



WAFS の設定

この章では、ブランチ オフィスのユーザが集中管理されたデータセンターに保存されているデータにより効率的にアクセスできる Wide Area File Services (WAFS) を設定する方法について説明します。WAFS 機能は、ブランチ オフィスのユーザ付近の Edge WAE でデータをキャッシュして、WAN の遅延と帯域幅制限を解決します。



(注)

この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine (WAE) を総称する用語として「WAAS デバイス」を使用します。「WAE」は、WAE アプライアンスおよび WAE ネットワーク モジュール (NME-WAE デバイス ファミリ) を示します。

この章の構成は、次のとおりです。

- [ファイル サービスについて \(p.11-2\)](#)
- [ファイル サービス機能の概要 \(p.11-4\)](#)
- [ファイル サービスの準備 \(p.11-9\)](#)
- [ファイル サービスの設定 \(p.11-10\)](#)
- [ファイル サービスの管理 \(p.11-36\)](#)

ファイル サービスについて

今日、企業は、国内と海外のさまざまな地域にリモート オフィスを構えています。一般に、これらのリモート オフィスには、ローカル ユーザに必要なデータを保存し、管理するために、独自のファイル サーバがあります。

このような運用には、各リモート オフィスでファイル サーバを購入し、管理し、アップグレードするためにコストがかかるという問題があります。これらのファイル サーバを保守するために、特にサーバの障害に備えてデータを保護するために、膨大なリソースと人員を配置する必要があります。リモート オフィスは、必要なレベルのデータ保証を実現するために、リモート サイトでデータをバックアップし、一般に遠隔の安全な場所まで輸送するための専任のリソースを割り当てる必要があります。このシナリオにリモート オフィスの数（数十、数百、数千など）を掛けると、このような企業データ管理の方法では、コストが急激に増加し、重大なデータのリスクが大幅に増えることが分かります。

このシナリオの論理的な解決策は、データを正しく管理するために必要な設備、訓練を受けた人員、およびストレージ容量が存在する中央の位置へ企業のすべての重要なデータを移動する方法です。データセンターがバックアップや他のストレージ管理設備を提供することで、企業は、社員の生産性とストレージの利用率を改善し、データ保証とセキュリティを強化することができます。

企業のデータセンターとリモート オフィス間の WAN は、帯域幅の制限と大きな遅延により、信頼性が低く、低速になる傾向があります。さらに、WAN には、データセンター ソリューションの実装に対する他の阻害要因があります。

その 1 つは、WAN 経由で動作するファイル サーバ プロトコルです。Windows 用のファイル サーバ プロトコルである CIFS は、LAN 経由で動作するように設計されています。ファイル操作のたびに、クライアントとファイル サーバの間で、複数のプロトコル メッセージが交換されます。この状況は、LAN では意識されませんが、WAN 経由の場合はただちに大きな遅延になります。また、このような大きな遅延により、ファイル サーバ プロトコル自体が停止する場合があります。

ファイル サーバ プロトコルが WAN 経由で正しく機能する場合でも、各トランザクションの間に長い遅延が存在します。通常、これらの遅延により、ワードプロセッシングプログラム、イメージ編集プログラム、および設計ツールのようなユーザ アプリケーションがタイムアウトし、正常に動作しなくなる場合があります。

信頼性の低い WAN、ファイル システム プロトコルの互換性、およびユーザ アプリケーションの互換性のような問題は、ユーザ 経験に影響し、生産性が低下する使いにくい作業環境の原因になります。

ファイル サービス ソリューション

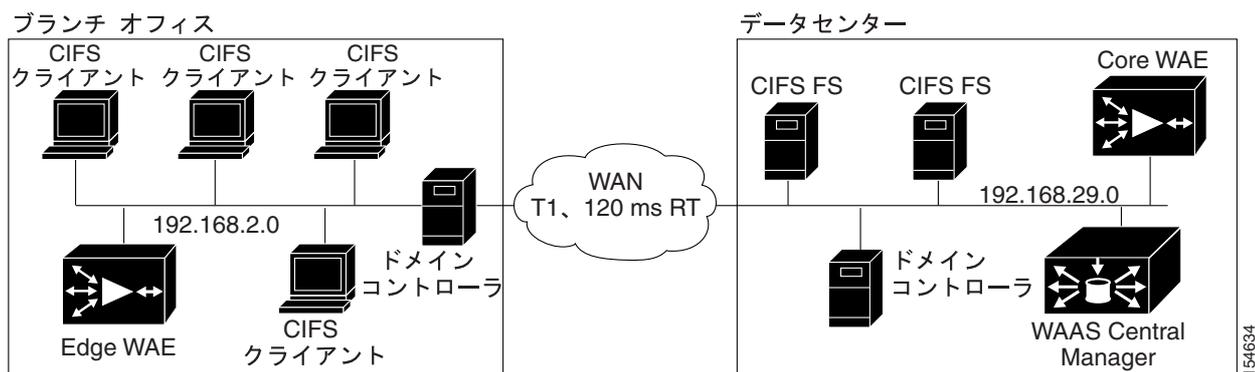
Wide Area Application Service (WAAS) ファイル サービス機能は、ブランチ オフィスのユーザ付近の Edge WAE でデータをキャッシュして、WAN の遅延と帯域幅制限を解決します。このデータ キャッシング方式により、ブランチ オフィスのユーザは、WAN 経由で LAN に似た速度で集中管理されたデータにアクセスできます。ソリューションは、いくつかの重要な概念に基づいています。

- **できるだけ WAN を使用しない** — WAAS は、WAN を横断する必要がある操作の数を最小限に抑えることで、実質的にユーザが WAN から受ける多くの障害をなくします。
- **WAN を最適利用する** — ファイル サービス機能は、システムが WAN を最適利用できる高度なキャッシング、圧縮、およびネットワーク最適化技術を使用します。
- **ファイル システム プロトコルの意味を維持する** — Cisco WAAS は、WAN 経由で独自のプロトコルを使用しますが、標準のファイル システム プロトコル コマンドの意味を完全に維持します。そのため、実質的にネットワーク内のデータの正確性と一貫性が維持されます。

- ソリューションをユーザに**透過的にする** — 最善のソリューションは、エンドユーザの操作を中断せず、ユーザが業務方法を変更する必要がないソリューションです。WAAS ファイル サービス ソリューションは、サーバ側とクライアント側のいずれにもソフトウェアをインストールする必要がなく、ユーザが新しいことを学習する必要もありません。ユーザは、仕事の進め方を変更せずに、安全なデータセンターがあることによるすべての利点を活用できます。

WAAS ファイル サービス機能を使用すると、企業は、データを正しく管理するために必要な設備、IT スタッフ、およびストレージ デバイスを提供するデータセンターにファイル サーバを集約できます。図 11-1 に、WASS ファイル サービスを設定したあとの典型的な構成シナリオを示します。

図 11-1 WAAS ファイル サービス ソリューション



ファイル サービス機能の概要

次の各項で、WAAS ファイル サービス機能について説明します。

- 自動検出 (p.11-4)
- 事前配置 (p.11-4)
- データー貫性 (p.11-5)
- データ並列性 (p.11-6)
- ファイルブロック (p.11-7)
- Microsoft との相互運用性 (p.11-7)

自動検出

自動検出機能により、「Edge WAE キャッシュへエクスポートするためのファイル サーバの設定」(p.11-17) の説明に従って、個々のファイル サーバを WAAS Central Manager に登録しなくても WAFS を有効にすることができます。自動検出機能により、WAAS は、透過モードの CIFS 要求を受信すると、自動的に新しいファイル サーバを発見し、そのファイル サーバに接続しようとします。ファイル サーバへのパスが複数ある場合、WAAS は最も遅延の小さいパスを選択します。

Core WAE と検出されたサーバの間の遅延が 25 ミリ秒を超える場合、サーバは遠すぎると判断され、接続は最適化されません。さらに、Edge WAE とサーバの間の遅延が 2 ミリ秒を超える場合、サーバはローカルと判断され、接続は最適化されません。

自動検出機能は、デフォルトでは、未登録のファイル サーバへの CIFS 要求に対して動作します。しかし、自動検出されたファイル サーバと通信するときには WAFS 機能が制限されるため、ファイル サーバを登録したい場合もあります。自動検出されたファイル サーバでは、事前配置、動的共有、ファイルブロック、および切断モードの WAFS 機能は使用できません。さらに、ファイル サーバにデジタル署名が必要な場合、WAFS はそのデータをキャッシュできません。

新しいファイル サーバはポリシー エンジンの動的マップに追加されるので、**show policy-engine application dynamic EXEC** コマンドを使用して、これらのファイル サーバを見ることができます。ファイル サーバは、最後の接続が閉じてから 3 分間動的マップに残っています。

事前配置

事前配置機能を使用すると、システム管理者は、頻繁に使用するファイルを中央のストレージから選択した Edge WAE のキャッシュに「事前に」配置できます。これにより、ユーザは最初からファイルに高速アクセスでき、使用可能な帯域幅の使用効率が上昇します。WAAS Central Manager GUI から、事前配置ディレクティブを作成します。

エンドユーザが Edge WAE キャッシュにないファイルを開こうとすると、Edge WAE は、ファイルが保存されているファイル サーバから WAN 経由でファイルを取得します。事前配置は、管理者が、定義済みのスケジュールに従って、頻繁にアクセスされる大型ファイルをファイル サーバから選択した Edge WAE キャッシュへ保存できる機能です。管理者が事前配置を正しく使用することで、ユーザは、これらのファイルに初めてアクセスするときでも、キャッシュ レベルのパフォーマンスを利用できます。事前配置は、ネットワークがアイドル状態にあるときに（夜間など）重い内容を転送し、日中は他のアプリケーションに帯域幅を解放して、WAN 帯域の利用率を改善します。

WAAS Central Manager GUI を使用すると、管理者は、(それぞれのスケジュールが設定された) 相互に重なる複数の事前配置ポリシー、対象 Edge WAE のリスト、および定義された時間とサイズの制約を作成できます。



(注) 事前配置には、複数のルートを設定する機能も含まれます。「[新しい事前配置ディレクティブの作成](#)」(p.11-29) を参照してください。

データ一貫性

Cisco WAAS は、相互に関係のある 2 つの機能を使用して、システム全体のデータ整合性を保証します。その 1 つは、データの最新性を管理する **一貫性** です。もう 1 つは、複数のクライアントによるデータ アクセスを制御する **並列性** です。

複数の位置で複数のコピーを維持すると、そのうちのいくつかのファイルが変更される可能性が増し、他のファイルとの一貫性が失われます。一貫性の意味は、最新性（コピーが最新であるかどうか）と元のファイルサーバと交換される更新の伝搬の保証のために使用されます。

Cisco WAAS は、組み込み一貫性ポリシーに次の一貫性の意味を適用します。

- **サイト内での厳格な CIFS 動作** — 同じキャッシュのユーザは、常に標準の厳格な CIFS 一貫性の意味が保証されます。
- **CIFS を開くときのキャッシュ検査** — CIFS では、**ファイルを開く**操作は、ファイルサーバへ転送されます。一貫性を守るため、Cisco WAAS は、ファイルを開くたびにファイルの最新性を検査し、ファイルサーバのファイルが更新されている場合、キャッシュされたファイルを無効にします。

Cisco WAAS は、キャッシュ内のファイルのタイムスタンプとファイルサーバ上のファイルのタイムスタンプを比較して、データを検査します。タイムスタンプが同一の場合、Edge WAE 上のキャッシュされたコピーは有効と見なされ、ユーザは Edge WAE キャッシュからファイルを開くことを許可されます。

タイムスタンプが異なる場合、Edge WAE は、キャッシュからファイルを削除し、ファイルサーバに最新のコピーを要求します。

- **キャッシュの事前更新** — Cisco WAAS は、Edge WAE でキャッシュされているデータの最新性を維持するために、CIFS 環境での変更通知の使用をサポートしています。

クライアントがディレクトリまたはファイルを変更すると、Edge WAE は、ファイルサーバへ変更通知を送信します。次に、ファイルサーバは、変更されたディレクトリとファイルのリストを含む変更通知をすべての Edge WAE へ送信します。変更通知を受信すると、各 Edge WAE は、キャッシュ内の通知にリストされているディレクトリとファイルを無効にし、最新バージョンでキャッシュを更新します。

たとえば、ユーザが既存の Word 文書を編集し、Edge WAE キャッシュに変更を保存すると、Edge WAE は、ファイルが変更されたことを知らせる変更通知をファイルサーバへ送信します。次に、Edge WAE は、変更されたセクションをファイルサーバへ送信し、ファイルサーバは予防的に変更通知をネットワーク内の他の Edge WAE へ送信します。次に、これらの Edge WAE は、すべてのアクセスポイント全体でファイルが一貫するようにキャッシュを更新します。

このプロセスは、ディレクトリの名前を変更する、新しいサブディレクトリを追加する、ファイルの名前を変更する、またはキャッシュされたディレクトリに新しいファイルを作成するときにも適用されます。

- **CIFS を閉じるときのフラッシュ** — CIFS では、**ファイルを閉じる**操作は、すべての書き込みバッファをファイルサーバにフラッシュし、すべての更新がファイルサーバに伝達されたあとでは、**閉じる**要求だけが許可されます。一貫性の観点からは、ファイルを開くときの有効性と検査ファイルを閉じるときのフラッシュとの組み合わせが、Microsoft Office のような良好なアプリケーションがセッションの意味で動作することを保証します。Cisco WAAS ネットワークでは、開く、ロック、編集、ロック解除、および閉じるコマンドが正しく動作することが保証されます。
- **経過時間に基づくディレクトリの検査 (CIFS)** — ディレクトリは、設定済みの経過時間に関連付けられています。経過時間が経過すると、Edge WAE キャッシュはディレクトリを再検査します。

ユーザが初めてディレクトリの内容を表示しようとする、Edge WAE は、ファイルサーバがユーザとグループのアクセス権を含むディレクトリの Access Control List (ACL; アクセスコントロールリスト) を使用して、許可検査を実行できるようにします。Edge WAE は、ユーザがどのディレクトリにアクセスし、ファイルサーバがそのアクセスを許可したかどうかを監視します。ユーザが短い期間 (経過時間) に同じディレクトリに再びアクセスしようとする、Edge WAE はファイルサーバにアクセスせず、その代わりにキャッシュされたアクセス権を使用して、ユーザにアクセスを提供するかを決定します。経過時間が経過すると、Edge WAE はファイルサーバにアクセスして、キャッシュされたユーザのアクセス権を更新します。

この許可プロセスは、ユーザがファイルサーバでアクセスする許可を持っていないキャッシュ内のディレクトリやファイルにアクセスすることを防止します。

データ並列性

並列性制御は、複数のユーザがキャッシュされた同じデータに読み取り、書き込み、またはその両方のアクセスを行うときに重要です。並列性制御は、ファイルシステムロックを確立および削除して、このアクセスを同期化します。このファイルロック機能は、データ整合性を保証し、次の利点を提供します。

- クライアントは、リモートファイルサーバからデータを取得しなくてもよいように、積極的にファイルデータをキャッシュできます。
- 既存の CIFS クライアント実装で動作する多くのアプリケーションのパフォーマンスを改善します。
- 一度に 1 人のユーザだけがファイルのセクションを変更できるので、データ整合性が維持されます。

Cisco WAAS は、ネットワーク帯域幅を使用して WAN 経由でファイルサーバでデータの読み取りや書き込みを実行する代わりに、ローカルキャッシュで安全にデータの読み取りや書き込みを実行できるように、ユーザがファイルをロックできる CIFS oplock 機能をサポートしています。oplock を使用すると、ユーザは、他のユーザがファイルにアクセスしていないことが分かっているため、キャッシュされたデータが古くなることなく、事前に先行読み出しデータをキャッシュできます。また、ユーザは、ローカルキャッシュにデータを書き込むことができ、ファイルを閉じるまで、または別のユーザが同じファイルを開くように要求するまで、ファイルサーバを更新する必要がありません。

oplock は、ファイルだけに適用されます。ファイルサーバは、ディレクトリと名前付きパイプに oplock 要求を許可しません。

ファイルロックプロセス

ユーザがファイルを開くと、ロック要求がファイルサーバへ送信されます。Edge WAE は、ユーザからファイルサーバへのすべてのロック要求とファイルサーバからユーザへのすべての応答を代行受信し、転送します。他のユーザがファイルにロックを設定していない場合、ファイルサーバは、ユーザが安全にファイルをキャッシュできるように排他ロック要求を許可します。

2 番目のユーザが同じファイルを開くように要求すると、次の処理が実行されます。

1. ファイルサーバは、最初のユーザが取得した排他的ファイルロックを取り消します。
2. 最初のユーザは、次の処理を実行します。
 - キャッシュに保存されたファイルの変更をファイルサーバにフラッシュします。この処理により、ファイルを開く 2 番目のユーザがファイルサーバから最新の情報を受信することが保証されます。
 - 2 番目のユーザがファイルを開いたためにそのデータの最新性が保証されないため、ファイル用の先行読み出しバッファを削除します。
3. ファイルサーバは、2 番目のユーザにファイルを開くことを許可します。

ファイル ブロック

ファイル ブロック オプションを使用すると、定義したファイル パターンと一致するファイルをユーザが開く、作成する、またはコピーすることを防止する 1 つまたは複数のファイル ブロック ディレクティブを定義できます。これらのディレクティブは、ファイル サービスが有効になっているすべての Edge WAE に適用され、ブロックするファイルで、限られた帯域幅、ファイル サーバ、およびキャッシュ空間が浪費されることを防止します。

Microsoft との相互運用性

WAAS ファイル サービス機能は、次の Microsoft CIFS 機能と相互運用できます。

- ユーザ認証と許可用の Active Directory
- Microsoft CIFS のオフライン フォルダ
- Microsoft DFS インフラストラクチャ
- 「共有フォルダ用の Windows シャドウ コピー」(p.11-7) の説明に従う共有フォルダ用の Windows シャドウ コピー

共有フォルダ用の Windows シャドウ コピー

WAAS ファイル サービスは、Windows Server 2003 オペレーティング システムの一部である共有フォルダ用のシャドウ コピー機能をサポートしています。この機能は、Microsoft Volume Shadow Copy Service を使用して、ユーザが前バージョンのフォルダやファイルを簡単に表示できるように、ファイル システムのスナップショットを作成します。

WAAS 環境では、ユーザは、ネイティブ Windows 環境と同様に、Edge WAE からフォルダまたはファイルを右クリックし、**[Properties]**、**[Previous Version]** プロパティを選択して、シャドウ コピーを表示します。

機能の制限事項を含む共有フォルダ用のシャドウ コピーの詳細については、Microsoft Windows Server 2003 の資料を参照してください。

ユーザは、Edge WAE 上のシャドウ コピー フォルダにアクセスするとき、ファイル サーバ上のネイティブ環境と同じ作業を実行できます。これらの作業は、次のとおりです。

- シャドウ コピー フォルダの参照
- シャドウ コピー フォルダの内容のコピーまたは復元
- シャドウ コピー フォルダ内のファイルの表示およびコピー

共有フォルダ機能用のシャドウ コピーは、次の作業をサポートしていません。

- シャドウ コピー ディレクトリの名前の変更または削除
- シャドウ コピー ディレクトリ内のファイルの名前の変更、作成、または削除

サポートされるサーバおよびクライアント

WAAS は、次のファイル サーバで共有フォルダ用のシャドウ コピーをサポートしています。

- Windows 2003 (SP1 付き、SP1 なし)
- NetApp Data ONTAP バージョン 6.5.2、6.5.4 および 7.0
- EMC Celerra バージョン 5.3 および 5.4

WAAS は、次のクライアント用の共有フォルダ用のシャドウ コピーをサポートしています。

- Windows XP Professional

- Windows 2000 (SP3 以降)
- Windows 2003



(注) Windows 2000 および Windows XP (SP2 なし) クライアントでは、共有フォルダ用のシャドウ コピーをサポートするために、前バージョンのクライアントをインストールする必要があります。詳細については、次の Microsoft 資料を参照してください。

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/22a0add1-d224-47ee-8f6e-65103fb63e23.mspx>

ファイル サービスの準備

WAE でファイル サービスを有効にする前に、必ず、次の作業を完了してください。

- 同一の設定で複数のデバイスを設定する場合は、ファイル サービスを有効にするすべてのエッジ デバイスを含むデバイス グループを作成したことを確認します。デバイス グループを作成する方法については、[第 3 章「デバイス グループとデバイス位置の使用」](#)を参照してください。
- ファイル サービスを有効にするエッジ デバイスを識別します。エッジ デバイスは、ローカル ファイル サーバを他のエッジ デバイスへエクスポートする場合、コア デバイスとしても機能できます。
- エクスポートするファイル サーバを識別し、[表 11-1](#) を参照してこれらのファイル サーバが Cisco WAAS によってサポートされていることを確認します。

表 11-1 サポートされているファイル サーバ

ベンダー	製品	バージョン
Dell	PowerVault	715N
Network Appliance	FAS270	ONTAP 7.0.1R.1
	FAS250	ONTAP 7.0.1R.1
	F760	6.5.2R1P16
	F85	6.4.5
Spinnaker	SpinServer 3300	2.5.5p2 (カーネル 2.4.18spinos)
EMC	Celerra NS702	5.4.17.5
	Celerra NS702	5.4.14-3
	Celerra NS501	5.3.12-3
Microsoft	Windows NT 4.0	
	Windows Server 2000	サービス パックなし、SP1、SP3、および SP4
	Windows Server 2003	サービス パックなし、SP1、および R2
Novell ¹	6.5	SP-3
RedHat	Samba	3.0.1.4a

1. WAAS は、NCP、eDirectory/NDS、および iPrint 用の CIFS 最適化、サーバ統合、および汎用のネットワーク加速のために、Novell6.5 をサポートしています。Novell ファイル サーバが NFAP オプションを使用する場合、WAAS は、WAAS CIFS アダプタを使用して、プロトコル層とトランスポート層で Novell トラフィックを最適化できます。NFAP は、Novell の NCP (Novell Core Protocol) のほかに CIFS プロトコルを使用する Novell のネットワーク ファイル アクセス パックです。

NME-WAE でのファイル サービスの使用

シスコ製アクセス ルータに搭載したネットワーク モジュールで WAAS を稼働している場合は、エッジおよびコア ファイル サービスをサポートするために特定のメモリ要件があります。エッジ ファイル サービスを有効にするには、NME-WAE に 1 GB 以上のメモリが必要です。コア ファイル サービスまたはコアおよびエッジ ファイル サービスの両方を有効にするには、NME-WAE に 2 GB 以上のメモリが必要です。デバイスに十分なメモリがないときにエッジまたはコア ファイル サービスを有効にしようとすると、WAAS Central Manager はエラー メッセージを表示します。

[Device Home] ウィンドウで、デバイスのメモリ量を確認できます。詳細については、[「\[Device Home\] ウィンドウ」 \(p.15-11\)](#) を参照してください。

ファイル サービスの設定

表 11-2 に、ファイル サービスを設定するために完了する必要がある手順の概要を提供します。

表 11-2 ファイル サービスを設定するためのチェックリスト

作業	追加情報と手順
1. ファイル サービスを準備する。	WAAS デバイスでファイル サービスを有効にし、設定する前に、完了する必要がある作業を提供します。詳細については、「 ファイル サービスの準備 」(p.11-9) を参照してください。
2. WAFS コア クラスタを設定する。	WAFS コア クラスタは、エクスポートされたファイル サーバから Edge WAE のキャッシュヘデータをコピーする必要があります。詳細については、「 コア クラスタの設定 」(p.11-10) を参照してください。
3. エッジ デバイスを設定する。	デフォルトで、ファイル サービスは、WAAS デバイスで有効になっていません。エッジ デバイスでファイル サービスを有効にし、開始するには、「 エッジ デバイスの設定 」(p.11-13) を参照してください。
4. ファイルサーバを WAAS に登録する (任意)。	どのファイル サーバをエクスポートするかを WAAS システムに指定します。また、この手順は、コア クラスタと登録したファイル サーバ間のリンクを作成します。詳細については、「 Edge WAE キャッシュヘエクスポートするためのファイル サーバの設定 」(p.11-17) を参照してください。自動検出を使用している場合、この手順はオプションです。
5. 動的共有を識別する (任意)。	エクスポートされたファイル サーバで、動的共有を識別します。ファイル サーバに動的共有がない場合は、この手順を省略できます。 詳細については、「 登録したファイル サーバ用の動的共有の作成 」(p.11-21) を参照してください。
6. コア クラスタとエッジ デバイス間の接続を作成する。	コア クラスタが Edge WAE キャッシュヘデータをコピーできるようにします。詳細については、「 コア クラスタと Edge WAE 間の接続の作成 」(p.11-23) を参照してください。
7. ファイル ブロック ディレクティブを作成する (任意)。	エンドユーザが開く、作成する、またはコピーできないファイルの種類を定義します。詳細については、「 ファイル ブロック ディレクティブの作成 」(p.11-27) を参照してください。
8. 事前配置ディレクティブを作成する (任意)。	エクスポートされたファイル サーバから Edge WAE キャッシュヘどのファイルを予防的にコピーするかを定義します。詳細については、「 事前配置ディレクティブの作成 」(p.11-28) を参照してください。

コア クラスタの設定

ファイル サービスを設定する最初の手順では、デバイスでコア サービスを有効にし、デバイスをコア クラスタに割り当てます。コア クラスタには、エクスポートされたファイル サーバ (または複数のファイル サーバ) から Edge WAE のキャッシュヘデータをコピーする役割があります。後続の各項で、クラスタがどのファイル サーバをエクスポートし、どのエッジ デバイスをキャッシュされたデータで満たすかが分かるように、エッジ デバイスとファイル サーバ (任意) をこのコア クラスタに割り当てます。

手順 1 ~ 7 で、コア サーバ サービスを有効にし、デバイスをコア クラスタに割り当てます。手順 8 ~ 12 で、新しいコア クラスタを設定します。この手順の最後の手順で、デバイスが Core WAE として機能するために必要なデバイスをリロードする方法について説明します。

WAFS コア クラスタを作成するには、次の手順に従ってください。

ステップ 1 WAAS Central Manager GUI から、**[Devices] > [Devices]** を選択します。

[Devices] ウィンドウに、WAAS システムに作成されているデバイスのリストが表示されます。

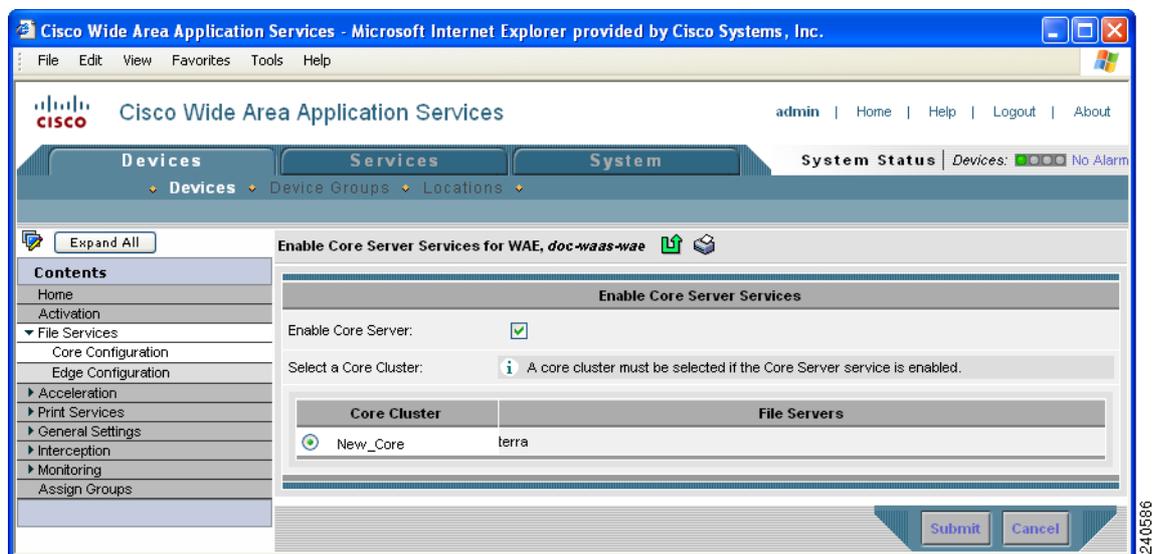
ステップ 2 新しいコア クラスタに入れたいデバイスの横にある **[Edit]** ボタンをクリックします。

[Device Home] ウィンドウが表示されます。

ステップ 3 [Contents] ペインから、**[File Services] > [Core Configuration]** を選択します。

[Enable Core Server Services] ウィンドウが表示されます (図 11-2 を参照)。

図 11-2 コア サーバ サービスの有効化



ステップ 4 **[Enable Core Server]** チェック ボックスを選択します。

ステップ 5 次のいずれかの方法を使用して、このデバイスをコア クラスタに割り当てます。

- このデバイス用の新しいコア クラスタを作成するには、空の [Core Cluster] フィールドの横にあるオプション ボタンを選択し、この空のフィールドに新しいコア クラスタの名前を入力します。この名前にはスペースや特殊文字を入れることができません。
- このデバイスを既存のコア クラスタに参加させるには、そのコア クラスタの横にあるオプション ボタンを選択します。既存のコア クラスタがない場合は、このデバイス用の新しいコア クラスタを作成します。

ステップ 6 **[Submit]** をクリックします。

デバイスがコア サーバとして機能するために、手動でデバイスをリブートする必要があることを知らせるポップアップ メッセージが表示されます。

ステップ 7 ポップアップメッセージを読んだら、[OK] をクリックします。

デバイスでコア サーバ サービスが有効になり、デバイスが指定したコア クラスタに参加します。この手順の最後で、コア サービスをアクティブにするために必要なデバイスをリブートする方法について説明します。

ポップアップメッセージで [Cancel] をクリックすると、[Enable Core Server window] ウィンドウへ戻り、変更は送信されません。

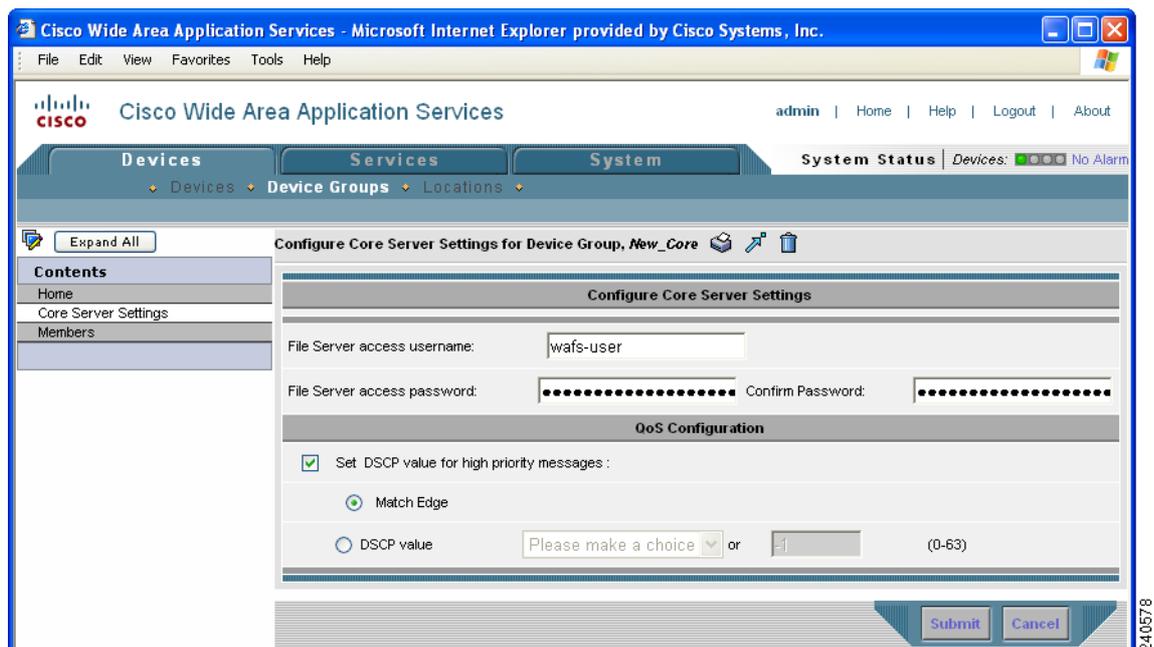
ファイル サーバを明示的に登録する代わりに自動検出機能に依存していて、オプションの Differentiated Services Code Point (DSCP; DiffServ コードポイント) を設定する必要がない場合、[ステップ 14](#)に移ることができます。

ステップ 8 WAAS Central Manager GUI から、[Devices] > [Device Groups] を選択します。

ステップ 9 新しいコア クラスタの横にある [Edit] アイコンをクリックします。

ステップ 10 [Contents] ペインから、[Core Server Settings] を選択します。[Configure Core Server Settings] ウィンドウが表示されます ([図 11-3](#) を参照)。

図 11-3 コア クラスタの設定例



ステップ 11 [File Server access username]、[File Server access password]、および [Confirm password] フィールドに、このコア クラスタがエクスポートする CIFS ファイル サーバに関するアクセス情報を入力します。ファイル サーバを明示的に登録する代わりに自動検出機能に依存している場合、これらのフィールドは必要ありません。

「Edge WAE キャッシュへエクスポートするためのファイル サーバの設定」(p.11-17) で、このコア クラスタがどのファイル サーバにエクスポートするかを指定します。

ステップ 12 オプションで、次の手順に従って、優先順位の高いメッセージ用の DSCP 値を設定します。

- a. **[Set DSCP value for high priority messages]** チェックボックスを選択します。
- b. 次のいずれかのオプションを選択します。
 - **[Match Edge]** — このコア クラスタに接続している Edge WAE の DSCP 値と照合します。この照合は、「コア クラスタと Edge WAE 間の接続の作成」(p.11-23) の説明に従ってエッジ デバイスとコア デバイス間の接続を作成するときに実行されます。
 - **[DSCP Value]** — このコア クラスタ用の DSCP 値を指定できます。
ドロップダウン リストから値を選択し、サポートされている値の説明について表 11-3 を参照します。ドロップダウン リストから **[Please Make a Choice]** を選択する場合は、対応するフィールドに 0 ~ 63 の値を入力します。

DSCP は、ネットワーク トラフィックに異なるレベルのサービスを割り当てることができる IP パケットのフィールドです。ネットワーク上の各パケットに (表 11-3 に示す) DSCP コードを付け、対応するサービスのレベルを割り当てて、サービスのレベルを割り当てます。DSCP は、[IP precedence] フィールドと [Type of Service (ToS)] フィールドの組み合わせです。詳細については、RFC 2474 を参照してください。

システムのパフォーマンスを改善するために、WAFS 制御トラフィック用の DSCP 値を設定することを推奨します。それには、QoS マーキングを実施するようにルータを設定する必要があります。

ステップ 13 **[Submit]** をクリックします。

ステップ 14 タスクバーの **[Reload WAE]** アイコンをクリックするか、次の手順を実行して、デバイスをリロードします。

- a. WAAS Central Manager GUI から、**[Devices] > [Devices]** を選択します。
- b. コア サービスを有効にしたデバイスの横にある **[Edit]** アイコンをクリックします。[Device Home] ウィンドウが表示されます。
- c. タスクバーの **[Reload WAE]** アイコンをクリックします。デバイスがリブートし、デバイスでコア サービスがアクティブになります。

エッジ デバイスの設定

コア クラスタを作成し、設定したら、次の手順では、キャッシュにエクスポートされたファイル サーバ データを含むエッジ デバイスを設定します。

デバイスまたはデバイス グループでエッジ サーバを有効にするには、次の手順に従ってください。

ステップ 1 WAAS Central Manager GUI から、**[Devices] > [Devices]** または **[Devices] > [Device Groups]** を選択します。



(注) ネットワークで Web Cache Communication Protocol (WCCP; Web キャッシュ通信プロトコル) が有効になっている場合は、エッジ デバイス グループでファイル サービスを有効にすることを推奨します。WCCP が無効になっている場合は、名前の競合を防止するために、個々のエッジ デバイスでファイル サービスを有効にする必要があります。

ステップ 2 ファイル サービスを有効にするデバイスまたはデバイス グループの横にある **[Edit]** アイコンをクリックします。

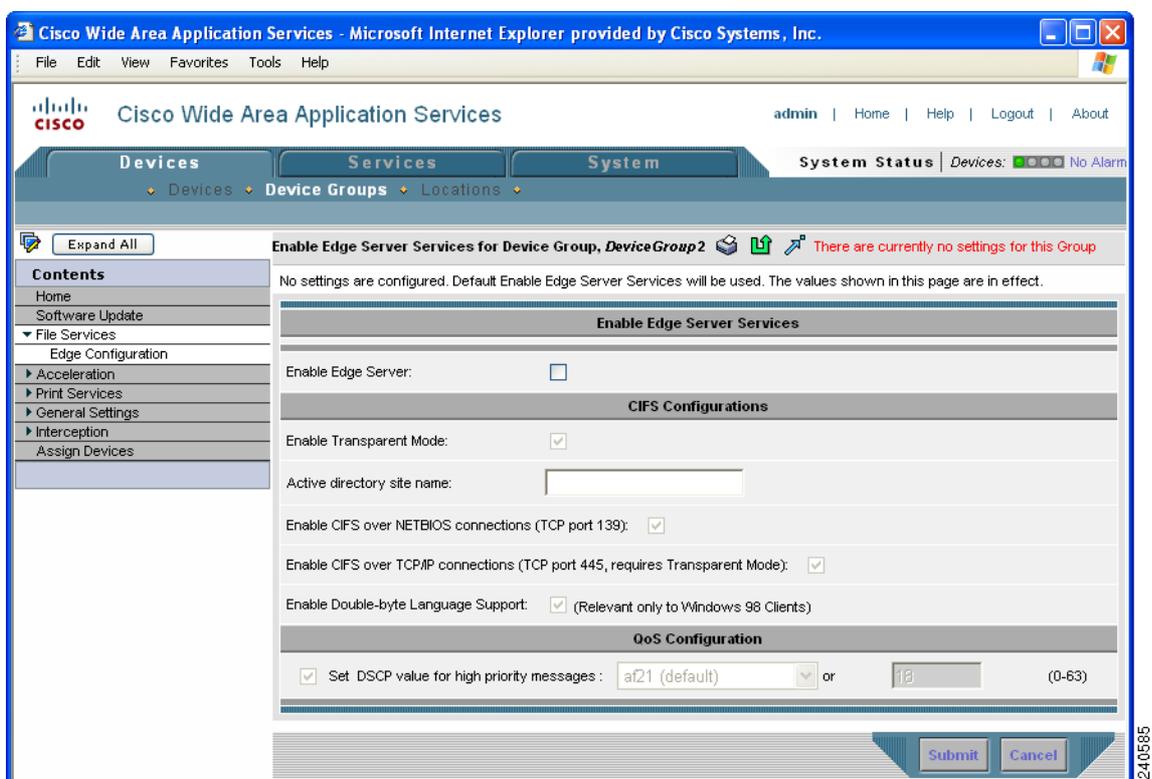
選択したオプションに応じて、**[Device Home]** ウィンドウまたは **[Modifying Device Group]** ウィンドウが表示されます。

WAAS Central Manager デバイスでは、エッジ サービスを有効にできません。

ステップ 3 **[Contents]** ペインから、**[File Services]** > **[Edge Configuration]** を選択します。

[Enable Edge Server Services] ウィンドウが表示されます (図 11-4 を参照)。

図 11-4 エッジ デバイス上のファイル サービスの有効化



ステップ 4 **[Enable Edge Server]** チェック ボックスを選択します。

ウィンドウの他のフィールドが有効になります。

ステップ 5 ネットワークで WCCP または PBR が有効になっている場合、またはインライン モードを使用している場合は、**[Enable Transparent Mode]** チェック ボックスを選択します。

透過モードが有効になっているかどうかに基づいて、ポート 139 と 445 を有効にするためのオプションが自動的に更新されます。

透過モードを有効にすると、TCP ポート 139 とポート 445 を有効にするためのオプションが自動的に選択されます。透過モードを無効にすると (**[Enable Transparent Mode]** を選択しないと)、TCP ポート 139 を有効にするオプションは選択され、ポート 445 は透過モードだけで使用されるため、TCP ポート 445 を有効にするオプションは選択されません。

ステップ 6 提供されるフィールドに、Active Directory サイトの名前を入力します。

ステップ 7 次のオプションを選択して (少なくとも 1 つは選択する必要がある)、Edge WAE で関連するポートを有効にします。

- **[Enable CIFS over NETBIOS connections (tcp port 139)]** — クライアントと Edge WAE 間およびコア クラスタとファイル サーバ間でポート 139 が開いている場合、このオプションを選択します。

セキュリティ上の理由から、ネットワークでポート 139 が開いていない場合は、このオプションの選択を解除し、次の作業を実行します。

- ルータ と Edge WAE で WCCP を有効にするか、または Edge WAE でインライン モードを有効にします。詳細については、[第 4 章「トラフィック代行受信の設定」](#)を参照してください。
- **[Enable CIFS Over TCP/IP Connections]** チェック ボックスを選択して、Edge WAE 上のポート 445 を有効にします。

- **[Enable CIFS over TCP/IP connections (tcp port 445, requires Transparent Mode)]** — ネットワークでポート 445 が開いている場合は、このオプションを選択します。

ネットワークでポート 445 が閉じている場合は、Edge WAE がこのポートで接続を確立しようと試みないようにこのオプションの選択を解除し、**[Enable CIFS over NETBIOS connections]** チェック ボックスを選択します。

ポート 445 を無効にすると、すべてのクライアントが Edge WAE のポート 139 に直接接続し、コア クラスタはファイル サーバのポート 139 に接続します。



(注) ポート 139 とポート 445 上の接続を有効または無効にしても、既存のクライアントは Edge WAE との接続を失いません。

ステップ 8 日本語のような 2 バイト言語をサポートする必要がある Windows 98 クライアントがある場合は、**[Enable Double-byte Language Support]** チェック ボックスを選択します。

次の状況では、このオプションを選択しないでください。

- 環境に Windows 98 クライアントが存在しない。
- 環境に Windows 98 クライアントが存在するが、1 バイト言語をサポートするだけでよい。

このオプションの設定に関係なく、英語は常にサポートされています。

ステップ 9 オプションで、次の手順に従って、優先順位の高いメッセージ用の DSCP 値を設定します。

- a. **[Set DSCP value for high priority messages]** チェックボックスを選択します。
- b. ドロップダウン リストから値を選択します。サポートされている値の説明については、[表 11-3](#)を参照してください。

ドロップダウン リストから **[Please Make a Choice]** を選択する場合は、対応するフィールドに 0 ~ 63 の値を入力します。

DSCP は、ネットワーク トラフィックに異なるレベルのサービスを割り当てることができる IP パケットのフィールドです。ネットワーク上の各パケットには DSCP コード ([表 11-3](#) に示す) が付き、対応するサービスのレベルが割り当てられます。DSCP は、**[IP precedence]** フィールドと **[Type of Service (ToS)]** フィールドの組み合わせです。詳細については、RFC 2474 を参照してください。

システムのパフォーマンスを改善するために、WAFS 制御トラフィック用の DSCP 値を設定することを推奨します。それには、QoS マーキングを実施するようにルータを設定する必要があります。

表 11-3 DSCP コード

DSCP コード	説明
af11	AF11 dscp (001010) でパケットを設定します。
af12	AF11 dscp (001100) でパケットを設定します。
af13	AF13 dscp (001110) でパケットを設定します。
af21	AF21 dscp (010010) でパケットを設定します。
af22	AF22 dscp (010100) でパケットを設定します。
af23	AF23 dscp (010110) でパケットを設定します。
af31	AF31 dscp (011010) でパケットを設定します。
af32	AF32 dscp (011100) でパケットを設定します。
af33	AF33 dscp (011110) でパケットを設定します。
af41	AF41 dscp (100010) でパケットを設定します。
af42	AF42 dscp (100100) でパケットを設定します。
af43	AF43 dscp (100110) でパケットを設定します。
cs1	CS1 (優先順位 1) dscp (001000) でパケットを設定します。
cs2	CS2 (優先順位 2) dscp (010000) でパケットを設定します。
cs3	CS3 (優先順位 3) dscp (011000) でパケットを設定します。
cs4	CS4 (優先順位 4) dscp (100000) でパケットを設定します。
cs5	CS5 (優先順位 5) dscp (101000) でパケットを設定します。
cs6	CS6 (優先順位 6) dscp (110000) でパケットを設定します。
cs7	CS7 (優先順位 7) dscp (111000) でパケットを設定します。
デフォルト	デフォルトの dscp (000000) でパケットを設定します。
ef	EF dscp (101110) でパケットを設定します。

ステップ 10 [Submit] をクリックします。デバイスがエッジサーバとして機能するために、手動でデバイスをリブートする必要があることを知らせるポップアップメッセージが表示されます。

ステップ 11 ポップアップメッセージを読んだら、[OK] をクリックします。デバイスでエッジサーバサービスが有効になります。

ポップアップメッセージで [Cancel] をクリックすると、[Edge Configuration] ウィンドウへ戻り、変更は送信されません。

ステップ 12 タスクバーの [Reload WAE] アイコンをクリックするか、次の手順を実行して、デバイスをリロードします。

- a. WAAS Central Manager GUI から、[Devices] > [Devices] または [Devices] > [Device Groups] を選択します。
- b. エッジ サービスを有効にしたデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。
- c. タスクバーの [Reload WAE] または [Reboot All Devices] アイコンをクリックします。デバイスがリブートし、デバイスでエッジ サービスがアクティブになります。

Edge WAE キャッシュへエクスポートするためのファイル サーバの設定

コア クラスタと Edge WAE でファイル サービスを有効にしたら、オプションで WAAS Central Manager GUI を使用して、エクスポートするファイル サーバを設定できます。ネットワークに WAAS ネットワークに定義する必要がある多くのファイル サーバが存在する(たとえば 10 台以上)場合は、プロセスを高速化するために、値をカンマで区切った (CSV) ファイルを作成し、インポートできます。

ファイル サーバを設定しない場合、自動検出機能を利用して、ユーザがファイル サーバにアクセスしたときに WAFS が自動的にファイルサーバを検出できます。ファイル サーバを明示的に登録しない場合は、この項を省略できます。

この項には、WAAS Central Manager GUI でファイル サーバを設定するための次の項目があります。

- [WAAS Central Manager へのファイル サーバの登録 \(p.11-17\)](#)
- [CSV ファイルを使用したファイル サーバ定義のインポート \(p.11-19\)](#)
- [登録したファイル サーバへのコア クラスタの割り当て \(p.11-20\)](#)
- [登録したファイル サーバ用の動的共有の作成 \(p.11-21\)](#)

WAAS Central Manager へのファイル サーバの登録

WAAS Central Manager にファイル サーバを登録するには、次の手順に従ってください。

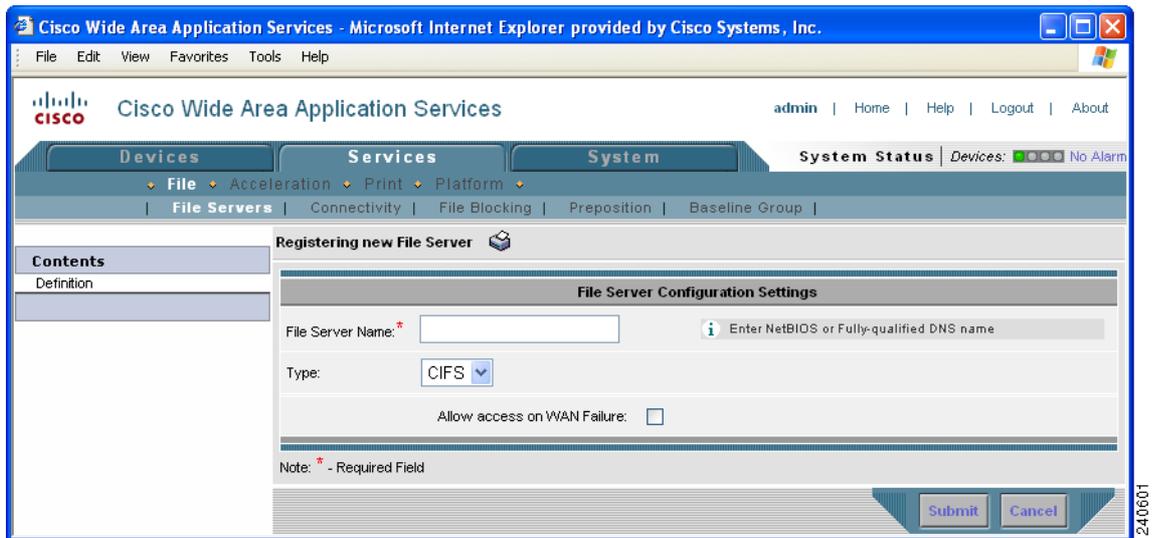
- ステップ 1** WAAS Central Manager GUI から、**[Services] > [File] > [File Servers]** を選択します。**[File Servers]** ウィンドウが表示されます。

このウィンドウから、次の作業を実行できます。

- ファイル サーバの横にある **[Edit]** アイコンをクリックして、既存ファイルサーバの設定を編集します。次に、ファイルサーバ設定を削除したり、任意のファイルサーバ設定を変更できます。
- タスク バーの **[Import from CSV]** アイコンをクリックし、CSV ファイルから複数のファイルサーバ定義をインポートします。(「[CSV ファイルを使用したファイル サーバ定義のインポート](#)」[\[p.11-19\]](#)を参照してください)。
- 次の手順の説明に従って、エクスポートする新しいファイルサーバを識別します。

- ステップ 2** タスクバーの **[Create New File Server]** アイコンをクリックして、エクスポートする新しいファイルサーバを識別します。**[Registering New File Server]** ウィンドウが表示されます。

図 11-5 [Registering New File Server] ウィンドウ



ステップ 3 [File Server Name] フィールドに、エクスポートするファイル サーバのホスト名を入力します。



(注) ファイル サーバに複数の NetBIOS 名または DNS 名がある場合は、ファイル サーバをそれぞれの名前で別々に登録する必要があります。そうでない場合、未登録の NetBIOS 名を使用するクライアントは、接続できません（ただし、TCP ポート 445 で CIFS を使用するクライアントは、正常に動作します）。ファイル サーバの IP アドレスを名前に指定することはできません。

ステップ 4 [Allow Access on WAN Failure] チェック ボックスを選択して、CIFS クライアントが WAN 障害時にこの Edge WAE にキャッシュされたデータに読み取り専用でアクセスできるようにします。

このオプションを有効にすると、WAN 障害が発生した場合に、CIFS クライアントは、キャッシュされるディレクトリ構造を参照し、キャッシュされたファイル全体を読み取ることができます。その間、認証と許可は維持されます。

詳細については、「WAN 障害に対する WAAS ネットワークの準備」(p.11-37) を参照してください。

ステップ 5 [Submit] をクリックします。

ファイル サーバが WAAS システムに登録され、[Contents] ペインが追加オプションで更新されません。

ステップ 6 「登録したファイルサーバへのコア クラスタの割り当て」(p.11-20) に進み、登録したファイルサーバにコア クラスタを割り当てます。

CSV ファイルを使用したファイル サーバ定義のインポート

ネットワークに WAAS ネットワークに定義する必要がある多くのファイル サーバが存在する（たとえば 10 台以上）場合は、プロセスを高速化するために、値をカンマで区切った（CSV）ファイルを作成し、インポートできます。Excel または別の表計算アプリケーションを使用して、CSV ファイルを作成できます。

ここでは、次の内容について説明します。

- CSV ファイル作成要件 (p.11-19)
- CSV ファイルに関する留意事項 (p.11-19)
- CSV ファイルのインポート (p.11-20)

CSV ファイル作成要件

表 11-4 に、CSV ファイルの要件を示します。

表 11-4 CSV ファイルの要件

列見出し	構文 / 意味	説明
名前	ファイル サーバの名前を指定します。[Registering New File Server] ウィンドウの [File Server Name] フィールド (図 11-5) に対応しています。	必須。 WAAS Central Manager へのファイル サーバの登録のステップ 3 と同じ制約。
AllowDisconnected	[Registering New File Server] ウィンドウの [Allow access on WAN Failure] チェック ボックス (図 11-5) に対応しています。適用する場合は「true」に、適用しない場合は「false」に設定します。	オプション。 指定しないと、「false」になります。
Cluster	ファイル サーバを割り当てる既存のコア クラスタの名前を指定します。	オプション。 指定しないと、ファイル サーバはコア クラスタに割り当てられません。 クラスタ名が複数回ファイル サーバに割り当てられている場合、エラー報告されません。

CSV ファイルに関する留意事項

CSV ファイルを作成するときは、次の点に注意してください。

- 最初の行には、指定する列見出しを列挙する必要があります。
- 少なくとも、ファイルには「Name」列が必要です（他の列はオプションです）。
- 列見出しは大文字と小文字を区別せず、任意の順序で指定できます。
- ファイル サーバを複数のコア クラスタに割り当てるには、複数の「Cluster」列を指定できます。データ行に複数のクラスタを指定する場合は、列見出し行に複数の「Cluster」列が必要です。
- 行を指定するときは、各列に値を入れる必要はありません。ただし、正しい数の列を指定する必要があります。すなわち、列の数は、見出し行に定義されるオブジェクトの数と対応する必要があります。次の例は、有効な CSV ファイル項目を示しています（コア クラスタ c-1、c-2、および c-5 が存在すると仮定しています）。カンマが連続する位置は、デフォルト値が使用されることを示します。

例 :

```
name,allowdisconnected,cluster,cluster
s71,TRUE,c-1,
s72,,c-2,c-5
```

CSV ファイルのインポート

CSV ファイルを作成したら、WAAS Central Manager GUI を使用してファイルをインポートします。
CSV ファイルをインポートするには、次の手順に従ってください。

ステップ 1 WAAS Central Manager GUI から、**[Services]** タブをクリックします。

ステップ 2 タスク バーの **[Import from CSV]** アイコン () をクリックします。

[Importing File Server Definitions] ウィンドウが表示されます。

ステップ 3 **[Browse]** をクリックします。

[Choose File] ウィンドウが表示されます。

ステップ 4 インポートする CSV ファイルまで移動してを選択し、**[Open]** をクリックします。[Path to File Server Definitions] フィールドに、パスとファイルサーバ名が表示されます。

ステップ 5 [Importing File Server Definitions] ウィンドウで、**[Submit]** をクリックします。

CSV ファイルがインポートされ、「successfully imported」メッセージが表示されます。

WAAS Central Manager は、次の事項を確認します。

- ファイル見出しが正しい。
- 各行にファイルサーバ名がある。
- ファイルに少なくとも 1 台のファイルサーバが指定されている。
- すべての行に正しい数の列があり、各行の構文が正しい。

ファイルが上記の条件に適合しない場合、WAAS Central Manager にエラーメッセージが表示され、ファイルサーバはインポートされません。エラーメッセージは、最大 10 行のエラーの説明を提供できます。ただし、エラーが見出しやファイルの読み取り不能に関係している場合、それ以上のチェックは行われません。

登録したファイルサーバへのコア クラスタの割り当て

ファイルサーバを WAAS Central Manager に登録したら、少なくとも 1 つのコア クラスタをファイルサーバに割り当てる必要があります。コア クラスタには、Edge WAE のキャッシュヘファイルサーバをエクスポートする役割があります。ファイルサーバを明示的に登録する代わりに自動検出機能に依存している場合は、この手順を行う必要はありません。

登録したファイルサーバにコア クラスタを割り当てるには、次の手順に従ってください。

ステップ 1 WAAS Central Manager GUI から、[Services] > [File] > [File Servers] を選択します。

[File Servers] ウィンドウが表示されます。

ステップ 2 コア クラスタに割り当てたいファイル サーバの横にある [Edit] アイコンをクリックします。

ステップ 3 [Contents] ペインで、[Assign Core Clusters] を選択します。[Core Cluster Assignments] ウィンドウが表示されます。

[Core Cluster Assignments] ウィンドウは、WAAS ネットワークに設定されているデバイス グループを表示します。デフォルトで、10 のデバイス グループが表示されます。

ステップ 4 次のいずれかを実行して、コア クラスタをファイル サーバに割り当てます。

- タスクバーの  をクリックして、使用できるすべてのコア クラスタをファイル サーバに割り当てます。
- ファイル サーバに割り当てたい各コア クラスタの横にある  をクリックします。選択すると、アイコンは  に変化します。



(注) ファイル サーバには、コア クラスタだけを割り当てることができます。ファイル サーバには、() で識別される) 通常のデバイス グループを割り当てることができません。

ステップ 5 選択した WAFS コア クラスタ用の [Resolve File Server Name] アイコン () をクリックします。このアイコンは [Type] 列の横にあり、ファイル サーバ用に入力した名前が IP アドレスに解決ができることを確認します。

このアイコンは、WAFS コア クラスタだけに使用できます。ファイル サーバ名を解決できない場合、[Comments] 列にエラー メッセージが表示されます。その場合は、ファイル サーバの正しい名前を入力したことを確認します。

ステップ 6 [Submit] をクリックします。

選択したコア クラスタの横にあるアイコンが  に変化します。

ステップ 7 (任意) 追加したファイル サーバに動的共有が含まれる場合は、「登録したファイル サーバ用の動的共有の作成」(p.11-21) を参照してください。

ファイル サーバに動的共有が含まれるときは、WAAS Central Manager GUI で動的共有を指定する必要があります。

登録したファイル サーバ用の動的共有の作成

多くのファイル サーバが、複数ユーザがユーザのクレデンシャルに基づいて自動的に別のディレクトリにマップされる同じ共有にアクセスできる動的共有を使用します。一般に、動的共有は、ファイル サーバでユーザ ホーム ディレクトリを設定するために使用されます。

たとえば、ファイル サーバで動的共有として **Home** という名前のディレクトリを設定できます。この共有にアクセスする各ユーザは、自動的にそれぞれの個人用ディレクトリへリダイレクションされます。

登録されたファイル サーバに動的共有が含まれる場合は、この項の説明に従って、その動的共有を **WAAS Central Manager** に登録する必要があります。

動的共有を追加する前に、次の制限事項に注意してください。

- 各動的共有は、ファイル サーバで一意でなければなりません。
- 事前配置ディレクティブを持つ動的共有は、追加できません。動的共有を追加する前に、事前配置ポリシーを削除する必要があります。
- 同じファイル サーバ名と同じ共有名を持つ 2 つの異なる動的共有を追加できますが、それぞれを別のコア クラスタに関連付ける必要があります。共有ごとに異なる ID を持ちます。
- **WAAS Central Manager GUI** を使用すると、動的共有として任意のディレクトリを定義できます。ただし、ファイル サーバで動的共有としてディレクトリを設定しないと、すべてのユーザが同じディレクトリから同じ内容を読み取り、または書き込み、クレデンシャルに基づいて異なるディレクトリへリダイレクションされません。
- 動的共有は、明示的に登録されたファイル サーバにのみ追加できます。動的共有は、自動検出されたファイル サーバではサポートされていません。

動的共有を追加するには、次の手順に従ってください。

ステップ 1 動的共有を追加する前に、次の事項を確認してください。

- 動的共有が、すでに **CIFS** ファイル サーバに設定されている。
- **WAAS Central Manager GUI** でファイル サーバを設定した。ファイル サーバを識別する方法の詳細については、「[Edge WAE キャッシュへエクスポートするためのファイル サーバの設定](#)」(p.11-17) を参照してください。

ステップ 2 **WAAS Central Manager GUI** から、**[Services] > [File] > [File Servers]** を選択します。

エクスポートされたファイル サーバのリストが表示されます。

ステップ 3 動的共有を含む **CIFS** ファイル サーバの横にある **[Edit]** アイコンをクリックします。**[Modifying File Server]** ウィンドウが表示されます。

ステップ 4 **[Contents]** ペインから、**[Dynamic Shares]** を選択します。

[Dynamic Shares] ウィンドウに、選択したファイル サーバ用に定義されたすべての動的共有が表示されます。このウィンドウから、次の作業を実行できます。

- 共有の横にある **[Edit]** アイコンをクリックして、既存の動的共有の設定を編集します。動的共有を削除したり、任意の動的共有設定を変更できます。
- 次の手順の説明に従って、新しい動的共有定義を追加します。

ステップ 5 タスクバーの **[Create New Dynamic Share]** アイコンをクリックして、新しい動的共有を追加します。**[Dynamic Share Configuration Settings]** ウィンドウが表示されます。

ステップ 6 動的共有の名前を入力します。この名前は、ユーザが **Edge WAE** キャッシュ上の共有にアクセスするとき、ユーザに表示されます。

動的共有名では、次の文字は使用できません。/:*?"<>|

ステップ 7 **[Share Name]** フィールドで次のいずれかの作業を実行して、動的共有の位置を指定します。

- ファイル サーバで動的共有の名前を入力します。共有名には、次の文字は使用できません。 \ / : * ? " < > |
- **[Share Name]** フィールドの横にある **[Browse]** をクリックして、正しいルート ディレクトリまで移動します。



(注) **[Browse]** ボタンを表示するには、ファイル サーバがコア クラスタに割り当てられ、クラスタに少なくとも 1 つの Core WAE が含まれる必要があります。この 2 つの条件に適合しない場合、**[Browse]** ボタンは表示されません。

ステップ 8 共有のステータスが **enabled** (有効) に設定されていることを確認します。ステータスを **disabled** (無効) に変更すると、共有は WAAS 環境での動的共有として設定されません。

ステップ 9 **[Submit]** をクリックします。

これで、指定したディレクトリは、Edge WAE キャッシュ上の動的共有として機能します。

コア クラスタと Edge WAE 間の接続の作成

WAAS システムにファイル サーバを登録したら、コア クラスタと Edge WAE 間の接続を作成する必要があります。この接続により、コア クラスタは、Edge WAE 上のキャッシュにファイルをコピーできます。

複数のコア クラスタと Edge WAE を含む接続を定義する前に、コア クラスタと Edge WAE の各リンクが、割り当て帯域幅や往復遅延のような同じ接続パラメータと同じエイリアス方式を持っていることを確認してください。このようになっていない場合は、リンクごとに個別の接続を定義する必要があります。

コア クラスタと 1 台または複数の Edge WAE 間の接続を作成するには、次の手順に従ってください。

ステップ 1 WAAS Central Manager GUI から、**[Services] > [File] > [Connectivity]** を選択します。

[Connectivity] ウィンドウが表示されます。

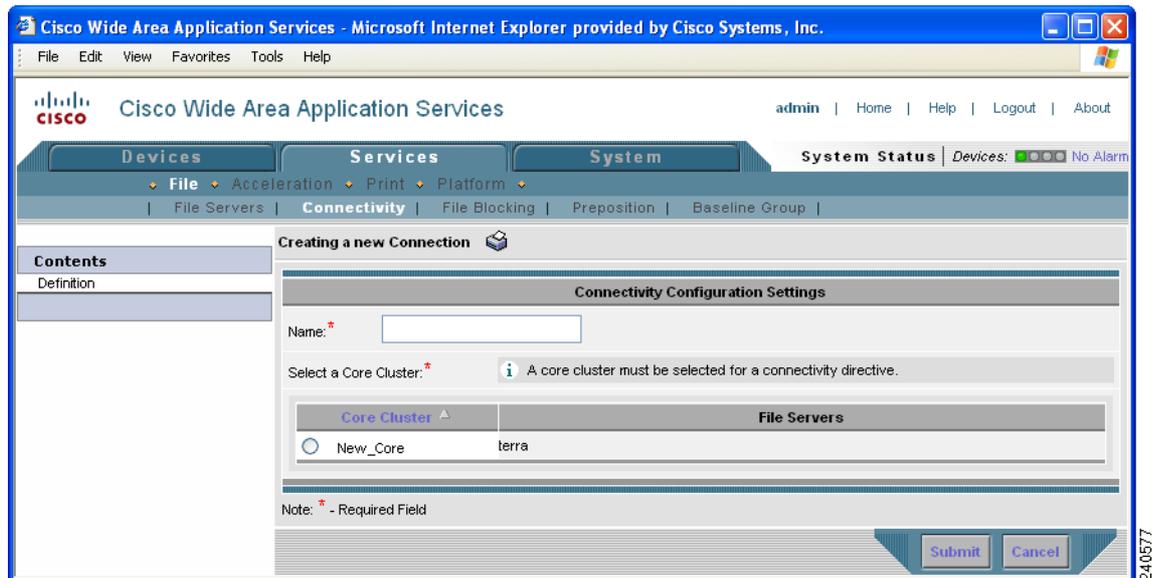
このウィンドウから、次の作業を実行できます。

- 接続の横にある **[Edit]** アイコンをクリックして、既存の接続の設定を編集します。接続を削除したり、任意の接続設定を変更できます。
- 次の手順の説明に従って、新しい接続を追加します。

ステップ 2 タスクバーの **[Create New Connection]** アイコンをクリックして、新しい接続を追加します。

[Creating a New Connection] ウィンドウが表示されます (図 11-6 を参照)。

図 11-6 [Creating a New Connectivity Directive] ウィンドウ



ステップ 3 接続の名前を入力します。

ステップ 4 この接続に入りたいコア クラスタの横にあるオプション ボタンを選択します。

ステップ 5 [Submit] をクリックします。

この接続用にファイル サーバをエクスポートしたくない場合は、エッジ デバイスやグループをこの接続に割り当てる前に、[File Server Settings] ウィンドウで各ファイル サーバの選択を解除する必要があります。このことを知らせるメッセージが表示されます。

ステップ 6 メッセージを読んだら、[OK] をクリックします。

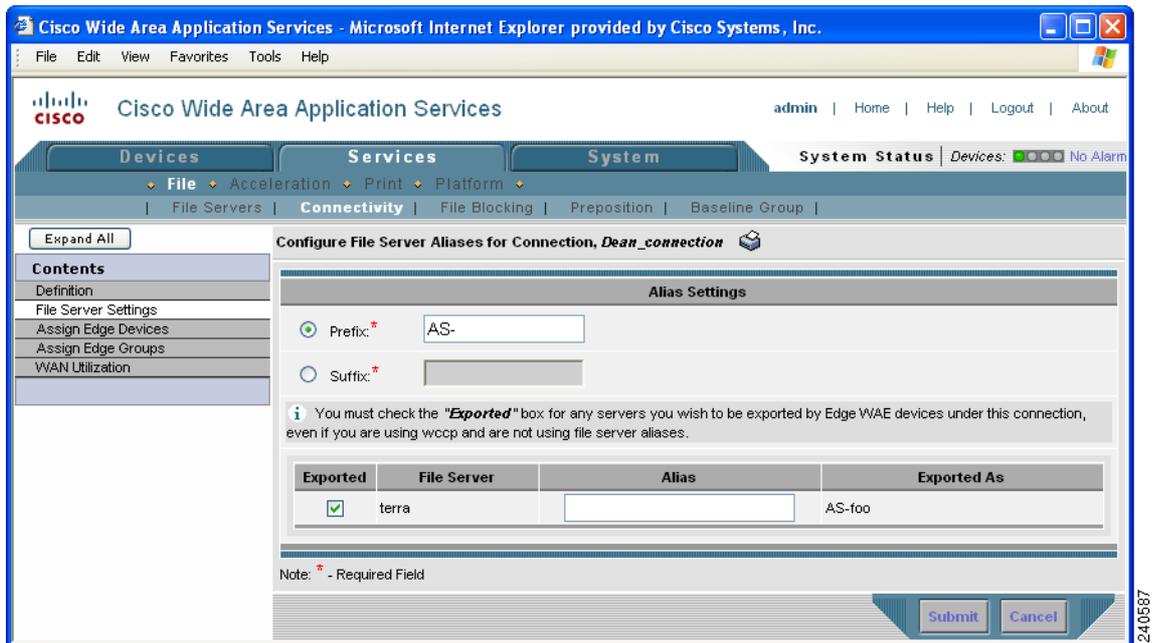
[Contents] ペインが、追加オプションで更新されます。

ファイル サーバを明示的に登録する代わりに自動検出機能に依存している場合、ファイル サーバを設定する必要がないので、[ステップ 12](#)に進みます。

ステップ 7 [Contents] ペインから、[File Server Settings] を選択します。

[Configure File Server Aliases] ウィンドウが表示されます ([図 11-7](#) を参照)。

図 11-7 ファイル サーバのエイリアスの設定



このウィンドウを使用すると、各ファイル サーバの命名方法を定義できます。元のファイル サーバ名、ファイル サーバ名 + プレフィクスまたは拡張子、または独自方式のエイリアスを使用できます。たとえば、プレフィクスとして **as-** を指定し、ファイル サーバの名前が **win3srv** の場合、このファイル サーバはユーザに **as-win3svr** として表示されます。

また、このウィンドウで、コア クラスタにエクスポートさせたいファイル サーバを選択できます。

ステップ 8 次のいずれかのオプションを選択して、プレフィクスまたは拡張子の値を指定します。

- **[Prefix]** — エクスポートされたファイル サーバのエイリアスの先頭に、入力したプレフィクスを追加します。
- **[Suffix]** — エクスポートされたファイル サーバのエイリアスの末尾に、入力した拡張子を追加します。

デフォルトで、WAAS は、ファイル サーバのエイリアスの先頭に **AS-** というプレフィクスを追加します。空白のプレフィクスや拡張子は、入力できません。ステップ 10 の説明に従ってエイリアスを指定すると、プレフィクスと拡張子の設定が更新されます。

ステップ 9 この接続でエクスポートする各ファイル サーバの横にあるチェック ボックスを選択します（少なくとも 1 つを選択する必要があります）。デフォルトで、すべてのファイル サーバが選択されます。



(注) このウィンドウのファイル サーバが表示されない場合は、「登録したファイル サーバへのコア クラスタの割り当て」(p.11-20) の説明のように、このコア クラスタがファイル サーバに割り当てられていないこととなります。先に進む前に、該当する項の手順を完了する必要があります。

ステップ 10 (任意) [Alias] 列に、選択したファイル サーバのエイリアスを入力します。

エイリアスには最大 15 文字の自由な名前を使用できますが、エイリアスは **ステップ 8** で定義したプレフィクスと拡張子のデフォルト設定を更新します。

ステップ 11 [Submit] をクリックします。

[Exported As] 列に、エクスポートされた各ファイル サーバの名前が、エンド ユーザに表示されるように表示されます。

ステップ 12 [Contents] ペインで、次のいずれかのオプションをクリックします。

- **[Assign Edge Devices]** — 個々のエッジ デバイスをこの接続に割り当てます。
- **[Assign Edge Groups]** — エッジ デバイス グループをこの接続に割り当てます。

選択したオプションに応じて、[Edge Device Assignments] ウィンドウまたは [Edge Group Assignments] ウィンドウが表示されます。

ステップ 13 次のいずれかを実行して、この接続に入れるエッジ デバイスを選択します。

- タスクバーの  をクリックして、使用できるすべてのエッジ デバイスまたはグループをこの接続に割り当てます。
- この接続に割り当てたい各エッジ デバイスまたはデバイス グループの横にある  をクリックします。選択すると、アイコンは  に変化します。



(注) エッジ サービスが有効になっているエッジ デバイスまたはデバイス グループだけを割り当てることができます。通常のコア クラスタやオフライン デバイス ( で識別される) は、接続に割り当てることができません。エッジ サービスを有効にする方法については、「[エッジ デバイスの設定](#)」(p.11-13) を参照してください。

ステップ 14 [Submit] をクリックします。

選択した各エッジ デバイスまたはデバイス グループの横にあるアイコンが  に変化します。

ステップ 15 (任意) この接続用の WAN 利用率設定を構成するには、次の作業を実行します。

- [Contents] ペインから **[WAN Utilization]** を選択します。[WAN Utilization] ウィンドウが表示されます。
- Edge WAE と Core WAE 間の WAFS トラフィックで使用される帯域幅を制御する次の WAN 利用率設定を定義します。
 - **[Maximum allocated bandwidth]** — 接続に割り当てる最大帯域幅 (キロビット / 秒) を入力します。この値は、この接続での WAE 間の物理 WAN リンクの最大帯域幅以下でなければなりません。デフォルト設定は、1544 KB / 秒です。WAFS は、帯域幅の使用をこの設定値の 1.5 倍に制限します。
 - **[Minimum roundtrip delay]** — リンクがアイドル状態のときに、1 ビットが、ある WAE と相手側の間の往復にかかる時間 (ミリ秒) を入力します。デフォルト設定は、80 ミリ秒です。



(注) あとでこの接続用の WAN 利用率設定を変更する場合は、新しい値を有効にするために、Edge WAE を再起動する必要があります。

ステップ 16 [Submit] をクリックします。

ファイル ブロック ディレクティブの作成

ファイル ブロック オプションを使用すると、定義したファイル パターンと一致するファイルをユーザが開く、作成する、またはコピーすることを防止する 1 つまたは複数のファイル ブロック ディレクティブを定義できます。これらのディレクティブは、ファイル サービスが有効になっているすべての Edge WAE に適用され、システム管理者がブロックすることに選択したファイルで、帯域幅、ファイル サーバ、およびキャッシュ空間が浪費されることを防止します。

たとえば、MP3 ファイル用のファイル ブロック ディレクティブを作成すると、Cisco WAAS ネットワークに接続しているすべてのユーザが、Edge WAE キャッシュから MP3 ファイルを作成する、開く、またはコピーすることができません。ユーザは、これらのファイルを削除することしかできません。

ファイル ブロック ディレクティブは、明示的に登録されたファイル サーバにのみ追加できます。ファイル ブロックは、自動検出されたファイル サーバではサポートされていません。



(注) ブロックされたファイルは、元のファイル サーバに直接アクセスしないとアクセスできません。

ファイル ブロック ディレクティブを作成するには、次の手順に従ってください。

ステップ 1 WAAS Central Manager GUI から、[Services] > [File] > [File Blocking] を選択します。[File Blocking Directives] ウィンドウが表示されます。

[File Blocking] ウィンドウは、各ファイル ブロック ディレクティブに関する次の情報を表示します。

- **[Name]** — ファイル ブロック ディレクティブの名前。
- **[Status]** — ファイル ブロック ディレクティブが有効であるか、無効であるか。
- **[Pattern Operation]** — 指定したパターンを明示する操作。
- **[Pattern]** — ポリシーでブロックするファイル パターン。

このウィンドウから、次の作業を実行できます。

- 定義の横にある **[Edit]** アイコンをクリックして、既存のブロック定義の設定を編集します。次に、ファイル ブロック ディレクティブを削除したり、任意の定義設定を変更できます。
- 次の手順の説明に従って、新しいファイル ブロック ディレクティブを作成します。

ステップ 2 タスクバーの **[Create New File Blocking Directive]** アイコンをクリックして、新しいファイル ブロック ディレクティブを作成します。[Creating a New File Blocking Directive] ウィンドウが表示されます。

ステップ 3 ディレクティブの名前を入力します。

ステップ 4 **[File Name]** ドロップダウン リストから、次のいずれの照合パターンを選択します。

- equals
- starts with
- ends with
- contains

ステップ 5 ドロップダウン リストの右側にあるフィールドで、ファイル パターン定義を完了します。たとえば、ドロップダウン リストから **[ends with]** を選択し、右側のフィールドに **.MP3** と入力すると、エクスポートされたファイル サーバ上の **.MP3** で終わるすべてのファイルがユーザからブロックされます。

ステップ 6 **[Status]** ドロップダウン リストから、ポリシーのステータス (**[enabled]** または **[disabled]**) を選択します。無効にしたポリシーは実行されません。

ステップ 7 **[Submit]** をクリックします。

すべてのエッジ デバイスが新しいディレクティブで更新され、**[File Blocking Directives]** ウィンドウの表にブロック定義が追加されます。

ステップ 8 上記の手順を繰り返して、他のファイル ブロック ディレクティブを作成します。

事前配置ディレクティブの作成

事前配置ディレクティブを使用すると、どのファイルも CIFS ファイル サーバから選択した Edge WAE のキャッシュへ事前にコピーする必要があるかを決定できます。事前配置を使用すると、WAN のアイドル時間を利用して、頻繁にアクセスされるファイルを選択した WAE へ転送できます。そのため、ユーザは、これらのファイルに初めてアクセスするときでも、キャッシュ レベルのパフォーマンスを利用できます。

事前配置ディレクティブは、明示的に登録されたファイル サーバにのみ追加できます。事前配置は、自動検出されたファイル サーバではサポートされていません。

事前配置ディレクティブを定義するときは、ファイル サーバからの内容を事前に配置する Edge WAE を選択し、事前に配置するファイル サーバ上のルート ディレクトリを指定します。当初、事前配置ディレクティブは、未スケジュール状態にあります。また、内容を事前に配置する日時と周期を決定するスケジュールを作成する必要があります。内容を定期的に事前配置できるため、作業の反復ごとに指定したすべてのファイルをコピーするか、指定した周期の間に変更されたファイルだけをコピーするかを指定できます。

さらに、事前配置作業が WAN 帯域幅や Edge WAE キャッシュ空間を過剰に使用しないように、時間とサイズの制限を指定できます。これらの制限を使用して、ネットワーク効率を最適化し、この機能の誤用を防止することを強く推奨します。

事前配置ディレクティブがアクティブになる時刻になると、Edge WAE で事前配置作業が開始します。WAAS Central Manager GUI で、処理中および処理後に各事前配置作業を監視できます。必要に応じて、アクティブな事前配置作業を停止することもできます。

WAAS の混合バージョンを実行しており、4.0.13 以前に Edge または Core デバイスを実行している場合、事前配置作業では常に Core デバイスの設定が使用されます。

事前配置では、ファイル サーバにアクセスするために必要なユーザ名とパスワードを **[Configure Core Server Settings]** ウィンドウで指定する必要があります。詳細については、「[コア クラスタの設定](#)」(p.11-10) の [ステップ 11](#) を参照してください。

事前配置には、複数のルートを設定する機能も含まれます。「[新しい事前配置ディレクティブの作成](#)」(p.11-29) を参照してください。



(注) 事前配置ディレクティブを定義するために必要な接続が存在しない場合、警告メッセージが表示されます。

次の項目で、事前配置ディレクティブを作成する方法について説明します。

- [新しい事前配置ディレクティブの作成 \(p.11-29\)](#)
- [事前配置ディレクティブへのエッジデバイスの割り当て \(p.11-33\)](#)
- [新しい事前配置スケジュールの作成 \(p.11-34\)](#)

新しい事前配置ディレクティブの作成

事前配置ディレクティブを作成するには、次の手順に従ってください。

ステップ 1 WAAS Central Manager GUI から、**[Services] > [File] > [Preposition]** を選択します。

[Preposition Directives] ウィンドウが表示されます。このウィンドウは、システムに存在する事前配置ディレクティブに関する次の情報を表示します。

- **[Preposition Directive]** — 事前配置ディレクティブの名前。
- **[Type]** — 事前配置ディレクティブがすべてのファイルに影響する (Full) か、最後の事前配置作業の後で変更されたファイルだけに影響する (Differential) か。
Full の場合、作業のフィルタと一致するすべてのファイルおよびファイル サーバで検出されたすべてのファイルが Edge に送信され、キャッシュと比較されます。
Differential の場合、最後に正しく事前配置された後に変更されたファイルだけが Edge キャッシュに送信されます。最後に正しく事前配置された時刻は Edge デバイスから取得されるので、Edge デバイスのクロックとファイル サーバのクロックが同期していることを確認してください。最初は常に完全スキャンされます。事前配置作業を変更すると、最後に正しくスキャンされた時刻がリセットされます。
- **[Status]** — 事前配置ディレクティブが有効であるか、無効であるか。
- **[File Server]** — エクスポートされたファイル サーバの名前。

[Preposition Directive] ウィンドウから、次の作業を実行できます。

- ディレクティブの横にある **[Edit]** アイコンをクリックして、既存の事前配置ディレクティブの設定を編集します。次に、事前配置ディレクティブを削除したり、任意の設定を変更できます。
- 次の手順の説明に従って、新しい事前配置ディレクティブを追加します。

ステップ 2 新しい事前配置ディレクティブを作成するには、新規作成事前配置ディレクティブタスクバーの **[Create New Preposition Directive]** アイコンをクリックします。

[Creating New Preposition Directive] ウィンドウが表示されます (図 11-8 を参照)。

図 11-8 新しい事前配置ディレクティブの作成

ステップ 3 ディレクティブの名前を入力します。

ステップ 4 [Status] ドロップダウン リストから、**[enabled]** または **[disabled]** を選択します。無効にしたディレクティブは、有効になりません。

ステップ 5 [File Server] ドロップダウン リストから、エクスポートするファイル サーバを選択します。

このドロップダウン リストには、登録したファイル サーバだけが表示されます。ファイル サーバを登録する方法の詳細については、「[WAAS Central Manager へのファイル サーバの登録](#)」(p.11-17)を参照してください。

ステップ 6 (任意) 提供されるフィールドを使用して、時間とサイズの制限を定義します。

表 11-5 で、時間とサイズを制限するフィールドについて説明します。

表 11-5 事前配置の時間とサイズの制限

フィールド	説明
Total Size as % of Cache Volume	<p>ファイルを事前配置する Edge WAE キャッシュ全体が消費できる比率 (%)。たとえば、この事前配置ディレクティブの使用量を WAE キャッシュの 30% に制限するには、このフィールドに 30 と入力します。デフォルト値は 5% です。</p> <p>事前配置で定義したキャッシュの比率により、キャッシュに保存されているサイズにかかわらず 1 回の作業で事前配置できる最大サイズが定義されます。</p> <p>キャッシュが満杯の場合は、理由を問わず、オンデマンド キャッシングのような事前配置が行われます。つまり除去プロセスが開始され、ファイルは、最後のアクセス時刻が古い順にキャッシュから削除されます。</p>
Max File Size	<p>エクスポートできる最大ファイル サイズ。この値を超えるファイルは、WAE キャッシュへエクスポートされません。</p>
Min File Size	<p>エクスポートできる最小ファイル サイズ。この値より小さいファイルは、WAE キャッシュへエクスポートされません。一般的な規則として、通常の WAAS を通じて WAN 経由で迅速に取得できるため、20 KB 未満のファイルを事前に配置することは効率的ではありません。</p> <p>デフォルト値は 20KB です。</p>
Duration	<p>WAAS がファイル サーバをエクスポートする最大時間。WAAS がファイル サーバをエクスポートするのにこの時間を超えると、すべてのファイルが Edge WAE キャッシュへコピーされる前に、WAAS はエクスポート プロセスを停止します。</p> <p>事前配置作業が予定時刻に開始されない場合（たとえば Edge と Core が接続されていない場合）、この時間中は開始が試行されます。</p> <p>このフィールドに値を指定しないと、WAAS は、必要な時間をかけてこのファイル サーバをエクスポートします。</p>
Type	<p>スキャンプロセスの時間フィルタ。[Type] ドロップダウン リストから、次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> • [All Files] — すべてのファイルを Edge WAE キャッシュへエクスポートします。これは、デフォルトの設定です。 • [Files changed since last preposition] — 最後の事前配置以後に変更されたファイルだけを Edge WAE キャッシュへエクスポートします。この遅延フィルタは、2 回目以降の作業に適用されます。 このオプションを指定すると、新しいディレクトリが最後の修正時刻が変更されずに事前配置済みのディレクトリに移動された場合、次の事前配置セッションではこの新しいディレクトリは事前配置されません。 • [Files changed since last] — 指定した時間内に変更されたファイルだけをエクスポートします。過去 2 時間にファイル サーバで行われたファイル更新をエクスポートする場合は、提供されるフィールドに 2 を入力し、ドロップダウン リストから [hour] を選択します。



(注) 事前配置作業中にいずれかの制限値を超えると、作業が停止し、メッセージが管理者ログへ送信されます。残っているファイルは、次の作業中にエクスポートされます。その前にユーザが残っているファイルの 1 つを要求すると、通常のように Cisco WAAS を通じて WAN 経由で取得されます。

ステップ 7 ファイル サーバに表示されないディレクトリを事前配置しない場合は、**[Ignore Hidden Directories]** チェック ボックスをチェックします。デフォルトでは、このチェック ボックスは選択されていません。このチェック ボックスが未選択のままであれば、表示されないディレクトリは事前配置されます。

WAAS の混合バージョンを実行しており、4.0.13 以前に Edge または Core デバイスを実行している場合、事前配置作業では常に Core デバイスの設定が使用されます。

ファイル サーバを明示的に登録する代わりに自動検出機能を使用している場合、自動検出されたファイル サーバには事前配置がサポートされていないため、このチェックボックスは適用されません。

ステップ 8 **[Root Share and Directory]** フィールドに、エクスポートするファイル サーバ上のディレクトリを入力します。次の任意の方法を使用して、ディレクトリを識別します。

- 次の形式で、1 つまたは複数のディレクトリ パスを手動で入力します。プロトコル:// サーバ/共有またはサーバ\共有。たとえば、`cifs://win12srv/home` または `win12srv\home`。複数のディレクトリを複数の行で入力することもできます。その場合は、それぞれの行にそれぞれのフルディレクトリ パスを入力します。

複数ルートの共有を定義する場合は、単一のルート設定を行う一連の事前配置をルートごとに反復します。

- **[Browse]** ボタンをクリックして、ファイル サーバ上のディレクトリを参照します。ディレクトリの中に移動するには、ディレクトリ名の左にあるファイル フォルダ アイコンをクリックします。エクスポートしたいディレクトリの横にあるチェック ボックスをチェックし、**[Select Directory]** ボタンをクリックします。ウィンドウが表示され、複数のディレクトリが選択できます。

[Browse] ボタンは、**[Configure Core Server Settings]** ウィンドウで **[File Server access username]** および **[File Server access password]** フィールドを設定した場合にだけ表示されます (図 11-3 を参照)。

- **[Include Sub Directories]** チェック ボックスを選択して、指定したルート ディレクトリの下にあるすべてのサブディレクトリを含めます。このオプションを指定しない場合は、指定したルート ディレクトリのフィールドだけが事前配置され、表示中にサブディレクトリを指定できません。
- **[File Name]** ドロップダウン リストからパターン演算子を選択し、隣接するテキスト ボックスにパターンを記述する自由な文面を入力して、特定のファイルの種類までポリシー定義を絞り込みます。たとえば、**ends with .doc** と入力します。

ステップ 9 **[Submit]** をクリックします。

ディレクトティブがシステムに保存され、**[Contents]** ペインに追加オプションが表示されます。

事前配置ディレクティブへのエッジ デバイスの割り当て

事前配置ディレクティブを作成したら、Edge WAE またはデバイス グループをディレクティブに割り当てる必要があります。この作業は、どの Edge WAE が事前配置内容をキャッシュに保存するかを決定します。



(注) 事前配置には、複数のルートを設定する機能も含まれます。「[新しい事前配置ディレクティブの作成](#)」(p.11-29) を参照してください。

Edge WAE またはデバイス グループを事前配置ディレクティブに割り当てるには、次の手順に従ってください。

- ステップ 1** WAAS Central Manager GUI から、[Services] > [File] > [Preposition] を選択します。
- [Preposition Directives] ウィンドウが表示され、システムに存在する事前配置ディレクティブが表示されます。
- ステップ 2** Edge WAE またはデバイス グループに割り当てたい事前配置ディレクティブの横にある [Edit] アイコンをクリックします。
- ステップ 3** [Contents] ペインで、次のいずれかのオプションをクリックします。
- [Assign Edge Devices] — このディレクティブに割り当てる 1 つまたは複数の Edge WAE を選択できます。
 - [Assign Edge Groups] — このディレクティブに割り当てるデバイス グループを選択できます。
- 選択したオプションに応じて、[Edge Device Assignments] ウィンドウまたは [Device Groups Assignments] ウィンドウが表示されます。
- ステップ 4** 次のいずれかを実行して、この事前配置ディレクティブに割り当てる Edge WAE またはデバイス グループを選択します。
- タスクバーの  をクリックして、使用できるすべての Edge WAE またはデバイス グループをこのディレクティブに割り当てます。
 - このディレクティブに割り当てたい各 Edge WAE またはデバイス グループの横にある  をクリックします。選択すると、アイコンは  に変化します。



(注) デバイスまたはデバイス グループはオフラインである (× で識別される) 場合、そのデバイスまたはグループをこのディレクティブに割り当てることはできません。デバイス グループに割り当てられた事前配置ディレクティブは、そのデバイス グループの接続先 Edge デバイスにだけ適用されます。

- ステップ 5** [Submit] をクリックします。

選択した各エッジ デバイスまたはデバイス グループの横にあるアイコンが  に変化します。

新しい事前配置スケジュールの作成

事前配置ディレクティブを作成し、WAE をディレクティブに割り当てたら、いつ何回事前配置を実行するかを決定するスケジュールを作成することを推奨します。

たとえば、営業時間内のトラフィック量を最小限に抑えるために、事前配置スケジュールを夜間に設定する場合があります。あるいは、エクスポートされるデータがよく変更される場合、事前配置スケジュールを反復実行に設定する場合があります。これにより、このディレクティブに割り当てられた WAE のキャッシュに、最新のファイル更新が存在することを保証できます。

Edge WAE の事前配置作業を異なる時間帯で同時に開始するスケジュールの場合、Edge WAE の作業は Core WAE の時間帯に基づいて開始されます。Edge WAE と Core WAE のクロックが同期していない場合、作業は予定通りに開始されません。

事前配置スケジュールを作成するには、次の手順に従ってください。

ステップ 1 WAAS Central Manager GUI から、**[Services] > [File] > [Preposition]** を選択します。

[Preposition Directives] ウィンドウが表示され、システムに存在する事前配置ディレクティブが表示されます。

ステップ 2 スケジュールを作成する事前配置ディレクティブの横にある **「Edit」** アイコンをクリックします。

ステップ 3 [Contents] ペインで、**[Schedule]** をクリックします。

[Creating New Preposition Schedule] ウィンドウが表示されます。デフォルトでは、スケジュールは設定されていません。

ステップ 4 次のいずれかのスケジュール オプションを選択します。

- **[Now]** — このスケジュールを送信してから数分以内に事前配置を実行します。
事前配置ディレクティブを変更して **[Submit]** ボタンをクリックするたびに、[Now] スケジュールが開始されます。リロードされたエッジ デバイスがオンラインに復帰した場合も、すぐに [Now] スケジュールが開始されます。
- **[Daily]** — 毎日の指定した時刻に事前配置を実行します。
- **[Date]** — 指定した日時に事前配置を実行します。
- **[Weekly]** — 選択した曜日の指定した時刻に事前配置を実行します。
- **[Monthly Days]** — 毎月、選択した日の指定した時刻に事前配置を実行します。
- **[Monthly Weekdays]** — 毎月、選択した曜日の指定した時刻に事前配置を実行します。たとえば、毎月の第 2 火曜日に事前配置を実行するスケジュールを作成できます。

ステップ 5 事前配置作業の開始時刻を指定します。

時刻は 24 時間形式で表し、00:00 は深夜の 0 時を表します。



(注) **[Now]** オプションでは、開始時刻を指定できません。

ステップ 6 [Submit] をクリックします。

スケジュールが保存されたことを確認する「Changes Submitted」メッセージが、ウィンドウの一番下に表示されます。

ステップ 7 事前配置ステータスを確認して、事前配置ディレクティブが正常に完了したことを確認します。詳細については、「[事前配置ステータスの確認](#)」(p.11-36) を参照してください。

ファイル サービスの管理

この項の次の項目で、ファイルサーバを管理する方法について説明します。

- [事前配置ステータスの確認 \(p.11-36\)](#)
- [事前配置作業の開始と停止 \(p.11-36\)](#)
- [WAN 障害に対する WAAS ネットワークの準備 \(p.11-37\)](#)
- [コア クラスターのメンバーの表示 \(p.11-38\)](#)

事前配置ステータスの確認

1 つまたは複数の事前配置ディレクティブを作成したら、すべての事前配置作業のステータスを確認して、正常に完了したことを確認できます。作業が正常に完了しない場合は、事前に配置された一部のファイルが Edge WAE キャッシュへ正常にコピーされていない場合があります。

事前配置作業のステータスを確認するには、次の手順に従ってください。

ステップ 1 WAAS Central Manager GUI から、**[Services] > [File] > [Preposition]** を選択します。

[Preposition Directives] ウィンドウが表示され、システムに存在する事前配置ディレクティブが表示されます。

ステップ 2 ステータスを確認する事前配置ディレクティブの横にある **「Edit」** アイコンをクリックします。

ステップ 3 [Contents] ペインで、**[Preposition Status]** をクリックします。[Preposition Status] ウィンドウが表示されます。

このページは、次の情報を表示します。

- **[WAE]** — 事前に配置されるファイルをキャッシュに受信する各 Edge WAE の名前。
- **[Start Time]** — 事前配置作業が開始した日時。
- **[Duration]** — 事前配置作業が完了するまでにかかった時間。
- **[Amount Copied]** — WAE キャッシュへコピーされたデータ量 (バイト)。
- **[Status]** — 事前配置作業が正常に完了したかどうか。
- **[Reason]** — 事前配置作業が失敗した理由。

ステップ 4 [Status] 列に [Completed] が表示されることを確認します。

この列に失敗が表示される場合は、[Reason] 列を参照して事前配置作業が失敗した理由を確認します。問題を解決したら、事前配置作業を今すぐ再実行するようにスケジュールを設定するか、スケジュール済みの開始時刻まで待ち、あとでステータスを確認できます。

事前配置作業の開始と停止

Device Manager GUI から、事前配置作業を開始または停止できます。詳細については、[第 10 章「WAE Device Manager GUI の使用方法」](#)を参照してください。

WAN 障害に対する WAAS ネットワークの準備

Edge WAE をコア クラスタにリンクする接続ディレクティブを設定するときは、WAN 障害によってコア クラスタとの接続が切断された場合に切断モードで動作するように Edge WAE を設定するオプションがあります。

ここでは、次の内容について説明します。

- 切断モードについて (p.11-37)
- DNS とドメイン コントローラの要件 (p.11-37)
- 切断モードでのデータ可用性 (p.11-38)
- 切断モードの設定 (p.11-38)

切断モードについて

切断モードを使用すると、WAN 障害が発生した場合でも、CIFS クライアントは、キャッシュ ディレクトリを参照し、Edge WAE 上のキャッシュされているファイル全体を読み取ることができます。WAN 障害時には Edge WAE がキャッシュされたデータをファイル サーバと比較できないため、CIFS クライアントは、キャッシュされたデータに読み取り専用アクセスしか行うことができません。

Edge WAE とコア クラスタ間の WAN 接続が復元すると、Edge WAE は自動的に通常の接続モードへ戻ります。

Edge WAE は、コア クラスタとの接続を失うと、切断モードに切り替わります。これを「WAN 障害」と呼びます。



(注)

ファイル サーバが故障しても、(Edge WAE がコア クラスタとの接続を維持している場合) 切断モードには切り替わりません。

Edge WAE は、1 つの接続が切断モードで動作し、別の接続が通常の接続モードで動作することができます。たとえば、Edge WAE 用に 1 つのディレクティブ リンクがコア クラスタ A に接続し、他のディレクティブ リンクがコア クラスタ B に接続する 2 つの接続ディレクティブを作成すると、WAN 障害によってコア クラスタとのリンクが切断された場合、Edge WAE はその接続を切断モードに切り替えます。Edge WAE のコア クラスタ B との通信は、通常の接続モードのまま残ります。

切断モードは、明示的に登録されたファイル サーバでのみ動作します。切断モードは、自動検出されたファイル サーバではサポートされていません。

DNS とドメイン コントローラの要件

切断モードでは、ブランチ オフィスのローカル ドメイン コントローラが、CIFS クライアントを認証する必要があります。切断モードで動作する Edge WAE は、Kerberos を除くすべての認証方式をサポートします。

DNS だけの環境では、ブランチ オフィスにローカル DNS サーバも必要です。DNS の代わりに WINS を使用する場合は、ブランチ オフィスにローカル WINS サーバが必要です。

キャッシュされたファイルへの切断モード アクセスを有効にするには、(WAN 障害時に Windows 認証を実行するために) Active Directory ドメインまたは Windows NT ドメインに Edge WAE を追加する必要があります。



(注) デフォルトで、Windows ドメイン コントローラは、認証プロセスの一環として自動マシン アカウント パスワード変更を実行します。Edge WAE 用のマシン アカウント パスワードは 7 日周期で Edge WAE とドメイン コントローラの間で自動的にネゴシエートされ、変更されます。ただし、認証サービスが停止している場合、このプロセスは実行されず、Edge WAE 用のマシン アカウント パスワードは失効します。この状況を防止するには、Edge WAE 用の自動マシン アカウント パスワード変更を無効にすることを推奨します。詳細については、「[Edge WAE 用の自動マシン アカウント パスワード変更の無効化](#)」(p.6-26) を参照してください。



(注) 一般に、WINS 登録のタイムアウトは 3 日です。その結果、WCCP が切断モードで有効になっている場合、元のファイル サーバの WINS 登録がタイムアウトし、クライアントで名前解決問題が発生する場合があります。

切断モードでのデータ可用性

Edge WAE が切断モードにある場合、CIFS クライアントは、Edge WAE で完全にキャッシュされているファイルに読み取り専用でアクセスできます。CIFS クライアントは、部分的にキャッシュされたファイルやキャッシュされていないファイルのディレクトリ構造を表示できますが、これらのファイルを開くことができません。

ディレクトリは、その ACL がキャッシュされている場合のみ、切断モードで使用できます。すなわち、アクセスされたことがなく、キャッシュされていない共有は、表示されません。

切断モードでファイルが使用できることを保証する最善の方法は、Edge WAE キャッシュにファイルのコピーを予防的に配置する事前配置ディレクティブを設定することです。詳細については、「[新しい事前配置ディレクティブの作成](#)」(p.11-29) を参照してください。

切断モードの設定

ファイル サーバを WAAS Central Manager に登録するとき、切断モードで動作するように Edge WAE を設定できます。詳細については、「[WAAS Central Manager へのファイル サーバの登録](#)」(p.11-17) を参照してください。

また、Active Directory ドメインまたは Windows NT ドメインに Edge WAE を追加する必要があります。詳細については、「[WAAS デバイス上の Windows ドメイン サーバ設定の集中構成](#)」(p.6-20) を参照してください。[Show Authentication Status] ボタンをクリックして、WAE が正常にドメインに追加されたことを確認します。認証ステータスが OK でない場合でも、`wbinfo -t` コマンドが正常に動作 (RPC 経由の信用が正常終了) するかぎり、WAE は読み取り専用切断モード用の認証を提供します。

コア クラスターのメンバーの表示

コア クラスター デバイス グループのメンバーである Core WAE を表示するには、次の手順に従ってください。

- ステップ 1** WAAS Central Manager GUI から、[Devices] > [Device Groups] を選択します。[Device Groups] ウィンドウが表示されます

- ステップ 2** それに属するメンバーを表示する WAFS コア クラスタ デバイス グループの横にある **[Edit]** アイコンをクリックします。[Modifying Device Group] ウィンドウが表示されます。
- ステップ 3** [Contents] ペインで、**[Members]** を選択します。選択したデバイス グループに属するデバイスのリストが表示されます。
-

