Cisco Security Management Suite 高可用性ソリューションのインストール

この章では、HA または DR の展開構成に Security Manager をインストールする方法について説明します。次のタスクをリストされた順番に実行する必要がありますが、一部のタスクは任意であるか、または構成に応じて適用されない可能性があります。

この章は次のトピックで構成されています。

イーサネット接続の確立

HA または DR 構成で必要なイーサネット接続を確立するには、次の手順に従います。

ステップ 1 クラスタ構成に応じて、図または図のようにサーバーとスイッチ間のイーサネット接続を確立します。

（注） サーバごとのルータ/スイッチネットワークへの 2 本目のイーサネット接続の使用は任意ですが、NIC またはローカルイーサネットスイッチで障害が発生した場合に、冗長性のレベルが高くなります。Veritas Cluster Server（VCS）には、IPMultiNicPlus エージェントが含まれます。このエージェントを使用すると、サーバ上に複数の NIC カードをセットアップできるため、サーバにルータ/スイッチネットワークへの冗長アクセスが提供されます。NIC カードの障害、ケーブルの取り外し、その他の障害が発生すると、VCS は障害を検出し、サーバ上の別の動作している NIC カードに動作する仮想 IP アドレスを再割り当てできます。IPMultiNicPlus エージェントの詳細については、『Veritas Cluster Server Bundled Agents Reference Guide』[英語] を参照してください。このマニュアルの例では、ネットワークアクセスのために単一の NIC カードを使用するケースを示します。代わりに、ベンダー固有の NIC チーミング（IEEE 802.3ad リンク集約）ソリューションを使用することもできます。

ステップ 2 デュアルノードクラスタの場合は、図に従って、サーバー間にイーサネットクラスタ通信接続を確立します。サーバ間を直接接続する場合は、インターフェイスが自動クロスオーバー検出をサポートするかどうかによって、クロスオーバーイーサネットケーブルを使用する必要がないことがあります。ほとんどの新しいイーサネットインターフェイスではこの機能がサポートされ、別のサーバに直接接続するときにストレート ケーブルを使用できます。

Microsoft Windows Server のインストール

サポートされている Microsoft Windows オペレーティング システムをインストールします。

- Microsoft Windows Server 2019 Standard および Datacenter エディション
- Microsoft Windows Server 2012 Standard および Datacenter エディション
- Microsoft Windows Server 2012 R2 Standard および Datacenter エディション
- Microsoft Windows Server 2016 Standard および Datacenter エディション

すべてのサーバで同じオペレーティングシステムを使用することを推奨します。

（注） Veritas Storage Foundation HA for Windows version 6.0.1/6.0.2/6.1/7.4/7.4.2 Veritas InfoScale 7.0/7.2/7.4/7.4.2 を使用するには、すべてのシステムで同じパスにオペレーティングシステムをインストールする必要があります。たとえば、あるノードの C:\WINDOWS に Windows をインストールする場合、他のすべてのノードで C:\WINDOWS にインストールする必要があります。同じドライブ文字がすべてのノードで使用可能であり、システムドライブにインストール用の十分な領域があることを確認します。

外部ストレージへのサーバの接続

デュアルノードクラスタを使用する場合は、共有外部ストレージが必要です。『Hardware Compatibility List for Veritas Storage Foundation & High Availability Solutions for Windows』のストレージハードウェアを使用できます。シングルノードクラスタでは内部ストレージまたは外部ストレージのどちらかを使用できます。

Veritas 製品のインストール

Veritas 製品およびコンポーネントをインストールして設定します。シングルローカルクラスタ、デュアル地理的クラスタ、またはクラスタリングが不要な複製を使用するかどうかに応じて、必要な製品およびコンポーネントが異なります。Volume Manager の GUI（Veritas Enterprise Administrator）など、一部のコンポーネントは任意です。表 1 : Veritas ソフトウェアコンポーネントを参照してください。

表 *1 : Veritas* ソフトウェアコンポーネント

Veritas 製品/コンポーネント	**シングルローカルクラスタ**	**デュアル地理的クラスタ**	**クラスタリングが不要な複製**
Storage Foundation for Windows	—	—	必須
Veritas Storage Foundation HA for Windows version 6.0.1/6.0.2/6.1/7.4/7.4.2 Veritas InfoScale 7.0/7.2/7.4/7.4.2	必須	必須	—
Volume Replicator Option	不要	必須	必須
Global Cluster Option	不要	必須	—
Dynamic Multipathing Option	（注）を参照[1]	（注）を参照	（注）を参照
Veritas Enterprise Administrator（GUI）[2]	必須	必須	必須
Cluster Manager（GUI）2	オプション	オプション	—

[1] サーバーとディスクストレージ間の複数のパスを提供する複数のホストバスアダプタを搭載した外部ストレージを使用する場合にのみ必要です。
[2] サーバーまたは別のクライアントマシンにインストールできます。

Veritas ソフトウェアのインストールの前提条件および手順については、Veritas の該当するリリースノートおよびインストールガイドを参照してください。

（注） 1 つの重要な前提条件は、Windows Server ドメインの一部としてサーバを設定することです。

ブート ディスクのミラーリング（任意）

ブートディスクのミラーリングは任意です。ただし、これにより、特定のサーバの保護が強化されます。ブートディスクで障害が発生すると、ミラーリングされた代替ブートディスクから起動することにより、マシンを迅速にリカバリできます。ミラーリングは、ブートディスクを Veritas Volume Manager の制御下のダイナミック ディスク グループに配置し、ミラーを追加することによって実現されます。

この手順の詳細については『Veritas Storage Foundation HA for Windows version 6.0.1 / 6.0.2 / 6.1 / 7.4/ 7.4.2 Veritas InfoScale 7.0 / 7.2 / 7.4/ 7.4.2 administrator's guide』の「Set up a Dynamic Boot and System Volume」の項 [英語] を参照してください。

Veritas Volume Manager の設定タスク

ここでは、Security Manager アプリケーションで必要なディスクグループおよびボリュームを設定します。設定は、サーバがプライマリサーバまたはセカンダリサーバであるかどうか、および複製が関係するかどうかによって異なります。VEA GUI またはコマンドラインから Volume Manager タスクを実行できます。VEA またはコマンドラインを使用したこれらの手順の詳細については、『Veritas Storage Foundation HA for Windows version 6.0.1 / 6.0.2 / 6.1/ 7.4/ 7.4.2 Veritas InfoScale 7.0 / 7.2 / 7.4/ 7.4.2 Administrator's Guide』[英語] を参照してください。

ここでは、次の内容について説明します。

プライマリサーバ（複製なし）

複製が関係しないシングルクラスタ構成でプライマリサーバ上の Security Manager に必要なディスクグループおよびボリュームを設定するには、次の手順を使用します。シングルクラスタ構成では、クラスタ内のすべてのサーバにアクセス可能な外部共有ストレージが使用されます。

ディスクグループおよびボリュームを設定するには、次の手順に従います。

ステップ 1 次の特性を持つディスクグループを作成します。

- グループ名：**datadg**

- タイプ：**ダイナミック（クラスタ）**
- ディスク数：ソフトウェア RAID を使用する場合、ミラーリング対象としてグループに少なくとも 2 台のディスクを含めます。それ以外の場合は、1 台の論理ディスク（ハードウェア RAID を使用）で十分です。このディスクグループに使用するディスクは、クラスタ内のすべてのノードにアクセス可能である必要があります。

（注） ソフトウェア RAID 5 の使用は推奨されません。

ステップ 2 次の特性を持つボリュームを datadg ディスクグループに作成します。

- ボリューム名：**cscopx**
- 割り当てられたドライブ文字：**<選択されたドライブ文字>**

（注） 使用可能なドライブ文字を選択できます。ただし、ドライブ文字は、すべてのシステムで同じである必要があります。

- ファイルタイプ：**NTFS**

プライマリサーバ（複製あり）

2 つのクラスタ間で複製が実行されるデュアル地理的構成でプライマリサーバ上の Security Manager に必要なディスクグループおよびボリュームを設定するには、次の手順を使用します。プライマリクラスタとセカンダリクラスタの両方のプライマリサーバでこの手順を実行します。各クラスタについて、シングルノードクラスタまたは共有ストレージを使用する複数ノードクラスタを使用できます。ただし、このマニュアルでは、デュアル地理的構成の複数ノードクラスタのケースについては説明しません。

ディスクグループおよびボリュームを設定するには、次の手順に従います。

ステップ 1 次の特性を持つディスクグループを作成します。

- グループ名：datadg
- タイプ：ダイナミック（クラスタ）（VCS を使用する場合）、ダイナミック（セカンダリ）（VCS を使用しない場合）
- ディスク数：ソフトウェア RAID を使用する場合、ミラーリング対象としてグループに少なくとも 2 台のディスクを含めます。それ以外の場合は、1 台の論理ディスク（ハードウェア RAID を使用）で十分です。これが複数ノードクラスタの場合、このディスクグループに使用するディスクは、クラスタ内のすべてのノードにアクセス可能である必要があります。

（注） ソフトウェア RAID 5 の使用は推奨されません。

ステップ 2 次の特性を持つボリュームを datadg ディスクグループに作成します。

- ボリューム名：cscopx
- 割り当てられたドライブ文字：**<選択されたドライブ文字>**（プライマリクラスタの場合）、なし（セカンダリクラスタの場合）
- ファイルタイプ：NTFS（プライマリクラスタの場合）、なし（セカンダリクラスタの場合）
- ボリュームのロギング：なし

ステップ 3 datadg ディスクグループに、Storage Replicator Log（SRL）として使用する次の特性を持つボリュームを作成します。

- ボリューム名：data_srl
- 割り当てられたドライブ文字：なし
- ファイルタイプ：Unformatted
- ボリュームのロギング：なし

（注） SRL の適正なサイズの選択の詳細については、『Volume Replicator administrator's guide』[英語]を参照してください。

セカンダリサーバとセカンダリ クラスタ内のプライマリサーバ

セカンダリサーバおよびセカンダリクラスタ内のプライマリサーバに Security Manager をインストールするために必要なディスクグループおよびボリュームを設定するには、次の手順を使用します。すべてのセカンダリサーバおよびセカンダリクラスタ内のプライマリサーバに Security Manager をインストールする必要があります。このような場合、スペアボリュームに Security Manager をインストールします。スペアボリュームは、インストール前に一時的にマウントされてからマウント解除され、Security Manager をサーバからアンインストールするか、またはアップグレードするまで再利用されません。プライマリクラスタのプライマリサーバに使用されたものと同じドライブ文字に一時ボリュームをマウントし、インストール時に同じインストールパス（たとえば、F:\Program Files\CSCOpx）を使用する必要があります。

ディスクグループおよびボリュームを設定するには、次の手順に従います。

ステップ 1 既存のディスクグループにスペアボリュームを作成していない場合は、次の特性を持つディスクグループを作成します。

- グループ名：**datadg_spare**
- タイプ：**ダイナミック（セカンダリ）**
- サイズ：**10GB**（ボリュームには、Security Manager をインストールするのに十分な容量のみ必要）
- ディスク数：このディスクグループはアプリケーションデータの格納に使用されないため、1 台の非冗長ディスクで十分です。

ステップ 2 次の特性を持つボリュームをディスクグループに作成します。

- ボリューム名：**cscopx_spare**
- 割り当てられたドライブ文字：**<選択されたドライブ文字>**

（注） プライマリサーバーの cscopx ドライブに使用したのと同じドライブ文字を使用する**必要があります**。

- ファイルタイプ：**NTFS**

Security Manager のインストール

Security Manager のインストーラは、Veritas Storage Foundation HA for Windows version 6.0.1/6.0.2/6.1/7.4/7.4.2 Veritas InfoScale 7.0/7.2/7.4/7.4.2 の存在を検出し、HA/DR 構成に Security Manager をインストールするかどうかを確認します。このオプションを選択した場合、通常のインストール時に加えて指定する唯一の情報はデータベースパスワードです。非 HA/DR インストールでは、データベースパスワードが自動的に生成されます。ただし、データベースパスワードはHA/DR構成のすべてのサーバで同じにする必要があるため、インストーラはパスワードを指定するよう要求します。HA/DR 構成のすべてのサーバでこの同じパスワードを使用する必要があります。

HA/DR インストールによって VCS 用 Cisco Security Manager エージェントがインストールされるため、VCS は新しい CSManager リソースタイプを認識し、Security Manager を制御およびモニターできます。

また、Veritas Cluster Server が代わりに HA/DR 構成の各サーバーにおける Security Manager の起動と停止を制御するため、Windows の Security Manager とその関連サービスのスタートアップの種類が自動ではなく手動として設定されます。そうしないと、Security Manager が常に 1 台のサーバーでのみ実行される場合、Security Manager アプリケーションは、サーバーのリブート後に HA/DR 構成のすべてのサーバで起動しようとします。

HA/DR 構成の各サーバーに Security Manager をインストールする必要があります。ただし、HA/DR 構成では、Security Manager のプライマリインスタンスだけが使用され、保護されます。その他のインストールは、構成内のセカンダリサーバのいずれかでプライマリインスタンスを実行できるようにするために実行されます。

ここでは、次の内容について説明します。

- プライマリ サーバへの Security Manager のインストール （8 ページ）
- セカンダリサーバへの Security Manager のインストール （11 ページ）

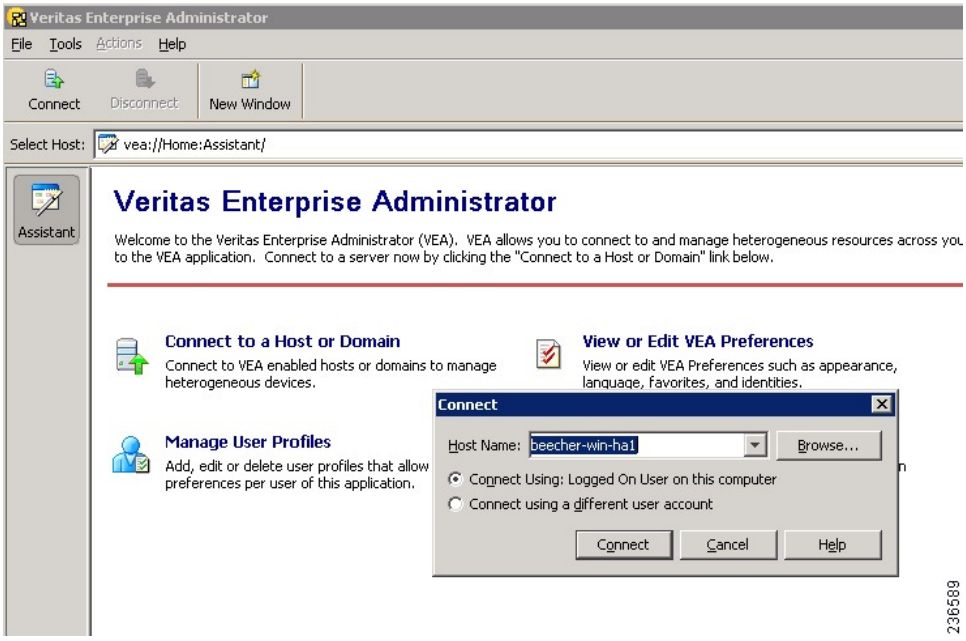
プライマリ サーバへの Security Manager のインストール

実稼働環境で使用され、HA/DR 構成によって保護される Security Manager のプライマリインスタンスをインストールするには、次の手順を使用します。

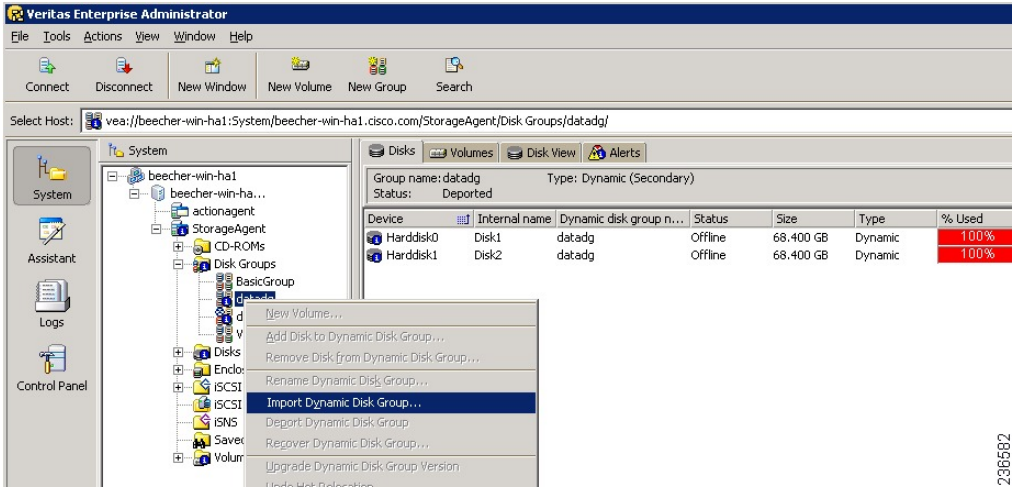
プライマリサーバ上に Security Manager をインストールするには、次の手順に従います。

ステップ 1 クラスタ内のプライマリサーバで、Veritas Enterprise Administrator（VEA GUI）アプリケーションを開き、ログインします。

図 236589



ステップ 2 datadg ディスクグループを右クリックし、[ダイナミックディスクグループのインポート（Import Dynamic Disk Group）] を選択します。



ステップ 3 [ダイナミックディスクグループとしてインポートする（Import as dynamic disk group）] オプションが選択されていることを確認し、[OK（OK）] をクリックします。

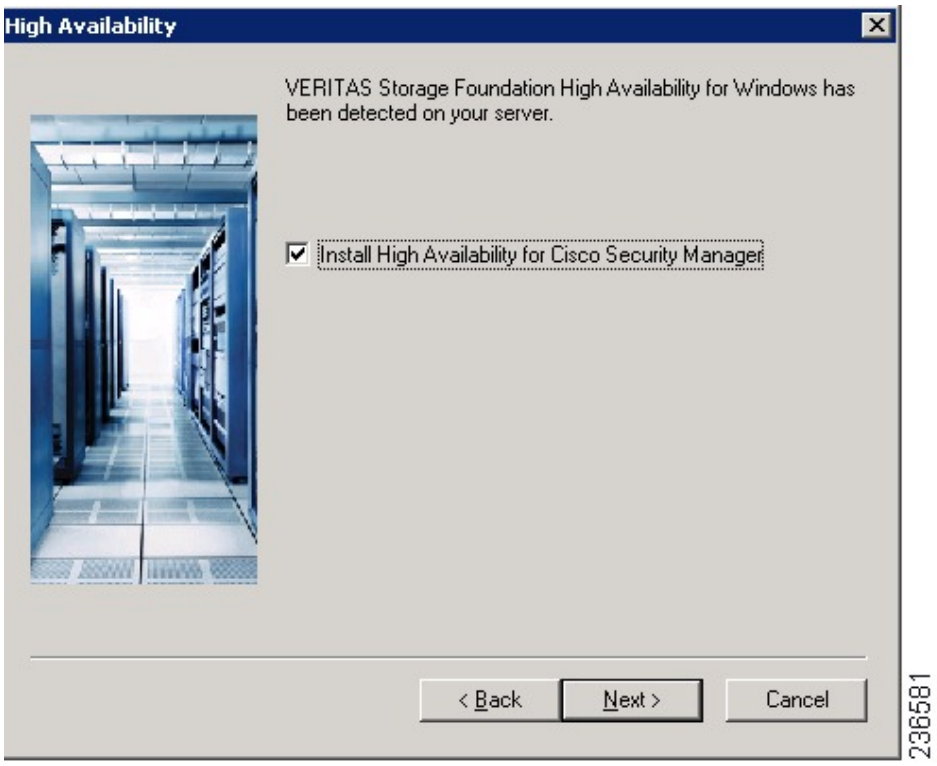
ステップ 4 [システム（System）] の [ボリューム（Volumes）] フォルダを展開します。

ステップ 5 cscopx ボリュームを右クリックし、**[ファイルシステム（File System）]** > **[ドライブ文字とパスの変更（Change Drive Letter and Path）]**を選択します。

ステップ 6 目的のドライブ文字を cscopx ボリュームに割り当て、[OK（OK）] をクリックします。ドライブの割り当てについては、ローカル冗長性構成のワークシートまたは地理的冗長性（DR）設定ワークシートを参照してください。

ステップ 7 次の HA 固有の項目に注意しながら『Security Manager Installation Guide』[英語] に従って Security Manager をインストールします。

a) HA 用に Security Manager をインストールするかどうかを尋ねるプロンプトが表示されたら、ボックスをオンにして yes を指定します。



b) インストールディレクトリの入力を求められたら、[<選択されたドライブ文字>:\Program Files\CSCOpx] を指定します。

c) データベースパスワードの指定を求められたら、適切なパスワードを選択し、忘れないようにします。HA/DR 構成のすべての Security Manager サーバーにこのパスワードを使用します。

（注） Security Manager のインストールの終了に近づくと、マルチホームサーバーを使用することと、gatekeeper.cfg ファイルを更新する必要があることを示すメッセージが表示されることがあります。HA/DR 構成で使用されるエージェントのスクリプトがこのファイルを修正するため、このメッセージは無視できます。

ステップ 8 Security Manager のインストール後、サーバーをリブートします。

ステップ 9 システムのリブート後、VEA GUI を開き、共有ディスクグループがインポートされているかどうかを確認します。ディスクグループのステータスがオフラインの場合、ステップ 2 ～ステップ 6 を繰り返してディスクグループをインポートし、インストール時に使用されたのと同じドライブ文字を割り当てます。

ステップ 10 online.pl スクリプトを使用して Security Manager を起動します。詳細については、Security Manager の手動での起動、停止、フェールオーバーを参照してください。

（注） Security Manager の正常動作に必要な Windows レジストリエントリの設定を完了するために、Security Manager を起動する必要があります。

ステップ 11 Security Manager の起動が完了するまで 5 ～ 10 分間待機してから、URL として **http://<サーバ ホスト名または IP アドレス>:1741** を使用してアプリケーションの Web インターフェイスにログインします。正常にログインできることを確認します。

ヒント　または、**pdshow** コマンドを使用して、Cisco Security Manager サービスが正常に動作していることを確認することもできます。

ステップ 12　アプリケーションの Web インターフェイスからログアウトし、offline.pl スクリプトを使用して Security Manager を停止します。詳細については、Security Manager の手動での起動、停止、フェールオーバーを参照してください。

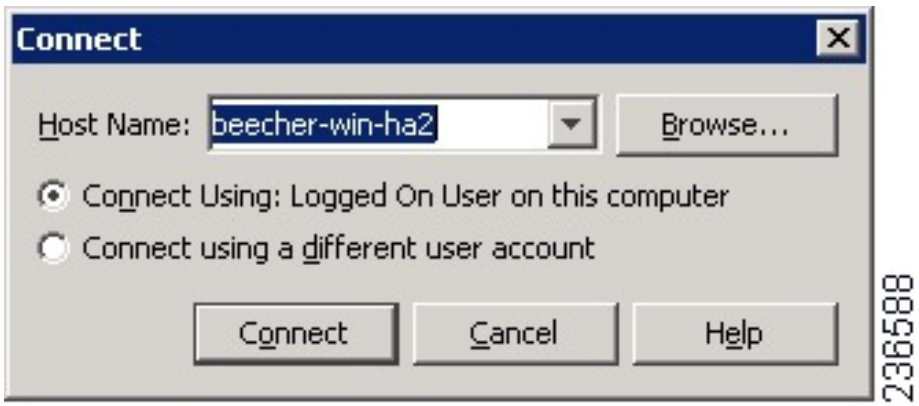
セカンダリサーバへの Security Manager のインストール

セカンダリサーバーに Security Manager をインストールするには、次の手順を使用します。セカンダリサーバーへの Security Manager のインストールは、プライマリサーバーへのインストールに似ていますが、重要な違いが 1 つあります。Security Manager をスペアボリューム（**cscopx_spare**）にインストールします。スペアボリュームは、特定のセカンダリサーバーに関連付けられ、Security Manager をアップグレードまたはアンインストールする場合に限り、再利用されます。このスペアボリュームには、空のデータベース（～2 GB）で Security Manager アプリケーションを保持するのに十分な容量が必要です。十分な領域が（可能であれば別のディスク グループで）使用可能な場合は、**datadg** ディスクグループにスペアボリュームを作成できます。

セカンダリサーバ上に Security Manager をインストールするには、次の手順に従います。

ステップ 1　セカンダリサーバで、Veritas Enterprise Administrator（VEA GUI）アプリケーションを開き、ログインします。

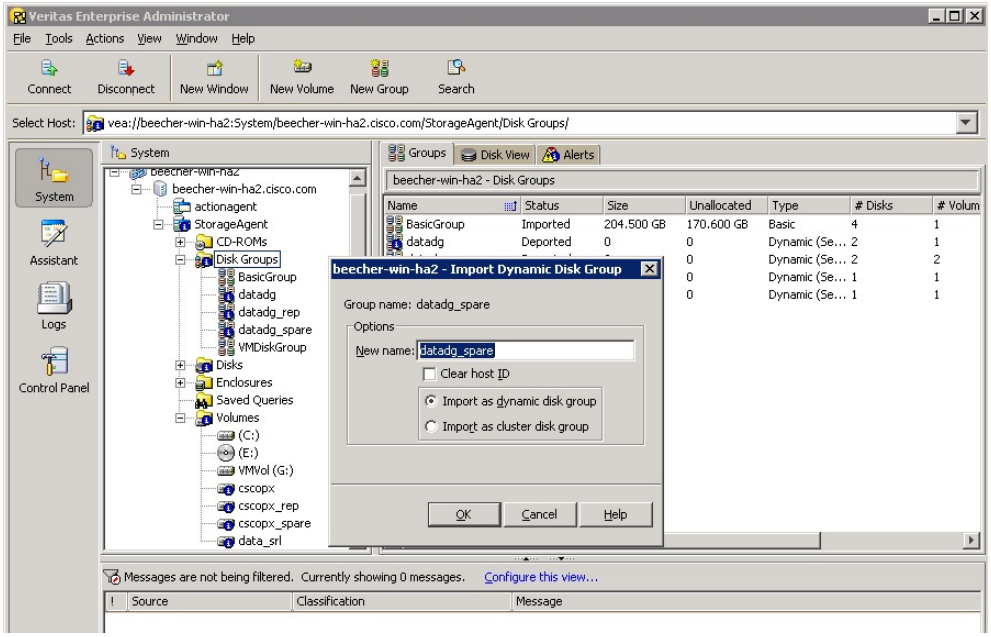
図 236588



ステップ 2　datadg_spare ディスクグループを右クリックし、[ダイナミックディスクグループのインポート（Import Dynamic Disk Group）] を選択します。

ステップ 3　[ダイナミックディスクグループとしてインポートする（Import as dynamic disk group）] オプションが選択されていることを確認し、[OK（OK）] をクリックします。

図 236583



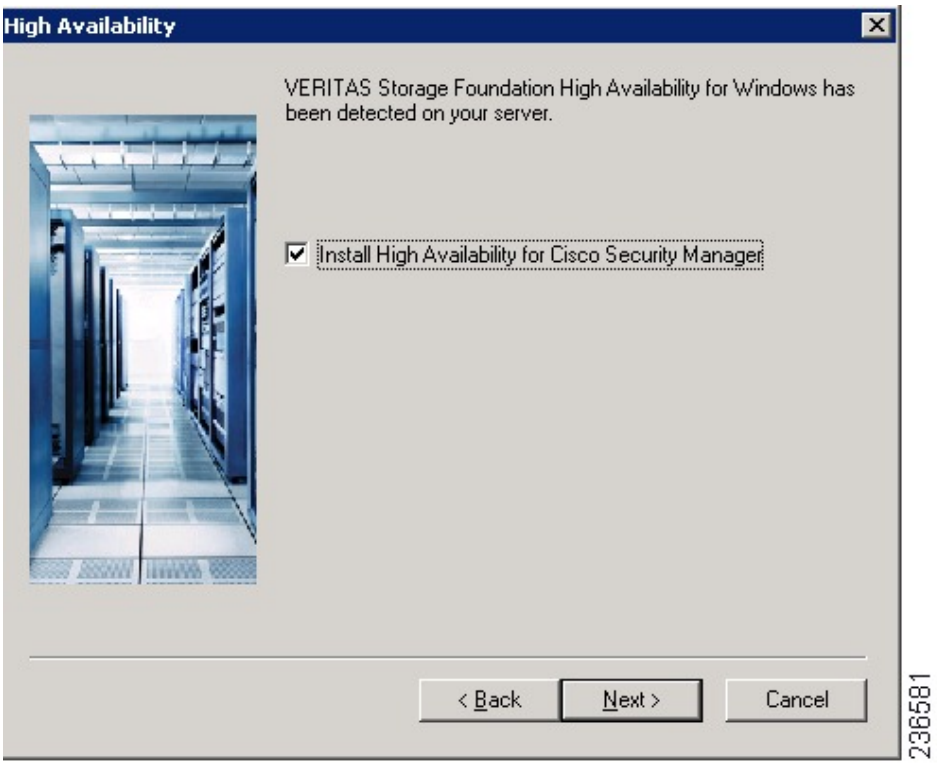
ステップ 4 [システム（System）] の [ボリューム（Volumes）] フォルダを展開します。

ステップ 5 cscopx_spare ボリュームを右クリックし、**[ファイルシステム（File System）]** > **[ドライブ文字とパスの変更（Change Drive Letter and Path）]**を選択します。

ステップ 6 目的のドライブ文字を cscopx_spare ボリュームに割り当て、[OK（OK）] をクリックします。ドライブの割り当てについては、ローカル冗長性構成のワークシートまたは地理的冗長性（DR）設定ワークシートを参照してください。

ステップ 7 次の HA 固有の項目に注意しながら『Security Manager Installation Guide』[英語] に従って Security Manager をインストールします。

a) HA 用に Security Manager をインストールするかどうかを尋ねるプロンプトが表示されたら、ボックスをオンにして yes を指定します。



b) インストールディレクトリの入力を求められたら、[<選択されたドライブ文字>:\Program Files\CSCOpx] を指定します。

c) データベースパスワードの指定を求められたら、プライマリ サーバに選択したのと同じパスワードを選択します。

（注） Security Manager のインストールの終了に近づくと、マルチホームサーバーを使用することと、gatekeeper.cfg ファイルを更新する必要があることを示すメッセージが表示されることがあります。HA/DR 構成で使用されるオンライン スクリプトがこのファイルを修正するため、このメッセージは無視できます。

ステップ 8 Security Manager のインストール後、サーバーをリブートします。

ステップ 9 システムのリブート後、VEA GUI を開き、共有ディスクグループがインポートされているかどうかを確認します。ディスクグループのステータスがオフラインの場合、ステップ 2 ～ステップ 6 を繰り返してディスクグループをインポートし、インストール時に使用されたのと同じドライブ文字を割り当てます。

ステップ 10 online.pl スクリプトを使用して Security Manager を起動します。詳細については、Security Manager の手動での起動、停止、フェールオーバーを参照してください。

（注） Security Manager の正常動作に必要な Windows レジストリエントリの設定を完了するために、Security Manager を起動する必要があります。

ステップ 11 Security Manager の起動が完了するまで 5 ～ 10 分間待機してから、URL として **http://<サーバ ホスト名または IP アドレス>:1741** を使用してアプリケーションの Web インターフェイスにログインします。正常にログインできることを確認します。

ヒント　または、**pdshow** コマンドを使用して、Cisco Security Manager サービスが正常に動作していることを確認することもできます。

ステップ 12　アプリケーションの Web インターフェイスからログアウトし、offline.pl スクリプトを使用して Security Manager を停止します。詳細については、Security Manager の手動での起動、停止、フェールオーバーを参照してください。

ステップ 13　インストールの完了後、スペアボリュームのドライブ文字の割り当てを解除します。

セカンダリ HA サーバーでの手動によるサービスの開始

Security Manager バージョン 4.13 で、1 つ以上のサービスが DR モードのセカンダリ HA サーバーで起動しない場合は、次の手順を実行します。

ステップ 1　casuser パスワードをリセットするには、次のコマンドを実行します。

<NMSROOT>\setup\support\resetcasuser.exe

例：C:\Progra~2\CSCOpx\setup\support\resetcasuser.exe

ステップ 2　表示された 2 つのオプションのうち、画面でオプション 2 - Enter casuser password を選択します。casuser のパスワードの入力を求められ、入力後、確認のためにパスワードを再入力するように求められます。

ステップ 3　ローカル セキュリティ ポリシーが設定されている場合は、ローカル セキュリティ ポリシーの「サービスとしてログオン（Log on as a service）」操作に casuser アカウントを追加します。

（注）　ネットワークからこのコンピュータにアクセスする（casusers）、ネットワークからこのコンピュータへのアクセスを拒否する（casuser）、ローカルでのログオンを拒否する（casuser）、バッチジョブとしてログオンする（casuser casusers）、およびサービスとしてログオンする（casuser）の 5 つの権限が Security Manager のインストール時に自動的に割り当てられ、設定されます。

ステップ 4　次のコマンドを実行して、NMSROOT に casuser 権限を適用します。

C:\Windows\System32\cacls.exe "<NMSROOT>" /E /T /G Administrators:F casusers:F

例：C:\Windows\System32\cacls.exe "C:\Progra~2\CSCOpx" /E /T /G Administrators:F casusers:F

ステップ 5　次のコマンドを実行して、データベースサービスに casuser を設定します。

<NMSROOT>\bin\perl <NMSROOT>\bin\ChangeService2Casuser.pl casuser <casuserpassword>

例：C:\Progra~2\CSCOpx\bin\perl C:\Progra~2\CSCOpx\bin\ChangeService2Casuser.pl casuser admin123

Veritas Volume Replicator タスク

クラスタ間で複製が動作するデュアル地理的クラスタ構成の複製を設定するには、次の手順を使用します。

複製を設定するには、次の手順に従います。

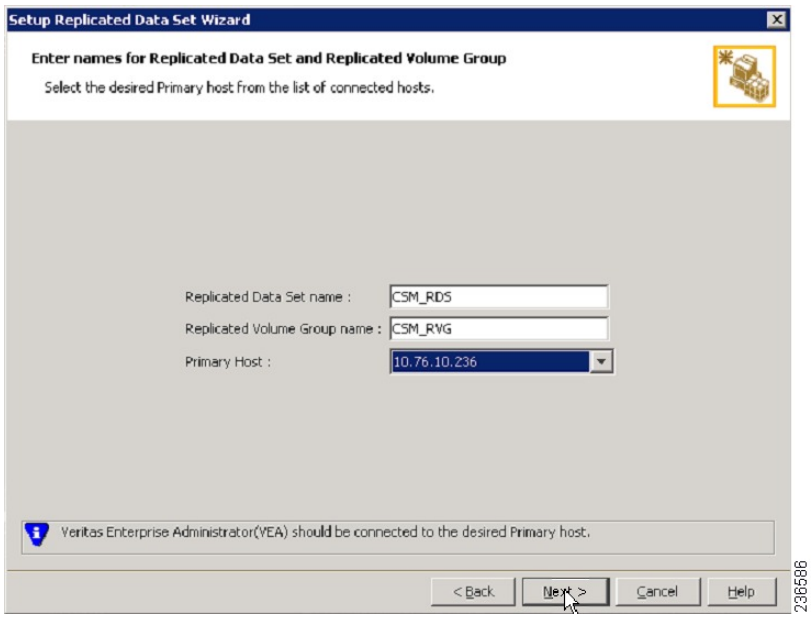
ステップ 1 VEA GUI を使用して、プライマリおよびセカンダリ ホストに接続します。

ステップ 2 *datadg* ディスクグループがプライマリサーバーとセカンダリサーバーの両方にインポートされていることを確認します。

ステップ 3 **[表示（View）] > [接続（Connection）] > [複製ネットワーク（Replication Network）]**を選択します。

ステップ 4 ツリーから [複製ネットワーク（Replication Network）] を選択し、ツールバーから [複製したデータセットを設定（Setup Replicated Data Set）] ウィザードを選択します。ウィザードの最初のパネルで次の項目を指定します。

- [複製データセット名（Replicated Data Set Name）]：**CSM_RDS**
- [複製ボリュームグループ名（Replicated Volume Group name）]：**CSM_RVG**
- ドロップダウンリストからプライマリホストを選択します。



ステップ 5 [次へ（Next）] をクリックし、[ダイナミックディスクと複製するボリュームを選択（Select Dynamic Disk Group and volumes to be replicated）] パネルで次の項目を指定します。

- [ダイナミックディスクグループ（Dynamic Disk Group）]：datadg
- [ボリューム（Volumes）]：cscopx

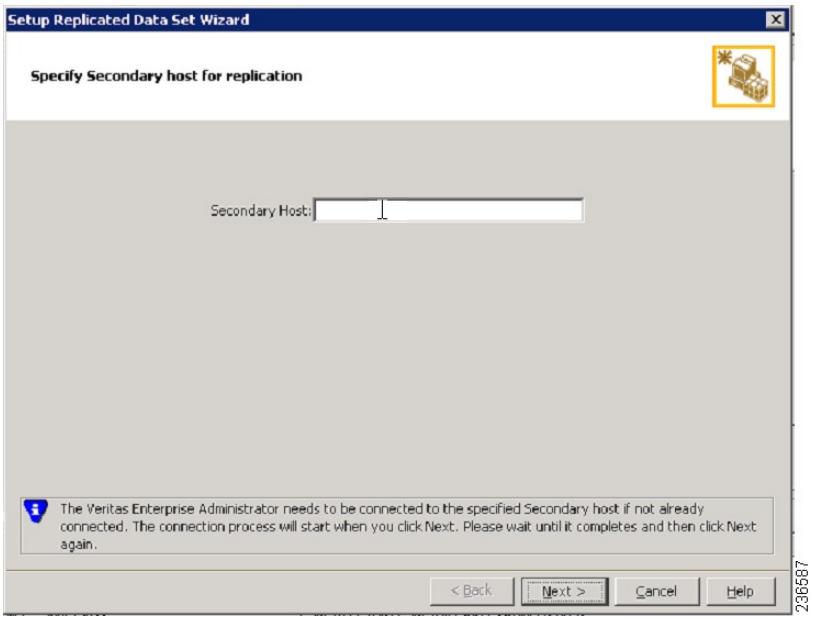
ステップ 6 [次へ（Next）] をクリックします。data_srl が他に利用できる唯一のボリュームの場合、レプリケータログのストレージボリュームとして自動的に認識されます。複数の追加ボリュームを使用できる場合、[ストレージレプリケータログ（Storage Replicator Log）] パネルが表示されます。次を指定します。

- [レプリケータログのボリューム（Volume for the Replicator Log）]：data_srl

ステップ 7 [次へ（Next）] をクリックし、サマリー情報を確認してから、[プライマリRVGの作成（Create Primary RVG）] をクリックして RVG を作成します。

ステップ 8 正常にプライマリ RVG を作成した後、RDS へのセカンダリ ホストの追加を求められたら、[はい（Yes）] をクリックします。

ステップ 9 [複製のセカンダリホストの指定（Specify Secondary host for replication）] パネルで、[セカンダリホスト（Secondary Host）] フィールドにセカンダリホストの名前または IP アドレスを入力します。

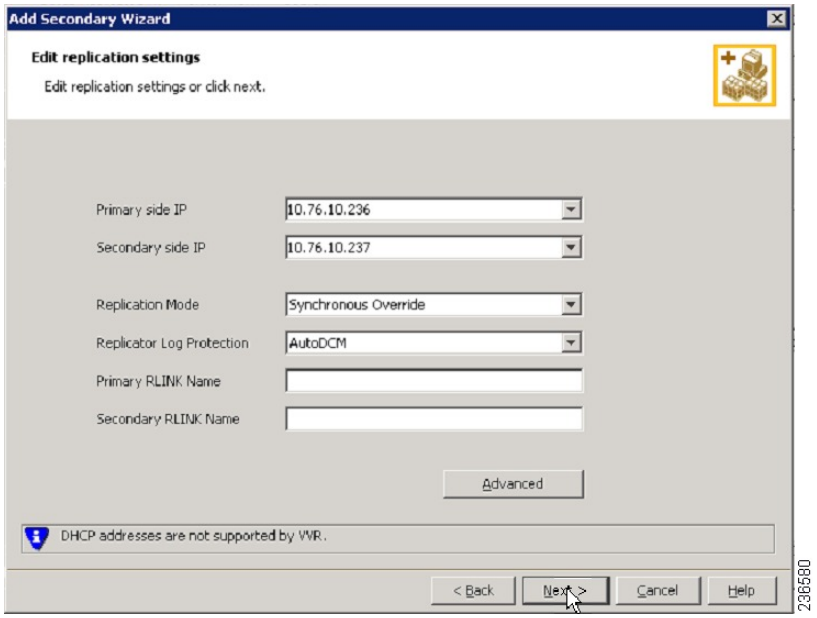


ステップ 10 [次へ（Next）] をクリックし、[レプリケーション設定の編集（Edit replication settings）] パネルで次の項目を指定します。

（注） プライマリおよびセカンダリ側の IP アドレスについては、NIC カードの固定 IP アドレスを指定できます。ただし、Veritas Cluster Server を使用する場合は、後で戻って VCS の制御下の仮想 IP アドレスを使用するように IP アドレスを更新する必要があります。VEA のツリーでセカンダリ RVG を選択し、[アクション（Actions）] > [複製設定の変更（Change Replication Settings）] を選択して、これを実行します。

- [プライマリ側IP（Primary side IP）]：<プライマリサーバの IP アドレス>
- [セカンダリ側IP（Secondary side IP）]：<セカンダリサーバの IP アドレス>
- [複製モード（Replication Mode）]：[同期上書き（Synchronous Override）]

- [レプリケータログ保護（Replicator Log Protection）]：<[オフ（Off）]、[失敗（Fail）]、[DCM（DCM）]、[AutoDCM（AutoDCM）]（デフォルト）、[オーバーライド（Override）] から選択>。各選択肢の説明については、『Volume Replicator Administrator's Guide』[英語]を参照してください。



ステップ 11 [次へ（Next）] をクリックして、デフォルトの設定で複製を開始します。[自動的に同期（Synchronize Automatically）] を選択し、[複製の開始（Start Replication）] がオンになっていることを確認します。

ステップ 12 [次へ（Next）] をクリックして [概要（Summary）] ページを表示してから [終了（Finish）] をクリックします。

作業ボリュームに対する権限の更新

Security Manager をインストールすると、Security Manager を実行するための特別なローカルユーザー（casuser）とグループ（casusers）が作成されます。セカンダリサーバーで Security Manager の保護されたインスタンスを実行するには、cscopx ボリュームにローカル casusers グループ権限を追加する必要があります。

ここでは、次の内容について説明します。

- 共有ストレージを使用する場合の権限の更新 （17 ページ）
- 複製を使用する場合の権限の更新 （18 ページ）

共有ストレージを使用する場合の権限の更新

共有ストレージを使用する場合にセカンダリサーバに対するローカル casusers グループ権限を追加するには、次の手順に従います。

ステップ 1 プライマリサーバで実行されている場合は、offline.pl スクリプトを使用して Security Manager を停止します。詳細については、Security Manager の手動での起動、停止、フェールオーバーを参照してください。

ステップ 2 プライマリサーバーから **datadg** ディスクグループをデポートします。

ステップ 3 セカンダリサーバーに **datadg** ディスクグループをインポートします。

ステップ 4 VEA GUI またはコマンドラインを使用して、選択したドライブ文字にプライマリボリューム（cscopx）を割り当てます。

ステップ 5 Windows Explorer で、**<選択されたドライブ文字>:\Program Files\CSCOpx** フォルダを右クリックし、[共有とセキュリティ（Sharing and Security）] メニュー項目を選択します。

ステップ 6 フォルダプロパティのダイアログボックスが表示されます。[セキュリティ（Security）] タブを選択して [追加（Add）] をクリックします。

ステップ 7 [ユーザーまたはグループの選択（Select Users or Groups）] ダイアログボックスの [場所（Location）] をクリックし、選択ツリーからローカルサーバーを選択します。

ステップ 8 オブジェクト名を入力するテキストボックスに casusers を入力し、[名前の確認（Check Names）] をクリックします。テキストボックスに、*<ServerName>\casusers* が表示されます。[OK] をクリック

ステップ 9 casuser が選択されていることを確認し、[許可（Allow）] の下の [フルコントロール（Full Control）] チェックボックスをオンにして、casusers グループに完全な制御権限を付与します。

ステップ 10 [詳細（Advanced）] をクリックします。

ステップ 11 [詳細設定（Advanced Settings）] で、[子オブジェクトのアクセス許可エントリすべてを、このオブジェクトからの継承可能なアクセス許可エントリで置き換える（Replace permission entries on all child objects with entries shown here that apply to child objects）] チェックボックスをオンにします。

ステップ 12 [適用（Apply）] をクリックし、CSCOpx ディレクトリのすべての子オブジェクトに権限が伝播されるまで待機します。

ステップ 13 伝播が完了したら、[OK（OK）] をクリックします。

ステップ 14 [OK（OK）] をクリックして [CSCOpxのプロパティ（CSCOpx Properties）] ダイアログボックスを閉じます。

ステップ 15 cscopx ボリュームのドライブ文字の割り当てを解除します。

ステップ 16 セカンダリサーバから datadg ディスクグループをデポートします。

ステップ 17 プライマリサーバに datadg ディスクグループをインポートします。

ステップ 18 VEA GUI またはコマンドラインを使用して、選択したドライブ文字にプライマリボリューム（cscopx）を割り当てます。

複製を使用する場合の権限の更新

複製を使用する場合にセカンダリサーバに対するローカル casusers グループ権限を追加するには、次の手順に従います。

ステップ 1 プライマリサーバで実行されている場合は、offline.pl スクリプトを使用して Security Manager を停止します。詳細については、Security Manager の手動での起動、停止、フェールオーバーを参照してください。

ステップ 2 cscopx ボリュームのドライブ文字の割り当てを解除します。

ステップ 3 複製のプライマリをセカンダリに移行します。

ステップ 4 セカンダリサーバの cscopx ボリュームに選択したドライブ文字を割り当てます。

ステップ 5 Windows Explorer で、**<選択されたドライブ文字>:\Program Files\CSCOpx**フォルダを右クリックし、[共有とセキュリティ（Sharing and Security）] メニュー項目を選択します。

ステップ 6 フォルダプロパティのダイアログボックスが表示されます。[セキュリティ（Security）] タブを選択して [追加（Add）] をクリックします。

ステップ 7 [ユーザーまたはグループの選択（Select Users or Groups）] ダイアログボックスの [場所（Location）] をクリックし、選択ツリーからローカルサーバーを選択します。

ステップ 8 オブジェクト名を入力するテキストボックスに **casusers** を入力し、[名前の確認（Check Names）] をクリックします。テキストボックスに、*<ServerName>\casusers* が表示されます。OK をクリックします。

ステップ 9 casuser が選択されていることを確認し、[許可（Allow）] の下の [フルコントロール（Full Control）] チェックボックスをオンにして、casusers グループに完全な制御権限を付与します。

ステップ 10 [詳細設定（Advanced）] をクリックします。

ステップ 11 [詳細設定（Advanced Settings）] で、[子オブジェクトのアクセス許可エントリすべてを、このオブジェクトからの継承可能なアクセス許可エントリで置き換える（Replace permission entries on all child objects with entries shown here that apply to child objects）] チェックボックスをオンにします。

ステップ 12 [適用（Apply）] をクリックし、CSCOpx ディレクトリのすべての子オブジェクトに権限が伝播されるまで待機します。

ステップ 13 伝播が完了したら、[OK（OK）] をクリックします。

（注） 権限の更新中に、「セキュリティ適用エラー（Error Applying Security）」というタイトルのエラーダイアログに「セキュリティ情報を<Selected Drive Letter>:\Program Files\CSCOpx\log\dcr.log に適用中にエラーが発生しました。アクセスは拒否されます（An error occurred applying security information to: *<Selected Drive Letter>*:\Program Files\CSCOpx\log\dcr.log Access denied）」というメッセージが表示されることがあります。このエラーを無視し、エラーダイアログで [続行（Continue）] をクリックして権限の更新プロセスを完了できます。

ステップ 14 [OK（OK）] をクリックして [CSCOpxのプロパティ（CSCOpx Properties）] ダイアログボックスを閉じます。

ステップ 15 cscopx ボリュームのドライブ文字の割り当てを解除します。

ステップ 16 プライマリサーバに複製を戻します。

ステップ 17 プライマリサーバの cscopx ボリュームに選択したドライブ文字を割り当てます。

Veritas Cluster Server タスク

ここでは、Veritas クラスタのセットアップおよび設定のプロセスについて説明します。2 つの特定のシナリオについて説明します。

シングルローカルクラスタ（デュアルノード）構成 （20 ページ）

デュアル地理的クラスタ構成 （24 ページ）

シングルローカルクラスタ（デュアルノード）構成

ここでは、クラスタ内に2ノード（プライマリとセカンダリ）を持つシングルローカルクラスタのセットアップおよび設定について説明します。

ここでは、次の内容について説明します。

クラスタの作成

クラスタを作成するには、次の手順に従います。

ステップ 1 VCS クラスタ設定ウィザードを使用してクラスタを作成します。

- Cluster Name = CSManager_Primary
- Cluster ID = 0

クラスタの定義にプライマリサーバとセカンダリサーバを含めます。ウィザードのクラスタ定義の一部はプライベートネットワークの NIC を指定します。VCS は、クラスタメンテナンスでのクラスタ ノード間の通信のためにプライベートネットワークを使用します。すべての専用クラスタ通信インターフェイスに障害が発生した場合に、プライオリティが低いクラスタ通信インターフェイスとして動作するように、ネットワーク イーサネット インターフェイスの 1 を割り当てることもできます。

ステップ 2 Cluster Manager を起動するには、**[スタート（Start）] > [すべてのプログラム（All Programs）] > [Cluster Manager - Java Console（Veritas Cluster Manager - Java Console）]** を選択し、クラスタにログインします。

ステップ 3 Cluster Manager を使用し、**[ファイル（File）] > [インポートタイプ（Import Types）]**を選択して、CSManage リソースタイプをインポートします。$VCS_ROOT\cluster server\conf\config の下にある CSManagerTypes.cf ファイルを参照し、[インポート（Import）] をクリックします。

アプリケーション サービス グループの作成

アプリケーション サービス グループを作成するには、次の手順に従います。

（注） プライマリクラスタとセカンダリクラスタの両方で次の手順を実行します。

ステップ 1 APP というサービスグループを追加します。

ステップ 2 [APP（APP）] サービスグループを右クリックし、[リソースの追加（Add Resource）] を選択します。

RVG プライマリ リソースを追加します。

- [リソース名（Resource name）] = **APP_RVGPrimary**
- [リソースタイプ（Resource Type）] = **RVGPrimary**
- [RvgResourceName（RvgResourceName）] = **APP_RVG**

ステップ 3 [APP（APP）] サービスグループを右クリックし、[リソースの追加（Add Resource）] を選択します。

MountV リソースを追加します。

- [リソース名（Resource name）] = **APP_MountV**
- [リソースタイプ（Resource Type）] = **MountV**
- [マウントパス（Mount Path）] = <選択されたドライブ文字>:\
- [ボリューム名（ボリューム名）] = **cscopx**
- [VMDgリソース名（VMDg Resource Name）] = **datadg**

ステップ 4 [APP（APP）] サービスグループを右クリックし、[リソースの追加（Add Resource）] を選択します。

RegRep リソースを追加し、[クリティカル（Critical）] および [有効（Enabled）] チェックボックスをオンにします。

- [リソース名（Resource name）] = **APP_RegRep**
- [MountResName（MountResName）] = **APP_MountV**
- [ReplicationDirectory（ReplicationDirectory）] = **\REGREP\DEFAULT**
- [Keys（Keys）] = **HKLM\Software\JavaSoft\Prefs\vms**

（注） Security Manager は、サーバーレジストリの HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Prefs\vms の下にクライアント ユーザー プリファレンスを保存します。レジストリ複製エージェント（RegRep）は、アクティブサーバの指定レジストリの場所の変更をモニタし、フェールオーバーの発生時にセカンダリサーバにこれらの変更を同期化します。

ステップ 5 [APP（APP）] サービスグループを右クリックし、[リソースの追加（Add Resource）] を選択します。

Proxy リソースを追加します。

- [リソース名（Resource name）] = **APP_NIC_Proxy**
- [リソースタイプ（Resource Type）] = **Proxy**
- [TargetResName（TargetResName）] = **NIC**

ステップ 6 [APP（APP）] サービスグループを右クリックし、[リソースの追加（Add Resource）] を選択します。

IP リソースを追加します。

- [リソース名（Resource name）] = **APP_IP**
- [リソースタイプ（Resource Type）] = **IP**
- [Address（Address）] = <アプリケーション用に割り当てられた仮想 IP アドレス>
- [SubNetMask（SubNetMask）] = <サブネットマスク>
- [MACAddress（MACAddress）] = <NIC カードに対応する MAC アドレス>

ステップ 7 [APP（APP）] サービスグループを右クリックし、[リソースの追加（Add Resource）] を選択します。

CSManager リソースを追加します。

- [リソース名（Resource name）] = **APP_CSManager**
- [リソースタイプ（Resource Type）] = **CSManager**
- [PathName（PathName）] = <選択されたドライブ文字>:\Program Files\CSCOpx
- [EventIPAddress（EventIPAddress）] = APP_IP で使用されているものと同じ IP アドレス
- [CertificateDir （CertificateDir）] = この属性の説明については、SSL 用のセキュリティ証明書を参照してください。

ステップ 8 次の表の定義に従ってリソースをリンクします（リソースビュー：APP グループ（デュアルクラスタ、シングルノード） を参照）。

親リソース	子リソース
APP_MountV	APP_RVGPrimary
APP_RegRep	APP_MountV
APP_CSManager	APP_RegRep
APP_IP	APP_NIC_Proxy
APP_CSManager	APP_IP

リソースをリンクするには、次の手順に従います。

a) 親リソースを右クリックし、[リンク（Link）] を選択します。

[リンクリソース（Link Resources）] ダイアログボックスが表示されます。

b) 子リソースを選択し、[OK（OK）] をクリックします。

選択したリソースがリンクされます。

ClusterService グループの作成

ClusterService グループを作成するには、次の手順を実行します。

（注） プライマリクラスタとセカンダリクラスタの両方で次の手順を実行します。

ヒント クラスタ間の通信用に ClusterService グループおよび wac リソースを作成するためのこの項の手順に代わる方法として VCS 設定ウィザードを使用できます。VCS 設定ウィザードでオプションの Cluster Manager（Web コンソール）と通知コンポーネントを設定することもできます。『Veritas Cluster Server Administrator's Guide』[英語] を参照してください。

ステップ 1 [CSManager（CSManager）] リソースを右クリックし、[サービスグループの追加（Add Service Group）] を選択します。

ClusterService というサービスグループを追加します。

ステップ 2 [ClusterService（ClusterService）] サービスグループを右クリックし、[リソースの追加（Add Resources）] を選択します。

NIC リソースを追加します。

- [リソース名（Resource name）] = **NIC**
- [リソース タイプ（Resource Type）] = **NIC**
- [MACAddress（MACAddress）] = <NIC カードの MAC アドレス>

（注） DOS レベルのコマンド **ipconfig -all** を使用して、各イーサネット インターフェイスに関連付けられた MAC アドレスを検索できます。

ステップ 3 [ClusterService（ClusterService）] サービスグループを右クリックし、[リソースの追加（Add Resources）] を選択します。

IP リソースを追加します

- [リソース名（Resource name）] = **VCS_IP**
- [リソースタイプ（Resource Type）] = **IP**
- [Address（Address）] = <クラスタに割り当てられた仮想 IP アドレス>
- [SubNetMask（SubNetMask）] = <サブネット マスク>
- [MACAddress（MACAddress）] = <NIC カードに対応する MAC アドレス>

ステップ 4 [ClusterService（ClusterService）] サービスグループを右クリックし、[リソースの追加（Add Resources）] を選択します。

wac リソースを追加します。

- [リソース名（Resource name）] = **wac**
- [リソースタイプ（Resource Type）] = **Process**
- [StartProgram（StartProgram）] = **C:\Program Files\Veritas\Cluster Server\bin\wac.exe**
- [StopProgram（StopProgram）] = **C:\Program Files\Veritas\Cluster Server\bin\wacstop.exe**
- [MonitorProgram（MonitorProgram）] = **C:\Program Files\Veritas\Cluster Server\bin\wacmonitor.exe**

ステップ 5 次の表の定義に従ってリソースをリンクします（リソースビュー：APP グループ（デュアルクラスタ、シングルノード） を参照）。

親リソース	子リソース
wac	VCS_IP
VCS_IP	NIC

リソースをリンクするには、次の手順に従います。

a) 親リソースを右クリックし、[リンク（Link）] を選択します。

[リンクリソース（Link Resources）] ダイアログボックスが表示されます。

b) 子リソースを選択し、[OK（OK）] をクリックします。

選択したリソースがリンクされます。

デュアル地理的クラスタ構成

ここでは、各クラスタ内に 1 つのノードを含む、地理的に離れた 2 つのクラスタのセットアップと設定について説明します。

（注） 一方または両方のクラスタ内に複数のノードがあるデュアル地理的クラスタ構成を作成することもできます。

ここでは、次の内容について説明します。

- プライマリおよびセカンダリクラスタの作成 （25 ページ）
- ClusterService グループの作成 （23 ページ）
- 複製サービスグループの作成 （27 ページ）
- アプリケーション サービス グループの作成 （20 ページ）

• クラスタレベル設定の作成 （36 ページ）

プライマリおよびセカンダリクラスタの作成

プライマリ クラスタとセカンダリクラスタを作成するには、次の手順を実行します。

ステップ 1 VCS クラスタ設定ウィザードを使用して、（プライマリクラスタ内の）プライマリサーバでクラスタを作成します。

- Cluster Name = CSManager_Primary
- Cluster ID = 0

ステップ 2 VCS クラスタ設定ウィザードを使用して、（セカンダリクラスタ内の）プライマリサーバでクラスタを作成します。

- Cluster Name = CSManager_Secondary
- Cluster ID = 1

ステップ 3 プライマリクラスタで、**[スタート（Start）]** > **[すべてのプログラム（All Programs）]** > **[Veritas Cluster Manager - Java Console（Veritas Cluster Manager - Java Console）]** を選択し、クラスタにログインします。

ステップ 4 Cluster Manager を使用し、**[ファイル（File）]** > **[インポートタイプ（Import Types）]**を選択して、CSManage リソースタイプをインポートします。$VCS_ROOT\cluster server\conf\config の下にある CSManagerTypes.cf ファイルを参照し、[インポート（Import）] をクリックします。

ステップ 5 セカンダリクラスタに対してステップ 3 と 4 を繰り返します。

ClusterService グループの作成

ClusterService グループを作成するには、次の手順を実行します。

（注） プライマリクラスタとセカンダリクラスタの両方で次の手順を実行します。

ヒント クラスタ間の通信用に ClusterService グループおよび wac リソースを作成するためのこの項の手順に代わる方法として VCS 設定ウィザードを使用できます。VCS 設定ウィザードでオプションの Cluster Manager（Web コンソール）と通知コンポーネントを設定することもできます。『Veritas Cluster Server Administrator's Guide』[英語] を参照してください。

ステップ 1 [CSManager（CSManager）] リソースを右クリックし、[サービスグループの追加（Add Service Group）] を選択します。

ClusterService というサービスグループを追加します。

ステップ 2 [ClusterService（ClusterService）] サービスグループを右クリックし、[リソースの追加（Add Resources）] を選択します。

NIC リソースを追加します。

- [リソース名（Resource name）] = **NIC**
- [リソース タイプ（Resource Type）] = **NIC**
- [MACAddress（MACAddress）] = <NIC カードの MAC アドレス>

（注） DOS レベルのコマンド **ipconfig -all** を使用して、各イーサネット インターフェイスに関連付けられた MAC アドレスを検索できます。

ステップ 3 [ClusterService（ClusterService）] サービスグループを右クリックし、[リソースの追加（Add Resources）] を選択します。

IP リソースを追加します

- [リソース名（Resource name）] = **VCS_IP**
- [リソースタイプ（Resource Type）] = **IP**
- [Address（Address）] = <クラスタに割り当てられた仮想 IP アドレス>
- [SubNetMask（SubNetMask）] = <サブネット マスク>
- [MACAddress（MACAddress）] = <NIC カードに対応する MAC アドレス>

ステップ 4 [ClusterService（ClusterService）] サービスグループを右クリックし、[リソースの追加（Add Resources）] を選択します。

wac リソースを追加します。

- [リソース名（Resource name）] = **wac**
- [リソースタイプ（Resource Type）] = **Process**
- [StartProgram（StartProgram）] = **C:\Program Files\Veritas\Cluster Server\bin\wac.exe**
- [StopProgram（StopProgram）] = **C:\Program Files\Veritas\Cluster Server\bin\wacstop.exe**
- [MonitorProgram（MonitorProgram）] = **C:\Program Files\Veritas\Cluster Server\bin\wacmonitor.exe**

ステップ 5 次の表の定義に従ってリソースをリンクします（リソースビュー：APP グループ（デュアルクラスタ、シングルノード） を参照）。

親リソース	子リソース
wac	VCS_IP
VCS_IP	NIC

リソースをリンクするには、次の手順に従います。

a) 親リソースを右クリックし、[リンク（Link）] を選択します。

[リンクリソース（Link Resources）] ダイアログボックスが表示されます。

b) 子リソースを選択し、[OK（OK）] をクリックします。

選択したリソースがリンクされます。

複製サービスグループの作成

複製サービスグループを作成するには、次の手順に従います。

（注） プライマリクラスタとセカンダリクラスタの両方で次の手順を実行します。

ステップ 1 [CSManager（CSManager）] リソースを右クリックし、[サービスグループの追加（Add Service Group）] を選択します。

APPrep というサービス グループを追加します。

ステップ 2 [APPrep（APPrep）] サービスグループを右クリックし、[リソースの追加（Add Resource）] を選択します。

Proxy リソースを追加します。

- [リソース名（Resource name）] = **VVR_NIC_Proxy**
- [リソースタイプ（Resource Type）] = **Proxy**
- [TargetResName（TargetResName）] = **NIC**

ステップ 3 [APPrep（APPrep）] サービスグループを右クリックし、[リソースの追加（Add Resource）] を選択します。

IP リソースを追加します。

- [リソース名（Resource name）] = **VVR_IP**
- [リソースタイプ（Resource Type）] = **IP**
- [Address（Address）] = <複製に割り当てられた仮想 IP アドレス>
- [SubNetMask（SubNetMask）] = <サブネット マスク>
- [MACAddress（MACAddress）] = <NIC カードに対応する MAC アドレス>

ステップ 4 [APPrep（APPrep）] サービスグループを右クリックし、[リソースの追加（Add Resource）] を選択します。

VMDg リソースを追加します。

- [リソース名（Resource name）] = datadg

- [リソースタイプ（Resource Type）] = VMDg
- [DiskGroupName（DiskGroupName）] = datadg

ステップ 5 [APPrep（APPrep）] サービスグループを右クリックし、[リソースの追加（Add Resource）] を選択します。]

VvrRvg リソースを追加します。

- [リソース名（Resource name）] = **APP_RVG**
- [リソースタイプ（Resource Type）] = **VvrRvg**
- [RVG（RVG）] = **CSM_RVG**
- [VMDGResName（VMDGResName）] = **datadg**
- [IPResName（IPResName）] = **VVR_IP**

ステップ 6 次の表の定義に従ってリソースをリンクします（リソースビュー：APPrep グループ（デュアルクラスタ、シングルノード） を参照）。

親リソース	子リソース
VVR_IP	VVR_NIC_Proxy
APP_RVG	VVR_IP
APP_RVG	datadg

リソースをリンクするには、次の手順に従います。

a) 親リソースを右クリックし、[リンク（Link）] を選択します。

[リンクリソース（Link Resources）] ダイアログボックスが表示されます。

b) 子リソースを選択し、[OK（OK）] をクリックします。

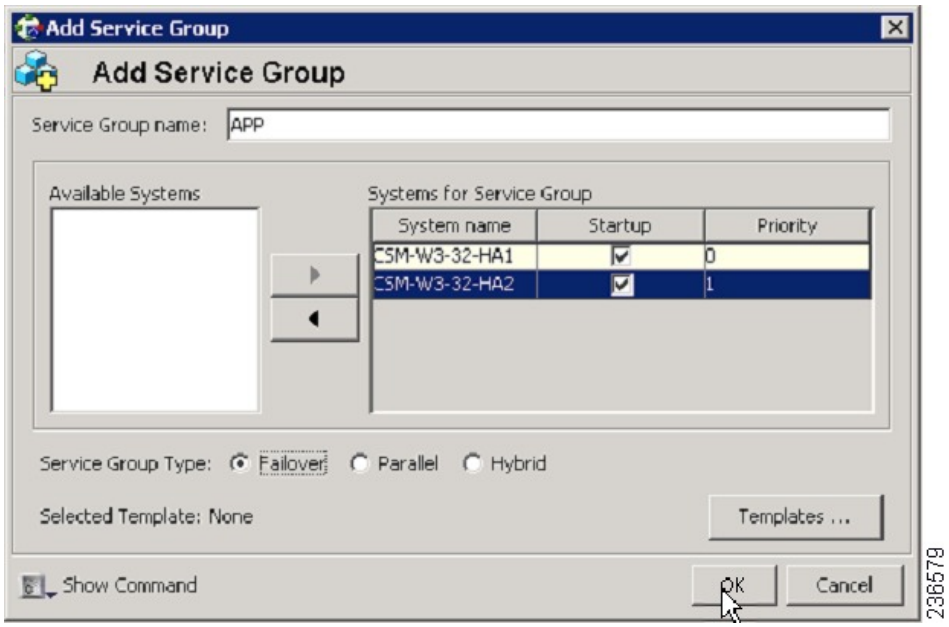
選択したリソースがリンクされます。

アプリケーション サービス グループの作成

アプリケーション サービス グループを作成するには、次の手順に従います。

ステップ 1 [CSManager（CSManager）] リソースを右クリックし、[サービスグループの追加（Add Service Group）] を選択します。

APP というサービスグループを追加し、このサービスグループの両方のサーバを含めて（各サーバの [スタートアップ（Startup）] オプションをオンにする）、サービスグループタイプを [フェールオーバー（Failover）] にします。

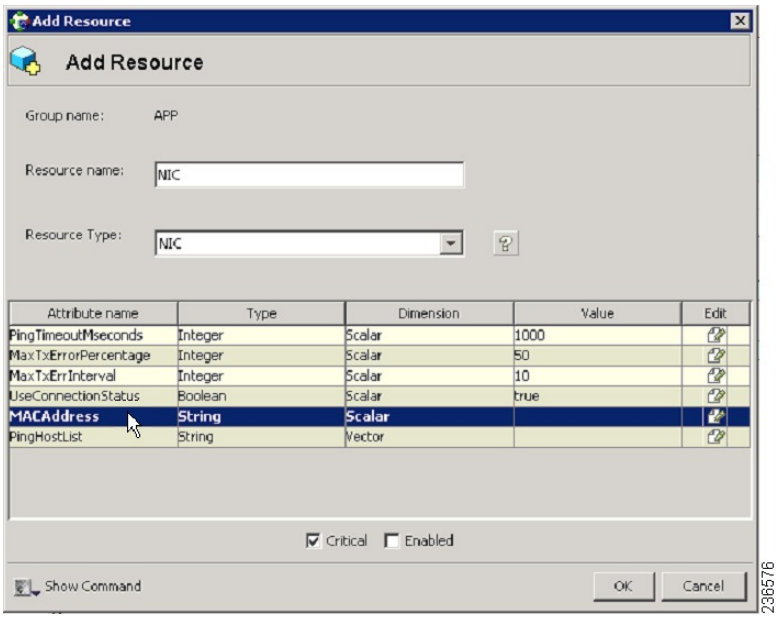


ステップ 2 [APP（APP）] サービスグループを右クリックし、[リソースの追加（Add Resource）] を選択します。

NIC リソースを追加し、[クリティカル（Critical）] および [有効（Enabled）] チェックボックスをオンにします。

- [リソース名（Resource name）] = NIC
- [リソースタイプ（Resource Type）] = NIC
- [MACAddress（MACAddress）] = <Security Manager アプリケーションにアクセスするために使用する NIC の MAC アドレス>（クラスタ内のサーバーごとに一意に定義されます）。

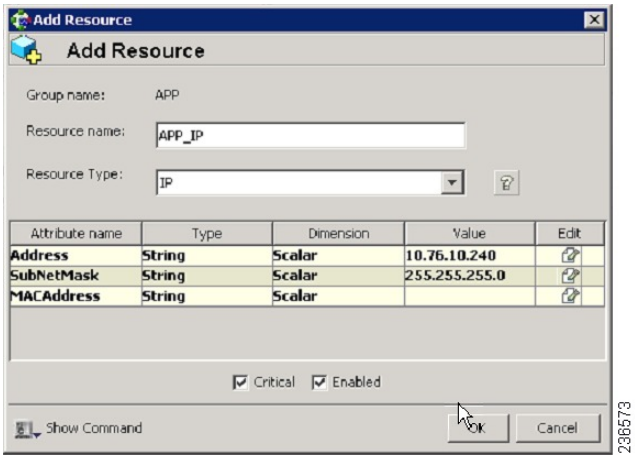
（注） DOS レベルのコマンド ipconfig -all を使用して、各イーサネット インターフェイスに関連付けられた MAC アドレスを検索できます。



ステップ 3 [APP（APP）] サービスグループを右クリックし、[リソースの追加（Add Resource）] を選択します。

IP リソースを追加し、[クリティカル（Critical）] および [有効（Enabled）] チェックボックスをオンにします。

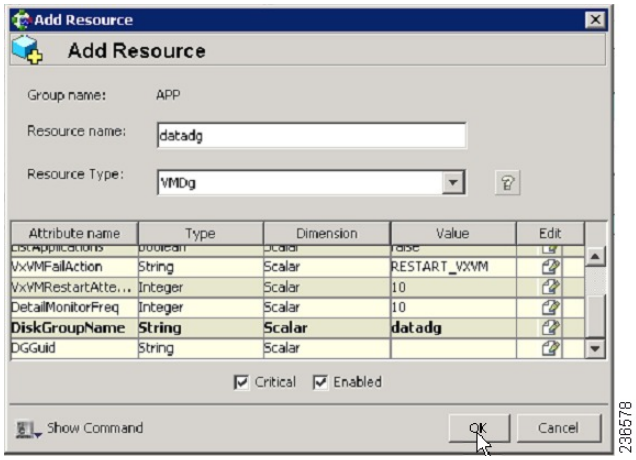
- [リソース名（Resource name）] = APP_IP
- [リソースタイプ（Resource Type）] = IP
- [Address（Address）] = <Security Manager アプリケーションで使用するために割り当てられた仮想 IP アドレス>（グローバル属性として定義）
- [SubNetMask（SubNetMask）] = <サブネットマスク> （グローバル属性として定義）
- [MACAddress（MACAddress）] = <アプリケーションにアクセスする NIC の MAC アドレス>（クラスタ内のサーバーごとに定義）



ステップ 4 [APP（APP）] サービスグループを右クリックし、[リソースの追加（Add Resource）] を選択します。

VMDg リソースを追加し、[クリティカル（Critical）] および [有効（Enabled）] チェックボックスをオンにします。

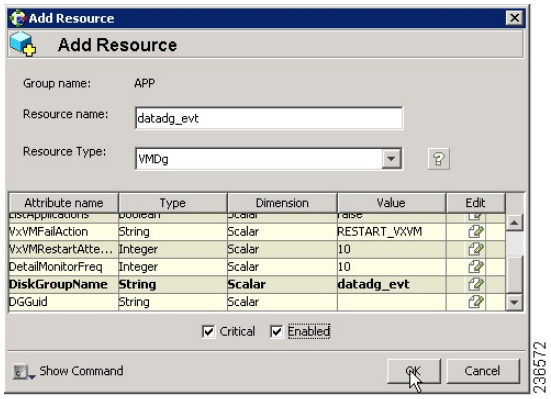
- [リソース名（Resource name）] = datadg
- [リソースタイプ（Resource Type）] = VMDg
- [DiskGroupName（DiskGroupName）] = datadg（グローバル属性として定義）



ステップ 5 [VMDg（VMDg）] リソースグループを右クリックし、[リソースの追加（Add Resource）] を選択します。

datadg_evt リソースを追加し、[クリティカル（Critical）] および [有効（Enabled）] チェックボックスをオンにします。

- [リソース名（Resource name）] = datadg_evt
- [リソースタイプ（Resource Type）] = VMDg
- [DiskGroupName（DiskGroupName）] = datadg_evt（グローバル属性として定義）



ステップ 6 [APP（APP）] サービスグループを右クリックし、[リソースの追加（Add Resource）] を選択します。

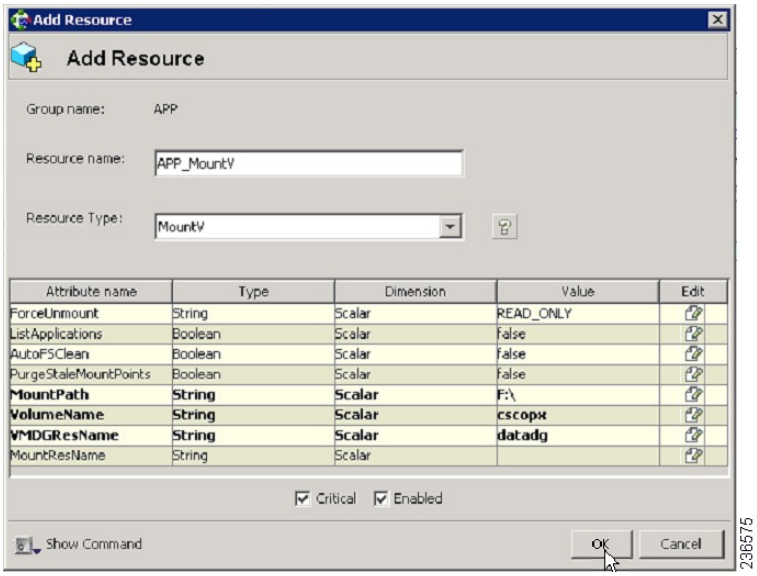
MountV リソースを追加し、[クリティカル（Critical）] および [有効（Enabled）] チェックボックスをオンにします。

- [リソース名（Resource name）] = APP_MountV
- [リソースタイプ（Resource Type）] = MountV
- [MountPath（MountPath）] =<選択したドライブ文字> :\（グローバル属性として定義）
- [VolumeName（VolumeName）] = cscopx（グローバル属性として定義）
- [DiskGroupName（DiskGroupName）] = datadg（グローバル属性として定義）
- [ForceUnmount（ForceUnmount）] = {NONE, READ-ONLY, ALL}

他のアプリケーションで使用されている場合に、エージェントが強制的にボリュームをアンマウントするかどうかを定義します。次のオプションを利用できます。

- [なし（NONE）] : エージェントは、アプリケーションがアクセスしている場合は、ボリュームをアンマウントしません。
- [読み取り専用（READ-ONLY）] : エージェントは、アプリケーションが読み取り専用モードでアクセスしている場合に、ボリュームをアンマウントします。
- [すべて（ALL）] : エージェントは、アプリケーションが持つアクセス権の種類に関係なくボリュームをアンマウントします。

デフォルトは [なし（NONE）] です。ボリュームをアンマウントできない場合、セカンダリサーバへの自動フェールオーバーが禁止されている場合があるため、[読み取り専用（READ-ONLY）] または [すべて（ALL）] の値の選択が必要になることがあります。



ステップ 7 [MountV（MountV）] リソースグループを右クリックし、[リソースの追加（Add Resource）] を選択します。

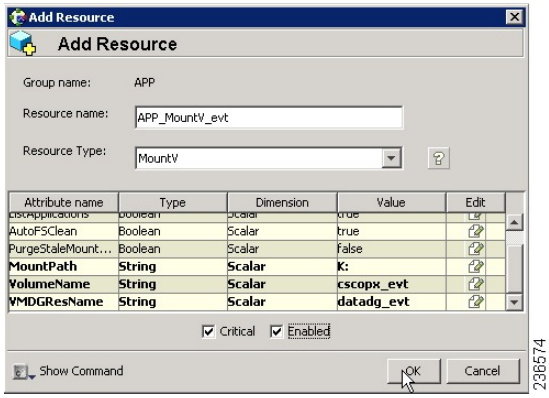
MountV_evt リソースを追加し、[クリティカル（Critical）]および[有効（Enabled）]チェックボックスをオンにします。

- [リソース名（Resource name）] = APP_MountV_evt
- [リソースタイプ（Resource Type）] = MountV
- [MountPath（MountPath）] =<選択したドライブ文字> :\（グローバル属性として定義）
- [VolumeName（VolumeName）] = cscopx_evt（グローバル属性として定義）
- [VMDGResName（VMDGResName）] = datadg_evt（グローバル属性として定義）
- [ForceUnmount（ForceUnmount）] = {NONE, READ-ONLY, ALL}

他のアプリケーションで使用されている場合に、エージェントが強制的にボリュームをアンマウントするかどうかを定義します。次のオプションを利用できます。

- [なし（NONE）] : エージェントは、アプリケーションがアクセスしている場合は、ボリュームをアンマウントしません。
- [読み取り専用（READ-ONLY）] : エージェントは、アプリケーションが読み取り専用モードでアクセスしている場合に、ボリュームをアンマウントします。
- [すべて（ALL）] : エージェントは、アプリケーションが持つアクセス権の種類に関係なくボリュームをアンマウントします。

デフォルトは [なし（NONE）] です。ボリュームをアンマウントできない場合、セカンダリサーバへの自動フェールオーバーが禁止されている場合があるため、[読み取り専用（READ-ONLY）] または [すべて（ALL）] の値の選択が必要になることがあります。

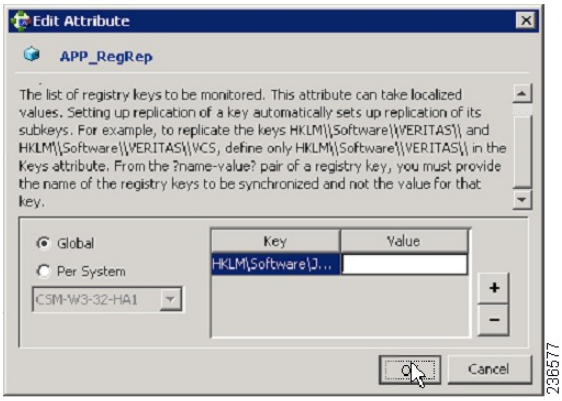


ステップ 8 [APP（APP）] サービスグループを右クリックし、[リソースの追加（Add Resource）] を選択します。

RegRep リソースを追加し、[クリティカル（Critical）] および [有効（Enabled）] チェックボックスをオンにします。

- [リソース名（Resource name）] = APP_RegRep
- [リソースタイプ（Resource Type）] = RegRep

- [MountResName（MountResName）] = APP_MountV（グローバル属性として定義）
- [ReplicationDirectory（ReplicationDirectory）] = \REGREP\DEFAULT（グローバル属性として定義）
- [Keys（グローバル属性として定義）Key（Keys (defined as a Global attribute)Key）] = HKLM\Software\JavaSoft\Prefs\vmsValue =<blank>

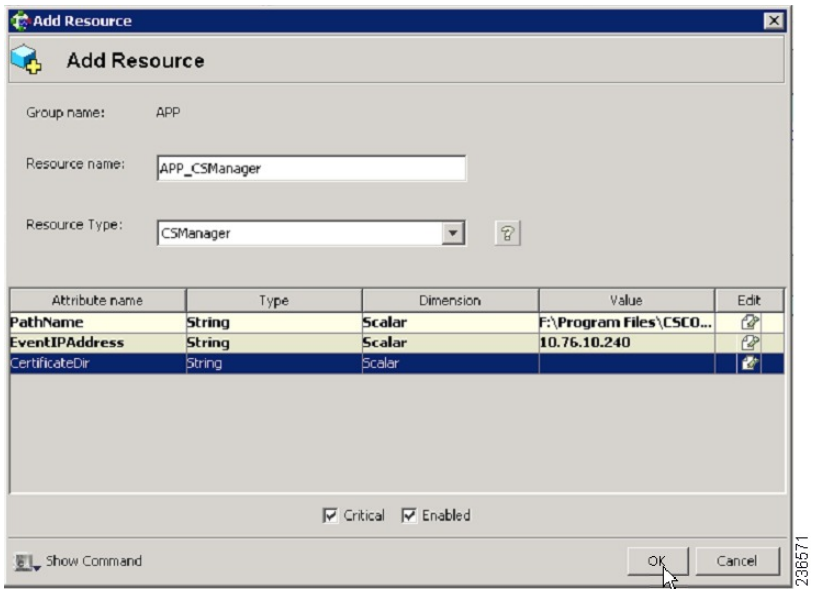


（注） Security Manager は、サーバーレジストリの HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Prefs\vms の下にクライアント ユーザー プリファレンスを保存します。レジストリ複製エージェント（RegRep）は、アクティブサーバの指定レジストリの場所の変更をモニタし、フェールオーバーの発生時にセカンダリサーバにこれらの変更を同期化します。

ステップ 9 [APP（APP）] サービスグループを右クリックし、[リソースの追加（Add Resource）] を選択します。

CSManager リソースを追加し、[クリティカル（Critical）] および [有効（Enabled）] チェックボックスをオンにします。

- [リソース名（Resource name）] = APP_CSManager
- [リソースタイプ（Resource Type）] = CSManager
- [PathName（PathName）] =<選択されたドライブ文字>:\Program Files\CSCOpx\（グローバル属性として定義）
- [EventIPAddress（EventIPAddress）] = APP_IP で使用されているものと同じ IP アドレス（グローバル属性として定義）
- [CertificateDir（CertificateDir）] = この属性の説明については、SSL 用のセキュリティ証明書を参照してください。



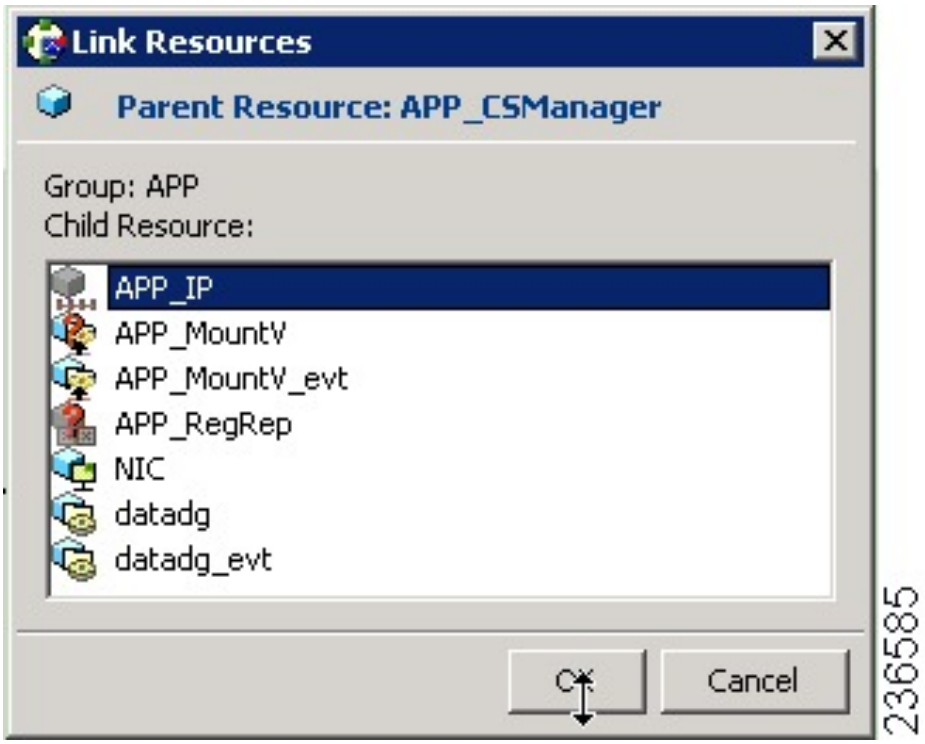
ステップ 10 次の表の定義に従ってリソースをリンクします（リソースビュー：APP グループ（デュアルクラスタ、シングルノード） を参照）。

親リソース	子リソース
APP_CSManager	APP_RegRep
APP_CSManager	APP_IP
APP_IP	NIC
APP_RegRep	APP_MountV
APP_RegRep	APP_MountV_evt
APP_MountV	datadg
APP_MountV_evt	datadg_evt

リソースをリンクするには、次の手順に従います。

a) 親リソースを右クリックし、[リンク（Link）] を選択します。

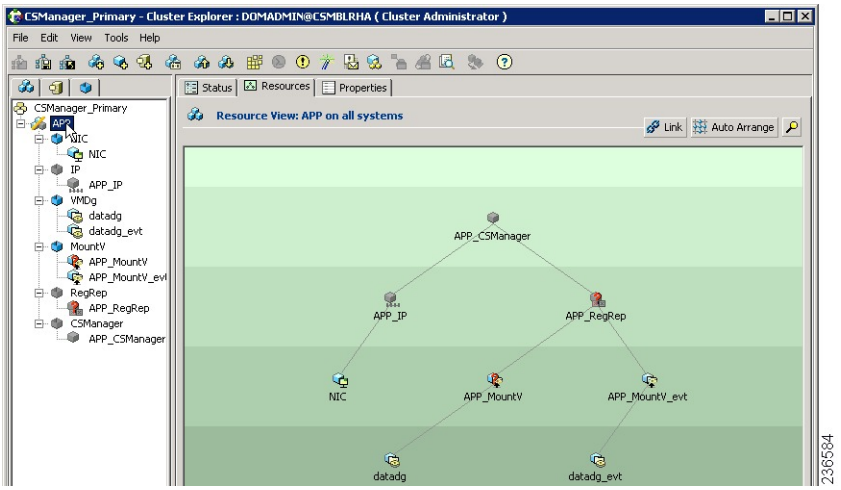
[リンクリソース（Link Resources）] ダイアログボックスが表示されます。



b) 子リソースを選択し、[OK（OK）] をクリックします。

選択したリソースがリンクされます。

すべてのリンクが作成されると、リソースビューは次のように表示されます。



クラスタレベル設定の作成

クラスタレベル設定を作成するには、次の手順に従います。

ステップ 1 APPrep サービスグループの親として APP サービスグループをオンライン ローカル ファーム依存関係にリンクします。プライマリクラスタとセカンダリクラスタの両方でこの手順を実行します。

ステップ 2 クラスタ プロパティで、VCS_IP リソースで使用したのと同じ IP アドレスであるクラスタ アドレスを指定します。

ステップ 3 プライマリクラスタから、**[編集（Edit）]**> **[リモートクラスタの追加/削除（Add/Delete Remote Cluster）]** を選択して、リモートクラスタ設定ウィザードでセカンダリクラスタを追加します。

ステップ 4 プライマリクラスタから、**[編集（Edit）]** > **[グローバルグループの設定（Configure Global Groups）]**を選択して、グローバルグループ設定ウィザードで APP サービスグループをグローバルグループとして設定します。

サービスグループビュー（デュアルクラスタ、シングルノード） を参照してください。

翻訳について
このドキュメントは、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。