

СНАРТЕК

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」(P.3-1)
- 「Microsoft Windows Server $\mathcal{O} \prec \mathcal{V} \land \mathcal{V} \land \mathcal{V} \land \mathcal{V}$ 」 (P.3-2)
- 「外部ストレージへのサーバの接続」(P.3-3)
- 「Symantec Veritas 製品のインストール」(P.3-3)
- 「起動ディスクのミラーリング (オプション)」(P.3-3)
- 「Veritas Volume Manager の設定タスク」(P.3-4)
- Security Manager $\mathcal{O} \prec \mathcal{V} \prec \mathcal{V} \rightarrow \mathcal{V} \downarrow$ (P.3-6)
- 「Veritas Volume Replicator のタスク」 (P.3-12)
- 「動作しているボリュームに対する権限の更新」(P.3-14)
- 「Veritas Cluster Server のタスク」 (P.3-16)

イーサネット接続の確立

Γ

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。



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。

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	—

表 3-1 Veritas のソフトウェア コンポーネント

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)

ſ

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)」(P.3-4)
- 「プライマリ サーバ (レプリケーションあり)」(P.3-5)
- 「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」(P.3-6)

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。



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。

1

• [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。



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)

ſ

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」(P.3-7)
- 「セカンダリ サーバへの Security Manager のインストール」(P.3-9)

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。

😢 Yeritas I	Interprise	Administrator				
<u>File T</u> ools	<u>A</u> ctions	<u>t</u> elp				
4	Br	<u> </u>				
Connect	Disconne	New Window				
Select Host:	💱 vea://	Home:Assistant/				
Assistant	Ver Welcom to the V	itas Enterp e to the Veritas Enterp EA application. Conne Connect to a Hos Connect to VEA enabl	orise Administrator (V orise Administrator (V oct to a server now b st or Domain ed hosts or domains i	to manage	o connect to and manage heteroge t to a Host or Domain" link below. View or Edit VEA Preferen View or edit VEA Preferences suc	eneous resources across you I CES h as appearance,
		heterogeneous device Manage User Pro Add, edit or delete us preferences per user	rs. files er profiles that allow of this application.	Connect Host Name: beech Connect Using: C Connect using a	er-win-ha1	Browse

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。

😤 Veritas I	Enterprise Adm	ninistrator								
<u>File T</u> ools	<u>A</u> ctions ⊻iew	<u>W</u> indow <u>H</u> elp								
B	3	<u> </u>	<u></u>	88	<u>_</u>					
Connect	Disconnect	New Window	New Volume	New Group S	iearch					
Select Host:	📷 vea://beed	ner-win-ha1:Syst	em/beecher-win-	ha1.cisco.com/Sto	rageAgent/Disk G	iroups/datadg/				
T.	ro System	I		Disks 📻	9 Volumes 🛛 🤤 🕻	Disk View 🛛 🙈 Alert	s			
비 태습	E 🔒 bee	cher-win-ha1		Group name:	datadg	Type: Dynamic (:	Secondary)			
System		beecher-win-ha		Status:	Deported	[]	[1-	[
	÷.	🚡 StorageAge	ent	Device Barddisk0	Dick1	ame Dynamic disk g datado	offline	5ize 68,400.GB	Type Dynamic	% Used
Assistant		E G CD-ROI	Ms	Harddisk1	Disk2	datadg	Offline	68,400 GB	Dynamic	100%
		E Bas	icGroup	_						
		- d - 4	ada			1				
Logs		- b ij d_	New Volume			_				
		E Salar	Add Disk to Dy	namic Disk Group, ,						
		Enclo:	Remove Disk fr	om Dynamic Disk G	roup	_				
Control Par	nel	🗄 Ğ iscsi	Rename Dynan	nic Dis <u>k</u> Group		_				
		iscsi 🛄	Import D <u>y</u> nami	c Disk Group						
		isns	Deport Dynami	c Disk Group						~
		Saver	Recover Dynam	nic Disk Group						282
			Upgrade Dynar	nic Disk Group Ver:	sion					39
			Linda Wat Dalay	skion						2

- 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。

High Availability	VERITAS Storage Foundation High Availability for Windows has been detected on your server.
	Imital High Availability for Cisco Security Manager
	<back next=""> Cancel</back>

- **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。



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

ſ

- 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 (scopx_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。

Reritas Ent	erprise Administrator tions View Window Help)								_ 🗆 X
Connect	Disconnect New Window	New Volume	New Group	Search						
Felect Host:	vea://beecher-win-ha2:5ys To System Deecher-win-haz Deecher-win-haz	tem/beecher-wir	n-ha2.cisco.com	n/StorageAgen roups 🛛 😅 Dis her-win-ha2 -	t/Disk Groups/ sk View 🏾 💑 Alert: Disk Groups	s		-		•
Assistant	Storagener S	Ant Ms oups icGroup tadg tadg_rep tadg_spare DiskGroup ures Queries s)) Vol (G;) - copx_rep copx_rep copx_rep copx_rep ta srl	Group name:	sicGroup tadg ha2 - Import datadg_spare datadg_spare Clear host C Import as C Import as	Imported Deported Dynamic Disk C ID ID dynamic disk group	204,500 GB 0 5roup X	0.2000 GB 0 0 0 0	Basic Dynamic (Se., Dynamic (Se., Dynamic (Se., Dynamic (Se.,	4 2 2 1 .1	1 1 2 1 1
	Messages are not being Source	filtered. Curren Classific	tly showing 0 m ation	essages. 🧕	onfigure this view. Message					

- 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。

High Availability	X
	VERITAS Storage Foundation High Availability for Windows has been detected on your server.
	Iratall High Availability for Cisco Security Manager
	< <u>Back</u> <u>N</u> ext> Cancel

- **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。

ſ

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。

Setup Replicated Data Set Wizard Enter names for Replicated Data Set and Replicated Volume Group Select the desired Primary host from the list of connected hosts.	×.
Replicated Data Set name : CSM_RDS Replicated Volume Group name : CSM_RVG Primary Host : 10.76.10.236	×
Yeritas Enterprise Administrator(VEA) should be connected to the desired	Primary host.
< Back	Next Cancel Help Grade

- **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。

Setup Replicated Data Set Wizard	X
Specify Secondary host for replication	
Secondary Host:	
The Veritas Enterprise Administrator needs to be connected to the specified Secondary host if not already connected. The connection process will start when you click Next. Please wait until it completes and then click Ne again	ext .
< Back Quert > Qancel He	236587

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)

Γ

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。

動作しているボリュームに対する権限の更新

Add Secondary Wizard Edit replication settings Edit replication settings or click next.				×
Primary side IP Secondary side IP	10.76.10.236	×.		
Replication Mode Replicator Log Protection Primary RLINK Name	Synchronous Override AutoDCM	x		
Secondary RLINK Name	Iby VVR.	Advanced		
		< Back Next >	Cancel	Telb 23658

- **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。

1

- **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。

Cisco Security Manager 4.0 ハイ アベイラビリティ インストレーション ガイド

- 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。

ſ

- **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)

Veritas Cluster Server のタスク

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。

rvice Group name:	APP			
wailable Systems		Systems for Service G	roup	
		System name	Startup	Priority
		C5M-W3-32-HA1	V	0
	P	CSM-W3-32-HA2		1
	•	1		

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。

	APP			
Resource name:	NIC			
Resource Type:	NIC	*	P	
Attribute name	Туре	Dimension	Value	Edit
ing Timeout Mseconds	Integer	Scalar	1000	
ing minoodal isocorias			50	100
laxTxErrorPercentage	Integer	Scalar	50	2
laxTxErrorPercentage laxTxErrInterval	Integer Integer	Scalar Scalar	10	
laxTxErrorPercentage laxTxErrInterval seConnectionStatus	Integer Integer Boolean	Scalar Scalar Scalar	10 true	
laxTxErrorPercentage laxTxErrInterval seConnectionStatus	Integer Integer Boolean String	Scalar Scalar Scalar <mark>Scalar</mark>	50 10 true	

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)。

Group name:	APP			
Resource name:	APP_IP			
Resource Type:	IP		▼	
Attribute name	Туре	Dimension	Value	Edit
Address	String	Scalar	10.76.10.240	2
SubNetMask	String	Scalar	255.255.255.0	2
MACAddress	String	Scalar		

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)

🕼 Add Resource					×
Add Re	esource				
Group name:	APP				
Resource name:	datadg				
Resource Type:	VMDg		•		
Attribute name	Type	Dimension	Value	Edit	_
ciscapplicacions	poolean	Juaia	rase	19	
V×VMFailAction	String	Scalar	RESTART_VXVM		
VXVMRestartAtte	Integer	Scalar	10	2	
DetailMonitorFreq	Integer	Scalar	10	2	
DiskGroupName	String	Scalar	datadg	2	
DGGuid	String	Scalar		2	-
	I	🗸 Critical 🔽 Enable	d		
			01/		

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**

Γ

 DiskGroupName = datadg_evt (グローバル属性として定義される)

🔞 Add Resource				>	<
😽 🛛 Add Re	esource				
Group name:	APP				
Resource name:	datadg_evt				
Resource Type:	VMDg		• ?		
Attribute name	Туре	Dimension	Value	Edit	-
ciscopplications	boolean	Juaiai	laise	8	
V×VMFailAction	String	Scalar	RESTART_VXVM		-
V×VMRestartAtte	Integer	Scalar	10		
DetailMonitorFreq	Integer	Scalar	10	2	
DiskGroupName	String	Scalar	datadg_evt	2	
DGGuid	String	Scalar		2	-
		Iritical 🔽 Enabled			
EL_ Show Comman	nd		_K_	Cancel	

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。

aroup numer M	VPP			
Resource name:	APP_MountV			
Resource Type:	MountV	*	SP.	
Attribute name	Туре	Dimension	Value	Edit
Attribute name ForceUnmount	Type	Dimension Scalar	Value READ_ONLY	Edit
Attribute name ForceUnmount ListApplications	Type String Boolean	Dimension Scalar Scalar	Value READ_ONLY false	Edit
Attribute name ForceUnmount ListApplications AutoFSClean	Type String Boolean Boolean	Dimension Scalar Scalar Scalar	Value READ_ONLY false false	Edit
Attribute name ForceUnmount ListApplications AutoFSClean PurgeStaleMountPoints	Type String Boolean Boolean Boolean	Dimension Scalar Scalar Scalar Scalar	Value READ_ONLY False False False	Edit
Attribute name ForceUnmount ListApplications AutoFSClean PurgeStaleMountPoints MountPath	Type String Boolean Boolean Boolean String	Dimension Scalar Scalar Scalar Scalar Scalar	Value READ_ONLY false false false f:\	Edit
Attribute name ForceUnmount ListApplications AutoFSClean PurgeStaleMountPoints MountPath VolumeName	Type String Boolean Boolean Boolean String String	Dimension Scalar Scalar Scalar Scalar Scalar Scalar Scalar	Value READ_ONLY false false false fils Fi\ cscopx	Edit 27 27 27 27 27 27 27 27 27 27
Attribute name ForceUnmount ListApplications AutoFSClean PurgeStaleMountPoints MountPath VolumeName VMDGResName	Type String Boolean Boolean String String String	Dimension Scalar Scalar Scalar Scalar Scalar Scalar Scalar Scalar	Value READ_ONLY false false false Fi\ cscopx datadg	Edit 27 27 27 27 27 27 27 27 27 27

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**

ſ

- 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。

🍘 Add Resource				×
🜏 🛛 Add Re	esource			
Group name:	APP			
Resource name:	APP_MountV_e	/t		
Resource Type:	MountV		• ?	
Attaile the manual	Turne	Dimension	Unive	
Attribute name	poolean	Dimension	value	Edit
AutoFSClean	Boolean	Scalar	true	
PurgeStaleMount	Boolean	Scalar	false	
MountPath	String	Scalar	К:	12
VolumeName	String	Scalar	cscopx_evt	2
VMDGResName	String	Scalar	datadg_evt	2 🗸
		Critical 🔽 Enable	ł	
Show Commar	nd		<u></u> K	Cancel

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>

The list of registry keys to	be monitored. This attrib	oute can take localized	
values. Setting up replicati	ion of a key automatically	y sets up replication of	fits
subkeys: For example, to i HKLM\\Software\\VERITAS	replicate the keys HKLM\ S\\VCS, define only HKLM	\Software\\VERITAS\\ h\\Software\\VERITAS\	land Uin the
the second s	· · · · · · · · · · · · · · · · · · ·		
(eys attribute. From the ?	name-value? pair of a re	gistry key, you must p	provide
Keys attribute. From the ? the name of the registry k	name-value? pair of a re eys to be synchronized a	gistry key, you must p and not the value for t	hat
Keys attribute. From the ? the name of the registry k key.	name-value? pair of a re eys to be synchronized a	gistry key, you must p and not the value for t	hat
(eys attribute. From the ? the name of the registry k (ey. Global	name-value? pair of a re eys to be synchronized a Key	gistry key, you must p and not the value for t Value	hat
Keys attribute. From the ? the name of the registry k (ey. Global C Per System	name-value? pair of a re eys to be synchronized a Key HKLM\Software\J	gistry key, you must p and not the value for t Value	
(eys attribute. From the ? the name of the registry k (ey. (C Global (C Per System) (SMAW3-32-Ha)	name-value? pair of a re eys to be synchronized a Key HKLM\Software\J	gistry key, you must p and not the value for t Value	

(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。

😨 Add Resource				×
😽 🛛 Add Reso	ource			
Group name:	APP			
Resource name:	APP_CSManager			
Resource Type:				
	CSManager	<u>·</u>	T.	
Attribute name	Туре	Dimension	Value	Edit
PathName	String	Scalar	F:\Program Files\CSCO	2
EventIPAddress	String	Scalar	10.76.10.240	2
CertificateDir	String	pcalar		
CertunicateDir	pung	plaa		2
		🔽 Critical 🔽 Enabled		
🗑 🖵 Show Command			oĶ	Cancel

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。

Γ

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。 Veritas Cluster Server のタスク

2	Parent Resource: APP_CSManager	
Groi Chili	up: APP d Resource:	
Q.,	APP_IP	1
1	APP_MountV	
ŵ	APP_MountV_evt	
2	APP_RegRep	
6	NIC	
Q.	datadg	
õ	datadg_evt	
		- 1

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 $\exists \vee \vee \neg \nu$)
- 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。

1

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」(P.3-25)
- 「ClusterService グループの作成」(P.3-26)
- 「レプリケーション サービス グループの作成」(P.3-27)
- 「アプリケーション サービス グループの作成」(P.3-28)
- 「クラスタレベルコンフィギュレーションの作成」(P.3-30)

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

ſ

- **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。

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。

- 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 \neg \neg \vdash \lor \lor \lor \lor \lor \lor \lor

(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 = $\langle \forall \forall \dot{x} \rangle \langle \forall z \rangle$
- 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。



Γ

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>

 - 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。

1

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

<u>》</u> (注) 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。

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**

Cisco Security Manager 4.0 ハイ アベイラビリティ インストレーション ガイド

- **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)

ſ

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>
- 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。