

# **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 (1ページ)
- Microsoft Windows Server のインストール  $(2 \sim ジ)$
- 外部ストレージへのサーバの接続 (3ページ)
- Veritas 製品のインストール (3ページ)
- ・ブートディスクのミラーリング(任意) (4ページ)
- Veritas Volume Manager の設定タスク (4 ページ)
- Security Manager のインストール (7 ~- ジ)
- Veritas Volume Replicator タスク  $(15 \, \sim \, \checkmark)$
- ・作業ボリュームに対する権限の更新 (17ページ)
- Veritas Cluster Server タスク  $(19 \, \sim \, \checkmark)$

# 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。

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 <u>1</u>	(注)を参照	(注)を参照
Veritas Enterprise Administrator (GUI) <sup>2</sup>	必須	必須	必須
Cluster Manager (GUI) 2	オプション	オプション	

表 1: Veritas ソフトウェアコンポーネント

<sup>1</sup> 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) (4ページ)
  - プライマリサーバ(複製あり) (5ページ)
  - ・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(6ページ)

### 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

🔁 Veritas	Enterprise Administrator	
<u>File T</u> ools	Actions Help	
4	Bµ	
Connect	Disconnect New Window	
Select Host:	: 🕼 vea://Home:Assistant/	_
Assistant	Veritas Enterprise Administrator (VEA). VEA allows you to connect to and manage heterogeneous resources across to the VEA application. Connect to a server now by clicking the "Connect to a Host or Domain" link below.         Image Connect to a Host or Domain       Image Connect to a Host or Domain         Connect to VEA enabled hosts or domains to manage heterogeneous devices.       View or Edit VEA Preferences such as appearance, language, favorites, and identities.         Image User Profiles       Add, edit or delete user profiles that allow preferences per user of this application.       Connect Using: Logged On User on this computer         Connect using a different user account       Connect       Gancel       Help	236589 Dot:

**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。

🔞 Yeritas I	Enterprise Adm	ninistrator								
Eile Tools	<u>A</u> ctions ⊻iew	Window Help								
8		<b>1</b>		88	2					
Connect	Disconnect	New Window	New Volume	New Group	Search					
Select Host:	👪 vea://beed	her-win-ha1:Syst	em/beecher-win-	ha1.cisco.com/Sti	orageAgent/Disk	Groups/datadg/				
	To System	1		Disks G	🕑 Volumes 🛛 🤤	Disk View 🔏 Alerts				
H K 🔁	⊡ 🍰 bee	cher-win-ha1		Group name	: datadg	Type: Dynamic (Secor	ndary)			
System	J 🖃 🖗	beecher-win-ha		Status:	Deported					
		Storage#ge	Int	Device	Internal	name Dynamic disk group	n Status	Size	Туре	% Used
			We	🕢 🗑 Harddisk0	) Disk1	datadg	Offline	68.400 GB	Dynamic	100%
Assistant		E- Disk Gro	oups	Harddisk1	l Disk2	datadg	Offline	68.400 GB	Dynamic	100%
a		Bas	icGroup							
			New Volume							
LOUS			Add Disk to Dy	namic Disk Group,		-				
-		🛨 👩 Disks	Remove Disk fr	om Dynamic Disk	Group					
Control Ban		Enclo:	Rename Dynan	nic Disk Group						
Condront dri			Import Dynami	ic Disk Group						
		isns	Deport Dynami	r Disk Group						
		Saver	Recover Dynar	mic Disk Group						52
		🗄 🚠 Volum –	Lieger of Dyna	nie Diel, Greue Her						356
			upgrade Dyna	mu biswaroup ver	DIDIT					23(

- **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。

High Availability	VERITAS Storage Foundation High Availability for Windows has been detected on your server.
	< <u>B</u> ack <u>N</u> ext > Cancel

- 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 (~2GB) 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。

 Connect
 X

 Host Name:
 beecher-win-ha2
 Browse...

 O Connect Using:
 Logged On User on this computer

 Connect using a different user account

 Connect
 Connect

 Help

- **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

図 236588

🔁 Veritas Enl	terprise Adm	inistrator									_ 🗆 X
<u>File T</u> ools <u>A</u>	<u>\</u> ctions <u>V</u> iew	<u>W</u> indow <u>H</u> elp									
Connect	E. Disconnect	new Window	🔛 New Volume	New Gro	up Search						
Select Host:	👩 vea://beech	ner-win-ha2:Syste	m/beecher-win	-ha2.cisco	.com/StorageAgen	t/Disk Groups/					-
System System Assistant Logs Control Panel	Cho System	Crier-Win-naz beecher-win-ha2 actionagent becher-win-ha2 concomentation becher-win-ha2 concomentation becher-win-ha2 be	.cisco.com it s ups Group dg_rep dg_rep dg_spare iskGroup es ueries of (G;) px px px_rep px_rep px_rep px_rep px_rep	Group nan Options New nat	Groups Die Die BasicGroup BasicGroup datadg in-ha2 - Import ne: datadg_spare Clear host Clear host Clear host Clear host Clear host Clear host	k View Alerto Disk Groups III Status Imported Deported Deported Dynamic Disk G gynamic disk group (Luster disk group)	s Size 204.500 GB 0 Siroup	Unallocated 170.600 GB 0 0 0	Type Basic Dynamic (Se Dynamic (Se Dynamic (Se	# Disks 4 2 2 1 1	# Volum 1 2 1 1
	Message	s are not being fil	tered. Current Classifica	ly showing ation	0 messages. 🤤	Message					

- **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。

High Availability	×
	VERITAS Storage Foundation High Availability for Windows has been detected on your server.
	✓ Install High Availability for Cisco Security Manager
	< <u>B</u> ack <u>N</u> ext > Cancel

- 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

|--|

54	Enter names for Replicated Data Set and Replicated Volume Group       Image: Comparison of Comparison
	Replicated Data Set name : CSM_RDS
	Replicated Volume Group name : CSM_RVG
	Primary Host : 10.76.10.236
	Veritas Enterprise Administrator(VEA) should be connected to the desired Primary host.
_	

- **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。

Setup Replicated Data Set Wizard		×
Specify Secondary host for replication	K	
Secondary Host:		
The Veritas Enterprise Administrator needs connected. The connection process will sta again.	s to be connected to the specified Secondary host if not already art when you click Next. Please wait until it completes and then click < Back	Next Help

- **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。

Add Secondary Wizard		X	
Edit replication settings Edit replication settings or click next.		+	
Primary side IP Secondary side IP Replication Mode Replicator Log Protection Primary RLINK Name Secondary RLINK Name	10.76.10.236 [10.76.10.237 [Synchronous Override [AutoDCM	Y Y anced	
DHCP addresses are not supported	by VVR.		_
	< <u>B</u> ack	<u>Nex</u> <u>Cancel</u> <u>H</u> elp	73658

- 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 (20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)
  - ClusterService グループの作成 (23 ページ)

#### 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
- $[J \lor \neg \neg \neg \neg] = \mathbf{RVGPrimary}$
- [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**
- $[J \lor \neg \neg \neg \neg] = \mathbf{IP}$
- [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

 $\mathcal{O}$ 

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**
    - $[J \lor \neg \neg \neg \neg \neg] = \mathbf{NIC}$
    - [MACAddress (MACAddress)] =  $\langle NIC$  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
    - $[J \lor \neg \neg \neg \neg \neg] = \mathbf{IP}$
    - •[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
- [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。
シ
レント 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**
    - $[J Y \lambda \beta T ]$  (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
    - $[J \lor \neg \neg \neg \neg] = \mathbf{IP}$
    - •[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
- $[J \mathcal{Y} \mathcal{X} \mathcal{P} \mathcal{T}]$  (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**
  - $[J \lor \neg \neg \neg \neg] = \mathbf{Proxy}$
  - [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**
  - $[\mathcal{Y} \mathcal{X} \mathcal{Y} \mathcal{X} \mathcal{Y}] = \mathbf{IP}$
  - [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

- [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
- $[UV \lambda \beta T]$  (Resource Type) ] = **VvrRvg**
- [RVG (RVG) ] =  $\mathbf{CSM}_{\mathbf{RVG}}$
- [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。

Available Systems Systems for Service Group System name Star CSM-W3-32-HA1 CSM-W3-32-HA2	rtup Priority 7 0 7 1
System name Star System name Star C5M-W3-32-HA1 C5M-W3-32-HA2	rtup Priority 7 0 7 1
Image: Sign with the second	
<b>SM-W3-32-HA2</b>	
ervice Group Type: 💿 Failover, 🔿 Parallel 🦳 Hybrid	
elected Template: None	Templates

- 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

  - [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。

🔁 Add Resource				×
🜏 🛛 Add Reso	urce			
Group name: A	PP			
Resource name:	NIC			
Resource Type:	чіс	<u>*</u>	8	
Attribute name	Туре	Dimension	Value	Edit
ingTimeoutMseconds	Integer	Scalar	1000	
laxTxErrorPercentage	Integer	Scalar	50	2
laxTxErrInterval	Integer	Scalar	10	2
IseConnectionStatus	Boolean	Scalar	true	2
1ACAddress	String	Scalar		2
ingHostList	String	Vector		2
PingnostList	pening			
1 Show Command			OK	Cancal

- 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

  - [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)

Group name:	APP			
Resource name:	APP_IP			
Resource Type:	IP		• 8	
Attribute name	Туре	Dimension	Value	Edit
Address	String	Scalar	10.76.10.240	2
5ubNetMask	String	Scalar	255.255.255.0	2
	Steina	Scalar		1

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)

	COLIFCO				
	source				
Group name:	APP				
Resource name:	datadg				
Resource Type:	VMDg		• 8		
Attribute name	Туре	Dimension	Value	Edit	Т
зсмррисасионь	poolean	Deala	aise	19	
/xVMFailAction	String	Scalar	RESTART_VXVM	2	-
/xVMRestartAtte	Integer	Scalar	10	2	
DetailMonitorFreq	Integer	Scalar	10	2	
DiskGroupName	String	Scalar	datadg	2	
GGuid	String	Scalar		2	-
	ſ	🗸 Critical 🔽 Enable	d		
mi et e	a		OK	Cance	. 1

- 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)

🕼 Add Resource					×
😽 🛛 Add Re	esource				
Group name:	APP				
Resource name:	datadg_evt				
Resource Type:	VMDg		•		
Attribute name	Туре	Dimension	Value	Edit	Т
ciscopplications	Chrise	Dualar Castar	DECTART UNUM	476	
vxvmrallAction	Tabagar	Caslar	RESTART_VAVM	200	
VXVMRestartAtte	Integer	Scalar	10	470	
DickGroupName	Stripg	Scalar	datado evt	479	111
DGGuid	String	Scalar	uacaug_crc	1	-
		Critical 🔽 Enable	ed		

**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
- $[J \lor \neg \neg \neg \neg]$  (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。

Group name: A	.PP			
Resource name:	APP_MountV			
Resource Type:	MountV	<b>.</b>	Q	
	Tuna	Dimension	Value	E GAD
U FERIDUISO D DESO	I IVDE	Dimension	Value	Eur
Attribute name	String	Scalar	READ ONLY	1
orceUnmount istApplications	String Boolean	Scalar Scalar	READ_ONLY false	<u> 2</u>
attribute name forceUnmount istApplications wtoESClean	String Boolean Boolean	Scalar Scalar Scalar	READ_ONLY false false	
attribute name forceUnmount istApplications lutoFSClean urgeStaleMountPoints	String Boolean Boolean Boolean	Scalar Scalar Scalar Scalar	READ_ONLY false false false	
Attribute name iorceUnmount istApplications lutoFSClean lurgeStaleMountPoints 10untPath	String Boolean Boolean Boolean String	Scalar Scalar Scalar Scalar <b>Scalar</b>	READ_ONLY false false false false F:\	
Attribute name ForceUnmount istApplications AutoFSClean PurgeStaleMountPoints fountPath folumeName	String Boolean Boolean Boolean String String	Scalar Scalar Scalar Scalar Scalar Scalar Scalar	READ_ONLY false false false F:\ cscopx	
Attribute name ForceUnimount istApplications AutoFSClean PurgeStaleMountPoints YountPath YolumeName YMDGResName	String Boolean Boolean Soolean String String String	Scalar Scalar Scalar Scalar Scalar Scalar Scalar	READ_ONLY false false false F:\ cscopx datadg	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2

**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。

🔞 Add Resource	1				×
😽 🛛 Add Re	esource				
Group name:	APP				
Resource name:	APP_Mount\	/_evt			
Resource Type:	MountV		<b>•</b>	3	
Attribute name	Type	Dimension	Value	Edit	Т
ciscopplications	Doolean	Juanan	urue	19	-
AutoFSClean	Boolean	bcalar	true	14	
PurgeStaleMount	Boolean	Scalar	talse	C2	
MountPath	String	Scalar	K:	2	
VolumeName	String	Scalar	cscopx_evt	2	1.00
VMDGResName	String	Scalar	datadg_evt	2	-
EL Show Commar	nd	Critical 🔽 Enable	eg Iók	Cancel	1

- 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>

Q			
APP_RegRep			
The list of registry keys to be values. Setting up replication subkeys. For example, to rep HKLM\\Software\\VERITAS\\ Keys attribute. From the ?na	e monitored. This attribute n of a key automatically se plicate the keys HKLM\\So VCS, define only HKLM\\Si ime-yalue? pair of a regist	e can take localized ts up replication of it ftware\\VERITAS\\ a oftware\\VERITAS\\ ry key, you must pro	ind in the pyide
the name of the registry key how	's to be synchronized and	not the value for tha	at _
key. (© Global	Key	Value	it _
key. © Global © Per System	Key HKLM\Software\J	Value	sc
Global     CPer System     CSM-W3-32-HA1	Key	Value	+ -
Global     C Per System     CSM-W3-32-HA1	Key HKLM\Software\J	Value	+ -

- (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。

🔅 Add Resource				×
🙀 🛛 Add Reso	urce			
Group name:	1.PP			
Resource name:	APP_CSManager			
Resource Type:	CSManager	V	2	
Attribute name	Туре	Dimension	Value	Edit
PathName	String	Scalar	F:\Program Files\CSCO	P
EventIPAddress	String	Scalar	10.76.10.240	2
CertificateDir	String	Scalar		
		5		
		IV Critical IV Enabled		
EL Show Command				Cancel

**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。

🗟 Li	ink Resources		×
9	Parent Resource: Al	PP_CSManager	
Gro Chil	up: APP d Resource:		
	APP_IP		
	APP_MountV		
12	APP_MountV_evt		
	АРР_Кедкер   NIC		
ā	datadq		
kõ	datadg_evt		
-			
		<u> </u>	Cancel

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。

クラスタレベル設定の作成

I

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

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。