があり、適切に設定されており、適切に機能していることを確認してください。
11036	ERROR	RADIUS	The Message-Authenticator RADIUS attribute is invalid.	無効な [Message-Authenticator] 属性が含まれている RADIUS パケットを受信しました。クライアント デバイスに AD Agent との互換性があり、適切に設定されており、適切に機能していることを確認してください。クライアント デバイスと AD Agent の両方で同じ RADIUS 共有秘密が適切に設定されていることを確認してください。
11037	ERROR	RADIUS	Dropped accounting request received via unsupported port.	サポートされていない UDP ポート番号で RADIUS Accounting-Request パケットを受信しました。クライアント デバイスに AD Agent との互換性があり、適切に設定されており、適切に機能していることを確認してください。

表 B-1　AD Agent のログ メッセージ（続き）

メッセージ コード	ロギング レベル	メッセージ クラス	メッセージ テキスト	説明
11038	ERROR	RADIUS	RADIUS Accounting-Request header contains invalid Authenticator field.	パケット ヘッダーに無効な [Authenticator] フィールドが含まれている RADIUS Accounting-Request パケットを受信しました。クライアント デバイスに AD Agent との互換性があり、適切に設定されており、適切に機能していることを確認してください。クライアント デバイスと AD Agent の両方で同じ RADIUS 共有秘密が適切に設定されていることを確認してください。
11039	INFO	RADIUS	RADIUS authentication request rejected due to critical logging error	内部ログ関連エラーが検出されました。十分な空きディスク容量がないことが原因である可能性があります。
11040	INFO	RADIUS	RADIUS accounting request dropped due to critical logging error.	内部ログ関連エラーが検出されました。十分な空きディスク容量がないことが原因である可能性があります。
11050	WARN	RADIUS	RADIUS request dropped due to system overload	内部ログ関連エラーが検出されました。十分な空きディスク容量がないことが原因である可能性があります。
11052	ERROR	RADIUS	Authentication request dropped due to unsupported port number	サポートされていない UDP ポート番号で RADIUS 要求パケットを受信しました。クライアント デバイスに AD Agent との互換性があり、適切に設定されており、適切に機能していることを確認してください。
11053	WARN	RADIUS	Invalid attributes in outgoing radius packet - possibly some attributes exceeded their size limit	内部が原因で発信 RADIUS 応答パケットが無効になっています。これは、パケット全体のサイズ、またはパケットの 1 つの関連属性のサイズが最大制限を超えたことが原因である可能性があります。
11103	ERROR	RADIUS-Client	RADIUS-Client encountered error during processing flow	着信 RADIUS パケットの処理中に内部エラーが検出されました。クライアント デバイスに AD Agent との互換性があり、適切に設定されており、適切に機能していることを確認してください。クライアント デバイスと AD Agent の両方で同じ RADIUS 共有秘密が適切に設定されていることを確認してください。

表 B-1　AD Agent のログ メッセージ（続き）

メッセージ コード	ロギング レベル	メッセージ クラス	メッセージ テキスト	説明
11213	WARN	Dynamic-Authorization	No response received from Network Access Device: lost communication with notification subscriber	AD Agent が以前に CoA-Request パケットを送信したデバイス クライアントから、確認パケット（肯定または否定）を受信しませんでした。 AD Agent はこのクライアント デバイスとの通信が失われたものと想定し、ステータスを「Out-Of-Sync」に設定します。
11214	WARN	Dynamic-Authorization	An invalid response received from Network Access Device: lost communication with notification subscriber	AD Agent が以前に CoA-Request パケットを送信したデバイス クライアントから無効な応答を受信しました。 AD Agent はこのクライアント デバイスとの通信が失われたものと想定し、ステータスを「Out-Of-Sync」に設定します。
32006	WARN	Logging	Could not log to critical logger	内部ログ関連エラーが検出されました。十分な空きディスク容量がないことが原因である可能性があります。
32016	FATAL	Logging	System reached low disk space limit	十分な空きディスク容量がありません。

APPENDIX C

Windows アプリケーション イベント ログ

この付録では、次に示す状況で AD Agent ソフトウェアが（カスタマー ログ メッセージに加えて）Windows アプリケーション イベント ログに記録するイベントの要約を示します。

- AD Agent ソフトウェアのインストール、アンインストール、および AD Agent マシンのリブートに伴い、AD Agent 自体（実際には内部の「ウォッチドッグ」機能）が開始または停止された。
- AD Agent の内部「AD Observer」および「RADIUS サーバ」コンポーネントが **adactrl** コマンドを使用して手動で開始または停止された。
- AD Agent ソフトウェアのウォッチドッグ機能によりこれらのプロセスの 1 つ以上でクラッシュまたは重大なエラーが検出された後で、AD Agent の内部「AD Observer」および「RADIUS サーバ」コンポーネントが自動的に停止または再起動された。

Windows でこれらのイベントを確認するには、次の場所にある「Event Viewer」ツールを使用します。

[Event Viewer (Local)] > [Applications and Services Log] > [Cisco AD Agent]

これらすべてのイベントには次の属性と値が設定されています。

- Source：Cisco AD Agent
- Level：Information
- Task Category：None

表 C-1 に、これらのイベントのイベント ID、メッセージ テキスト、説明を示します。

表 C-1　Windows アプリケーション イベント ログ

イベント ID	メッセージ テキスト	説明
10	Watchdog Service Was Started	AD Agent の内部ウォッチドッグ サービスが開始しました。 通常、このメッセージは AD Agent のインストール直後、または AD Agent マシンのリブート後に表示されます。
11	Watchdog Service Was Shutdown	AD Agent の内部ウォッチドッグ サービスが停止しました。 通常、このメッセージは AD Agent のアンインストール時に表示されます。また、[Windows Services] パネルで Cisco AD Agent を手動で停止または再起動した場合にも表示されることがあります。
20	C:¥¥IBF¥¥watchdog¥¥radiusServer.bat Was Started	AD Agent の「RADIUS サーバ」サブコンポーネントが（**adactrl** コマンドを使用して）手動で開始されたか、または（クラッシュまたは障害発生後に）自動的に再起動されました。
20	C:¥¥IBF¥¥watchdog¥¥adObserver.bat Was Started	AD Agent の「AD Observer」サブコンポーネントが（**adactrl** コマンドを使用して）手動で開始されているか、または（クラッシュまたは障害発生後に）自動的に再起動されました。
21	C:¥¥IBF¥¥watchdog¥¥radiusServer.bat Was Shutdown	AD Agent の「RADIUS サーバ」サブコンポーネントがクラッシュしたか、または障害の検出後に停止しました。
21	C:¥¥IBF¥¥watchdog¥¥adObserver.bat Was Shutdown	AD Agent の「AD Observer」サブコンポーネントがクラッシュしたか、または障害の検出後に停止しました。
21	rt_daemon.exe Was Shutdown	AD Agent の「RADIUS サーバ」サブコンポーネントが（**adactrl** コマンドを使用して）手動で停止されました。
21	ADObserver.exe Was Shutdown	AD Agent の「AD Observer」サブコンポーネントが（**adactrl** コマンドを使用して）手動で停止されました。
22	C:¥¥IBF¥¥watchdog¥¥radiusServer.bat Failed To Start	AD Agent の「RADIUS サーバ」サブコンポーネントが適切に開始できませんでした。
22	C:¥¥IBF¥¥watchdog¥¥adObserver.bat Failed To Start	AD Agent の「AD Observer」サブコンポーネントが適切に開始できませんでした。

APPENDIX D

Active Directory Agent の問題のトラブルシューティング

この付録は、AD Agent の使用中に発生する可能性がある問題を特定および解決する際に役立つ情報を収録しています。この付録の構成は、次のとおりです。

トラブルシューティング情報の取得

トラブルシューティング情報は、AD Agent により生成される正式なカスタマー ログから取得できます。これらのログは AD Agent マシンのディレクトリ **C:¥IBF¥radiusServer¥runtime¥logs¥localStore** にあります。

また、AD Agent のカスタマー ログを Syslog サーバに送信することもできます。これらのログを受信するように Syslog サーバを設定する方法については、「AD Agent での Syslog サーバへのログ送信の設定」（P.2-9）を参照してください。

adacfg options set -logLevel コマンドを使用して、localStore と Syslog の両方のカスタマー ログでの詳細レベルを制御できます。

関連するカスタマー ログ メッセージのリストについては、付録 B「カスタマー ログ メッセージ」を参照してください。

デフォルトでは、ログ レベルは INFO に設定され、情報メッセージのみが報告されます。特定の問題のトラブルシューティングを行う場合は、追加情報を取得するためにこのログ レベルを変更することができます。ログ レベルの有効なオプションを詳細度の高いものから順に示します。

- DEBUG
- INFO
- WARN
- ERROR
- FATAL

このコマンドの詳細については、「adacfg options set」（P.A-11）を参照してください。

トラブルシューティングに役立つ情報源として、カスタマー ログの他に Windows アプリケーション イベント ログがあります。このログは、Windows Event Viewer ツール（[Event Viewer (Local)] > [Applications and Services Log] > [Cisco AD Agent]）を使用して表示できます。このツールは AD

Agent ソフトウェア、内部プロセス「AD Observer」および「RADIUS サーバ」の開始イベントと停止イベントを記録します。詳細については、付録 C「Windows アプリケーション イベント ログ」を参照してください。

問題の報告時に、AD Agent マシンで内部デバッグ ログを有効にするかどうか、およびカスタマー ログとともにこれらのログを送信するかどうかが尋ねられます。これらのログは問題を診断および解決する際に役立ちます。これらの内部デバッグ ログを有効にするには、「AD Agent での内部デバッグ ログの有効化」（P.D-2）を参照してください。

AD Agent での内部デバッグ ログの有効化

高度なトラブルシューティングのために、次の 2 種類の内部デバッグ ログを有効化できます。

- 「AD Observer ログ」（P.D-2）
- 「RADIUS サーバ ログ」（P.D-3）

AD Observer ログ

「C:¥IBF¥adObserver¥logconfig.ini」ファイルに、AD Observer サブコンポーネントの内部デバッグ ログ レベルが指定されています。デフォルトでは LOG_LEVEL は LOG_NONE に設定されています。この設定では、AD Observer サブコンポーネントの内部デバッグ ログは生成されません。

LOG_LEVEL には次の値のいずれかを指定できます。

- LOG_VERBOSE：最も詳細なログ。
- LOG_DEBUG：トラブルシューティングおよびデバッグ情報が含まれます。
- LOG_INFO：情報メッセージが含まれます。
- LOG_WARN：警告メッセージが含まれます。
- LOG_ERROR：エラー メッセージが含まれます。
- LOG_FATAL：重大なエラー メッセージのみが含まれます。

ログ レベルは LOG_VERBOSE（最も情報が多い）から LOG_FATAL（最も情報が少ない）までで、この順にレベルが低くなります。トラブルシューティング情報を取得するため、LOG_DEBUG を選択することをお勧めします。

AD Observer 内部デバッグ ログを有効にするには、次の手順を実行します。

ステップ 1　AD Agent マシンで **C:¥IBF¥adObserver** ディレクトリに移動します。

ステップ 2　[Notepad] などの任意のテキスト エディタで **logconfig.ini** ファイルを開きます。

ステップ 3　このコンフィギュレーション ファイルの最後のセンテンスを次のように変更します。

LOG_LEVEL=LOG_VERBOSE

ステップ 4　**logconfig.ini** ファイルを保存します。

ステップ 5　この変更を反映するため、**adactrl restart** コマンドを使用して AD Agent を再起動します。

これで、AD Observer 内部デバッグ ログが有効化されました。AD Agent により ADObserverLog.txt ファイルが **C:¥IBF¥adObserver** ディレクトリに生成されます。

（注）　AD Observer サブコンポーネントの内部デバッグ メカニズムの「LOG_LEVEL」設定は、**adacfg options set** コマンドの -logLevel 設定オプションとは関係ありません。

RADIUS サーバ ログ

RADIUS サーバ実行時デバッグ ログ コンフィギュレーション ファイルでは、さまざまな RADIUS サーバ サブコンポーネントの内部デバッグ ロギングを有効または無効にできます。このファイルの場所は **C:¥IBF¥radiusServer¥runtime¥win32¥config¥RuntimeDebugLog.config** です。

デフォルトでは、すべてのサブコンポーネントでデバッグ ロギングが無効です。

このコンフィギュレーション ファイルでは、デバッグ ロギングをオフまたはオンにできる RADIUS サーバ サブコンポーネントが次の形式のセンテンスにリストされます。

#components.[Acs.RT.]*variable*=off

variable には次のサブコンポーネントのいずれかを指定できます。

- ConfigVersionManager
- ConfigManager.XmlManager
- Statistics
- ConfigManager
- Logging
- Dictionary
- MessageCatalog.CatalogRepository
- Crypto.CRLHttpWorker
- EventHandler
- EventHandler.EventDispatchTable

RADIUS サーバ サブコンポーネントの内部デバッグ ロギングを有効にするには、次の手順を実行します。

ステップ 1　AD Agent マシンで **C:¥IBF¥radiusServer¥runtime¥win32¥config** に移動します。

ステップ 2　任意のテキスト エディタ（WordPad など）で **RuntimeDebugLog.config** ファイルを開きます。

ステップ 3　このコンフィギュレーション ファイルで、デバッグ ログを有効にする RADIUS サーバ サブコンポーネントをリストする行の終わりにある単語 **off** を **on** に置き換えます。

デバッグ ログを有効にするすべてのサブコンポーネントについて、単語 **off** を **on** に置き換えます。

（注）　この値では大文字と小文字が区別されます。単語 **off** と **on** には小文字を使用してください。

ステップ 4　**RuntimeDebugLog.config** ファイルを保存します。

AD Agent により RADIUS サーバ コンフィギュレーション ファイルの変更が自動的に検出され、RADIUS サーバ デバッグ ログが有効になります。これらのログは次の場所にあります。

C:¥IBF¥radiusServer¥runtime¥logs¥radiusServer_debug.log

設定の問題

このセクションでは、よく見られる設定の問題について説明します。ここでは、次の項目について説明します。

クライアント デバイスからの要求が無視される

症状または問題	クライアント デバイスからの要求が AD Agent マシンに到達していないか、無視されている可能性があります。
考えられる原因	1. AD Agent と通信するようにクライアント デバイスが適切に設定されていない可能性があります。 2. Windows ファイアウォールによって RADIUS トラフィックがブロックされている可能性があります。 3. AD Agent マシンで **adacfg client create** コマンドを使用してクライアント デバイスを設定したときに入力された RADIUS 共有秘密が誤っています。
解決策	1. クライアント デバイスが、AD Agent マシンと通信するように適切に設定されていることを確認します。 2. Windows ファイアウォールまたは類似のファイアウォール ソフトウェアが実行されている場合は、「接続要件」（P.2-2）で説明するように必要なファイアウォール例外が設定されていることを確認します。 3. カスタマー ログ（localStore または Syslog）を調べ、無効な [RADIUS Authenticator] フィールドまたは [Message-Authenticator] 属性を示すログ メッセージが記録されているかどうかを確認します。このようなメッセージが検出された場合は、クライアント デバイスと AD Agent の両方が、同じ RADIUS 共有秘密を使用するように正しく設定されていることを確認します。

adacfg client status コマンドによりクライアント デバイスが「Out-of-Sync」であると報告されるが、原因が不明である

症状または問題	AD Agent マシンが RADIUS CoA-Request によって通知更新をクライアント デバイスに送信した後、クライアント デバイスから CoA-ACK を受信しません。
考えられる原因	1. クライアント デバイスが現在ダウンしているか、または適切に設定されていないことが原因で RADIUS CoA-ACK を送信しなかった可能性があります。 2. Windows ファイアウォールによって RADIUS トラフィックがブロックされている可能性があります。 3. クライアント デバイスが CoA-ACK を送信するが、RADIUS 共有秘密が誤っているために AD Agent マシンがこの要求をドロップしている可能性があります。
解決策	1. クライアント デバイスが現在アップしており、AD Agent マシンと通信するように適切に設定されていることを確認します。 2. Windows ファイアウォールまたは類似のファイアウォール ソフトウェアが実行されている場合は、「接続要件」（P.2-2）で説明するように必要なファイアウォール例外が設定されていることを確認します。 3. カスタマー ログ（localStore または Syslog）を調べ、無効な [RADIUS Authenticator] フィールドまたは [Message-Authenticator] 属性を示すログ メッセージが記録されているかどうかを確認します。このようなメッセージが検出された場合は、クライアント デバイスと AD Agent の両方が、同じ RADIUS 共有秘密を使用するように正しく設定されていることを確認します。

IP-to-user-identity マッピングが短期間で AD Agent キャッシュから消去される

症状または問題	IP-to-user-identity マッピングが AD Agent キャッシュから短期間で消去されます。
考えられる原因	**adacfg options set** コマンドの「userLogonTTL」設定オプションの現行設定に対応する期間が短すぎます。
解決策	ユーザ ログオン TTL の期間を長く設定してください。詳細については、「adacfg options set」（P.A-11）を参照してください。

特定の DC マシンにより認証されたユーザ ログオンが AD Agent により検出（および処理）されない

症状または問題	特定の DC マシンにより認証されたユーザ ログオンが AD Agent により検出（および処理）されません。
考えられる原因	**1.** 特定の DC マシンにパッチが適切に適用されていない可能性があります。これが原因で、認証イベントがセキュリティ ログに書き込まれないことがあります。 **2.** その DC マシンの監査ポリシーが適切に設定されていない可能性があります。 **3.** AD Agent がマッピング更新を検出したが、（カスタマー ログに記録されている）何らかの理由によりこの更新をドロップした可能性があります。考えられる原因の 1 つとして、「マッピング更新に将来のタイムスタンプが含まれている」ことがあります。これは、DC マシンのクロックが AD Agent マシンのクロックよりも 10 分を超えて進んでいる場合に発生します。
解決策	**1.** 特定の DC マシンにパッチが正しく適用されていることを確認します。 **2.** 特定の DC マシンの監査ポリシーが正しく設定されていることを確認します。 **3.** AD Agent マシンの localStore リポジトリ（または Syslog）を使用して、AD Agent マシンが対応するマッピング更新を受信し、どのような理由でもドロップしないようにします。 AD Agent マシンが何らかの理由でマッピング更新をドロップする場合は、この問題が訂正されていることを確認します。たとえば、マッピング更新に「将来のタイムスタンプ」が含まれている場合は、DC マシンのクロックと AD Agent マシンのクロックが適切に同期されているようにします。

adacfg dc list コマンドを実行すると、ドメイン コントローラ マシンが「up」状態に達していないことが示される

症状または問題	**adacfg dc list** コマンドを実行すると、ドメイン コントローラ マシンが「up」状態になっていないことが示されます。
考えられる原因	**1.** ドメイン コントローラ マシンでサポートされているバージョンの Windows Server が実行されていない可能性があります。 **2.** ドメイン コントローラにパッチが正しく適用されていない可能性があります。 **3.** Windows ファイアウォールまたは類似のファイアウォール ソフトウェアにより、ドメイン コントローラ マシンと AD Agent マシンの間の WMI トラフィックがブロックされている可能性があります。 **4.** AD Agent マシンが AD ドメインに参加していないか、ドメイン コントローラ マシンの AD ドメインと AD Agent マシンが参加している AD ドメインの間に適切な信頼関係が設定されていない可能性があります。 **5.** adacfg dc create コマンドに入力された値が誤っている可能性があります。特に、ドメインの完全 DNS 名が入力されていないか、アカウント クレデンシャルが誤っているか、ドメイン コントローラ マシンのセキュリティ ログを読み取るための十分な特権がアカウントに付与されていない可能性があります。
解決策	**1.** ドメイン コントローラ マシンで実行されている Windows Server のバージョンがサポートされているバージョンであり、Windows Server にパッチが適切に適用されていることを確認してください。 **2.** Windows ファイアウォールまたは類似のファイアウォール ソフトウェアが実行されている場合は、必要な WMI 例外が適切に設定されていることを確認します。 **3.** ドメイン コントローラ マシンの AD ドメインとの適切な信頼関係が設定されている AD ドメインに AD Agent マシンが参加していることを確認します。 **4.** adacfg dc create コマンドに入力した値が正しいことを確認します。特に、ドメインの完全 DNS 名を指定しており、ドメイン コントローラ マシンのセキュリティ ログを読み取るための十分な特権が付与されているアカウントのクレデンシャルを指定していることを確認します。 **5.** 必要に応じて AD Observer サブコンポーネントの内部デバッグ ログを有効にし、以下の内容が含まれているかどうかを確認します。 – The RPC server is unavailable (0x800706ba)：このメッセージが含まれている場合、ドメイン コントローラ マシンがダウンしているか、または必要な例外を設定せずにファイアウォールを使用しているために通信がブロックされている可能性があります。 – Access is Denied (0x80070005)：このメッセージが含まれている場合は、指定されたアカウントに、ドメイン コントローラ マシンのセキュリティ ログを読み取るための十分な特権がないか、またはクレデンシャルが誤っている可能性があります。

AD Agent がまったく機能しない

症状または問題	AD Agent がまったく機能せず、各種 CLI コマンドを入力すると、エラー メッセージ「`Couldn't connect to server!`」が常に表示されます。
考えられる原因	一部のアンチウィルス ソフトウェア プログラムでは、cygwin1.dll が仮想化関連の脅威としてブロックされることが判明しています。ただし、この報告は誤検知として扱われる必要があります。AD Agent にはマルウェアは含まれていません。
解決策	1. AD Agent インストーラ実行ファイルを実行した後で、アンチウィルス ソフトウェアのログを調べ、C:¥IBF¥radiusServer¥cygwin¥bin¥cygwin1.dll（または C:¥IBF フォルダ内のその他のアイテム）が潜在的な脅威としてブロックされているかどうかを確認します。 2. このような AD Agent サブコンポーネントがブロックされている場合は、サブコンポーネントをブロックせずに実行することを明示的に許可するようにアンチウィルス ソフトウェアを設定します。

「adacfg dc list」コマンドを実行すると、ドメイン コントローラ マシンが「down(no-retry)」状態に達したことが示される

症状または問題	**adacfg dc list** コマンドを実行すると、ドメイン コントローラ マシンが「down(no-retry)」状態に達したことが示されます。
考えられる原因	ドメイン コントローラ マシンにパッチが適切に適用されていないため、このドメイン コントローラ マシンの WMI サービスが応答していない可能性があります。
解決策	1. ドメイン コントローラ マシンにパッチが正しく適用されていることを確認します。 2. ドメイン コントローラ マシンの WMI サービスを再起動してください。 3. AD Agent の接続を強制的に再試行するには、次のいずれかを行います。 – ドメイン コントローラ設定を削除してから、**adacfg dc create** コマンドを使用して再作成します。 – **adactrl restart** コマンドを使用して AD Agent を再起動します。

AD Agent マシンをリブートするとログオンが失敗する

症状または問題	AD Agent をリブートすると次のエラーが発生します。 `Windows could not start the Cisco AD Agent service on Local Computer. ERROR 1069: The service did not start due to a logon failure`

考えられる原因	AD Agent が（同じ AD ドメインの）複数のドメイン コントローラ マシンに直接インストールされている可能性があります。
	この場合、AD Agent のインストール中に次のメッセージを示すダイアログ ボックスが表示されます。
	`'IBF_SERVICE_USER' account already exists. OK to recreate? (Pressing 'No' will abort the installation.)`
	`WARNING: Make sure you are NOT attempting to install AD Agent directly on more than one DC machine (for the same AD domain)!`
	[Yes] を選択したことで、この問題が発生します。

解決策	**1.** ドメインに作成された非ローカル アカウント「IBF_SERVICE_USER」のパスワードとして、既知の値を手動で設定します。 **2.** AD Agent がインストールされている各ドメイン コントローラ マシンで、新しいパスワードを使用するように「Services」パネルの「Cisco AD Agent」項目を手動で変更してから、このサービスを再起動するか、またはドメイン コントローラ マシンをリブートします。