CHAPTER 3

Cisco Security Management Suite ハイ アベイラビリティ ソリューションのインストール

この章では、HA または DR の導入コンフィギュレーションに Security Manager をインストールする方法を説明します。次のタスクを順序どおりに実行する必要があります。ただし、一部のタスクは任意であるか、またはコンフィギュレーションによっては適用されない場合もあります。インストールおよび設定の作業概要については、「ローカル冗長性（HA）設定手順」（P.1-2）または「地理的冗長性（DR）の設定手順」（P.1-4）を参照してください。

この章の内容は以下のとおりです。

イーサネット接続の確立

HA または DR コンフィギュレーションで必要となるイーサネット接続を確立するには、次の手順を実行します。

ステップ 1　クラスタ コンフィギュレーションに応じて、図 2-1 または 図 2-2 に従ってサーバとスイッチの間のイーサネット接続を確立します。

（注）　各サーバのルータ / スイッチ ネットワークへの 2 番目のイーサネット接続の使用はオプションですが、NIC またはローカル イーサネットの障害時に冗長性のレベルが追加されます。Veritas Cluster Server（VCS）には IPMultiNicPlus エージェントが含まれています。このエージェントでは、複数の NIC カードをサーバ上でセットアップでき、これによってサーバにルータ / 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 カードの故障、ケーブルの切断、またはその他の何らかの障害が発生した場合、VCS は障害を検出して、動作中の仮想 IP アドレスをサーバ上で動作中の別の NIC カードに再割り当てすることができます。IPMultiNicPlus エージェントの詳細については、『Veritas Cluster Server Bundled Agents Reference Guide』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 アクセスに単一の NIC カードを使用する場合のみを示します。

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、図 2-2 に従ってサーバ間のイーサネット クラスタ通信接続を確立します。サーバ間で直接接続する場合、インターフェイスで自動クロスオーバー検出がサポートされているかどうかに応じて、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場合もあります。最新のイーサネット インターフェイスではこの機能がサポートされており、別のサーバに直接接続する場合、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

サポートされるいずれかの 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 2008、Enterprise Edition SP2（32 ビットまたは 64 ビット）
- Microsoft Windows Server 2003 R2、Enterprise Edition SP2（32 ビット）

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お勧めします。

（注）　Veritas Storage Foundation HA では、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、1 つのノードで 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も C:¥WINDOWS にインストールする必要があります。すべてのノードで同じドライブ文字を使用でき、システム ドライブにインストールするための十分な空き容量があることを確認してください。

外部ストレージへのサーバの接続

デュアルノード クラスタを使用している場合は、共有の外部ストレージが必要です。『*Hardware Compatibility List for Veritas Storage Foundation & High Availability Solutions for Windows*』に記載されているストレージ ハードウェアを使用できます。シングルノード クラスタには内部ストレージまたは外部ストレージを使用できます。

Symantec Veritas 製品のインストール

Symantec 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。必要な製品およびコンポーネントは、単一のローカル クラスタ、デュアル地域クラスタ、またはクラスタリング コンフィギュレーションなしのレプリケーションのいずれを使用するかに応じて異なります。Volume Manager（Veritas Enterprise Administrator）の GUI など、一部のコンポーネントはオプションです。表 3-1 を参照してください。

表 3-1　Veritas のソフトウェア コンポーネント

Veritas 製品 / コンポーネント	単一のローカル クラスタ	デュアル地域クラスタ	クラスタリングなしのレプリケーション
Storage Foundation for Windows	—	—	必須
Storage Foundation HA for Windows	必須	必須	—
Volume Replicator Option	任意	必須	必須
Global Cluster Option	任意	必須	—
Dynamic Multipathing Option	「注」を参照[1]	「注[1]」を参照	「注[1]」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. サーバとディスク ストレージの間に複数のパスを提供する、複数のホスト バス アダプタ付きの外部ストレージを使用している場合に限り必須です。
2. サーバまたは個別のクライアント 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ための前提条件と手順については、該当する Veritas のリリースノートおよびインストレーション 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。

起動ディスクのミラーリング（オプション）

起動ディスクのミラーリングはオプションですが、特定のサーバの保護レベルが上がります。起動ディスクに障害が発生した場合、ミラーリングされた別の起動ディスクから起動すると、すばやくマシンを回復できます。ミラーリングは Veritas Volume Manager の制御下にあるダイナミックなディスク グループに起動ディスクを配置し、ミラーを追加することによって実行できます。

この手順の詳細については、『Veritas Storage Foundation administrator's guide』の「Set up a Dynamic Boot and System Volume」を参照してください。

Veritas Volume Manager の設定タスク

ここでは、Security Manager アプリケーションに必要なディスク グループとボリュームを設定します。設定は、含まれるサーバがプライマリ サーバであるかどうか、またはレプリケーションが含まれるかどうかに応じて異なります。VEA GUI またはコマンド ラインから Volume Manager のタスクを実行できます。これらの手順のための VEA またはコマンド ラインの仕様の詳細については、『Veritas Storage Foundation for Windows administrator's guide』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（レプリケーションなし）

この項の手順を実行して、レプリケーションが含まれる場合の単一クラスタ コンフィギュレーションでのプライマリ サーバ上の Security Manager に必要なディスク グループとボリュームを設定します。単一クラスタ コンフィギュレーションでは、クラスタ内のすべてのサーバからアクセスできる外部の共有ストレージが使用されます。

ディスク グループと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。

- [Group Name]：**datadg**
- [Type]：**Dynamic (Cluster)**
- [Number of Disks]：ソフトウェア RAID を使用する場合、ミラーリングに 2 台以上のディスクを含めてください。そうでない場合は、単一の論理ディスク（ハードウェア RAID を使用する）で十分です。このディスク グループに使用されるディスクは、クラスタ内のすべてのノードからアクセスできる必要があります。

（注）　ソフトウェア RAID 5 を使用することはお勧めしません。

ステップ 2　次の特性を持つ **datadg** ディスク グループ内にボリュームを作成します。

- [Volume Name]：**cscopx**
- [Assigned Drive Letter]：**<選択したドライブ文字>**

（注）　使用可能な任意のドライブ文字を選択できますが、ドライブ文字はすべてのシステムで同じにする必要があります。

- [File Type]：**NTFS**

プライマリ サーバ（レプリケーションあり）

この項の手順を実行して、2 つのクラスタ間でレプリケーションを実行している場合のデュアル地域クラスタ コンフィギュレーションでのプライマリ サーバ上の Security Manager に必要なディスク グループとボリュームを設定します。プライマリ クラスタとセカンダリ クラスタの両方でプライマリ サーバ上で、次の手順を実行します。単一ノードのクラスタまたは共有ストレージを使用する複数ノードのクラスタのいずれかを使用できますが、このマニュアルではデュアル地域クラスタ内の複数ノードのクラスタの場合については説明しません。

ディスク グループと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。

- [Group Name] : **datadg**
- [Type] : **Dynamic (Cluster)**（VCS を使用する場合）、**Dynamic (Secondary)**（VCS を使用しない場合）
- [Number of Disks] : ソフトウェア RAID を使用する場合、ミラーリングに 2 台以上のディスクを含めてください。そうでない場合は、単一の論理ディスク（ハードウェア RAID を使用する）で十分です。マルチノード クラスタの場合、このディスク グループに使用されるディスクは、クラスタ内のすべてのノードからアクセスできる必要があります。

（注）　ソフトウェア RAID 5 を使用することはお勧めしません。

ステップ 2　次の特性を持つ **datadg** ディスク グループ内にボリュームを作成します。

- [Volume Name] : **cscopx**
- [Assigned Drive Letter] : **<選択したドライブ文字>**（プライマリ クラスタの場合）、**None**（セカンダリ クラスタの場合）
- [File Type] : **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）
- [Volume Logging] : **None**

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

- [Volume Name] : **data_srl**
- [Assigned Drive Letter] : **None**
- [File Type] : **Unformatted**
- [Volume Logging] : **None**

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

セカンダリ クラスタ内のセカンダリ サーバとプライマリ サーバ

この項の手順を実行して、セカンダリ クラスタ内のセカンダリ サーバおよびプライマリ サーバへの Security Manager のインストールに必要なディスク グループとボリュームを設定します。セカンダリ クラスタ内のプライマリ サーバと同様に、すべてのセカンダリ 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た後にマウント解除され、サーバから Security Manager をアンインストールするか、Security Manager をアップグレードするときまで使用されません。プライマリ クラスタ内のプライマリ サーバに使用されるのと同じドライブ文字で一時的な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 グループと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ない場合、次の特性を持つディスク グループを作成します。

- [Group Name]：**datadg_spare**
- [Type]：**Dynamic (Secondary)**
- [Size]：**5GB**（ボリュームに必要な容量は、Security Manager をインストールするために必要な容量のみ）
- [Number of Disks]：このディスク グループはアプリケーション データの保存には使用されないため、単一の冗長でないディスクで十分です。

ステップ 2　次の特性を持つディスク グループ内にボリュームを作成します。

- [Volume Name]：**cscopx_spare**
- [Assigned Drive Letter]：**<選択したドライブ文字>**

（注）　プライマリ サーバの cscopx ドライブに使用されるのと同じドライブ文字を使用する**必要があります**。

- [File Type]：**NTFS**

Security Manager のインストール

Security Manager のインストーラでは Storage Foundation がインストールされているかどうかが確認され、HA/DR コンフィギュレーションで Security Manager をインストールするかどうかが質問されます。このオプションを選択する場合、通常のインストール時に指定する情報以外に必要とされるのは、データベースのパスワードだけです。HA/DR 以外のインストールでは、データベースのパスワードが自動的に生成されます。ただし、データベースのパスワードは HA/DR コンフィギュレーションのすべてのサーバで同じにする必要があるため、インストーラでパスワードを指定するように求められます。HA/DR コンフィギュレーション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 のインストール時に VCS 用の 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 を制御および監視できます。

また、代わりに Veritas クラスタ サーバが HA/DR コンフィギュレーションの各サーバで Security Manager の起動と終了を制御するため、HA/DR のインストール時に Security Manager および Windows の関連サービスの Startup Type が [Automatic] ではなく [Manual] に設定されます。そうでない場合、Security Manager が一度に 1 台のサーバのみで稼動する必要がある場合に、いずれかのサーバの起動後に、HA/DR 内のすべてのサーバで Security Manager アプリケーションが起動を試行します。

HA/DR コンフィギュレーションの各サーバに、Security Manager をインストールする必要があります。ただし、HA/DR コンフィギュレーションでは Security Manager のプライマリ インスタンスのみが使用され、保護されます。コンフィギュレーション内のいずれかのセカンダリ サーバでプライマリ インスタンスを実行できるようにするには、その他のインストールを実行します。

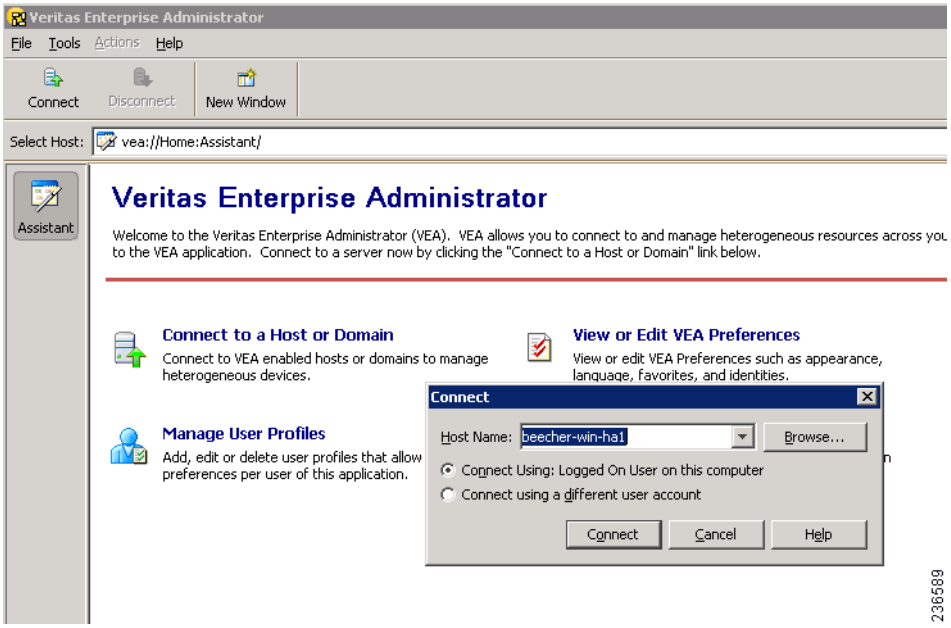
ここでは、次の内容について説明します。

プライマリ サーバへの Security Manager のインストール

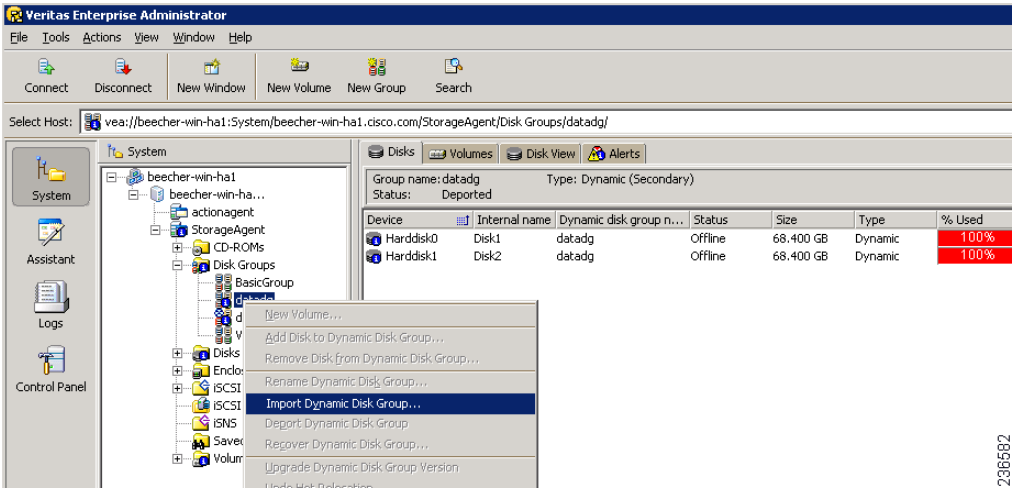
この項の手順を実行して、実動環境で使用され、HA/DR コンフィギュレーションによって保護される Security Manager のプライマリ インスタンスをインストールします。

プライマリ サーバに 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。



ステップ 2　[datadg] ディスク グループを右クリックし、[Import Dynamic Disk Group] を選択します。



ステップ 3　[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] をクリックします。

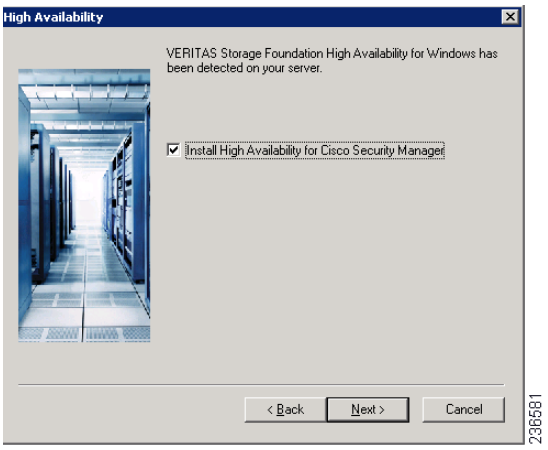
ステップ 4　[System] の下の **Volumes** フォルダを展開します。

ステップ 5　[cscopx] ボリュームを右クリックし、[File System] > [Change Drive Letter and Path] を選択します。

ステップ 6　**cscopx** ボリュームに目的のドライブ文字を割り当て、[OK] をクリックします。ドライブの割り当てについては、「ローカル冗長性コンフィギュレーションのワークシート」（P.2-5）または「地理的冗長性（DR）コンフィギュレーションのワークシート」（P.2-6）を参照してください。

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

a. HA 用の Security Manager をインストールするかどうかを質問されたら、チェックボックスをオンにして、インストールすることを選択します。



b. インストール ディレクトリを選択するように求められたら、*<選択したドライブ文字>:¥Program Files¥CSCOpx* を指定します。

c. データベースのパスワードを指定するように求められたら、適切なパスワードを選択し、それを記憶しておきます。HA/DR コンフィギュレーションのすべての Security Manager サーバにこのパスワードを使用します。

（注）　Security Manager インストールの完了間近で、マルチホーム サーバを使用していて、gatekeeper.cfg ファイルを更新する必要があるというメッセージが表示される場合があります。HA/DR コンフィギュレーションで使用されるエージェント スクリプトでこのファイルが変更されるため、このメッセージは無視してかまいません。

ステップ 8　Security Manager のインストールが完了したら、サーバを再起動します。

ステップ 9　システムの再起動後、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 [Offline] 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、終了、またはフェールオーバー」（P.4-3）を参照してください。

（注）　Security Manager が正常に動作するために必要な Windows レジストリ エントリの設定を完了するには、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 分待ち、URL : **http://<サーバのホスト名または 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。

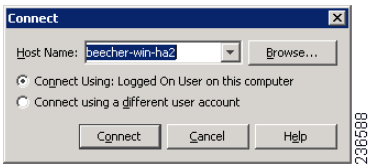
ステップ 12　アプリケーションの Web インターフェイスからログアウトし、offline.pl スクリプトを使用して Security Manager を終了します。詳細については、「Security Manager の手動での起動、終了、またはフェールオーバー」（P.4-3）を参照してください。

セカンダリ サーバへの Security Manager のインストール

この項の手順を実行して、セカンダリ サーバに Security Manager をインストールします。セカンダリ サーバへの Security Manager のインストールはプライマリ サーバへのインストールと同様ですが、1 つ重要な違いがあります。特定のセカンダリ サーバに関連付けられたスペア ボリューム（**cscopx_spare**）に Security Manager をインストールします。これは 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だけ使用されます。このスペア ボリュームには Security Manager アプリケーションおよび空のデータベースを保存できるだけの容量（最大 2 GB）が必要です。十分な領域を使用できる場合にだけ **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。可能な場合は、別のディスク グループに作成してください。

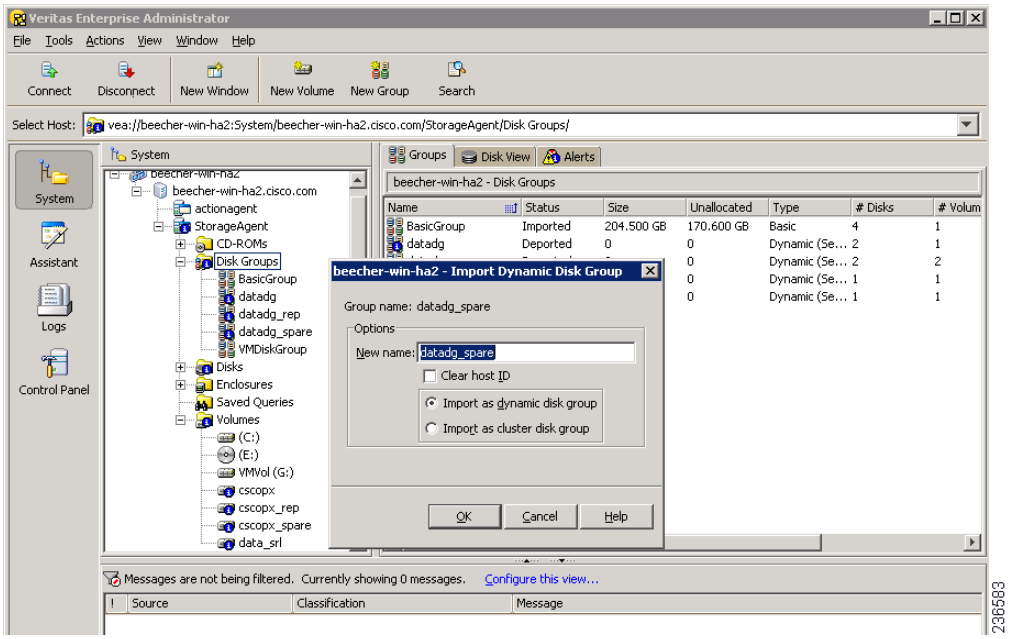
セカンダリ サーバに Security Manager をインストールするには、次の手順に従います。

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。



ステップ 2　[datadg_spare] を右クリックし、[Import Dynamic Disk Group] を選択します。

ステップ 3　[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] をクリックします。



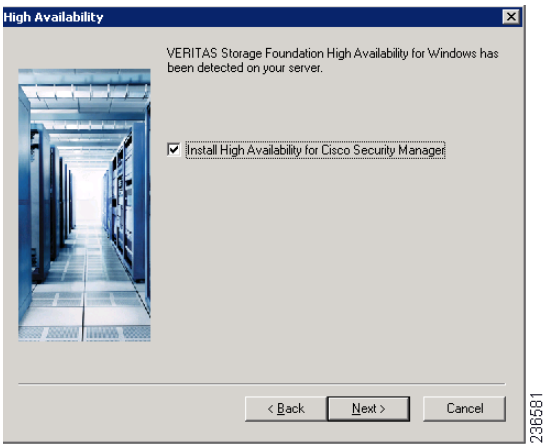
ステップ 4　[System] の下の **Volumes** フォルダを展開します。

ステップ 5　[cscopx_spare] ボリュームを右クリックし、[File System] > [Change Drive Letter and Path] を選択します。

ステップ 6　**cscopx_spare** ボリュームに目的のドライブ文字を割り当て、[OK] をクリックします。ドライブの割り当てについては、「ローカル冗長性コンフィギュレーションのワークシート」（P.2-5）または「地理的冗長性（DR）コンフィギュレーションのワークシート」（P.2-6）を参照してください。

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

a.　HA 用の Security Manager をインストールするかどうかを質問されたら、チェックボックスをオンにして、インストールすることを選択します。



b. インストール ディレクトリを選択するように求められたら、*<選択したドライブ文字>:¥Program Files¥CSCOpx* を指定します。

c. データベースのパスワードを指定するように求められたら、プライマリ サーバに選択したものと同じパスワードを選択します。

（注） Security Manager インストールの完了間近で、マルチホーム サーバを使用していて、gatekeeper.cfg ファイルを更新する必要があるというメッセージが表示される場合があります。HA/DR コンフィギュレーションで使用されるオンライン スクリプトでこのファイルが変更されるため、このメッセージは無視してかまいません。

ステップ 8　Security Manager のインストールが完了したら、サーバを再起動します。

ステップ 9　システムの再起動後、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 [Offline] 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、終了、またはフェールオーバー」（P.4-3）を参照してください。

（注） Security Manager が正常に動作するために必要な Windows レジストリ エントリの設定を完了するには、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 分待ち、URL : **http://<サーバのホスト名または 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 を終了します。詳細については、「Security Manager の手動での起動、終了、またはフェールオーバー」（P.4-3）を参照してください。

ステップ 13　インストールが完了したら、スペア ボリュームからドライブ文字の割り当てを解除します。

Veritas Volume Replicator のタスク

この項の手順を実行して、クラスタ間でレプリケーションが実行される場合のデュアル地域クラスタ コンフィギュレーションにレプリケーションを設定します。

レプリケーションを設定するには、次の作業を行います。

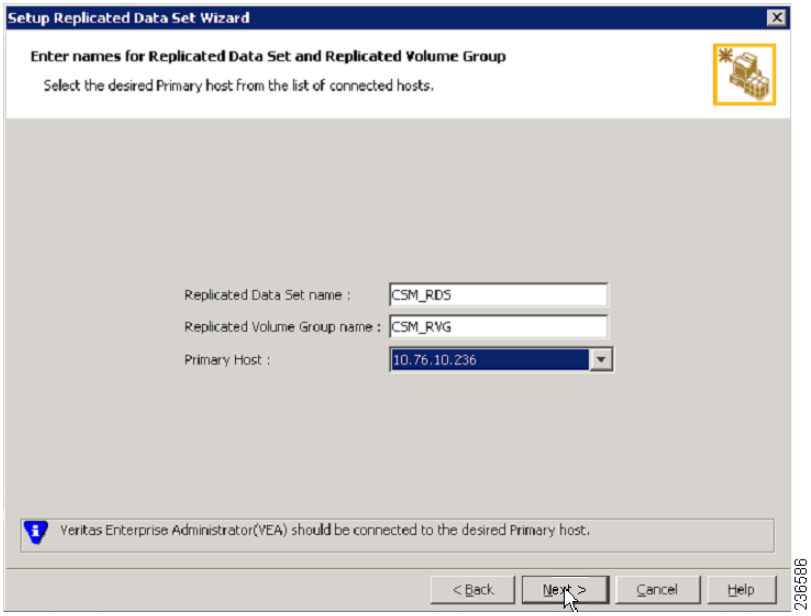
ステップ 1　VEA GUI を使用して、プライマリ ホストおよびセカンダリ ホストに接続します。

ステップ 2　*datadg* ディスク グループがプライマリ サーバとセカンダリ サーバ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　[View] > [Connection] > [Replication Network] を選択します。

ステップ 4　ツリーから [Replication Network] を選択し、ツールバーから [Setup Replicated Data Set] ウィザードを選択して、ウィザードの最初のパネルで次の内容を指定します。

- [Replicated Data Set Name] : **CSM_RDS**
- [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　[Next] をクリックし、ウィザードの [Select Dynamic Disk Group and volumes to be replicated] パネルで、次の内容を指定します。

- [Dynamic Disk Group] : **datadg**
- [Volumes] : **cscopx**

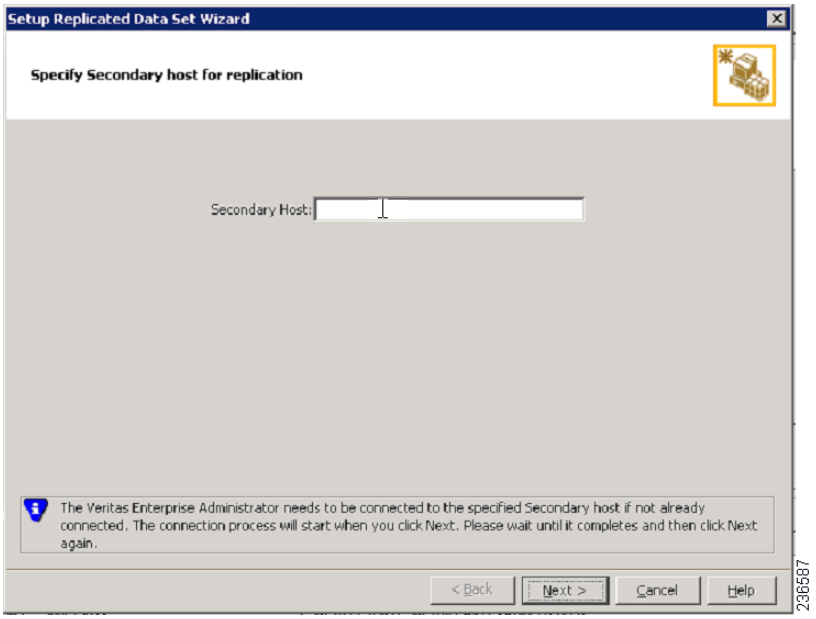
ステップ 6　[Next] をクリックします。他に使用できるボリュームが data_srl だけの場合、Replicator Log のストレージ ボリュームとして自動的に選択されます。複数の追加ボリュームを使用できる場合、[Storage Replicator Log] パネルが表示されます。次の内容を指定します。

- [Volume for the Replicator Log] : **data_srl**

ステップ 7　[Next] をクリックし、概要情報を確認して、[Create Primary RVG] をクリックして RVG を作成します。

ステップ 8　プライマリ RVG が正常に作成された後、RDS にセカンダリ ホストを追加するかどうか尋ねられたら [Yes] をクリックします。

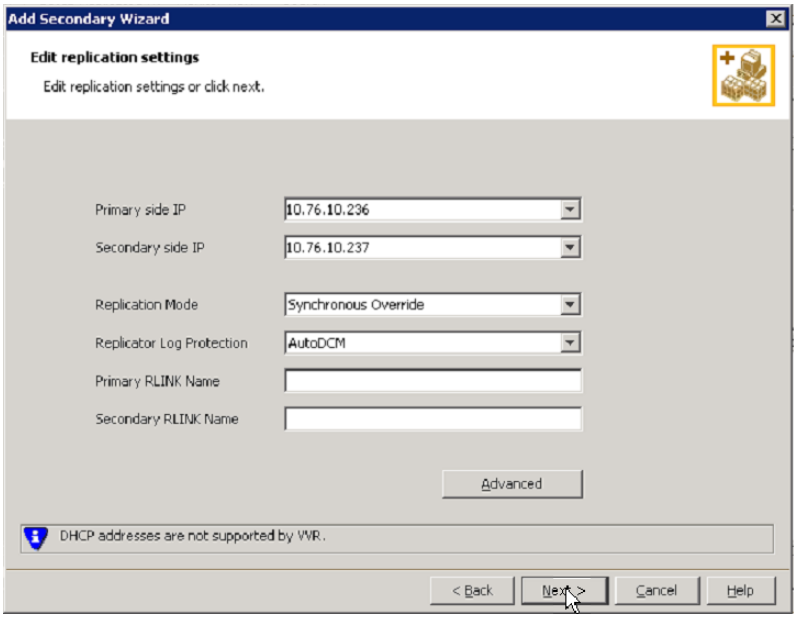
ステップ 9　[Specify Secondary host for replication] パネルで、[Secondary Host] フィールドにセカンダリ ホストの名前または IP アドレスを入力します。



ステップ 10　[Next] をクリックし、[edit replication settings] パネルで、次の内容を指定します。

（注）　プライマリ側とセカンダリ側の IP アドレスについて、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、後でこのパネルに戻って、VCS の制御下で仮想 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 からこれを実行するには、ツリーでセカンダリ RVG を選択し、[Actions] > [Change Replication Settings] を選択します。

- [Primary side IP] : <プライマリ サーバの IP アドレス>
- [Secondary side IP] : <セカンダリ サーバの IP アドレス>
- [Replication Mode] : **Synchronous Override**
- [Replicator Log Protection] : <[Off]、[Fail]、[DCM]、[AutoDCM]（デフォルト）、[Override] から選択>。各選択肢の説明については、『Volume Replicator administrator's guide』を参照してください。



ステップ 11　[Next] をクリックして、デフォルトの設定でレプリケーションを開始します。[Synchronize Automatically] を選択し、[Start Replication] がオンになっていることを確認します。

ステップ 12　[Next] をクリックして [Summary] ページを表示し、[Finish] をクリックします。

動作している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（casuser）とグループ（casusers）が作成されます。セカンダリ サーバで Security Manager の保護されている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 グループの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」（P.3-14）
- 「レプリケーションを使用する場合の権限の更新」（P.3-15）

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 グループの権限を追加するには、次の作業を行います。

ステップ 1　プライマリ サーバで実行している場合は、offline.pl スクリプトを使用して Security Manager を終了します。詳細については、「Security Manager の手動での起動、終了、またはフェールオーバー」（P.4-3）を参照してください。

ステップ 2　プライマリ 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 3　セカンダリ 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 4　VEA GUI またはコマンド ラインを使用して、プライマリ ボリューム（cscopx）を選択したドライブ文字に割り当てます。

ステップ 5　Windows Explorer から、**<選択したドライブ文字>:¥Program Files¥CSCOpx** フォルダを右クリックし、[Sharing and Security] メニュー項目を選択します。

ステップ 6　このフォルダのプロパティのダイアログボックスが表示されます。[Security] タブを選択し、[Add] をクリックします。

ステップ 7　[Select Users or Groups] ダイアログ ボックスで、[Location] をクリックし、選択ツリーからローカル サーバを選択します。

ステップ 8　[enter object names] ボックスで **casusers** と入力し、[Check Names] をクリックします。このテキストボックスに [<サーバ名>¥casusers] と表示されるはずです。[OK] をクリックします。

ステップ 9　[casusers] が選択されていることを確認し、[Allow] の下の [Full Control] チェックボックスをオンにして、casusers グループに full control 権限を付与します。

ステップ 10　[Advanced] をクリックします。

ステップ 11　[Advanced Settings] で、[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　[Apply] をクリックし、CSCOpx ディレクトリの下のすべての子オブジェクトに権限が伝播されるのを待ちます。

ステップ 13　伝播が完了したら、[OK] をクリックします。

ステップ 14　[OK] をクリックし、[CSCOpx Properties] ダイアログボックスを閉じます。

ステップ 15　cscopx ボリュームから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、プライマリ ボリューム（cscopx）を選択したドライブ文字に割り当てます。

レプリケーションを使用する場合の権限の更新

レプリケーション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 グループの権限を追加するには、次の作業を行います。

ステップ 1　プライマリ サーバで実行している場合は、offline.pl スクリプトを使用して Security Manager を終了します。詳細については、「Security Manager の手動での起動、終了、またはフェールオーバー」（P.4-3）を参照してください。

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

ステップ 3　レプリケーション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 から、**<選択したドライブ文字>:¥Program Files¥CSCOpx** フォルダを右クリックし、[Sharing and Security] メニュー項目を選択します。

ステップ 6　このフォルダのプロパティのダイアログボックスが表示されます。[Security] タブを選択し、[Add] をクリックします。

ステップ 7　[Select Users or Groups] ダイアログ ボックスで、[Location] をクリックし、選択ツリーからローカル サーバを選択します。

ステップ 8　[enter object names] ボックスで **casusers** と入力し、[Check Names] をクリックします。このテキスト ボックスに [<サーバ名>¥casusers] と表示されるはずです。[OK] をクリックします。

ステップ 9　[casusers] が選択されていることを確認し、[Allow] の下の [Full Control] チェックボックスをオンにして、casusers グループに full control 権限を付与します。

ステップ 10　[Advanced] をクリックします。

ステップ 11　[Advanced Settings] で、[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　[Apply] をクリックし、CSCOpx ディレクトリの下のすべての子オブジェクトに権限が伝播されるのを待ちます。

ステップ 13　伝播が完了したら、[OK] をクリックします。

（注）　権限の更新中に、「Error Applying Security」というタイトルのエラー ダイアログに次のメッセージが表示される場合があります。「An error occurred applying security information to: *<選択したドライブ文字>*:¥Program Files¥CSCOpx¥log¥dcr.log.Access is denied.」。このメッセージは無視しても問題ありません。エラー ダイアログで [Continue] をクリックして、権限の更新プロセスを完了します。

ステップ 14　[OK] をクリックし、[CSCOpx Properties] ダイアログボックスを閉じます。

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

ステップ 16　レプリケーションをプライマリ サーバに再び移行します。

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 のタスク

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。次の 2 つのシナリオについて説明します。

「単一のローカル クラスタ（デュアルノード）コンフィギュレーション」（P.3-16）
「デュアル地域クラスタ コンフィギュレーション」（P.3-25）

単一のローカル クラスタ（デュアルノード）コンフィギュレーション

ここでは、クラスタ内に 2 つのノード（プライマリとセカンダリ）がある単一のローカル 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」（P.3-17）
- 「アプリケーション サービス グループの作成」（P.3-17）
- 「ClusterService グループの作成（オプション）」（P.3-24）

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 Cluster Configuration ウィザードを使用して、次のように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。この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 を指定することです。VCS では、クラスタのメンテナンスのためにクラスタ間の通信にプライベート ネットワークを使用します。また、すべての専用クラスタ通信インターフェイスで障害が発生した場合、優先度の低いクラスタ通信インターフェイスとして動作する 1 つのネットワーク イーサネット インターフェイス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、[Start] > [All Programs] > [Symantec] > [Veritas Cluster Server] > [Veritas Cluster Manager - Java Console] を選択して、クラスタにログインします。

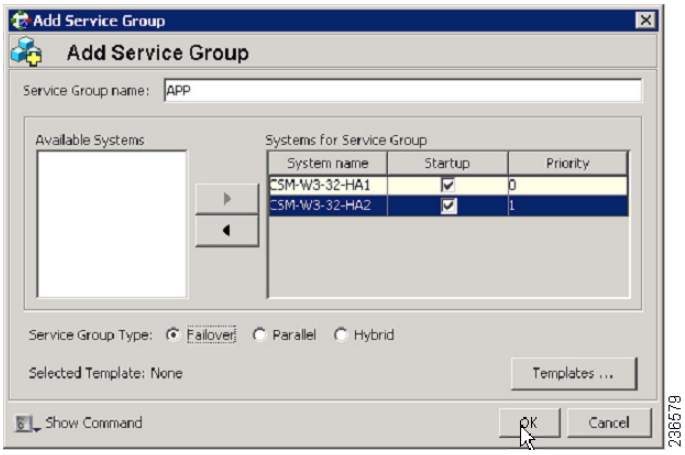
ステップ 3　Cluster Manager を使用して、[File] > [Import Types] を選択し、[CSManager] リソース タイプをインポートします。$VCS_ROOT¥cluster server¥conf¥config に配置されている CSManagerTypes.cf ファイルを参照し、[Import] をクリックします。

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。

ステップ 1　[CSManager] リソースを右クリックし、[Add Service Group] を選択します。

APP という名前のサービス グループを追加し、[Startup] オプションがオンになっているこのサービス グループのサーバと、タイプが [Failover] の各サーバおよびサービス グループのサーバの両方を含めます。



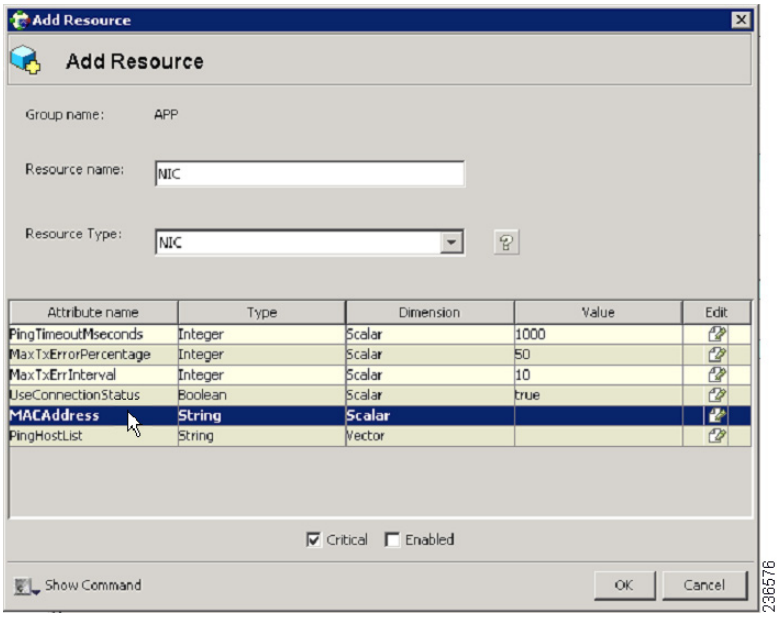
ステップ 2　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

NIC リソースを追加し、[Critical] チェックボックスと [Enabled] チェックボックスをオンにします。

- Resource name = **NIC**
- Resource Type = **NIC**

- MACAddress = <Security Manager アプリケーションにアクセスするために使用される NIC の MAC アドレス>。クラスタ内の各サーバに一意に定義されます。

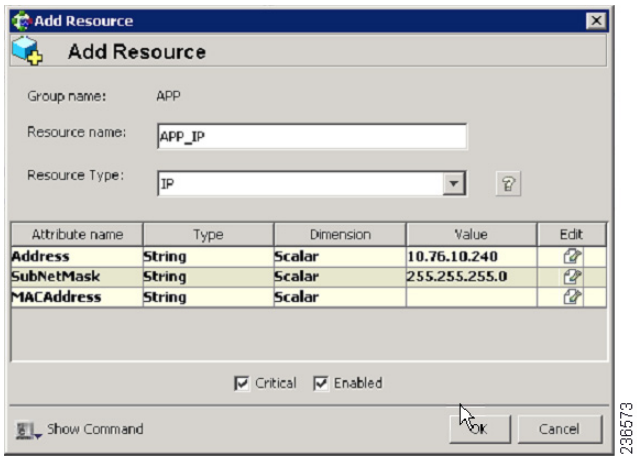
（注）　DOS レベルのコマンド **ipconfig -all** を使用して、各イーサネット インターフェイスに関連付けられた MAC アドレスを検索できます。



ステップ 3　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

IP リソースを追加し、[Critical] チェックボックスと [Enabled] チェックボックスをオンにします。

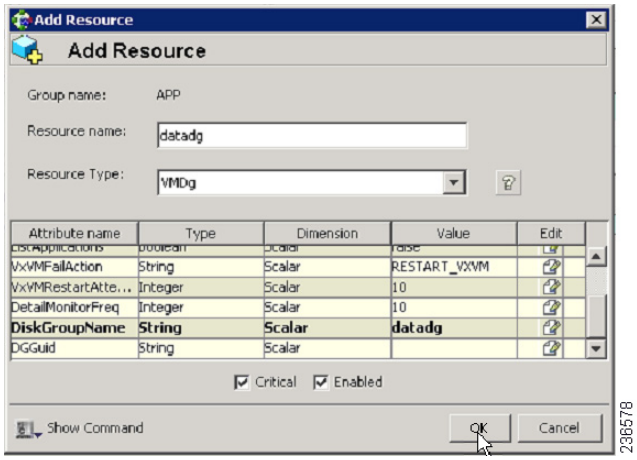
- Resource name = **APP_IP**
- Resource Type = **IP**
- Address = <Security Manager アプリケーションが使用するように割り当てられた仮想 IP アドレス>（グローバル属性として定義される）
- SubNetMask = <サブネット マスク>（グローバル属性として定義される）
- MACAddress = <Security Manager アプリケーションにアクセスするために使用される NIC の MAC アドレス>（クラスタ内の各サーバに対して定義される）。



ステップ 4　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

VMDg リソースを追加し、[Critical] チェックボックスと [Enabled] チェックボックスをオンにします。

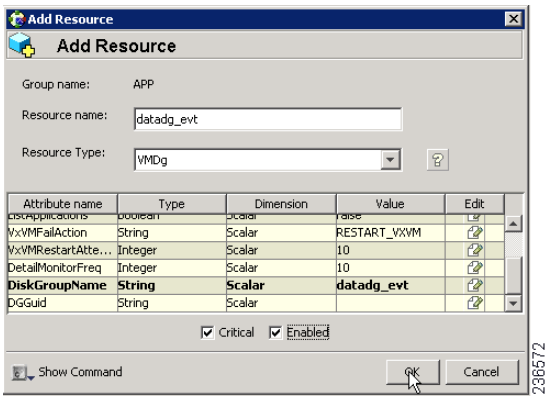
- Resource name = **datadg**
- Resource Type = **VMDg**
- DiskGroupName = **datadg**
  （グローバル属性として定義される）



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

datadg_evt リソースを追加し、[Critical] チェックボックスと [Enabled] チェックボックスをオンにします。

- Resource name = **datadg_evt**
- Resource Type = **VMDg**
- DiskGroupName = **datadg_evt**
  （グローバル属性として定義される）



ステップ 6　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

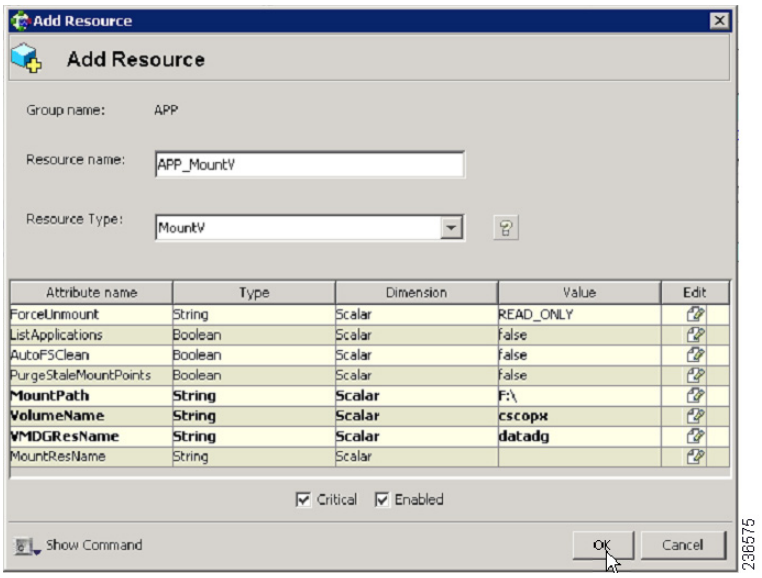
MountV リソースを追加し、[Critical] チェックボックスと [Enabled] チェックボックスをオンにします。

- Resource name = **APP_MountV**
- Resource Type = **MountV**
- MountPath = <選択したドライブ文字>:¥
  （グローバル属性として定義される）
- VolumeName = **cscopx**
  （グローバル属性として定義される）
- VMDGResName = **datadg**
  （グローバル属性として定義される）
- ForceUnmount = {NONE、READ-ONLY、ALL}

  他のアプリケーションで使用される場合、エージェントがドライブを強制的にアンマウントするかどうかを定義します。次の選択肢があります。

  - [NONE]：アプリケーションがアクセスしている場合、エージェントはボリュームをアンマウントしません。
  - [READ-ONLY]：アプリケーションが Read Only モードでアクセスしている場合、エージェントはボリュームをアンマウントします。
  - [ALL]：アプリケーションのアクセスの種類に関係なく、エージェントはボリュームをアンマウントします。

  デフォルトは [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阻止される可能性があるため、[READ-ONLY] または [ALL] の値を選択することがあります。



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

MountV_evt リソースを追加し、[Critical] チェックボックスと [Enabled] チェックボックスをオンにします。

- Resource name = **APP_MountV_evt**
- Resource Type = **MountV**
- MountPath = <選択したドライブ文字>:¥
  （グローバル属性として定義される）
- VolumeName = **cscopx_evt**
  (グローバル属性として定義される)
- VMDGResName = **datadg_evt**
  （グローバル属性として定義される）
- ForceUnmount = {NONE、READ-ONLY、ALL}

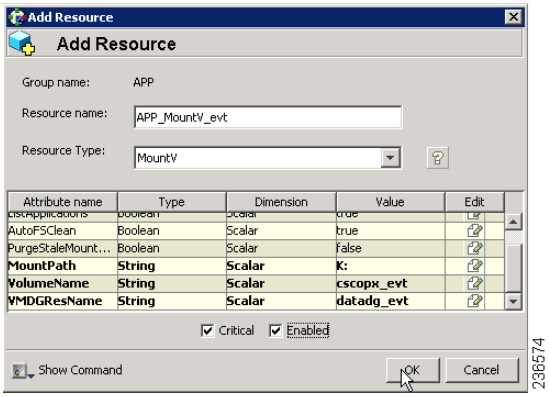
  他のアプリケーションで使用される場合、エージェントがドライブを強制的にアンマウントするかどうかを定義します。次の選択肢があります。

  – [NONE] : アプリケーションがアクセスしている場合、エージェントはボリュームをアンマウントしません。

  – [READ-ONLY] : アプリケーションが Read Only モードでアクセスしている場合、エージェントはボリュームをアンマウントします。

  – [ALL] : アプリケーションのアクセスの種類に関係なく、エージェントはボリュームをアンマウントします。

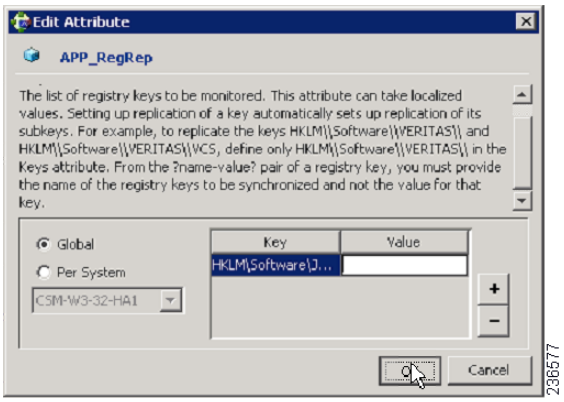
  デフォルトは [NONE] です。ボリュームをアンマウントできない場合、セカンダリ サーバへの自動フェールオーバーが阻止される可能性があるため、[READ-ONLY] または [ALL] の値を選択することがあります。



ステップ 8　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

RegRep リソースを追加し、[Critical] チェックボックスと [Enabled] チェックボックスをオンにします。

- Resource name = **APP_RegRep**
- Resource Type = **RegRep**
- MountResName = **APP_MountV**
  （グローバル属性として定義される）
- ReplicationDirectory = **¥REGREP¥DEFAULT**
  （グローバル属性として定義される）
- キー（グローバル属性として定義される）
  Key = **HKLM¥Software¥JavaSoft¥Prefs¥vms**
  Value = <空白>

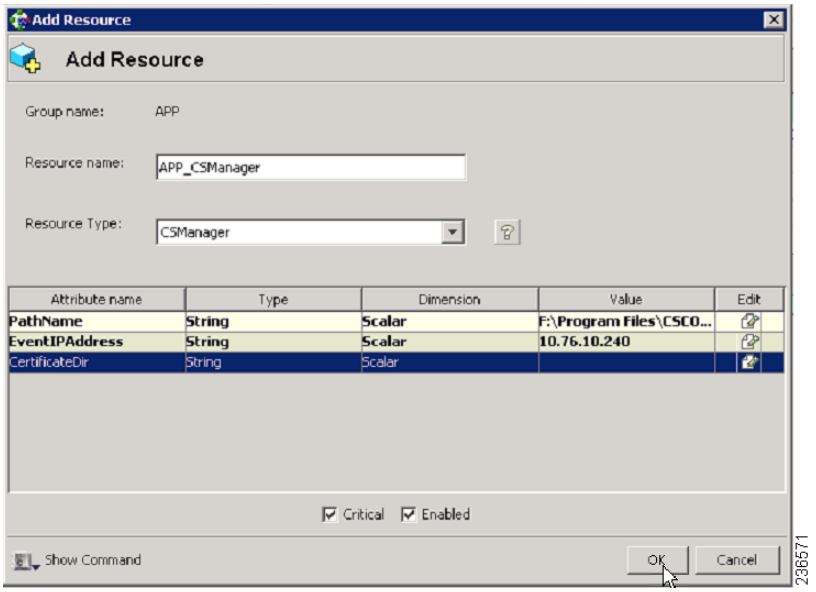


（注）　Security Manager は HKEY_LOCAL_MACHINE¥SOFTWARE¥JavaSoft¥Prefs¥vms の下のサーバ レジストリにクライアント ユーザ プリファレンスを保存します。レジストリ レプリケーション エージェント（RegRep）は、アクティブ サーバ上の指定されたレジストリの場所への変更を監視し、フェールオーバーの発生時にセカンダリ サーバにこれらの変更を同期化します。

ステップ 9　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

CSManager リソースを追加し、[Critical] チェックボックスと [Enabled] チェックボックスをオンにします。

- Resource name = **APP_CSManager**
- Resource Type = **CSManager**
- PathName = **<選択したドライブ文字>:¥Program Files¥CSCOpx¥**
  （グローバル属性として定義される）
- EventIPAddress = APP_IP で使用されるのと同じ IP アドレス
  （グローバル属性として定義される）
- 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」（P.4-2）を参照してください。

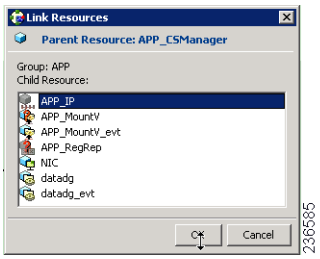


ステップ 10　次の表に定義されているように、リソースをリンクします（図 A-1（P.A-2）を参照）。

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、次の作業を行います。

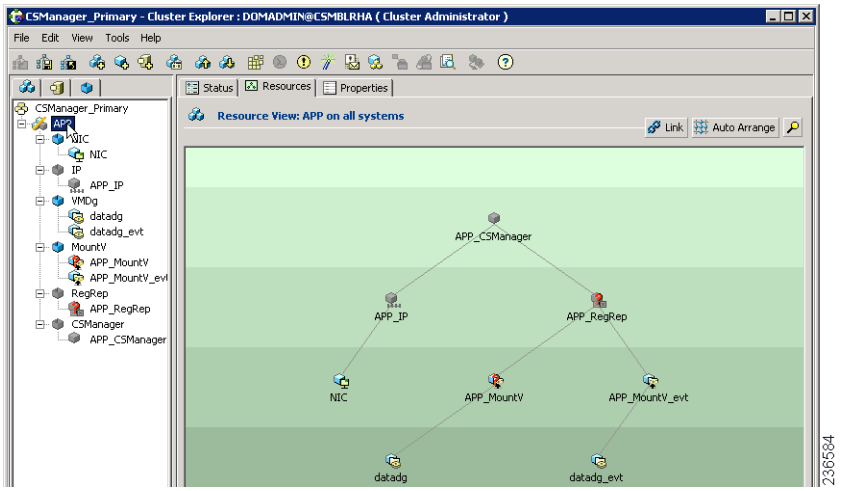
a.　親リソースを右クリックし、[Link] を選択します。
[Link Resources] ダイアログボックスが表示されます。



b. 子リソースを選択し、[OK] 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、次のようなリソース ビューが表示されます。



ClusterService グループの作成（オプション）

オプションで ClusterService グループを作成して、次のオプション コンポーネントを実行できます。

- Cluster Manager（Web コンソール）
- 通知

VCS Configuration ウィザードを使用して、これらのコンポーネットを設定できます。詳細については、『Veritas Cluster Server administrator's guide』を参照してください。電子メールまたは SNMP トラップによって、クラスタ内で発生したイベントを通知できるため、通知サービスは有益です。

デュアル地域クラスタ コンフィギュレーション

ここでは、各クラスタに単一のノードがある地理的に離れた 2 つの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。

（注）　また、1 つのクラスタまたは両方のクラスタに複数のノードがあるデュアル地域クラスタ コンフィギュレーション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 クラスタとセカンダリ 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、次の手順に従います。

ステップ 1　VCS Cluster Configuration 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、次のクラスタを作成します。

- Cluster Name = CSManager_Primary
- Cluster ID = 0

ステップ 2　VCS Configuration 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、次の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、[Start] > [All Programs] > [Symantec] > [Veritas Cluster Server] > [Veritas Cluster Manager - Java Console] を選択して、クラスタにログインし、Cluster Manager を起動します。

ステップ 4　Cluster Manager を使用して、[File] > [Import Types] を選択し、[CSManager] リソース タイプをインポートします。$VCS_ROOT¥cluster server¥conf¥config に配置されている CSManagerTypes.cf ファイルを参照し、[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 および 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 クラスタの両方でこれらの手順を実行します。

ヒント　ここで説明しているクラスタ間通信のための ClusterService グループと wac リソースの作成手順の代わりに、VCS Configuration ウィザードを使用できます。また、オプションで VCS Configuration ウィザードを使用して、Cluster Manager（Web コンソール）および通知コンポーネントを設定することもできます。詳細については、『Veritas Cluster Server administrator's guide』を参照してください。

ステップ 1　[CSManager] リソースを右クリックし、[Add Service Group] を選択します。

ClusterService という名前のサービス グループを追加します。

ステップ 2　[ClusterService] サービス グループを右クリックし、[Add Resource] を選択します。

NIC リソースを追加します。

- Resource name = **NIC**
- Resource Type = **NIC**
- 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] サービス グループを右クリックし、[Add Resource] を選択します。

IP リソースを追加します。

- Resource name = **VCS_IP**
- Resource Type = **IP**
- Address = <クラスタに割り当てられた仮想 IP アドレス>
- SubNetMask = <サブネット マスク>
- MACAddress = <対応する NIC カードの MAC アドレス>

ステップ 4　[ClusterService] サービス グループを右クリックし、[Add Resource] を選択します。

wac リソースを追加します。

- Resource name = **wac**
- Resource Type = **Process**
- StartProgram = **C:¥Program Files¥Veritas¥Cluster Server¥bin¥wac.exe**
- StopProgram = **C:¥Program Files¥Veritas¥Cluster Server¥bin¥wacstop.exe**
- MonitorProgram = **C:¥Program Files¥Veritas¥Cluster Server¥bin¥wacmonitor.exe**

ステップ 5　次の表に定義されているように、リソースをリンクします（図 A-4（P.A-4）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、次の作業を行います。

a. 親リソースを右クリックし、[Link] を選択します。
[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] をクリックします。
選択したリソースがリンクされます。

レプリケーション サービス グループの作成

レプリケーション 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 クラスタの両方でこれらの手順を実行します。

ステップ 1　[CSManager] リソースを右クリックし、[Add Service Group] を選択します。
APPrep という名前のサービス グループを追加します。

ステップ 2　[APPrep] サービス グループを右クリックし、[Add Resource] を選択します。
Proxy リソースを追加します。

- Resource name = **VVR_NIC_Proxy**
- Resource Type = **Proxy**
- TargetResName = **NIC**

ステップ 3　[APPrep] サービス グループを右クリックし、[Add Resource] を選択します。
IP リソースを追加します。

- Resource name = **VVR_IP**
- Resource Type = **IP**
- Address = <レプリケーションに割り当てられた仮想 IP アドレス>
- SubNetMask = <サブネット マスク>
- MACAddress = <対応する NIC カードの MAC アドレス>

ステップ 4　[APPrep] サービス グループを右クリックし、[Add Resource] を選択します。
VMDg リソースを追加します。

- Resource name = **datadg**
- Resource Type = **VMDg**
- DiskGroupName = **datadg**

ステップ 5　[APPrep] サービス グループを右クリックし、[Add Resource] を選択します。

VvrRvg リソースを追加します。

- Resource name = **APP_RVG**
- Resource Type = **VvrRvg**
- RVG = **CSM_RVG**
- VMDGResName = **datadg**
- IPResName = **VVR_IP**

ステップ 6　次の表に定義されているように、リソースをリンクします（図 A-3（P.A-3）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、次の作業を行います。

a. 親リソースを右クリックし、[Link] を選択します。
[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] 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。

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

ステップ 1　APP という名前のサービス グループを追加します。

ステップ 2　[APP] サービス グループを右クリックし、[Add Resource] を選択します。
RVG プライマリ リソースを追加します。

- Resource name = **APP_RVGPrimary**
- Resource Type = **RVGPrimary**
- RvgResourceName = **APP_RVG**

ステップ 3　[APP] サービス グループを右クリックし、[Add Resource] を選択します。
MountV リソースを追加します。

- Resource name = **APP_MountV**
- Resource Type = **MountV**
- Mount Path = <選択したドライブ文字>:¥
- Volume Name = **cscopx**
- VMDg Resource Name = **datadg**

ステップ 4　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

RegRep リソースを追加し、[Critical] チェックボックスと [Enabled] チェックボックスをオンにします。

- Resource name = **APP_RegRep**
- MountResName = **APP_MountV**
- ReplicationDirectory = **¥REGREP¥DEFAULT**
- Keys = **HKLM¥Software¥JavaSoft¥Prefs¥vms**

（注） Security Manager は HKEY_LOCAL_MACHINE¥SOFTWARE¥JavaSoft¥Prefs¥vms の下のサーバ レジストリにクライアント ユーザ プリファレンスを保存します。レジストリ レプリケーション エージェント（RegRep）は、アクティブ サーバ上の指定されたレジストリの場所への変更を監視し、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] サービス グループを右クリックし、[Add Resource] を選択します。

Proxy リソースを追加します。

- Resource name = **APP_NIC_Proxy**
- Resource Type = **Proxy**
- TargetResName = **NIC**

ステップ 6　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

IP リソースを追加します。

- Resource name = **APP_IP**
- Resource Type = **IP**
- Address = <アプリケーションに割り当てられた仮想 IP アドレス>
- SubNetMask = <サブネット マスク>
- MACAddress = <対応する NIC カードの MAC アドレス>

ステップ 7　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

CSManager リソースを追加します。

- Resource name = **APP_CSManager**
- Resource Type = **CSManager**
- PathName = <***選択したドライブ文字***>**:¥Program Files¥CSCOpx**
- EventIPAddress = APP_IP で使用するのと同じ IP アドレス
- 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」（P.4-2）を参照してください。

ステップ 8　次の表に定義されているように、リソースをリンクします（図 A-2（P.A-3）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

親リソース	子リソース
APP_IP	APP_NIC_Proxy
APP_CSManager	APP_IP

リソースをリンクするには、次の作業を行います。

a. 親リソースを右クリックし、[Link] を選択します。

[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] をクリックします。

選択したリソースがリンクされます。

クラスタ レベル コンフィギュレーションの作成

クラスタ レベル コンフィギュレーションを作成するには、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の APP サービス グループをオンライン ローカル ファームの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 プロパティの下でクラスタ アドレスを指定します。このアドレスは VCS_IP リソースに使用したのと同じ IP アドレスです。

ステップ 3　プライマリ クラスタから、[Edit] > [Add/Delete Remote Cluster] を選択して、Remote Cluster Configuration ウィザードを使用してセカンダリ 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、[Edit] > [Configure Global Groups] を選択して、Global Group Configuration ウィザードを使用して 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。

図 A-5（P.A-4）を参照してください。