CHAPTER 11

サービス リクエストの導入、モニタリング、および監査

この章では、L2VPN、VPLS、または FlexUNI/EVC のサービス リクエストを導入、モニタリング、および監査する方法、およびタスク ログにアクセスする方法について説明します。次の事項について説明します。

サービス リクエストの導入

L2VPN、VPLS、または FlexUNI ポリシーをネットワーク デバイスに適用するには、サービス リクエストを導入する必要があります。サービス リクエストを導入すると、ISC はリポジトリ（ISC データベース）内のデバイス情報を現在のデバイスのコンフィギュレーションと比較して、コンフィグレットを生成します。

導入前の変更点

L2VPN または VPLS のサービス リクエストを導入する前に、Dynamic Component Properties Library（DCPL）パラメータ **actionTakenOnUNIVlanList** を変更できます。この変更は、[trunk allowed vlan] のリストが User-Network Interface（UNI; ユーザネットワーク インターフェイス）上に存在しない場合に必要になります。

この変更を行うには、次の手順を実行します。

ステップ 1 [Administration] > [Control Center] を選択します。

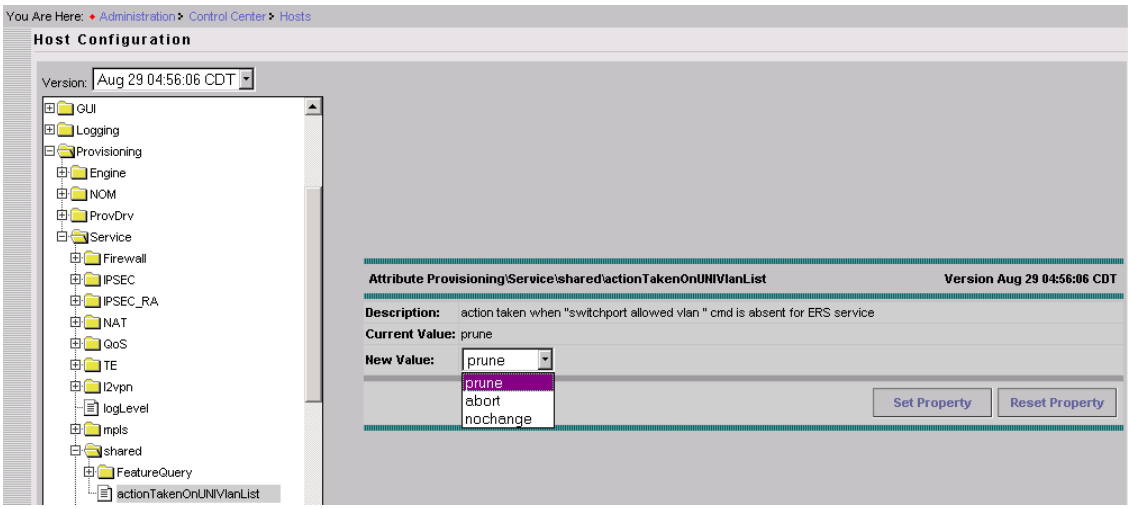
ステップ 2 変更するホストを選択します。

ステップ 3 [Config] をクリックします。

ステップ 4 [Provisioning] > [Service] > [shared] > [actionTakenOnUNIVlanList] を選択します。

図 11-1 に示すウィンドウが表示されます。

図 11-1　DCPL パラメータの変更



ステップ 5　次のいずれかを選択します。

- [prune]：ISC は最小 VLAN リストを作成します。これがデフォルトです。
- [abort]：ISC は、「trunk allowed vlan list is absent on ERS UNI」というエラーメッセージを表示し、L2VPN または VPLS のサービス リクエストのプロビジョニングを停止します。
- [nochange]：ISC はすべての VLAN を許可します。

ステップ 6　[Set Property] をクリックします。

サービスの導入

サービス リクエストを作成して ISC リポジトリに保存した後、それを導入または強制導入できます。次の手順を実行します。

ステップ 1　[Service Inventory] > [Inventory and Connection Manager] > [Service Requests] を選択します。

[Service Requests] ウィンドウが表示されます。

ステップ 2　サービス リクエストを選択します。

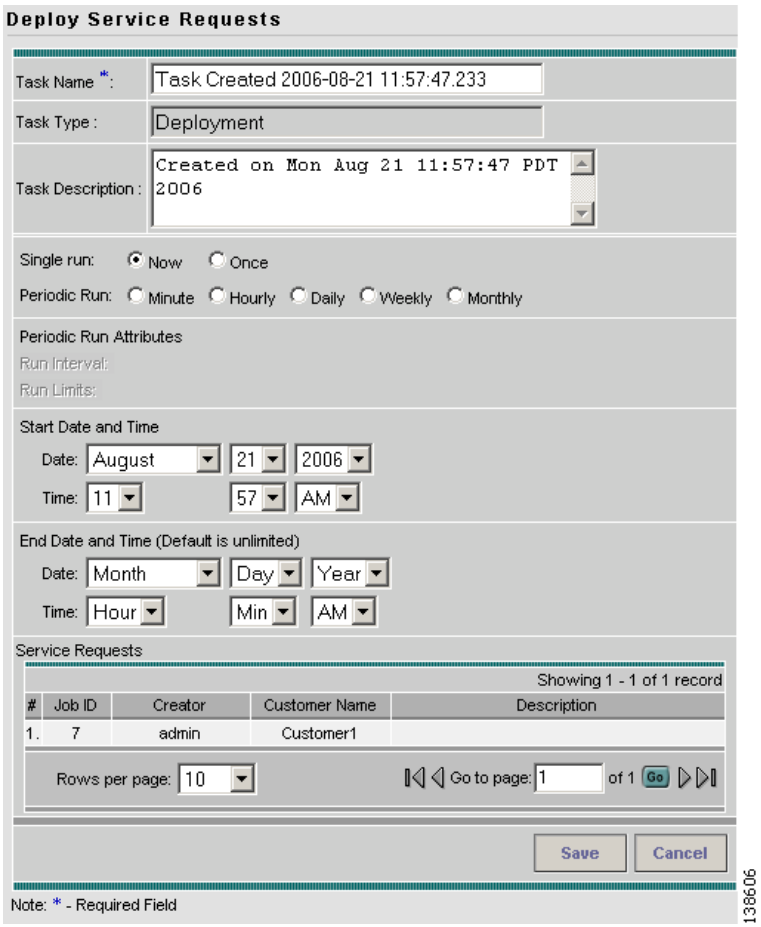
ステップ 3　[Deploy] をクリックして、[Deploy] または [Force Deploy] を選択します。

サービス リクエストの状態が [Requested] または [Invalid] の場合は、[Deploy] を使用します。

サービス リクエストの状態が [Deployed]、[Failed Deployed]、または [Failed Audit] の場合は、[Force Deploy] を使用します。

[Deploy Service Requests] ウィンドウが表示されます（図 11-2 を参照）。

図 11-2　サービスのアクティベーションのスケジュール設定



ステップ 4　サービスのアクティベーションを行うスケジュールを選択します。

ステップ 5　サービス リクエストをスケジュール設定したら、[Save] をクリックします。

サービス リクエストをスケジュール設定すると、導入中のサービス リクエストをモニタできます。詳細については、「サービス リクエストの確認」（P.11-3）および「サービス リクエストのモニタリング」（P.11-10）を参照してください。

サービス リクエストの確認

サービス リクエストを導入した後、エラーがないことを確認する必要があります。

次の方法でサービス リクエストを確認できます。

- 移行状態：サービス リクエストの移行状態は、[Service Requests] ウィンドウの [State] カラムにリストされます。サービス リクエストが正常に導入されると、状態は [DEPLOYED] に変化します。詳細については、「サービス リクエストの状態」（P.11-4）を参照してください。

- サービス リクエストの状態の表示：[Service Requests Details] ウィンドウで、リンク エンドポイントおよび対象のサービス リクエストのコンフィグレットを表示できます。詳細については、「サービス リクエストの詳細の表示」（P.11-7）を参照してください。
- タスク ログ：[Monitoring] タブからタスク ログにアクセスして、失敗したサービス リクエストのトラブルシューティングに役立てたり、サービス リクエストの詳細を表示したりできます。詳細については、「サービス リクエストのモニタリング」（P.11-10）を参照してください。

サービス リクエストの状態

サービス リクエストの移行状態は、プロビジョニング プロセスにおけるサービス リクエストの複数の異なる段階を示します。たとえば、サービス リクエストを導入すると、ISC はリポジトリ（ISC データベース）内のデバイス情報を現在のデバイスのコンフィギュレーションと比較して、コンフィグレットを生成します。コンフィグレットが生成され、デバイスにダウンロードされると、サービス リクエストは [Pending] 状態になります。デバイスが監査されると、サービス リクエストは [Deployed] 状態になります。

図 11-3 の「サービス リクエスト状態の移行図」は、ISC サービス リクエスト状態の間の関係および移行の概要図です。

図 11-3　サービス リクエスト状態の移行図

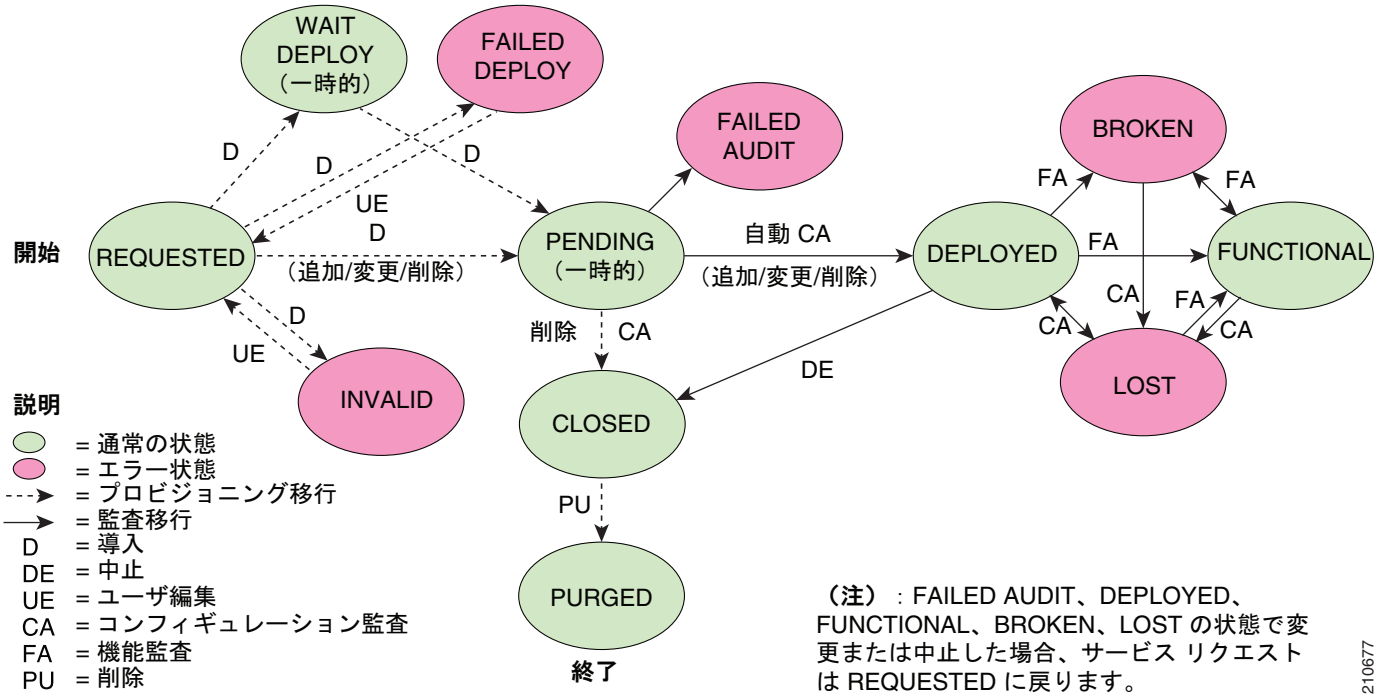


表 11-1 の「Cisco IP Solution Center サービス リクエスト状態の概要」は、それぞれの ISC サービス リクエスト状態の機能について説明しています。アルファベット順にリストされています。

表 11-1　Cisco IP Solution Center サービス リクエスト状態の概要

サービス リクエストの種類	説明
Broken （MPLS サービスのみで有効）	ルータは正しく設定されていますが、サービスが使用できません（たとえば、ケーブルの断線やレイヤ 2 の問題など）。 このサービスのルーティングおよび転送テーブルがオーディタによって検出され、サービスの目的と一致しない場合、MPLS サービス リクエストは [Broken] に移行します。
Closed	サービス リクエストがプロビジョニングまたは監査のプロセスで使用されなくなった場合、そのサービス リクエストは [Closed] に移行します。サービス リクエストは、サービス リクエストの中止の監査が正常に終了した場合のみ、[Closed] 状態に移行します。ISC は、拡張監査を許可するためにサービス リクエストをデータベースから削除しません。特定の管理者の削除操作によってのみ、サービス リクエストは削除されます。
Deployed	サービス リクエストの目的がルータのコンフィギュレーション ファイルに見つかった場合、サービス リクエストは [Deployed] に移行します。[Deployed] は、コンフィギュレーション ファイルがルータにダウンロードされ、リクエストの目的がコンフィギュレーション レベルで確認されたことを示します。つまり、ISC がコンフィグレットをルータにダウンロードし、サービス リクエストが監査プロセスを通過したことを示します。
Failed Audit	この状態は、ISC が正常にコンフィグレットをルータにダウンロードしたものの、サービス リクエストが監査プロセスを通過しなかったことを示します。したがって、サービスは [Deployed] 状態には移行しません。[Failed Audit] 状態は、[Pending] 状態から開始されます。サービス リクエストは、正常に導入された後に再び [Failed Audit] 状態になることはありません（サービス リクエストが再導入された場合を除く）。
Failed Deploy	[Failed Deploy] 状態の原因は、（接続の切断、正しくないパスワードなどによる）初期コンフィギュレーション ファイルのルータからのアップロード失敗、またはコンフィギュレーション更新のルータへのダウンロード失敗のいずれかを DCS がレポートしていることです。
Functional （MPLS サービスのみで有効）	このサービスの VPN Routing and Forwarding（VRF; VPN ルーティング/転送）テーブルがオーディタによって検出され、サービスの目的と一致する場合、MPLS サービス リクエストは [Functional] に移行します。この状態になるためには、コンフィギュレーション ファイルの監査およびルーティングの監査の両方が成功している必要があります。
Invalid	[Invalid] は、サービス リクエストの情報が正しくないことを示します。リクエストがそれ自体矛盾している場合、または他の既存のネットワークやルータのコンフィギュレーションと不整合である場合（たとえば、ルータ上で使用できるインターフェイスがない場合など）、サービス リクエストは [Invalid] に移行します。プロビジョニング ドライバは、このリクエストを処理するためにコンフィギュレーションの更新を生成できません。
Lost	オーディタがルータのコンフィギュレーション ファイル内でコンフィギュレーション レベルでの目的の確認を検出できなかった場合、サービス リクエストは [Lost] に移行します。サービス リクエストは [Deployed] 状態でしたが、一部または全部のルータのコンフィギュレーション情報が見つかりません。サービス リクエストが [Deployed] となっていた場合のみ、[Lost] 状態に移行する可能性があります。

表 11-1　Cisco IP Solution Center サービス リクエスト状態の概要（続き）

サービス リクエストの種類	説明
Pending	プロビジョニング ドライバが、リクエストが一致していると見なし、このリクエストに必要なコンフィギュレーション更新を生成できた場合、サービス リクエストは [Pending] に移行します。[Pending] は、サービス リクエストがコンフィギュレーション更新を生成し、コンフィギュレーション更新がルータに正常にダウンロードされていることを示します。 オーディタは、保留中のサービス リクエストを新しいリクエストと見なし、監査を開始します。サービスが新規にプロビジョニングされ、まだ監査されていない場合は、エラーではありません（保留中の監査）。ただし、監査の実行後もサービスが停止中のままの場合、サービスはエラー状態です。
Requested	サービスが新たに入力され、まだ導入されていない場合は、エラーではありません。ただし、導入の完了後も [Requested] のままの場合、サービスはエラー状態です。
Wait Deploy	このサービス リクエスト状態は、Cisco Configuration Engine を実行しているサーバにコンフィグレットをダウンロードする場合にのみ関係します。[Wait Deploy] は、コンフィグレットが生成されたものの、デバイスが現在オンラインでないために Cisco Configuration Engine サーバにダウンロードされていないことを示します。コンフィグレットは、Cisco Configuration Engine サーバが稼動状態であることを ISC に通知するまで、レポジトリに一時保管されます。その後、[Wait Deploy] 状態のコンフィグレットは Cisco Configuration Engine サーバにダウンロードされます。

表 11-2 の「ISC サービス リクエストに対するユーザ操作」は、ユーザ操作およびその ISC サービス リクエストへの影響を説明しています。

表 11-2　ISC サービス リクエストに対するユーザ操作

ユーザの操作	説明
Decommission	このユーザ操作は、サービス リクエストのすべてのデバイスからサービスを削除します。
Force Deploy	このユーザ操作により、[Closed] を除くすべての状態からサービス リクエストを [Deploy] できます。これは、前記の状態図を再度はじめから開始するのと同等です。サービス リクエストは、現在の状態から、移行可能ないずれの状態にも移行できます。ただし、[Requested] 状態に移行することはありません。
Force Purge	このユーザ操作は、データベースからサービス リクエストをその状態に関係なく削除します。サービス リクエストを中止する前に ISC リポジトリからサービス リクエストを [Force Purge] すると、サービスはネットワーク上で実行しているまま（特に、コンフィギュレーションがサービスをプロビジョニングしたデバイス上に）残りますが、サービスを作成したサービス リクエストのすべてのレコードは ISC から削除されます。
Purged	サービス リクエストは [Purged] になると、ISC データベースから削除されます。

サービス リクエストの詳細の表示

サービス リクエストの詳細には、サービス リクエストのリンク エンドポイント、履歴、およびサービス リクエストの導入操作で生成されたコンフィグレットが含まれます。サービス リクエストの詳細を使用して、サービス リクエストの問題やエラーのトラブルシューティングに役立てたり、コンフィグレットのコマンドを確認したりできます。

[Service Request Details] ページから、次の項目についての詳細情報を表示できます。

- リンク：リンク エンドポイントの詳細
- 履歴：サービス リクエストの履歴レポート
- 監査：リンク ID の監査レポート
- コンフィグレット：ISC により生成された L2VPN または VPLS サービス リクエストのコンフィグレットの表示

次の各項では、リンク、履歴、および L2VPN または VPLS サービス リクエストのコンフィグレットの詳細について説明します。監査の詳細については、「サービス リクエストの監査」（P.11-12）を参照してください。

サービス リクエストの詳細を表示するには、次の手順を実行します。

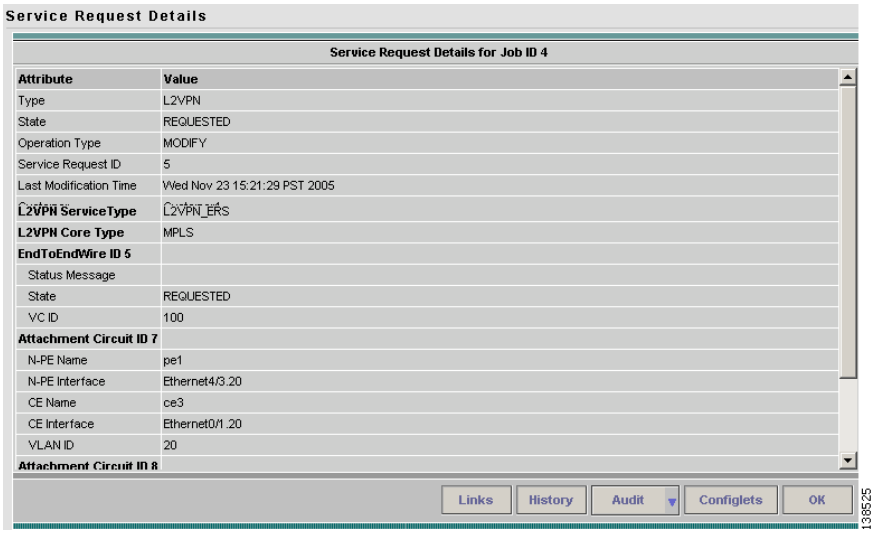
ステップ 1　[Service Inventory] > [Inventory and Connection Manager] > [Service Requests] を選択します。

[Service Requests] ウィンドウが表示されます。

ステップ 2　サービス リクエストを選択して、[Details] をクリックします。

[Service Request Details] ウィンドウが表示されます（図 11-4 を参照）。

図 11-4　[Service Request Details] ウィンドウの例



サービス リクエストの属性の詳細には、種類、移行状態、操作タイプ、ID、変更履歴、カスタマー、およびポリシー名が含まれます。

リンク

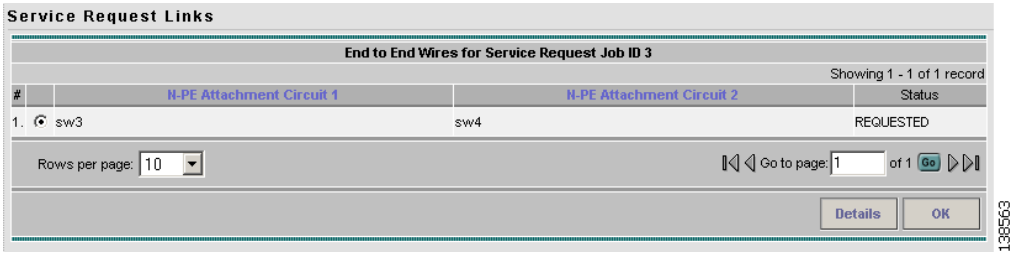
サービス リクエストのリンクの詳細には、リンク エンドポイント、PE セキュア インターフェイス、VLAN ID、CE の有無が含まれます。

この情報を表示するには、次の手順を実行します。

ステップ 1　[Service Request Details] ウィンドウで、[Links] をクリックします（図 11-4 を参照）。

[Service Request Links] ウィンドウが表示されます（図 11-5 を参照）。

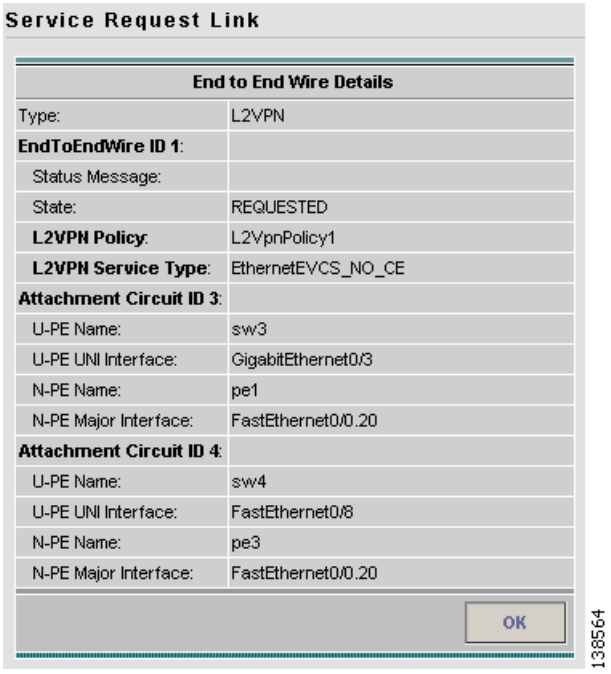
図 11-5　サービス リクエストのリンク



ステップ 2　リンクを選択して、[Details] をクリックします。

[Link Details] ウィンドウが表示されます（図 11-6 を参照）。

図 11-6　[Link Details] ウィンドウ



ステップ 3　[OK] をクリックして [Service Request Links] ウィンドウに戻ります。

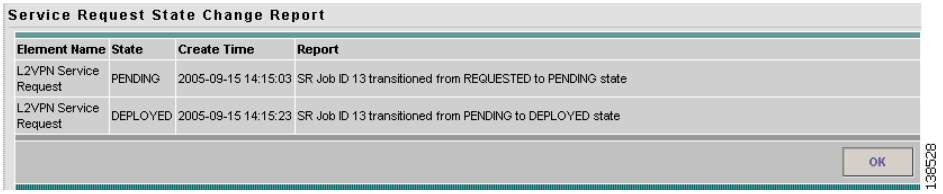
ステップ 4　別のリンクを選択して表示するか、[OK] をクリックして [Service Request Details] ウィンドウに戻ります。

履歴

サービス リクエストの履歴情報を表示するには、次の手順を実行します。

ステップ 1　[Service Request Details] ウィンドウで、[History] をクリックします（図 11-4 を参照）。
[Service Request State Change Report] ウィンドウが表示されます（図 11-7 を参照）。

図 11-7　　サービス リクエストの状態変遷レポート



履歴レポートでは、サービス リクエストについての次の情報が一覧表示されます。

- [Element Name]：このサービス リクエストに関係するデバイス、インターフェイス、およびサブインターフェイス
- [State]：エレメントの過去の移行状態
- [Create Time]：このサービス リクエストに対してエレメントが作成された時間
- [Report]：このサービス リクエストのエレメントに対する ISC の操作

ステップ 2　[OK] をクリックして [Service Request Details] ウィンドウに戻ります。

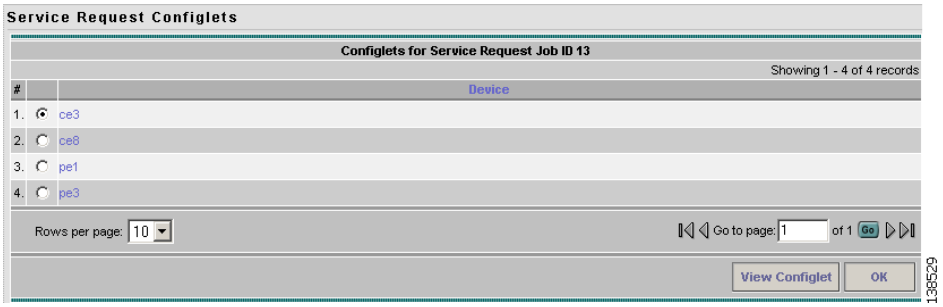
コンフィグレット

サービス リクエストを導入すると、ISC は Cisco IOS コマンドを生成して、サービス リクエストに関係するすべてのネットワーク デバイス上で、L2VPN または VPLS サービスをオンにします。

生成されたコンフィグレットを表示するには、次の手順を実行します。

ステップ 1　[Service Request Details] ウィンドウで、[Configlets] をクリックします（図 11-4 を参照）。
コンフィグレットが生成されたネットワーク デバイスのリストが表示されます（図 11-8 を参照）。

図 11-8　　サービス リクエストのコンフィグレット

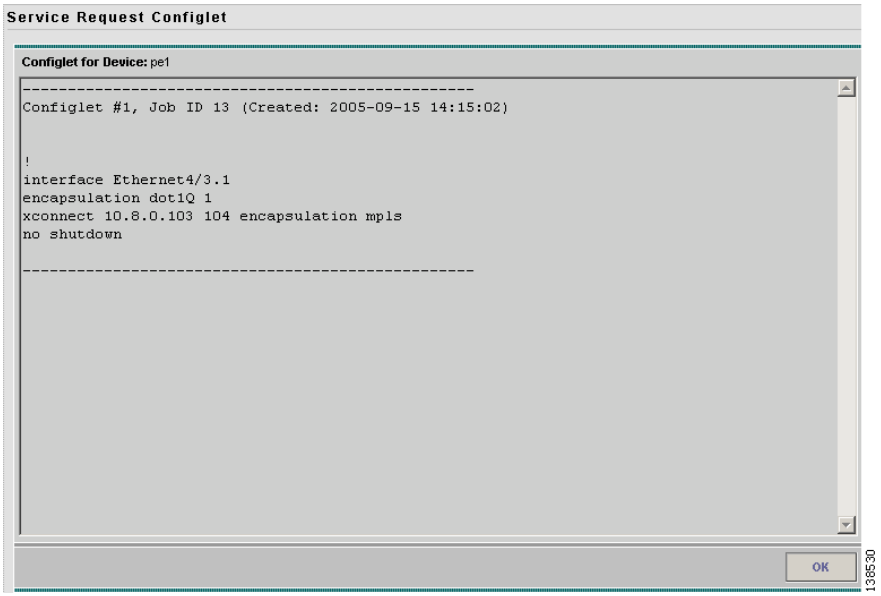


ステップ 2　コンフィグレットを表示するデバイスを選択します。

ステップ 3　[View Configlet] をクリックします。

[Configlet for Device] ウィンドウが表示されます（図 11-9 を参照）。

図 11-9　　L2VPN または VPLS のコンフィグレットの例



デバイスのコンフィグレットは、サービス リクエストの導入操作でデバイスのコンフィギュレーションにダウンロードされたすべてのコマンドを示します。

ステップ 4　[OK] をクリックして終了します。

サービス リクエストのモニタリング

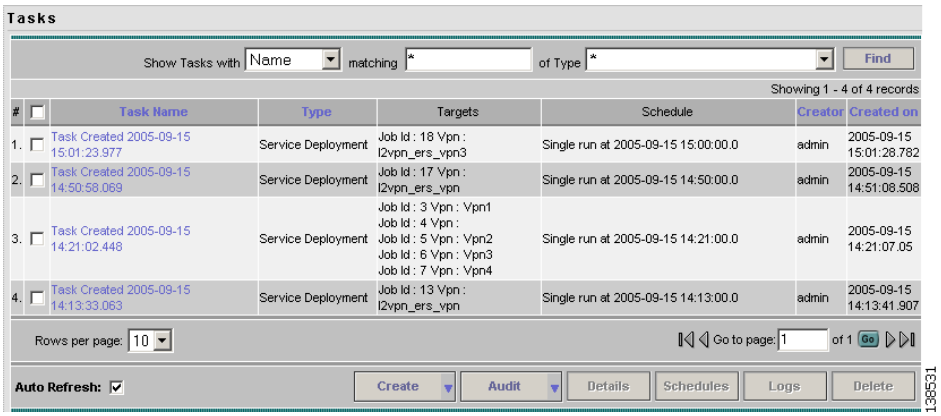
導入中のサービス リクエストをモニタするには、タスク ログを使用してサービス リクエストが失敗した原因をトラブルシューティングするか、サービス リクエストの詳細を確認する必要があります。

サービス リクエストをモニタするには、次の手順を実行します。

ステップ 1　[Monitoring] > [Task Manager] を選択します。

[Tasks] ウィンドウが表示されます（図 11-10 を参照）。

図 11-10　[Tasks] ウィンドウ



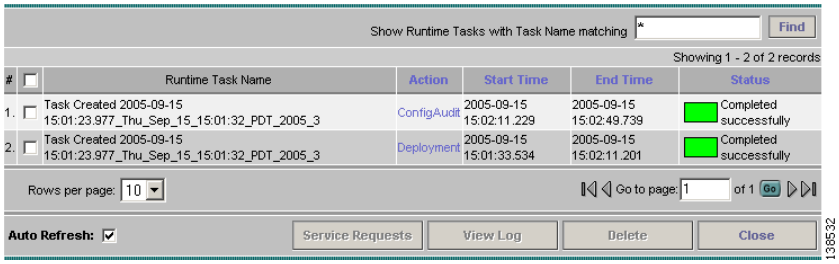
ステップ 2　[Find] をクリックしてウィンドウをリフレッシュします。

実行しているタスクが、ISC で実行されているタスクのリストの最初に表示されます。

ステップ 3　モニタするタスクを選択して、[Logs] をクリックします。

[Task Logs] ウィンドウが表示されます（図 11-11 を参照）。

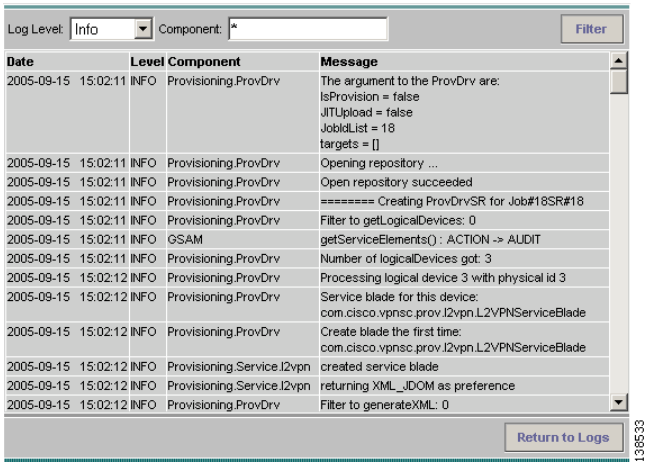
図 11-11　タスク ログ



ステップ 4　モニタするランタイム タスクを選択して、[View Log] をクリックします。

図 11-12 に示すようなウィンドウが表示されます。

図 11-12　タスク ログ



ステップ 5　ドロップダウン リストからログ レベルを選択して、[Filter] をクリックします。

ログ レベルは、[All]、[Severe]、[Warning]、[Info]、[Config]、[Fine]、[Finer]、および [Finest] です。

ステップ 6　[Return to Logs] をクリックします。

ステップ 7　[Task Logs] ウィンドウで [Close] をクリックします。

サービス リクエストの監査

サービス リクエストが Cisco IP Solution Center（ISC）で導入されるたびに、コンフィギュレーション監査が発生します。コンフィギュレーション監査レポートで、これらの監査の結果を表示できます。コンフィギュレーション監査およびレポートを使用して、ネットワーク デバイスのコンフィギュレーションが提供されるサービスに対して正しいことを確認します。

コンフィギュレーション監査は、サービス リクエストを導入するたびに自動的に発生します。このコンフィギュレーション監査では、ISC はすべての Cisco IOS コマンドが存在し、正しい構文であることを確認します。また、監査では、導入中にエラーがなかったことも確認します。

コンフィギュレーション監査は、ターゲット デバイス上のサービス リクエストによって設定されたコマンドを検証することにより、サービス リクエストの導入を確認します。デバイスのコンフィギュレーションがサービス リクエストで定義された内容と一致しない場合、監査により警告のフラグが立てられ、サービス リクエストが [Failed Audit] または [Lost] 状態に設定されます。

新規または既存のサービス リクエストの監査レポートを作成できます。

- 新規サービスの監査：この種類の監査は、導入されたばかりのサービス リクエストを対象とします。監査では、デバイスにダウンロードされたコンフィギュレーション ファイルの問題を特定します。
- 既存サービスの監査：この種類の監査は、導入済みのサービス リクエストのコンフィギュレーションを確認および評価し、サービス リクエストがまだ有効かどうかを確認します。

サービス リクエスト監査を定期的に実行するようスケジュール設定し、ネットワーク プロビジョニング リクエストの状態を確認することを推奨します。

この項では、手動でコンフィギュレーション監査を生成する方法、および監査レポートを表示する方法を説明します。

コンフィギュレーション監査レポートを表示するには、次の手順を実行します。

ステップ 1　[Service Inventory] > [Inventory and Connection Manager] > [Service Requests] を選択します。

[Service Requests] ウィンドウが表示されます。

ステップ 2　コンフィギュレーション監査を行うサービス リクエストを選択します。

ステップ 3　[Details] をクリックします。

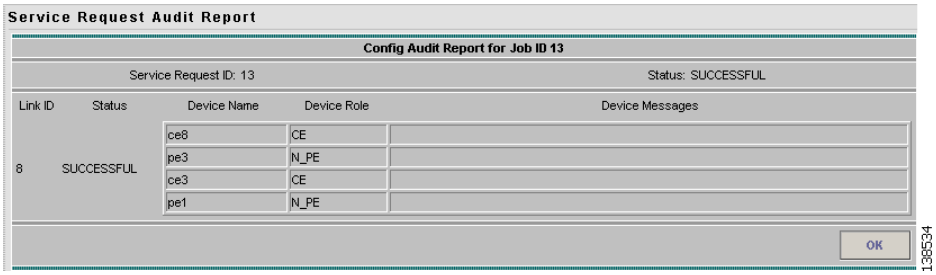
[Service Request Details] ウィンドウが表示されます。

ステップ 4　[Audit] をクリックします。

ステップ 5　[Config] をクリックします。

[Service Request Audit] ウィンドウが表示されます。図 11-13 は、成功したコンフィギュレーション監査の例を示しています。

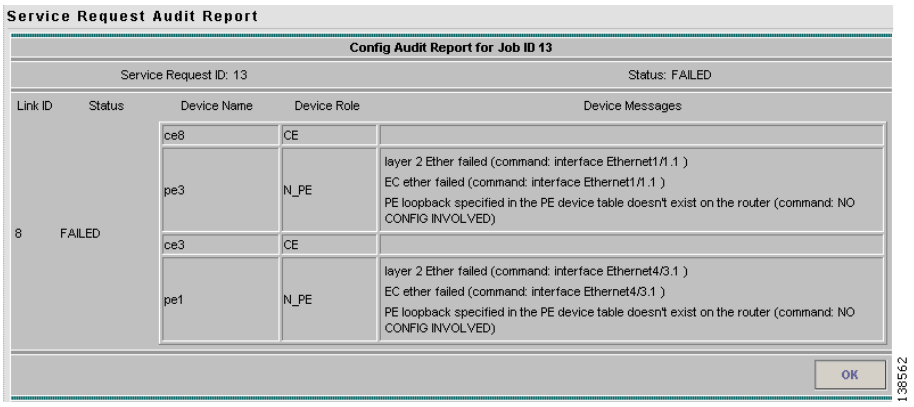
図 11-13　サービス リクエスト監査レポート：成功



このウィンドウには、デバイス名とロール、およびコンフィギュレーション監査の状態に関連するメッセージが表示されます。

監査が成功しなかった場合は、メッセージ フィールドに失敗した監査の詳細が表示されます。図 11-14 は、サービス リクエストに対する失敗した監査のメッセージの例を示しています。

図 11-14　サービス リクエスト監査レポート：失敗



監査失敗のメッセージは、見つからないコマンドおよびコンフィギュレーションの問題を示しています。メッセージ フィールドの情報を注意深く確認してください。監査が失敗した場合は、すべてのエラーを修正し、サービス リクエストを再導入する必要があります。

ステップ 6　[OK] をクリックして [Service Request Details] ウィンドウに戻ります。