CHAPTER 2

Cisco Context Directory Agent のインストール

Cisco Context Directory Agent（CDA）は、ISO イメージとしてパッケージ化されているソフトウェア アプリケーションです。Cisco.com からダウンロードできます。これは、VMware ESX サーバ上の専用 X86 マシンまたは仮想マシンにインストールし、クライアント デバイスと Active Directory ドメイン コントローラで設定する必要があります。

この章の内容は、次のとおりです。

- 「要件」（P.2-1）
- 「Context Directory Agent のインストール」（P.2-12）
- 「Cisco AD Agent から Cisco CDA へのマイグレーション」（P.2-15）

要件

ここでは、次の項目について説明します。

- 「サポートされるオペレーティング システム」（P.2-1）
- 「ハードウェア要件」（P.2-2）
- 「接続要件」（P.2-3）
- 「オープン ポートのリスト」（P.2-3）
- 「Cisco CDA との正常な接続のための Active Directory の要件」（P.2-4）

サポートされるオペレーティング システム

Cisco CDA は、バンドルされる Cisco Linux OS にインストールされています。Cisco CDA ISO イメージをスタンドアロン マシンまたは VMWare サーバにインストールすると、Linux が OS としてインストールされ、Cisco CDA はその上でアプリケーションとして実行されます。

関連項目

- 「ハードウェア要件」（P.2-2）
- 「接続要件」（P.2-3）
- 「Cisco CDA との正常な接続のための Active Directory の要件」（P.2-4）

サポートされる Active Directory バージョン

Cisco CDA は、次の Active Directory バージョンをサポートしています。

- Windows 2003
- Windows 2003 R2
- Windows 2008
- Windows 2008 R2
- Windows 2012

ハードウェア要件

Cisco CDA マシンは別個の専用アプライアンスまたは VMware である必要があります。

すべての場合において、Cisco CDA マシンは表 2-1 に記載されている標準ハードウェア仕様と VMWare 仕様を満たす必要があります。

表 2-1　同等のリソースを持つスタンドアロン アプライアンスまたは VMWare の標準/パフォーマンス ハードウェア要件

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	250 GB
NIC	1 つの NIC または仮想 NIC

表 2-2 には、Cisco CDA を VMWare にインストールするための最小限のハードウェア要件がリストされています。

表 2-2　VMWare の最小限のハードウェア要件

コンポーネント	仕様
CPU	2 つの仮想プロセッサ
システム メモリ	2 GB の SDRAM
ハード ディスクの空き容量	120 GB
NIC	1 つの仮想 NIC

関連項目

- 「サポートされるオペレーティング システム」（P.2-1）
- 「接続要件」（P.2-3）
- 「Cisco CDA との正常な接続のための Active Directory の要件」（P.2-4）

接続要件

Cisco CDA が適切に機能するためには、この Cisco CDA で設定されているすべてのコンシューマ デバイス、Active Directory ドメイン コントローラ マシン、およびターゲット Syslog サーバと自由に通信できる必要があります。Windows Firewall（またはその他の同等のサードパーティ ファイアウォール ソフトウェア）がいずれかの 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、これらの各エンドポイントのファイアウォール ソフトウェアで、自由に通信を行うために必要な例外を設定する必要があります。

この項では Windows Firewall を例にして、Windows Firewall を実行する可能性のあるすべてのエンドポイントに定義する必要のある例外について詳しく説明します。

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。

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

Cisco CDA マシンで GUI を使用して設定されている個々の Active Directory ドメイン コントローラ マシンで、Windows Firewall がその個々のドメイン コントローラ マシンで有効な場合は、その特定のドメイン 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 または Windows Server 2003 R2（SP1 以降がインストールされている状態）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
```

関連項目

- 「サポートされるオペレーティング システム」（P.2-1）
- 「ハードウェア要件」（P.2-2）
- 「Cisco CDA との正常な接続のための Active Directory の要件」（P.2-4）

オープン ポートのリスト

表 2-3 に、Cisco CDA 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。Cisco CDA では、これらのポートはデフォルトで空いています。

表 2-3　Cisco CDA でデフォルトで空いているポートのリスト

ポート番号	プロトコル	サービス
22	TCP	Secure Shell（SSH）プロトコル
80	TCP	HTTP（Web GUI、HTTPS にリダイレクト）
123	UDP	NTP

表 2-3　Cisco CDA でデフォルトで空いているポートのリスト （続き）

ポート番号	プロトコル	サービス
443	TCP	HTTPS（セキュアな Web GUI）
1645	UDP	RADIUS
1646	UDP	RADIUS
1812	UDP	RADIUS
1813	UDP	RADIUS Accounting
3799	UDP	ASA リスニング リスニング ポートは、CDA から ASA または WSA への認証要求の変更を送信するために使用されます。

表 2-3 に記載されたポートは CDA と ASA または WSA 間の正常な通信を確立するために開いている必要があります。

次のポートは、Cisco CDA プロセス間の内部コミュニケーションに対して空いていますが、Linux ファイアウォールによって、外部アプライアンスからのアクセスに対してブロックされます。

- 8005
- 8009
- 8020
- 8090
- 8091
- 8092
- 8093

Cisco CDA との正常な接続のための Active Directory の要件

Cisco CDA は、Active Directory ドメイン コントローラによって生成される Active Directory ログイン監査イベントを利用してユーザ ログイン情報を収集します。Cisco CDA が適切に動作するには、CDA が Active Directory に接続し、ユーザ ログイン情報を取得できる必要があります。Active Directory ドメイン コントローラで、次の手順が必要になります。

1. Active Directory のバージョンがサポートされ（サポートされる Active Directory バージョンを参照）、アクティブなドメイン コントローラと CDA の間にネットワーク接続があることを確認します（接続要件を参照）。
2. 該当する Microsoft のパッチが Active Directory ドメイン コントローラにインストールされていることを確認します。Active Directory ドメイン コントローラのマシンは Windows Server 2008 または Windows Server 2008 R2 を実行し、適切な Microsoft の修正プログラムがインストールされている必要があります。

   Windows Server 2008 には次のパッチが必要です。

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

このパッチは、CDA がドメイン コントローラと正常な接続を確立するのを妨げる Microsoft WMI でのメモリ リークを解消します（CDA 管理者は、CDA Active Directory ドメイン コントローラの GUI ページでこの問題を体験する場合があります。この GUI ページでは、接続が正常に確立されたときにステータスが「up」になる必要があります）。

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

このパッチは、Microsoft WMI の別のメモリ リークを解消します。このメモリ リークは、Active Directory ドメイン コントローラが必要なユーザ ログイン イベントをドメイン コントローラのセキュリティ ログに書き込むのを散発的に妨げます。結果として、CDA はこのドメイン コントローラからすべてのユーザ ログイン イベントを取得できない場合があります。

Windows Server 2008 R2 では、（SP1 がインストールされていない場合）次のパッチが必要です。

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

このパッチは、Microsoft WMI のメモリ リークを解消します。このメモリ リークは、Active Directory ドメイン コントローラが必要なユーザ ログイン イベントをドメイン コントローラのセキュリティ ログに書き込むのを散発的に妨げます。結果として、CDA はこのドメイン コントローラからすべてのユーザ ログイン イベントを取得できない場合があります。

3. Active Directory がユーザ ログイン イベントを Windows セキュリティ ログに記録するのを確認します。

「監査ポリシー」（「Group Policy Management」設定の一部）が、正常なログインによって、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（これはデフォルトの Windows 設定ですが、この設定が適切であることを明示的に確認する必要があります）。「監査ポリシーの設定」（P.2-6）を参照してください。

4. Active Directory に接続するために CDA が使用する十分な権限を持つ Active Directory ユーザが設定されている必要があります。CDA パッチ 1 以降、このユーザが Active Directory ドメインの管理グループのメンバーであるかどうかを選択できます。次の手順に従って、管理ドメイン グループのユーザ、または管理ドメイン グループではないユーザに対して権限を定義します。

   - 「Active Directory ユーザが Domain Admin グループのメンバーである場合に必要な権限」（P.2-7）
   - 「Active Directory ユーザが Domain Admin グループのメンバーでない場合に必要な権限」（P.2-7）

5. CAD によって使用される Active Directory ユーザは、NTLMv1 または NTLMv2 のいずれかによって認証を受けることができます。CDA と Active Directory ドメイン コントローラ間の正常な認証済み接続を確実に行うために、Active Directory NTLM の設定が CDA NTLM の設定と合っていることを確認する必要があります。図 2-1 に、すべての Microsoft NTLM オプションを示します。CDA が NTLMv2 に設定される場合、図 2-1 に記載された 6 つのオプションがすべてサポートされます。NTLMv1 をサポートするように CDA が設定されている場合、最初の 5 つのオプションだけがサポートされます。これも表 2-4 に要約されています。

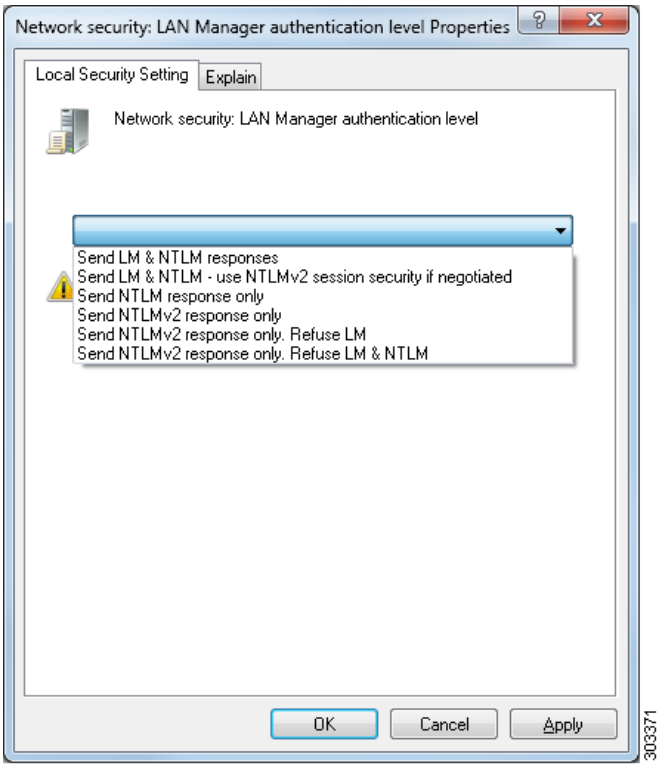
表 2-4　CDA と AD NTLM のバージョン設定に基づいてサポートされる認証タイプ

CDA NTLM の設定オプションおよび Active Directory（AD）NTLM の設定オプション	NTLMv1	NTLMv2
Send LM & NTLM responses	接続が受け入れられます	接続が受け入れられます
Send LM & NTLM - use NTLMv2 session security if negotiated	接続が受け入れられます	接続が受け入れられます
Send NTLM response only	接続が受け入れられます	接続が受け入れられます
Send NTLMv2 response only	接続が受け入れられます	接続が受け入れられます

表 2-4　CDA と AD NTLM のバージョン設定に基づいてサポートされる認証タイプ （続き）

CDA NTLM の設定オプションおよび Active Directory（AD）NTLM の設定オプション	NTLMv1	NTLMv2
Send NTLMv2 response only.Refuse LM	接続が受け入れられます	接続が受け入れられます
Send NTLMv2 response only.Refuse LM & NTLM	接続は拒否されます	接続が受け入れられます

図 2-1　MS NTLM 認証タイプのプション



関連項目

- 「サポートされるオペレーティング システム」（P.2-1）
- 「ハードウェア要件」（P.2-2）
- 「接続要件」（P.2-3）

監査ポリシーの設定

「監査ポリシー」（「Group Policy Management」の設定の一部）が、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（これは Windows のデフォルト設定ですが、この設定が適切であることを明示的に確認する必要があります）。

ステップ 1　[Start] > [Programs] > [Administrative Tools] > [Group Policy Management] を選択します。

ステップ 2　[Domains] の下で該当するドメインに移動します。

ステップ 3　ナビゲーション ツリーを展開します。

ステップ 4　デフォルトのドメイン ポリシーを右クリックします。

ステップ 5　[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。

ステップ 6　[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。

ステップ 7　[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 および Windows 2012 の場合、[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。

ステップ 8　[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。

Active Directory ユーザが Domain Admin グループのメンバーである場合に必要な権限

次の Active Directory のバージョンには、特別な権限は必要ありません。

- Windows 2003
- Windows 2003 R2
- Windows 2008

Windows 2008 R2 および Windows 2012 の場合、Domain Admin グループは、デフォルトで Windows オペレーティング システムの特定のレジストリ キーを完全に制御することができません。CDA を動作させるには、Active Directory 管理者は Active Directory ユーザに、次のレジストリ キーを完全に制御するアクセス許可を付与する必要があります。
HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

完全な制御を許可するには、まず Active Directory 管理者がキーの所有権を取得する必要があります。次の手順を実行します。

ステップ 1　キーを右クリックして [Owner] タブに移動します。

ステップ 2　[Permissions] をクリックします。

ステップ 3　[Advanced] をクリックします。

Active Directory ユーザが Domain Admin グループのメンバーでない場合に必要な権限

次は、Active Directory ユーザが Domain Admin グループの一部ではなく、Domain Users グループの一部である場合に必要な権限です。

- 「必要なレジストリの変更」（P.2-8）
- 「ドメイン コントローラで DCOM を使用する権限」（P.2-8）
- 「WMI Root\CIMv2 名前空間に対する権限」（P.2-10）
- 「Active Directory ドメイン コントローラのセキュリティ イベント ログの読み取りアクセス」（P.2-11）

これらの権限は、次のすべての Active Directory のバージョンで有効です。

- Windows 2003
- Windows 2003 R2
- Windows 2008
- Windows 2008 R2
- Windows 2012

必要なレジストリの変更

Cisco CDA がドメイン ユーザを操作する場合、特定のレジストリ キーを手動で追加する必要があります。変更は、次のレジストリのスクリプトに記述されています。Active Directory 管理者は、これを .reg 拡張子のテキスト ファイルにコピーして貼り付け、ダブル クリックしてレジストリを変更することも可能です。レジストリ キーを次のように追加するには、ルート キーのオーナーである必要があります。

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "
```

キー "DllSurrogate" の値には、2 つのスペースが含まれていることを確認します。

上記のスクリプトに示すように、ファイルの末尾の空の行を含む、空の行を保持する必要があります。

ドメイン コントローラで DCOM を使用する権限

Active Directory ユーザは、ドメイン コントローラで DCOM（リモート COM）を使用する権限がなければなりません。**dcomcnfg** ツールを使用してこれを実行できます。

ステップ 1　コマンドラインから **dcomcnfg** ツールを起動します。

ステップ 2　[Component Services] を展開します。

ステップ 3　[Computers] を展開し、[My Computer] をクリックします。

ステップ 4　メニュー バーで [Action] を選択し、[properties] をクリックし、[COM Security] をクリックします。

ステップ 5　アクセスおよび起動の両方に対して CDA アカウントが許可権限を持っていることを確認します。Active Directory ユーザは、4 つのオプション（[Access Permissions] および [Launch and Activation Permissions] の両方に対する [Edit Limits] と [Edit Default]）のすべてに追加される必要があります。図 2-2 を参照してください。

ステップ 6　[Access Permissions] および [Launch and Activation Permissions] の両方に対してローカルおよびリモート アクセスをすべて許可します。

図 2-2　[My Computer Properties]

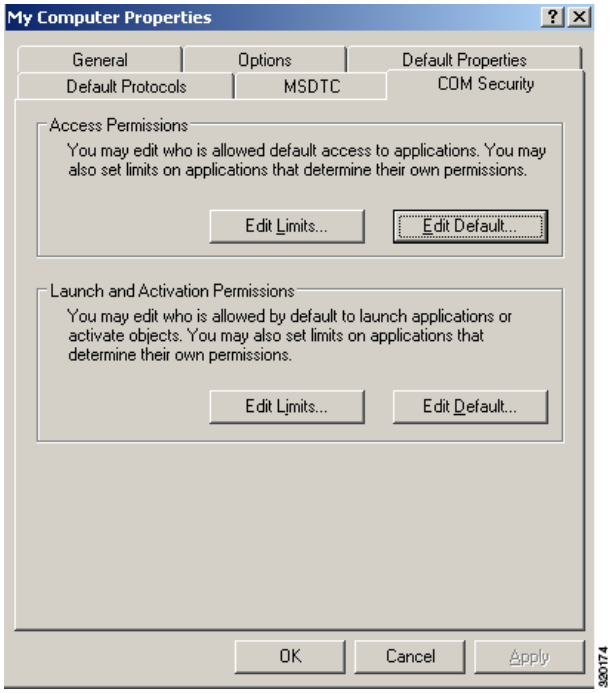


図 2-3　[Access Permissions] のローカルおよびリモート アクセス

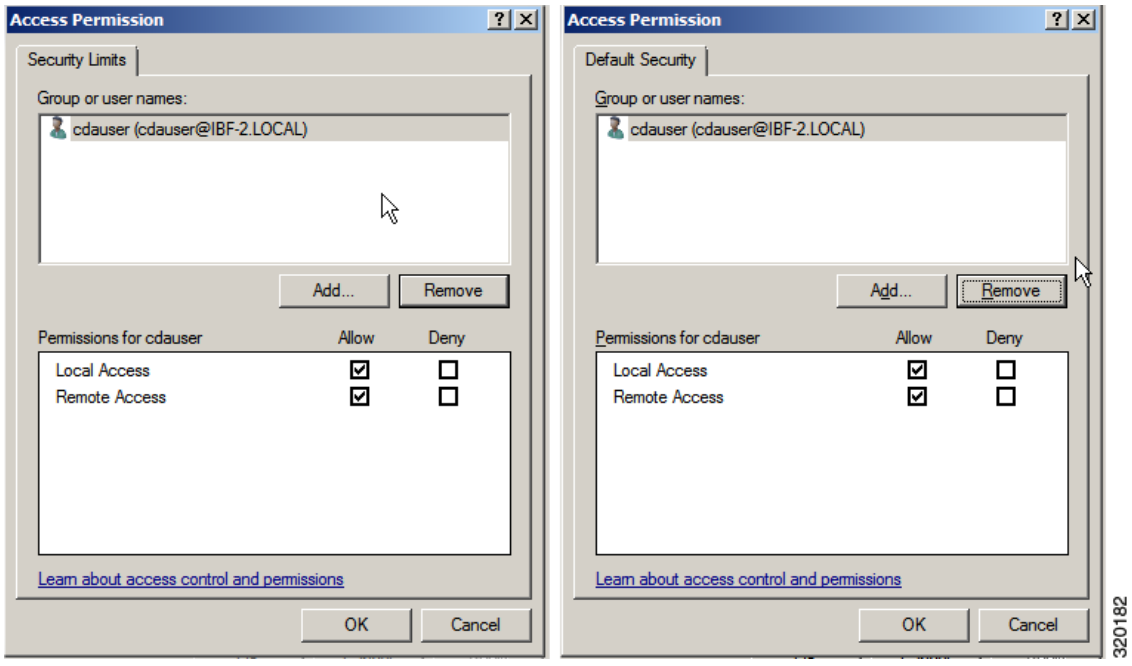
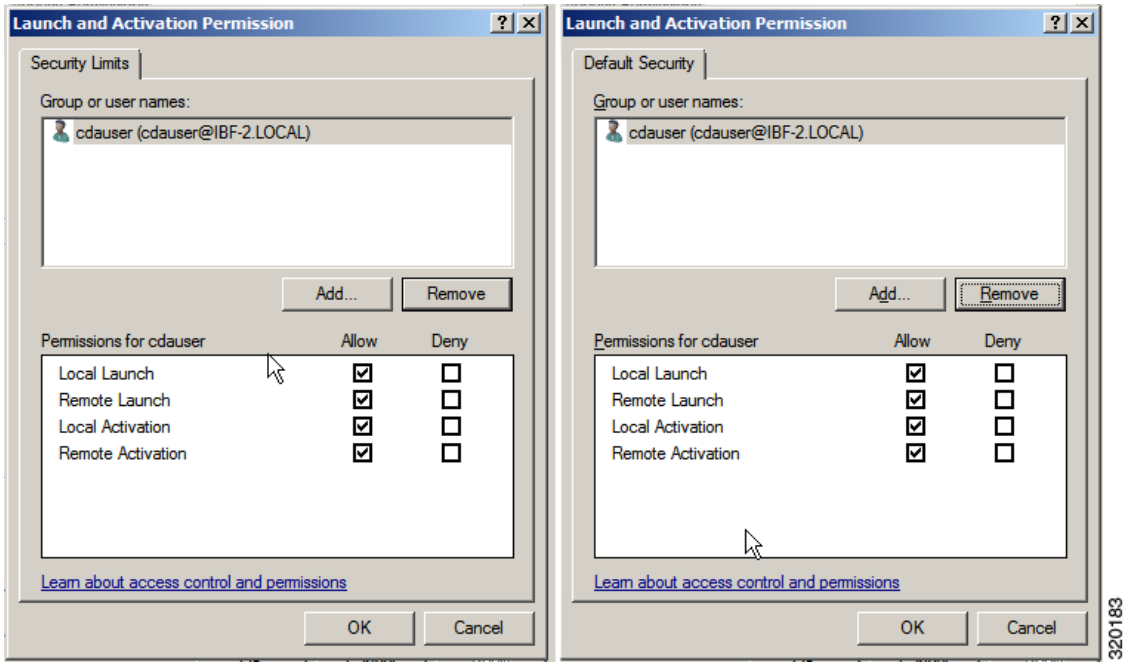


図 2-4　[Launch and Activation Permissions] のローカルおよびリモート アクセス



WMI Root\CIMv2 名前空間に対する権限

Active Directory ユーザには、デフォルトでメソッドの実行およびリモートの有効化の権限がありません。これらは wmimgmt.msc MMC コンソールを使用して付与することができます。

ステップ 1　[Start] > [Run] をクリックし、wmimgmt.msc と入力します。

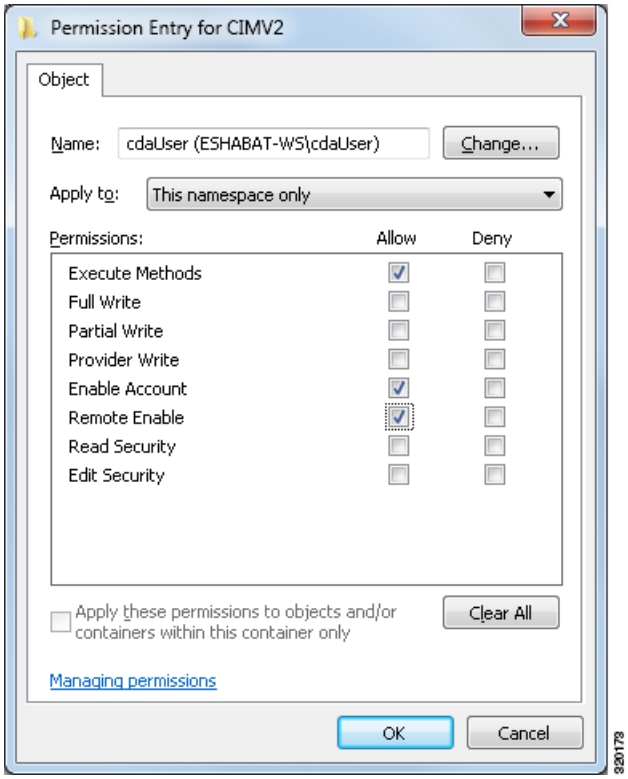
ステップ 2　[WMI Control] を右クリックし、[Properties] をクリックします。

ステップ 3　[Security] タブで [Root] を展開し、[CIMV2] を選択します。

ステップ 4　[Security] をクリックします。

ステップ 5　図 2-5 で示すように、Active Directory ユーザを追加し、必要な権限を提供します。

図 2-5　WMI Root\CIMv2 名前空間の必要な権限



Active Directory ドメイン コントローラのセキュリティ イベント ログの読み取りアクセス

Windows 2008 以降では、Event Log Readers と呼ばれるグループにユーザを追加することで実行できます。

Windows のすべての旧バージョンでは、レジストリ キーを次のように編集することで実行できます。

ステップ 1　セキュリティ イベント ログへのアクセスを委任するために、アカウントの SID を見つけます。

ステップ 2　すべての SID アカウントを表示するには、図 2-6 に示すように、コマンド ラインから次のコマンドを使用します。

```
wmic useraccount get name,sid
```

特定のユーザ名とドメインに対して、次のコマンドを使用することもできます。

```
wmic useraccount where name="cdaUser"get domain,name,sid
```

ステップ 3　SID を見つけ、レジストリ エディタを開き、次の場所を参照します。

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Eventlog

ステップ 4　[Security] をクリックし、[CustomDS] をダブルクリックします。図 2-7 を参照してください。

たとえば、cda_agent アカウント（SID：S-1-5-21-1742827456-3351963980-3809373604-1107）への読み取りアクセスを許可するには、「(A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107)」と入力します。

ステップ 5　DC 上で WMI サービスを再起動します。次の 2 通りの方法で WMI サービスを再起動できます。

a.　CLI から次のコマンドを実行します。

```
net stop winmgmt
```

```
net start winmgmt
```

b. Services.msc を実行します（これにより、Windows サービス管理ウィンドウが開きます）。

Windows サービス管理ウィンドウで、「Windows Management Instrumentation」サービスを検索し、右クリックして [Restart] を選択します。

図 2-6　すべての SID アカウントの表示

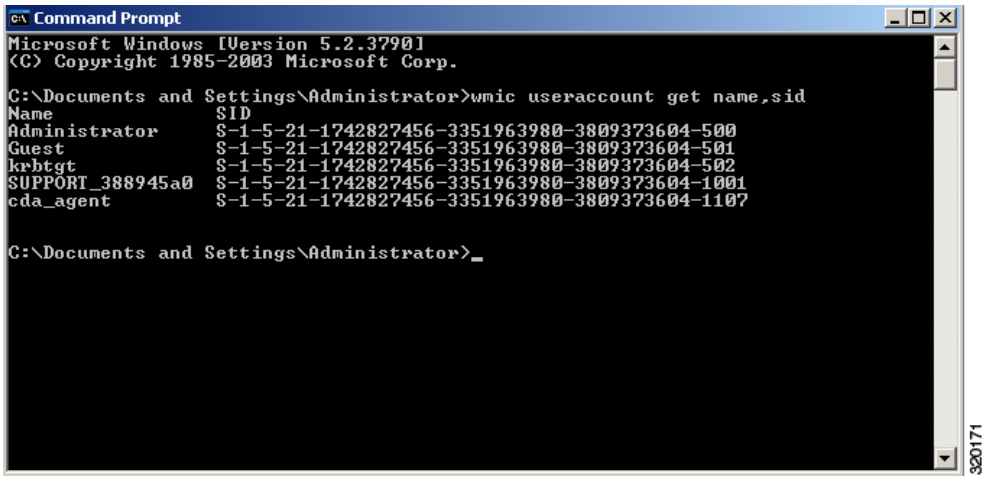
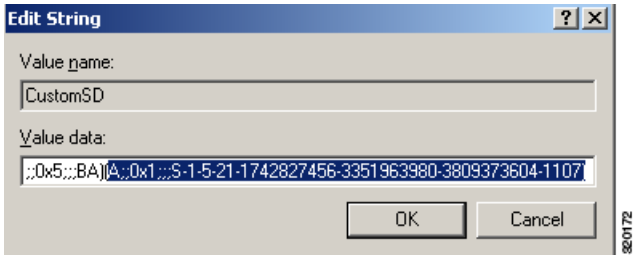


図 2-7　CustomSD 文字列の編集



Context Directory Agent のインストール

Context Directory Agent は ISO イメージとしてパッケージされています。Cisco.com からパッケージをダウンロードして、それを専用の X86 マシンまたは VMWare ESX サーバにインストールすることができます。

（注） Cisco CDA を VMWare にインストールする場合は、[Use Guest OS as Linux CentOS 4/5 32 bit] を必ず選択する必要があります。ゲスト OS の設定を誤ると、パフォーマンスが非常に下がる場合があります。

（注） Cisco CDA を VMWare サーバにインストールすると、VMWare ツールが自動的にインストールされます。

Context 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　Cisco CDA ISO イメージ *cda-1.0.0.xxx.i386.iso* をダウンロードして、それをローカル リポジトリに保存します。

ステップ 2　ISO イメージを DVD に書き込みます。

ステップ 3　DVD を挿入して、光学ドライブからイメージをインストールするオプションを選択します。

Cisco CDA パッケージのインストールが開始します。インストールが完了すると、マシンがリブートします。ブート シーケンスが完了すると、次のプロンプトが表示されます。

```
********************************************
Please type 'setup' to configure the appliance
********************************************
```

ブート シーケンスは約 2 分間で完了します。

ステップ 4　プロンプトに「setup」と入力して、セットアップ プログラムを開始します。ネットワーキング パラメータと最初のクレデンシャルの入力を求めるプロンプトが表示されます。

次は、サンプルのセットアップ プログラムとデフォルト プロンプトを示しています。

```
localhost.localdomain login: setup
Press 'Ctrl-C' to abort setup
Enter Hostname[]: cda-server
Enter IP address []: 192.168.10.10
Enter IP netmask []: 255.255.255.0
Enter IP default gateway []: 192.168.10.100
Enter default DNS domain []: cisco.com
Enter primary nameserver []: 200.150.200.150
Enter secondary nameserver?Y/N: n
Enter primary NTP server [time.nist.gov]: clock.cisco.com
Enter secondary NTP server?Y/N: n
Enter system timezone [UTC]: UTC
Enter username [admin]: admin
Enter password:
Enter password again:
Bringing up the network interface...
Pinging the gateway...
Pinging the primary nameserver...
Do not use 'Ctrl-C' from this point on...
Installing applications...
Installing cda...
Pre install
Post Install

Application bundle (cda) installed successfully
=== Initial setup for application: cda ===
Generating configuration...
Rebooting...
```

ステップ 5　Cisco CDA のパッチ 1 をインストールします。「Context Directory Agent 1.0 パッチ 1 のインストール」（P.2-14）を参照してください。

ステップ 6　マシンがリブートした後、Cisco CDA CLI にログインしてパッケージのインストールを確認できます。次はサンプルの確認手順を示しています。

```
# login: admin
/admin# show application
<name> <description>
cda Cisco Context Directory Agent
/admin# show application status cda

CDA application server is running PID:2840
```

ステップ 7　これで、Cisco CDA ユーザ インターフェイスにログインして、Cisco CDA の設定を開始できるようになりました。

（注）　初期セットアップ プログラム中に指定したユーザ名とパスワードは、CLI と GUI の両方に使用できます。ユーザ インターフェイスを使用して GUI パスワードを変更しても、CLI パスワードは変更されず、その逆の場合も同じです。

関連項目

- 「サポートされるオペレーティング システム」（P.2-1）
- 「ハードウェア要件」（P.2-2）
- 「接続要件」（P.2-3）
- 「Cisco CDA との正常な接続のための Active Directory の要件」（P.2-4）

Context Directory Agent 1.0 パッチ 1 のインストール

Cisco.com から Cisco CDA 1.0 パッチ 1 をダウンロードし、インストールできます。

ステップ 1　パッチを CDA にアップロードできるようにリポジトリを作成します。リポジトリの作成方法の手順については、「repository」（P.4-112）を参照してください。

ステップ 2　定義したリポジトリに Cisco CDA パッチ 1 をダウンロードします。

ステップ 3　「patch install」（P.4-29）の説明に従って、Cisco CAD パッチ 1 をインストールします。

ステップ 4　次の手順に従って、パッチがインストールされていることを確認します。

```
/admin# sh application version cda

Cisco Context Directory Agent
--------------------------------------------
Version      : 1.0.0.011
Build Date   : Tue May  8 15:34:26 2012
Install Date : Mon Dec 17 08:53:18 2012
```

```
Cisco Context Directory Agent Patch
-------------------------------------------
Version      : 1
Build number : NA
Install Date : Mon Dec 31 09:35:09 2012
```

Cisco AD Agent から Cisco CDA へのマイグレーション

Cisco CDA は Cisco AD Agent と互換性があります。AD Agent がネットワークにすでにデプロイされている場合、同様の対応する設定を使用して、Cisco CDA によってそれを置き換えることができます。ID ベースのファイアウォール ソリューションの他のコンポーネント（Active Directory サーバと Identity コンシューマ デバイス（ASA/WSA））で、ソフトウェアの変更やアップグレードを行う必要はありません。

Cisco AD Agent から Cisco CDA に遷移する前に、次の AD Agent 設定の詳細を記録しておきます。

- 一般設定のオプション

  AD エージェント コマンド **adacfg options list** を使用
- IP アドレスおよび機能を含む Syslog サーバ

  AD エージェント コマンド **adacfg syslog list** を使用
- ユーザ名、パスワード、ホスト、およびドメイン FQDN を含む接続済みの Active Directory DC リスト

  AD エージェント コマンド **adacfg dc list** を使用（パスワードを表示しない）
- IP アドレス/サブネット、共有秘密を含むコンシューマ デバイス（またはサブセット）

  AD エージェント コマンド **adacfg client list** を使用（共有秘密を表示しない）

上記のコマンドのすべての構文と出力例については、『*Installation and Setup Guide for the Active Directory Agent, Release 1.0*』を参照してください。

既存の Cisco AD Agent アプリケーションに対応するように Cisco CDA をインストールおよび設定します。

- オプションで、Active Directory の基本設定を設定します。Cisco CDA の AD モニタリングは、Cisco AD エージェントの **dcStatusTime** に相当します（Cisco CDA ではデフォルトで 10 秒ですが、Cisco AD エージェントではデフォルトで 60 秒である点が異なります）。

  Cisco CDA の履歴は、AD エージェントの **dcHistoryTime** に相当します（CDA ではデフォルトで 10 秒ですが、AD エージェントではデフォルトで 24 時間である点が異なります）。

  CDA のユーザ ログイン有効期限は、AD エージェントの **userLogonTTL** に相当します（デフォルトの 24 時間は同じです）。
- DC マシンにセキュリティ ポリシーを設定します。Active Directory のセキュリティ ポリシー設定に関する Cisco AD エージェントと Cisco CDA 間の相違は、Windows 2008R2 サーバに対してのみ適用できます。Cisco CDA の場合、「Active Directory サーバの追加と編集」（P.7）のステップ 2 で説明されているように、Microsoft Windows 2008 R2 サーバにアカウント権限を設定します。
- オプションで、AD エージェントの **logLevel** に対応するように、ログ レベル設定を Cisco CDA に設定します。
- オプションで、**adacfg syslog list** から Cisco CDA に syslog サーバを追加します。
- すべての Active Directory サーバを **adacfg dc list** から Cisco CDA に追加します。

- すべての Identity コンシューマを **adacfg client list** から Cisco CDA に追加します。

同じホスト名 /IP アドレスを使用して AD エージェント サーバを Cisco CDA サーバと置き換える場合、コンシューマ デバイス（ASA/WSA）設定を変更する必要はなく、コンシューマ デバイスは自動的に Cisco CDA に接続して、ID マッピング情報を取得します。

これとは異なり、新たに Cisco CDA サーバを導入に追加する場合、その新しい Cisco CDA サーバを指すように、コンシューマ デバイスの設定を更新する必要があります。詳細については、Cisco.com の ASA および WSA の資料を参照してください。