



設定のワークフローとチェックリスト

この章は大きな 2 つの項で構成されており、さまざまなテクノロジーをサポートするように BAC コンポーネントを設定する際のプロセスを定義します。次の項で構成されています。

- [コンポーネントのワークフロー \(P.3-1\)](#)
- [技術のワークフロー \(P.3-3\)](#)

コンポーネントのワークフロー

この項では、BAC でサポートされるテクノロジーに合わせて各 BAC コンポーネントを設定する際に必要なワークフローについて説明します。これらの設定作業を行ってから、特定のテクノロジーをサポートするように BAC を設定します。

この項で説明するコンポーネントのワークフローはチェックリストの形式で用意されており、次のものがあります。

- [RDU チェックリスト](#)
- [DPE チェックリスト](#)

RDU チェックリスト

表 3-1 は、RDU 設定時のワークフローを示しています。

表 3-1 RDU ワークフロー チェックリスト

手順	参照先
1. BAC に利用されるシステム syslog サービスを設定する。	『 <i>Installation Guide for Cisco Broadband Access Center, 3.0</i> 』
2. BAC 管理者のユーザ インターフェイスにアクセスする。	管理者のユーザ インターフェイスの設定 (P.15-2)
3. 管理者のパスワードを変更する。	管理者のユーザ インターフェイスの設定 (P.15-2)
4. 適切なライセンス キーを追加する。	ライセンス キーの管理 (P.17-18)
5. RDU データベース バックアップ手順を設定する。	バックアップと回復 (P.10-6)
6. RDU SNMP エージェントを設定する。	snmpAgentCfgUtil.sh ツールの使用方法 (P.11-6)

DPE チェックリスト

表 3-2 に示されている作業は、表 3-1 に示されている作業の後で実行する必要があります。



(注) アスタリスク (*) が付いている項目は、必須の作業または手順です。

表 3-2 DPE 設定チェックリスト

手順	参照先
1. BAC に利用されるシステム syslog サービスを設定する。	『 <i>Installation Guide for Cisco Broadband Access Center, 3.0</i> 』
2. パスワードを変更する。*	『 <i>Cisco Broadband Access Center DPE CLI Reference, 3.0</i> 』に示されている password コマンド
3. プロビジョニング インターフェイスを設定する。	『 <i>Cisco Broadband Access Center CPE CLI Reference, 3.0</i> 』に示されている interface ethernet [intf0 intf1] コマンド
4. BAC の共有秘密情報を設定する。*	『 <i>Cisco Broadband Access Center DPE CLI Reference, 3.0</i> 』に示されている dpe shared-secret コマンド
5. 目的の RDU に接続するために DPE を設定する。*	『 <i>Cisco Broadband Access Center DPE CLI Reference, 3.0</i> 』に示されている dpe rdu-server コマンド
6. ネットワーク タイム プロトコル (NTP) を設定する。	Solaris のマニュアルに示されている設定情報
7. プロビジョニング グループの名前を設定する。*	『 <i>Cisco Broadband Access Center DPE CLI Reference, 3.0</i> 』に示されている dpe provisioning-group primary コマンド
8. RDU およびネットワーク内のデバイスへの必要なルートを設定する。	Solaris のマニュアルに示されている設定情報
9. DPE SNMP エージェントを設定する。	『 <i>Cisco Broadband Access Center DPE CLI Reference, 3.0</i> 』に示されている SNMP エージェント コマンド
(注) SNMP エージェントを設定するには、DPE のコマンドライン インターフェイスまたは <code>snmpAgentCfgUtil.sh</code> ツールを使用します。詳細については、P.11-6 の「 snmpAgentCfgUtil.sh ツールの使用方法 」を参照してください。	
10. DPE が RDU に正常に接続され、登録されたことを確認する。	サーバの表示 (P.16-24)



(注) SNMP エージェントを設定するには、DPE のコマンドライン インターフェイスまたは `snmpAgentCfgUtil.sh` ツールを使用します。詳細については、P.11-6 の「[snmpAgentCfgUtil.sh ツールの使用方法](#)」を参照してください。

10. DPE が RDU に正常に接続され、登録されたことを確認する。 [サーバの表示 \(P.16-24\)](#)

技術のワークフロー

この項では、特定の技術（この場合は CWMP）をサポートするように BAC を設定する際に必要な作業について説明します。これらの設定作業は、BAC コンポーネントの設定後に実行します。

この項で説明する CWMP 技術のワークフローはチェックリストの形式で用意されており、次のものがあります。

- [RDU の設定ワークフロー \(P.3-3\)](#)
- [DPE の設定ワークフロー \(P.3-5\)](#)
- [プロビジョニンググループの設定ワークフロー \(P.3-8\)](#)

RDU の設定ワークフロー

表 3-3 は、CWMP 技術について RDU を設定するのに必要な設定作業を示しています。

表 3-3 RDU の設定ワークフロー

手順	参照先
<p>1. BAC のサービス クラスを使用してサービス プロファイルを作成する。</p> <p>管理者のユーザ インターフェイスから、テンプレートで参照されるカスタム プロパティを定義します。カスタム プロパティは、設定およびファームウェア ルール テンプレートで参照できます。</p> <p>サービスごとに、次の作業を行う必要があります。</p> <p>a. 設定テンプレートを作成する。</p> <p>管理者のユーザ インターフェイスから、設定テンプレートを RDU に追加します。</p> <p>b. ファームウェア ルール テンプレートを作成する。</p> <ul style="list-style-type: none"> – 管理者のユーザ インターフェイスから、ファームウェア イメージを RDU に追加する。 – 管理者のユーザ インターフェイスから、ファームウェア ルール テンプレートを RDU に追加する。 <p>c. 管理者のユーザ インターフェイスから、サービス クラスを作成する。</p> <p>次の作業を確実に行います。</p> <ul style="list-style-type: none"> – 設定テンプレート ファイルを指定する。 – ファームウェア ルール ファイルを指定する。 – (オプション) プロパティを指定する。 	<p>カスタム プロパティの設定 (P.17-7)</p> <p>ファイルの追加 (P.17-15)</p> <p>ファイルの追加 (P.17-15)</p> <p>ファイルの追加 (P.17-15)</p> <p>サービス クラスの設定 (P.17-2)</p>
<p>2. 管理者のユーザ インターフェイスから、CWMP 技術に関するデフォルト設定値を設定する。</p> <ul style="list-style-type: none"> – デフォルトのサービス クラスを設定する（たとえば、不明なデバイス用）。 – 次のいずれかのページで、接続要求サービスのデフォルトを設定する (Configuration > Class of Service、Configuration > Defaults、および Devices)。 	<p>デフォルトの設定 (P.17-8)</p>
<p>3. CWMP デバイスを登録する。</p>	<p>BAC でのデバイス データの事前登録 (P.3-4)</p>

BAC でのデバイス データの事前登録

事前登録とは、デバイスが DPE と最初に通信する前に、デバイス レコードを RDU に追加する作業を指します。DPE は自動構成サーバ (ACS) と呼ばれます。この作業は、通常、プロビジョニング API から実行されます。ただし、管理者のユーザ インターフェイスからデバイス データを事前登録することも可能です。

BAC でデバイス データを事前登録するには、次の手順に従います。

ステップ 1 API または管理者のユーザ インターフェイスを使用して、デバイス レコードを RDU データベースに追加します。

管理者のユーザ インターフェイスからデバイス レコードを追加するには、次の手順に従います。

- a. **Devices > Manage Devices** の順に選択します。
- b. Manage Devices ページで、**Add** をクリックします。
- c. Add Device ページが表示されます。適切なフィールドに値を入力します。事前登録するデバイスの必須および推奨プロビジョニング属性は、次のとおりです。

必須

- デバイス識別子
- 登録されているサービス クラス
- ホーム プロビジョニング グループ

一般的な追加属性



(注) 追加属性は、顧客宅内装置 (CPE) の認証方式に応じて、必須となる場合や、サポートされる場合があります。

- オーナー識別情報
- CPE パスワード (一意のクライアント証明書を使用するクライアント認証がイネーブルになっていない場合)
- 接続要求ユーザ名 (このステップはオプション)
- 接続要求パスワード (このステップはオプション)

オプション

サービス クラスの接続要求方式 (このステップはオプション)

接続要求方式を設定すると、自動構成サーバのデバイス認証がイネーブルになります。次のいずれかを選択します。

- Discovered
- Use FQDN
- Use IP

ステップ 2 デバイス レコードが事前登録されたかどうかを確認します。次の手順に従います。

- Device Details ページを調べる。次の手順に従います。
Devices > Manage Devices ページで、デバイスに対応する **View Details** アイコン (🔍) をクリックします。Device Details ページで、次の作業を行います。
 - デバイス設定が正しいかどうかを確認する。
 - 検出されたパラメータを検索する。デバイスが DPE との最初の通信をまだ開始していない場合、このパラメータは表示されません。

- デバイス履歴のログを確認する。
- RDU と DPE のログ ファイルを調べる (P.19-3 の「ロギング」を参照)。

ステップ3 DPE に定期的な通知を送信するようにデバイスを設定します。これを行うには、設定テンプレートに *PeriodicInformEnable* 変数と *PeriodicInformInterval* 変数を設定します。

ステップ4 BAC との最初のデバイス交信を開始します。次の手順に従います。

- API から接続要求を開始する。
- デバイスから次の定期交信があるまで待機する。
- リポートする。

ステップ5 BAC との最初のデバイス交信を確認します。**Device > Manage Devices > Device Details** の順に選択し、検出されたプロパティが表示されるかどうかを確認します。また、履歴ログで詳細を確認します。

DPE の設定ワークフロー

この項では、DPE で CWMP をサポートできるようにする方法について説明します。これを行うには、次の設定を行います。

- CWMP 管理のための CWMP サービスを DPE に設定する。
P.3-5 の「DPE に対する CWMP サービスの設定」を参照してください。
- ファームウェア管理のための HTTP ファイル サービスを DPE に設定する。
P.3-7 の「DPE に対する HTTP ファイル サービスの設定」を参照してください。



DPE に対する CWMP サービスの設定

表 3-4 は、CWMP サービスを DPE に設定するのに必要な設定作業を示しています。

表 3-4 DPE の設定ワークフロー : CWMP 管理

手順	参照先
<p>DPE 上で動作する CWMP サービスを設定します。</p> <p>CWMP 技術を DPE に設定するには、CWMP サービスを少なくとも 1 つイネーブルにする必要があります。CWMP サービスをイネーブルにするには、次のコマンドを入力します。</p> <pre>service cwmp num enable true</pre> <p><i>num</i> は CWMP サービスを示します。1 または 2 を指定します。</p> <p>デフォルトでは、CWMP サービスは次の状態になります。</p> <ul style="list-style-type: none"> — サービス 1 の場合はイネーブル — サービス 2 の場合はディセーブル 	<p>『Cisco Broadband Access Center DPE CLI Reference, 3.0』に示されている CWMP 技術のコマンド</p>


表 3-4 DPE の設定ワークフロー : CWMP 管理 (続き)

手順	参照先
<p>1. CWMP サービスが CPE と通信するときのポートを設定する。</p> <p>デフォルトでは、CWMP サービスは次のポートでリスンするように設定されています。</p> <ul style="list-style-type: none"> — サーバ 1 の場合はポート 7547 — サーバ 2 の場合はポート 7548 	『Cisco Broadband Access Center DPE CLI Reference, 3.0』に示されている service cwmp num port port コマンド
<p>2. CWMP サービスに対して、HTTP を使用したクライアント認証を設定する。</p> <p> (注) クライアント認証時のセキュリティ リスクを制限するため、Digest モード (デフォルト設定) を使用することをお勧めします。クライアント認証を Basic モードで使用することや、Basic 認証と Digest 認証を両方ともディセーブルにすることはお勧めできません。</p>	『Cisco Broadband Access Center DPE CLI Reference, 3.0』に示されている service cwmp num client-auth mode コマンド
<p>3. CWMP サービスに対して、SSL 経由の証明書を使用したクライアント認証を設定する。</p>	『Cisco Broadband Access Center DPE CLI Reference, 3.0』に示されている service cwmp num ssl client-auth mode コマンド
<p>4. DPE でデバイスを認識できない場合に構成を RDU に要求するように DPE を設定する。</p> <p> (注) この機能をイネーブルにすると、RDU が DoS 攻撃 (サービス拒絶攻撃) を受ける可能性があります。</p>	『Cisco Broadband Access Center DPE CLI Reference, 3.0』に示されている service cwmp num allow-unknown-cpe コマンド

DPE に対する HTTP ファイル サービスの設定

表 3-5 は、DPE 上で動作する HTTP ファイル サービスを設定するのに必要な設定作業を示しています。

表 3-5 DPE の設定ワークフロー：ファームウェア管理

手順	参照先
<p>DPE 上で動作する HTTP ファイル サービスを設定します。</p> <p>ファームウェア管理を DPE に設定するには、HTTP ファイル サービスを少なくとも 1 つイネーブルにする必要があります。HTTP ファイル サービスをイネーブルにするには、次のコマンドを入力します。</p> <pre>service http num enable true</pre> <p><i>num</i> は HTTP ファイル サービスを示します。1 または 2 を指定します。</p> <p>デフォルトでは、HTTP サービスは次の状態になります。</p> <ul style="list-style-type: none"> — サービス 1 の場合はイネーブル — サービス 2 の場合はディセーブル 	『Cisco Broadband Access Center DPE CLI Reference, 3.0』に示されている CWMP 技術のコマンド
<p>1. HTTP ファイル サービスが CPE と通信するときのポートを設定する。</p> <p>デフォルトでは、HTTP ファイル サービスは次のポートでリッスンするように設定されています。</p> <ul style="list-style-type: none"> — サーバ 1 の場合はポート 7549 — サーバ 2 の場合はポート 7550 	『Cisco Broadband Access Center DPE CLI Reference, 3.0』に示されている service http num port port コマンド
<p>2. HTTP ファイル サービスに対して、クライアント認証を設定する。</p> <p> (注) クライアント認証時のセキュリティ リスクを制限するため、Digest モード (デフォルト設定) を使用することをお勧めします。クライアント認証を Basic モードで使用することや、Basic 認証と Digest 認証を両方ともディセーブルにすることは避ける必要があります。</p>	『Cisco Broadband Access Center DPE CLI Reference, 3.0』に示されている service http num client-auth mode コマンド
<p>3. HTTP ファイル サービスに対して、SSL 経由の証明書を使用したクライアント認証を設定する。</p>	『Cisco Broadband Access Center DPE CLI Reference, 3.0』に示されている service http num ssl client-auth mode コマンド

プロビジョニンググループの設定ワークフロー

まず、DPE が特定のプロビジョニンググループに追加されるように設定します (P.12-12 の「[プロビジョニンググループへの DPE の追加](#)」を参照)。その後、DPE が RDU への登録を行うと、プロビジョニンググループが自動的に作成されます。プロビジョニンググループが作成されたら、管理者のユーザ インターフェイスから BAC サーバの URL を割り当てて設定します。

プロビジョニンググループの URL を設定する前に、ローカルおよび地域の冗長性に関する BAC の概念を十分に理解しておいてください (P.12-11 の「[プロビジョニンググループのスケーラビリティとフェールオーバー](#)」を参照)。



(注)

プロビジョニンググループを作成したら、ただちにプロビジョニンググループに URL を割り当てることをお勧めします。URL を割り当てると、プロビジョニンググループ間の CPE リダイレクションがイネーブルになります。ロード バランサを使用する場合は、ロード バランサのアドレスが ACS URL として使用されていることを確認します。

管理者のユーザ インターフェイスからプロビジョニンググループの ACS URL を設定するには、次の手順に従います。

-
- ステップ 1** プライマリ ナビゲーションバーで、**Servers > Provisioning Groups** の順にクリックします。
 - ステップ 2** Manage Provisioning Groups ページが表示されます。適切なプロビジョニンググループの Identifier リンクをクリックします。
 - ステップ 3** View Provisioning Group Details ページが表示されます。Provisioning Group Properties 領域で、ACS URL フィールドに URL を入力します。



(注)

設定する URL によって、検出された ACS URL が上書きされることに留意してください。

- ステップ 4** **Submit** をクリックします。

これで、プロビジョニンググループが、設定した URL にある BAC と交信するようになりました。
