



## **Cisco Security Manager 4.27 ハイ アベイラビリティ インストレーションガイド**

初版：2023年9月7日

### **シスコシステムズ合同会社**

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター  
0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>





## 目次

---

第 1 章	はじめに 1
	対象読者 1
	表記法 4
	関連資料 5

---

第 2 章	概要 9
	ローカル冗長性 (HA) プロセスの概要 10
	ローカル冗長性 (HA) の設定手順 11
	地理的冗長性 (DR) プロセスの概要 12
	地理的冗長性 (DR) の設定手順 13
	Veritas 製品 14

---

第 3 章	システム要件 17
	シングルノードサイトのハードウェア要件 17
	デュアルノードサイトのハードウェア要件 18
	ローカル冗長性構成のソフトウェア要件 19
	地理的冗長性 (DR) 構成のソフトウェア要件 21
	クラスタリングが不要な複製のソフトウェア要件 21
	プリインストール ワークシート 22
	ローカル冗長性構成のワークシート 22
	地理的冗長性 (DR) 設定ワークシート 24

---

第 4 章	Cisco Security Management Suite 高可用性ソリューションのインストール 27
	イーサネット接続の確立 27

Microsoft Windows Server のインストール	28
外部ストレージへのサーバの接続	29
Veritas 製品のインストール	29
ブート ディスクのミラーリング (任意)	30
Veritas Volume Manager の設定タスク	30
プライマリサーバ (複製なし)	30
プライマリサーバ (複製あり)	31
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	32
Security Manager のインストール	33
プライマリ サーバへの Security Manager のインストール	34
セカンダリサーバへの Security Manager のインストール	37
セカンダリ HA サーバーでの手動によるサービスの開始	40
Veritas Volume Replicator タスク	41
作業ボリュームに対する権限の更新	43
共有ストレージを使用する場合の権限の更新	43
複製を使用する場合の権限の更新	44
Veritas Cluster Server タスク	46
シングルローカルクラスタ (デュアルノード) 構成	46
クラスタの作成	46
アプリケーション サービス グループの作成	47
ClusterService グループの作成	49
デュアル地理的クラスタ構成	50
プライマリおよびセカンダリクラスタの作成	51
ClusterService グループの作成	51
複製サービスグループの作成	53
アプリケーション サービス グループの作成	55
クラスタレベル設定の作成	62
第 5 章	メンテナンス作業 65
	VCS 動作のカスタマイズ 65
	SSL 用のセキュリティ証明書 66

Security Manager の手動での起動、停止、フェールオーバー	67
VCS の場合	68
VCS 以外の場合	68
Cisco Secure ACS と Security Manager の統合	70
Security Manager のアップグレード	71
Security Manager のバックアップ	72
Security Manager のアンインストール	72
非 HA Security Manager の HA への移行	73

---

**第 6 章**

<b>仮想マシンの高可用性とディザスタリカバリ</b>	<b>75</b>
ホストベースのフェールオーバー（ローカル HA）	75
VMware HA クラスタ作成の前提条件	76
ホストベースのフェールオーバー用 Security Manager の設定	76
制限事項	77
フォールトトレランス	77
耐障害性システムの作成	78
ディザスタ カバリ	81
システム要件	81
ハードウェア要件	81
ソフトウェア要件	81
VMware Site Recovery Manager の設定	82
vCenter の設定	84
リカバリサイトの設定	87
複製の設定	88
ディザスタリカバリ環境での Security Manager のインストール	88

---

**付録 A :**

<b>参照構成の VCS リソース ビュー</b>	<b>91</b>
参照構成の VCS リソースビュー	91
シングルローカルクラスタ（デュアルノード）構成	91
デュアル地理的クラスタ（シングルノード）構成	92

---

付録 B :	<b>ハイ アベイラビリティおよびディザスタ リカバリ証明テスト計画</b>	<b>97</b>
	<b>手動切り替え</b>	<b>97</b>
	<b>クラスタ内切り替え</b>	<b>98</b>
	<b>クラスタ間切り替え</b>	<b>98</b>
	<b>イーサネット/ネットワーク障害</b>	<b>99</b>
	<b>ネットワーク通信障害</b>	<b>99</b>
	<b>セカンダリサーバ、シングルクラスタにおけるネットワークイーサネット障害</b>	<b>100</b>
	<b>プライマリサーバ、シングルクラスタにおけるネットワークイーサネット障害</b>	<b>101</b>
	<b>セカンダリサーバ、デュアルクラスタにおけるネットワークイーサネット障害</b>	<b>102</b>
	<b>プライマリサーバ、デュアルクラスタにおけるネットワークイーサネット障害</b>	<b>104</b>
	<b>クラスタ通信障害</b>	<b>105</b>
	<b>サーバの障害</b>	<b>107</b>
	<b>スタンバイサーバの障害、シングルクラスタ</b>	<b>108</b>
	<b>プライマリサーバの障害、シングルクラスタ</b>	<b>108</b>
	<b>スタンバイサーバの障害、デュアルクラスタ</b>	<b>109</b>
	<b>プライマリサーバの障害、デュアルクラスタ</b>	<b>111</b>
	<b>アプリケーションの障害</b>	<b>114</b>
	<b>アプリケーションの障害、シングルクラスタ</b>	<b>114</b>
	<b>アプリケーションの障害、デュアルクラスタ</b>	<b>115</b>



# 第 1 章

## はじめに

---

このマニュアルでは、高可用性（HA）環境やディザスタリカバリ（DR）環境に Cisco Security Management Suite（Security Manager）をインストールする方法について説明します。Security Manager HA/DR ソリューションは、Veritas Storage Foundation and High Availability Solutions に基づいています。

VMware ベースの高可用性（HA）またはディザスタリカバリ（DR）環境に Security Manager をインストールする手順については、[仮想マシンの高可用性とディザスタリカバリ（75 ページ）](#) を参照してください。

- [対象読者（1 ページ）](#)
- [表記法（4 ページ）](#)
- [関連資料（5 ページ）](#)

## 対象読者

このマニュアルの主な対象読者は、HA/DR ソリューションのインストールおよび管理を担当するシステム管理者です。このマニュアルでは、[表](#)の内容をよく理解していることを前提としています。

表 1: このマニュアルの内容

設定	トピック
ローカル冗長性	<ul style="list-style-type: none"> <li>• Cisco Security Management Suite</li> <li>• 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、または Microsoft Windows Server 2012 R2 Standard および Datacenter エディションまたは Microsoft Windows Server 2016 Standard および Datacenter エディション</li> </ul> <p>(注) CSM 4.27 の Microsoft Windows Server 2019 および 2016 プラットフォームでテスト済み。</p> <ul style="list-style-type: none"> <li>• Veritas Storage Foundation HA for Windows 6.0.1、6.0.2、6.1、Veritas InfoScale 7.0、Veritas InfoScale 7.2、Veritas InfoScale 7.4 <ul style="list-style-type: none"> <li>• Veritas InfoScale 7.4.2 以降は Windows Server 2019 をサポートしていません。</li> <li>• Windows 2019 : Veritas Storage Foundation for Windows Version : 7.4.2</li> <li>• Windows 2016 : Veritas Storage Foundation for Windows Version : 7.4</li> </ul> </li> </ul>



設定	トピック
地理的冗長性	<ul style="list-style-type: none"><li>• Cisco Security Management Suite</li><li>• 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、または Microsoft Windows Server 2012 R2 Standard および Datacenter エディションまたは Microsoft Windows Server 2016 Standard および Datacenter エディション</li></ul> <p>(注) CSM 4.27 の Microsoft Windows Server 2019 および 2016 プラットフォームでテスト済み。</p> <ul style="list-style-type: none"><li>• Veritas Storage Foundation HA for Windows 6.0.1、6.0.2、6.1、Veritas InfoScale 7.0、Veritas InfoScale 7.2、Veritas InfoScale 7.4<ul style="list-style-type: none"><li>• Veritas InfoScale 7.4.2 以降は Windows Server 2019 をサポートしています。</li><li>• Windows 2019 : Veritas Storage Foundation for Windows Version : 7.4.2</li><li>• Windows 2016 : Veritas Storage Foundation for Windows Version : 7.4</li></ul></li><li>• Veritas Volume Replicator Option</li></ul>

設定	トピック
地理的冗長性 (クラスタリングなし)	<ul style="list-style-type: none"> <li>• Cisco Security Management Suite</li> <li>• 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、または Microsoft Windows Server 2012 R2 Standard および Datacenter エディションまたは Microsoft Windows Server 2016 Standard および Datacenter エディション</li> </ul> <p>(注) CSM 4.27 の Microsoft Windows Server 2019 および 2016 プラットフォームでテスト済み。</p> <ul style="list-style-type: none"> <li>• Veritas Storage Foundation HA for Windows 6.0.1、6.0.2、6.1、Veritas InfoScale 7.0、Veritas InfoScale 7.2、Veritas InfoScale 7.4 <ul style="list-style-type: none"> <li>• Veritas InfoScale 7.4.2 以降は Windows Server 2019 をサポートしています。</li> <li>• Windows 2019 : Veritas Storage Foundation for Windows Version : 7.4.2</li> <li>• Windows 2016 : Veritas Storage Foundation for Windows Version : 7.4</li> </ul> </li> <li>• Veritas Volume Replicator Option</li> </ul>

Security Manager HA/DR ソリューションは Veritas Storage Foundation and High Availability Solutions for Windows を利用するため、ローカル冗長性ソリューションに関する次のコースを推奨します。

- Veritas Storage Foundation for Windows
- Veritas Cluster Server for Windows

地理的冗長性については、次のコースを受講することを強く推奨します。

- Veritas Volume Replicator for Windows
- Disaster Recovery Using Veritas Volume Replicator and Global Cluster Option for Windows

## 表記法

このマニュアルでは、次の表記法を使用しています。

項目	表記法
手順で選択する必要があるコマンド、キーワード、特殊な用語、およびオプション	太字
ユーザが値を指定する変数、および新しい用語や重要な用語	<i>italic</i> フォント
セッション情報、システム情報、パス、およびファイル名の表示出力	screen font
ユーザーが入力する情報	太字の screen フォント
ユーザーが入力する変数	イタリック体の screen フォント
メニュー項目およびボタン名	太字
メニュー項目の選択順序	[オプション (Option)] > [ネットワーク設定 (Network Preferences)]



ヒント 製品を最大限に活用できる情報を示します。



(注) 「注釈」です。次に進む前に検討する必要がある重要情報、役に立つ情報、このマニュアル以外の参照資料などを紹介しています。



注意 「要注意」の意味です。機器の損傷、データの損失、またはネットワークセキュリティの侵害を予防するための注意事項が記述されています。



警告 ユーザの身体、ソフトウェアの状態、または機器に被害が及ぶのを防ぐために、留意する必要がある注意事項が記述されています。記載された注意事項に従わない場合に、結果として発生するセキュリティ侵害が明確に特定されています。

## 関連資料

追加情報については、次のシスコの資料を参照してください。このドキュメントは <http://www.cisco.com/c/en/us/support/security/security-manager/tsd-products-support-series-home.html> から入手できます。

- 『*Installation Guide for Cisco Security Manager 4.27*』 [英語]

- 『*User Guide for Cisco Security Manager 4.27*』 [英語]
- 『*Release Notes for Cisco Security Manager 4.27*』 [英語]

Veritas Storage Foundation に関連する詳細情報については、次の資料を参照してください。

- 『*Veritas Storage Foundation™ and High Availability Solutions Getting Started Guide*』 [英語]
- 『*Veritas Storage Foundation™ and High Availability Solutions Release Notes*』 [英語]
- 『*Veritas Storage Foundation™ and High Availability Solutions Installation and Upgrade Guide*』 [英語]
- 『*Veritas Storage Foundation™ Administrator's Guide*』 [英語]
- 『*Veritas™ Cluster Server Release Notes*』 [英語]
- 『*Veritas™ Cluster Server Installation and Upgrade Guide*』 [英語]
- 『*Veritas™ Cluster Server Bundled Agents Reference Guide*』 [英語]
- 『*Veritas™ Cluster Server Administrator's Guide*』 [英語]
- 『*Veritas™ Volume Replicator Administrator's Guide*』 [英語]
- 『*Veritas™ Volume Replicator Advisor User's Guide*』 [英語]
- 『*Hardware Compatibility List (HCL) for Veritas Storage Foundation™ and High Availability Solutions for Windows*』 [英語]
- 『*Software Compatibility List (SCL) for Veritas Storage Foundation™ and High Availability Solutions for Windows*』 [英語]

#### 通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) [英語] でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[シスコサービス](#) [英語] にアクセスしてください。
- サービス リクエストを送信するには、[シスコサポート](#) [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco Marketplace](#) [英語] にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) [英語] にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) [英語] にアクセスしてください。

### Cisco バグ検索ツール

[Cisco バグ検索ツール](#) (BST) [英語] は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。





## 第 2 章

### 概要

---

このマニュアルでは、高可用性（HA）環境やディザスタリカバリ（DR）環境に Cisco Security Management Suite（Security Manager）をインストールする方法について説明します。Security Manager HA/DR ソリューションは、Veritas Storage Foundation and High Availability Solutions に基づいています。このマニュアルで説明する Security Manager HA/DR ソリューションは次のアプリケーションをサポートしています。

- Security Manager 4.27

HA ソリューションは、ローカル冗長性（HA）と地理的冗長性（DR）の両方の構成をサポートします。



- 
- (注) Cisco Prime Security Manager（PRSM）アプリケーションの相互起動は、HA および DR 構成の両方でサポートされます。ただし、シングルサインオン（SSO）機能を使った Security Manager から PRSM へのシームレスな直接アクセスは、HA モードでのみサポートされます。
- 



- 
- (注) バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーションサービスルータ、統合サービスルータ、埋め込み型サービスルータ、および次のデバイスを含む Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。

- Cisco Catalyst 6500 および 7600 シリーズファイアウォールサービスモジュール（EOL8184）
  - Cisco Catalyst 6500 シリーズ Intrusion Detection System サービスモジュール 2（EOL8843）
  - Cisco Intrusion Prevention System : IPS 4200、4300、および 4500 シリーズ センサー（EOL9916）
  - Cisco SR 500 シリーズ Secure Router（EOL7687、EOL7657）
  - PIX ファイアウォール（EOL）
- 

この章は、次のセクションで構成されています。

- [ローカル冗長性 \(HA\) プロセスの概要 \(10 ページ\)](#)
- [地理的冗長性 \(DR\) プロセスの概要 \(12 ページ\)](#)
- [Veritas 製品 \(14 ページ\)](#)

## ローカル冗長性 (HA) プロセスの概要

ローカル冗長性の構成は、ソフトウェアまたはハードウェア障害の際にも、スイッチドネットワークおよびルーテッドネットワークで IP アドレスや DNS エントリを再設定する必要がない、自動フェールオーバー ソリューションを提供します。

[図](#)に、ローカル冗長性 HA の構成を示します。



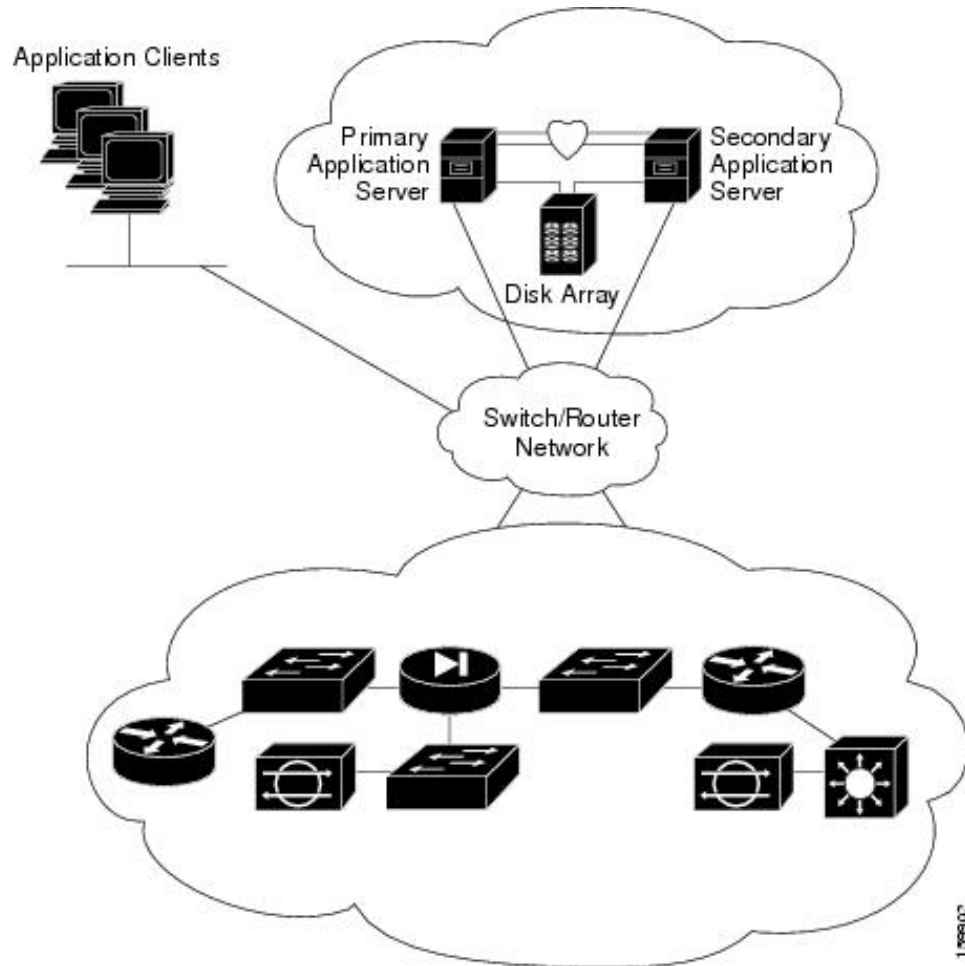
---

(注) [図](#)のサーバーには、ミラーリングされた内蔵ブートディスクが含まれることがあります。同じメーカー、モデル、およびストレージ容量にすることを推奨します。HA サーバとの通信にはフォールトトレラントなスイッチド/ルーテッドネットワークを推奨します。

---



図 1: ローカル冗長性 HA の構成



1.0599.02

## ローカル冗長性 (HA) の設定手順

次の表に、Cisco Security Manager のローカルな冗長性を持つインストールを設定するために必要な手順を示します。


### 手順

	コマンドまたはアクション	目的
ステップ 1	物理接続を確立します。	<a href="#">イーサネット接続の確立 (27 ページ)</a>
ステップ 2	Microsoft Windows サーバとすべての必要なドライバをインストールします。	<a href="#">Microsoft Windows Server のインストール (28 ページ)</a>
ステップ 3	ストレージ接続を確立します。	<a href="#">外部ストレージへのサーバの接続 (29 ページ)</a>

	コマンドまたはアクション	目的
ステップ 4	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。	Veritas 製品のインストール (29 ページ)
ステップ 5	ブートディスクをミラーリングします。	ブートディスクのミラーリング (任意) (30 ページ)
ステップ 6	共有アレイに必要なボリュームをセットアップします。	Veritas Volume Manager の設定タスク (30 ページ)
ステップ 7	プライマリサーバの共有ボリューム上に Cisco Security Manager をインストールします。	Security Manager のインストール (33 ページ)
ステップ 8	セカンダリサーバのスペア (ダミー) ボリューム上に Cisco Security Manager をインストールします。	Security Manager のインストール (33 ページ)
ステップ 9	セカンダリサーバに対する権限を更新します。	作業ボリュームに対する権限の更新 (43 ページ)
ステップ 10	クラスタを作成し、設定します。	Veritas Cluster Server タスク (46 ページ)

## 地理的冗長性（DR）プロセスの概要

地理的冗長性の構成では、2つのサイト間でアプリケーションデータを複製することにより、ディザスタリカバリを提供します。サイト間のフェールオーバーを手動で開始するか、自動的に実行できます。

に、地理的冗長性（DR）の構成を示します。




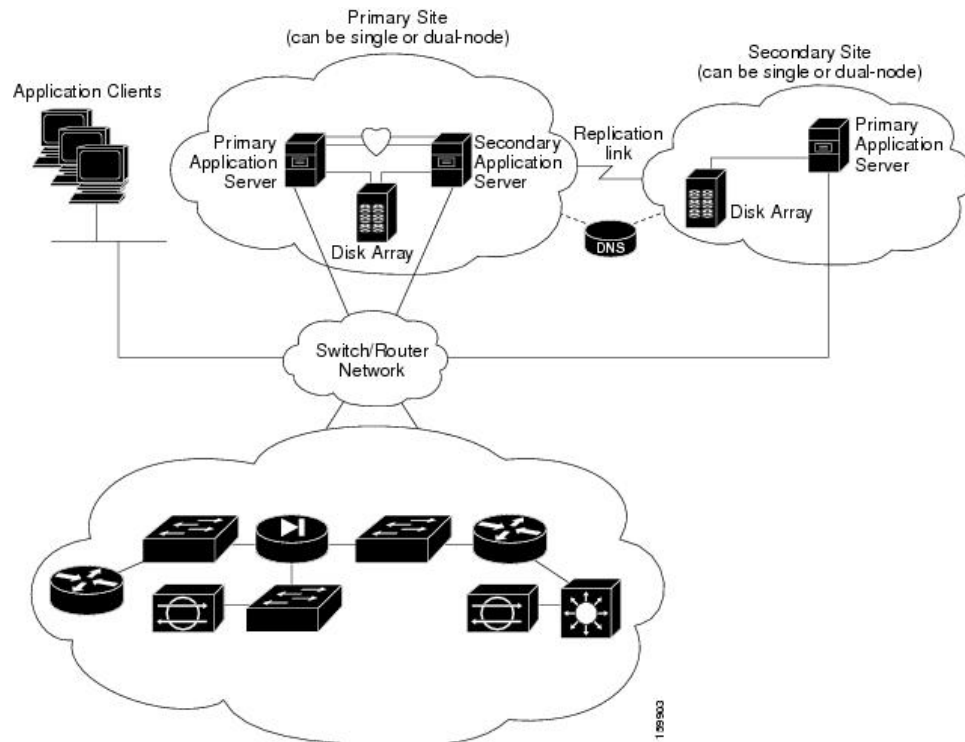
(注) のサーバーには、ミラーリングされた内蔵ブートディスクが含まれることがあります。同じメーカー、モデル、およびストレージ容量にすることを推奨します。サーバとの通信にはフォールトトレラントなスイッチド/ルーテッドネットワークを推奨します。

図 2: 地理的冗長性 (DR) の構成



## 地理的冗長性 (DR) の設定手順

次の表に、Cisco Security Manager の地理的な冗長性を持つインストールを設定するために必要な手順を示します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	物理接続を確立します。	イーサネット接続の確立 (27 ページ)
ステップ 2	Microsoft Windows サーバとすべての必要なドライバをインストールします。	Microsoft Windows Server のインストール (28 ページ)
ステップ 3	ストレージ接続を確立します。	外部ストレージへのサーバの接続 (29 ページ)
ステップ 4	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。	Veritas 製品のインストール (29 ページ)
ステップ 5	ブートディスクをミラーリングします。	ブートディスクのミラーリング (任意) (30 ページ)
ステップ 6	共有アレイに必要なボリュームをセットアップします。	Veritas Volume Manager の設定タスク (30 ページ)

	コマンドまたはアクション	目的
ステップ 7	プライマリサーバの共有ボリューム上に Cisco Security Manager をインストールします。	<a href="#">Security Manager のインストール (33 ページ)</a>
ステップ 8	セカンダリサーバのスペア (ダミー) ボリューム上に Cisco Security Manager をインストールします。	<a href="#">Security Manager のインストール (33 ページ)</a>
ステップ 9	複製を設定します。	<a href="#">Veritas Volume Replicator タスク (41 ページ)</a>
ステップ 10	セカンダリサーバに対する権限を更新します。	<a href="#">作業ボリュームに対する権限の更新 (43 ページ)</a>
ステップ 11	クラスタを作成し、設定します。	<a href="#">Veritas Cluster Server タスク (46 ページ)</a>

## Veritas 製品

このマニュアルで説明されている Security Manager HA/DR ソリューションは、Veritas 製品に基づいています。ここでは、各 Veritas アプリケーションの概要を示します。

- Veritas Storage Foundation for Windows (VSW)

VSW は、Windows 企業コンピューティング環境で、ボリューム管理テクノロジー、迅速なリカバリ、およびフォールトトレラント機能を提供します。VSW は VCS および VVR の基盤を提供します。

- Veritas Cluster Server (VCS)

VCS は、アプリケーションのダウンタイムを減らすためのクラスタリングソリューションです。VCS の Global Cluster Option (GCO) は、(DR 構成などで使用される) 複数のクラスタの管理をサポートします。

- Veritas Volume Replicator (VVR)

VVR は、IP ネットワークを介して継続的にデータを複製することにより、リモートリカバリサイトで重要なアプリケーションを迅速に、高い信頼性でリカバリできます。

- Veritas Enterprise Administrator (VEA GUI) コンソール

VEA GUI コンソールウィンドウは、システムのすべてのストレージオブジェクトを表示および処理するためのグラフィカルな方法を提供します。

- Cluster Manager (Java コンソール)

Cluster Manager (Java コンソール) は、クラスタのすべての管理機能を提供します。クラスタと、サービスグループ、システム、リソース、リソースタイプなどの VCS オブジェクトをモニタするには、Java コンソールのさまざまなビューを使用します。

- Cluster Monitor

Cluster Monitor は、実際のクラスタまたはシミュレートされたクラスタに関する一般情報を表示します。Cluster Monitor を使用して、クラスタへのログインやクラスタからのログオフ、さまざまな VCS オブジェクトのサマリー情報の表示、表示のカスタマイズ、VCS シミュレータの使用、および Cluster Manager の終了を行います。

- Cluster Explorer

Cluster Explorer はクラスタ管理のメインウィンドウです。このウィンドウから、VCS オブジェクトのステータスを表示したり、さまざまな操作を実行したりできます。





## 第 3 章

# システム要件



(注) 異なるハードウェアセットアップを使用する多くの構成があります。Microsoft と Symantec/Veritas のそれぞれのハードウェア互換性リスト (HCL) を参照してください。



(注) 当社は、Security Manager 用に指定されたサードパーティのハードウェアおよびソフトウェアのプラットフォームの可用性を確保するために最大限の努力をしますが、当社の制御を超えるサードパーティベンダー製品の可用性や変更によるシステム要件の変更または修正の権利を留保します。

この章では、HA または DR 環境に Security Manager をインストールするための参照構成について説明します。この章は、次の項で構成されています。

- [シングルノードサイトのハードウェア要件 \(17 ページ\)](#)
- [デュアルノードサイトのハードウェア要件 \(18 ページ\)](#)
- [ローカル冗長性構成のソフトウェア要件 \(19 ページ\)](#)
- [地理的冗長性 \(DR\) 構成のソフトウェア要件 \(21 ページ\)](#)
- [クラスタリングが不要な複製のソフトウェア要件 \(21 ページ\)](#)
- [プリインストールワークシート \(22 ページ\)](#)

## シングルノードサイトのハードウェア要件

シングルノードの HA 環境に Security Manager をインストールするには、フォールトトレラントなストレージレイを設定するか、内蔵ディスクを使用できます。

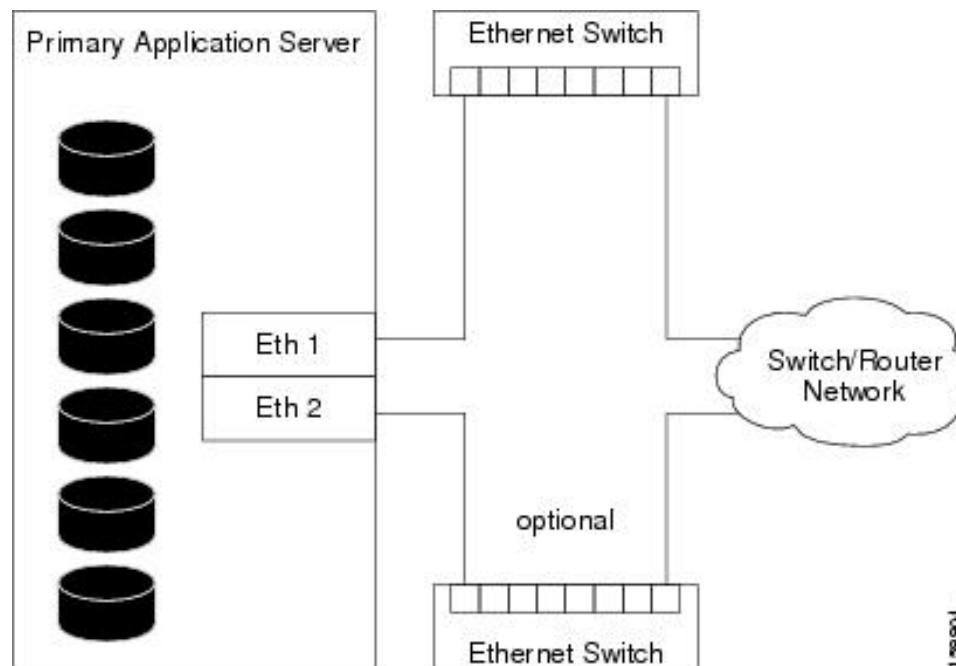
次は、シングルノードサイトのサーバハードウェア仕様です。

- 『*Installation Guide for Cisco Security Manager 4.27*』 [英語] に記載されているプロセッサと RAM の基本要件を満たすサーバー
- 1 つ以上のイーサネット インターフェイス (2 つを推奨)

- 2 台以上の物理ドライブ（6 台を推奨）

図 3: シングルノードサイトのイーサネット接続では、冗長性のためにサーバーからスイッチ/ルータネットワークへの 2 本のイーサネット接続を使用しています。イーサネットポートまたはスイッチで障害が発生しても、サーバとの通信は保持されます。このレベルのネットワーク冗長性が不要な場合は、スイッチ/ルータネットワークへの 1 本の接続を使用できます（つまり、Eth 2 および関連するイーサネットスイッチは任意です）。

図 3: シングルノードサイトのイーサネット接続



## デュアルノードサイトのハードウェア要件

デュアルノード HA 環境に Security Manager をインストールするには、共有ストレージアレイにアクセス可能な 2 台のサーバーが必要です。

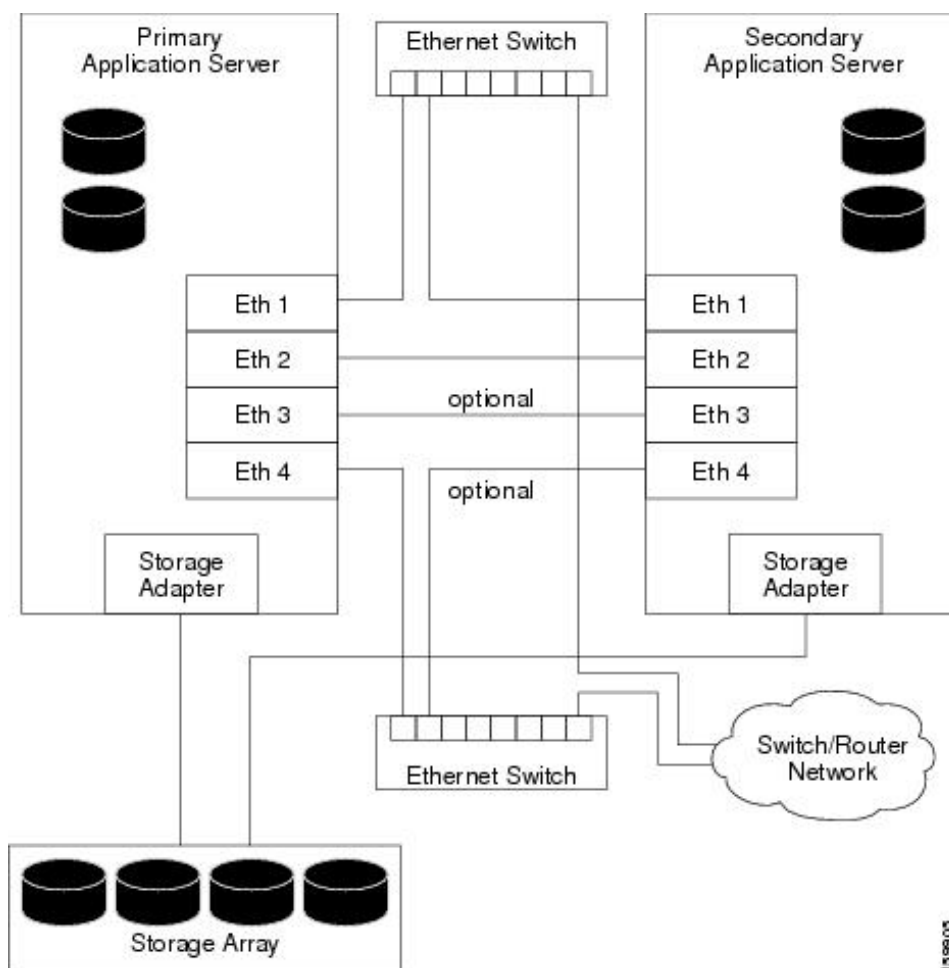
次は、デュアルノードサイトのサーバハードウェア仕様です。

- 『*Installation Guide for Cisco Security Manager 4.26*』 [英語] に記載されているプロセッサと RAM の基本要件を満たすサーバー
- 『*Installation Guide for Cisco Security Manager 4.27*』 [英語] に記載されているプロセッサと RAM の基本要件を満たすサーバー
- 2 つ以上のイーサネット インターフェイス（4 つを推奨）
- 1 台以上の内蔵物理ドライブ（2 台を推奨）
- 1 台以上の外部ドライブ（2 台を推奨、複製を使用する場合は 4 台を推奨）



図4:デュアルノードサイトのイーサネット接続とストレージ接続に、イーサネット接続および外部ストレージ接続を示すデュアルノードサイトの構成を示します。冗長性のためにサーバからスイッチ/ルータネットワークへの2本のイーサネット接続が使用されています。イーサネットポートまたはスイッチで障害が発生しても、サーバとの通信は保持されます。このレベルのネットワーク冗長性が不要な場合は、スイッチ/ルータネットワークへの1本の接続を使用できます（つまり、Eth 4 および関連するイーサネットスイッチは任意です）。クラスタのハートビート通信のためにサーバ間に2本の直接イーサネット接続が確立されていますが、2本目のハートビート接続（Eth 3）は任意です。

図4:デュアルノードサイトのイーサネット接続とストレージ接続



159603

## ローカル冗長性構成のソフトウェア要件

ローカル冗長性 HA 構成に Security Manager をインストールするには、次のソフトウェアが必要です。

- Cisco Security Management Suite 4.27

- Microsoft Windows Server 2019 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



(注) バージョン 4.24 以降、Cisco Security Manager は Microsoft Windows Server 2019 をサポートしています。



(注) バージョン 4.13 以降、Cisco Security Manager は Microsoft Windows Server 2016 をサポートしています。

- Veritas Storage Foundation HA for Windows version 6.0.1/6.0.2/6.1/Veritas InfoScale 7.0/7.2/7.4
  - Veritas InfoScale 7.4.2 以降は Windows Server 2019 をサポートしています。
  - Windows 2019 :  
Veritas Storage Foundation for Windows Version : 7.4.2
  - Windows 2016 :  
Veritas Storage Foundation for Windows Version : 7.4



(注) Veritas Infoscale 7.0 は Windows Sever 2016 をサポートしていません。ただし、Veritas Infoscale 7.2/7.4 は Windows Server 2016 をサポートしています。



(注) Veritas InfoScale 7.4.2 以降は、Windows Server 2019 をサポートしています。

- Dynamic Multipathing Option

Security Manager のライセンスは、HA/DR 構成のアクティブサーバーでのみ必要です。スタンバイサーバーの追加ライセンスは必要ではありません。

Veritas Storage Foundation HA for Windows は、ノードごとにライセンスされます。同じローカル冗長性構成の例では、各サーバーに Veritas Storage Foundation HA for Windows を実行するためのライセンスが必要です。

Veritas Dynamic Multipathing Option は、サーバーと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サーバーで使用する場合にのみ必要です。



(注) バージョン 4.20 以降、Cisco Security Manager は VERITAS Infoscale 7.4 をサポートしています。

## 地理的冗長性 (DR) 構成のソフトウェア要件

地理的冗長性 (DR) 構成に Security Manager をインストールするには、次のソフトウェアが必要です。

- Cisco Security Management Suite 4.27
- Microsoft Windows Server 2019 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
- Veritas Storage Foundation HA/DR for Windows 6.0.1/6.0.2/6.1/Veritas InfoScale 7.0/7.2/7.4
  - Veritas InfoScale 7.4.2 以降は Windows Server 2019 をサポートしています。
  - Windows 2019 :  
Veritas Storage Foundation for Windows Version : 7.4.2
  - Windows 2016 :  
Veritas Storage Foundation for Windows Version : 7.4
- Veritas Volume Replicator Option
- Veritas Dynamic Multipathing Option

Security Manager は、HA/DR 構成のアクティブサーバーごとにライセンスされます。たとえば、サイト A にシングルノードクラスタ、サイト B にシングルノードクラスタが配置された地理的冗長性構成では、Security Manager のコピーを 1 つのみ購入する必要があります。これは、Security Manager は常に 1 台のサーバでのみアクティブになるためです。

Veritas Storage Foundation HA for Windows は、ノードごとにライセンスされます。2 台のサーバ (クラスタごとに 1 台) が配置された同じ地理的冗長性構成の例では、各サーバに Veritas Storage Foundation HA for Windows を実行するためのライセンスが必要です。

Veritas Volume Replicator Option は、ノードごとにライセンスされます。

Veritas Dynamic Multipathing Option は、サーバと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サーバで使用する場合にのみ必要です。

## クラスタリングが不要な複製のソフトウェア要件

クラスタリングが不要な地理的冗長性 (DR) 構成に Security Manager をインストールするには、次のソフトウェアが必要です。

- Cisco Security Management Suite 4.27
- 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
- Veritas Storage Foundation Basic for Windows 6.0.1/6.0.2/6.1/Veritas InfoScale 7.0/7.2/7.4

- Veritas InfoScale 7.4.2 以降は Windows Server 2019 をサポートしています。
- Windows 2019 :  
Veritas Storage Foundation for Windows Version : 7.4.2
- Windows 2016 :  
Veritas Storage Foundation for Windows Version : 7.4
- Veritas Volume Replicator Option
- Veritas Dynamic Multipathing Option

Security Manager は、HA/DR 構成のアクティブサーバーごとにライセンスされます。たとえば、プライマリサーバーとセカンダリサーバーの間で複製が実行される地理的冗長性構成では、Security Manager のコピーを 1 つのみ購入する必要があります、これは、Security Manager は常に 1 台のサーバーでのみアクティブになるためです。

Veritas Storage Foundation for Windows は、ノードごとにライセンスされます。2 台のサーバが配置された同じ地理的冗長性構成の例では、各サーバに Veritas Storage Foundation for Windows を実行するためのライセンスが必要です。

Veritas Storage Foundation Basic 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 は、最大 4 つのボリュームと連携し、無料でダウンロードできます。

Veritas Volume Replicator Option は、ノードごとにライセンスされます。

Veritas Dynamic Multipathing Option は、サーバと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サーバで使用する場合にのみ必要です。

## プリインストールワークシート

インストールを計画して設定中に必要な情報を収集するには、プリインストールワークシートを使用します。ここでは、次の内容について説明します。

- [ローカル冗長性構成のワークシート \(22 ページ\)](#)
- [地理的冗長性 \(DR\) 設定ワークシート \(24 ページ\)](#)

## ローカル冗長性構成のワークシート

ローカル冗長性 HA 構成に Security Manager をインストールする前に、表に記載されたインストールの完了に役立つ情報を書き留めます。

表 2: ローカル冗長性構成のプリインストールワークシート

情報	プライマリサイト
共有ディスクグループ名	datadg

情報	プライマリサイト	
共有ボリューム名	cscopx	
Security Manager データのドライブ文字		
イベントデータの共有ディスクグループ名 <sup>1</sup>	datadg_evt	
イベントデータの共有ボリューム名 <sup>2</sup>	cscopx_evt	
Security Manager イベントデータのドライブ文字 <sup>3</sup>		
クラスタ名	CSManager_Primary	
クラスタ ID	0 <sup>4</sup>	
Security Manager 仮想 IP アドレス/サブネットマスク		
クラスタサービスの仮想 IP アドレス/サブネットマスク <sup>5</sup>		
	プライマリサーバー	セカンダリサーバー
ホスト名		
パブリック ネットワーク インターフェイス #1 と IP アドレス/サブネットマスク		
パブリック ネットワーク インターフェイス #2 <sup>6</sup> および IP アドレス/サブネットマスク		
プライベートクラスタ相互接続 #1		
プライベートクラスタ相互接続 #2		

<sup>1</sup> 任意：別に保存されたイベントデータが必要な場合は、これらのフィールドを使用します。

<sup>2</sup> 任意：別に保存されたイベントデータが必要な場合は、これらのフィールドを使用します。

<sup>3</sup> 任意：別に保存されたイベントデータが必要な場合は、これらのフィールドを使用します。

<sup>4</sup> 0～255の整数で、同一サブネット上のクラスタで一意にする必要があります。

<sup>5</sup> これは、Security Manager 仮想 IP アドレス/サブネットマスクと同じ値です。

<sup>6</sup> 冗長性を確保するためにパブリックネットワークへのアクセスに2番目のNICを使用する場合に必要です。

7

<sup>7</sup> 1. 任意：別に保存されたイベントデータが必要な場合は、これらのフィールドを使用します。

2. 0～255の整数で、同一サブネット上のクラスタで一意にする必要があります。

3. これは、Security Manager 仮想 IP アドレス/サブネットマスクと同じ値です。

4. 冗長性を確保するためにパブリックネットワークへのアクセスに2番目のNICを使用する場合に必要です。

## 地理的冗長性 (DR) 設定ワークシート

地理的冗長性 (DR) 構成に Security Manager をインストールする場合は、表に記載されたインストールの完了に役立つ情報を書き留めます。

表 3: 地理的冗長性 (DR) 構成のプリインストールワークシート

情報	プライマリサイト		セカンダリサイト	
ディスクグループ	datadg		datadg	
データボリューム	cscopx		cscopx	
Security Manager のドライブ文字				
イベントデータのディスクグループ <sup>8</sup>	datadg_evt		datadg_evt	
イベントデータのデータボリューム	cscopx_evt		cscopx_evt	
イベントデータのドライブ文字				
Storage Replicator Log ボリューム	data_srl		data_srl	
複製されたデータセット	CSM_RDS			
複製されたボリュームグループ	CSM_RVG			
クラスタ名	CSManager_Primary		CSManager_Secondary	
クラスタ ID	0 <sup>9</sup>		1 <sup>10</sup>	
Security Manager 仮想 IP アドレス/サブネットマスク				
複製仮想 IP アドレス/サブネットマスク				
クラスタサービスの仮想 IP アドレス/サブネットマスク <sup>1112</sup>				
	プライマリサーバー	セカンダリサーバー	プライマリサーバー	セカンダリサーバー
ホスト名				
パブリック ネットワーク インターフェイス #1 と IP アドレス/サブネットマスク				
パブリック ネットワーク インターフェイス #2 と IP アドレス/サブネットマスク <sup>13</sup>				
プライベートクラスタ相互接続 #1 <sup>14</sup>				

情報	プライマリサイト	セカンダリサイト
プライベートクラスタ相互接続 #2 <sup>15</sup>		

<sup>8</sup> 任意：別に保存されたイベントデータが必要な場合は、これらのフィールドを使用します。

<sup>9</sup> 0～255 の整数で、同一サブネット上のクラスタで一意にする必要があります。

<sup>10</sup> 0～255 の整数で、同一サブネット上のクラスタで一意にする必要があります。

<sup>11</sup> 2 台のサーバーまたは複数のアダプタを使用してパブリックネットワークにアクセスするクラスタでのみ必要です。1つのネットワークアダプタのみを使用してパブリックネットワークにアクセスする単一サーバクラスタでは、このアダプタの固定 IP アドレスを使用できます。

<sup>12</sup> これは、Security Manager 仮想 IP アドレス/サブネットマスクと同じ値です。

<sup>13</sup> 冗長性を確保するためにパブリックネットワークへのアクセスに 2 番目の NIC を使用する場合に必要です。

<sup>14</sup> 2 台のサーバーを使用するクラスタでのみ必要です。

<sup>15</sup> 2 台のサーバーを使用するクラスタでのみ必要です。

16

<sup>16</sup> 1. 任意：別に保存されたイベントデータが必要な場合は、これらのフィールドを使用します。

2. 0～255 の整数で、同一サブネット上のクラスタで一意にする必要があります。

3. 2 台のサーバーまたは複数のアダプタを使用してパブリックネットワークにアクセスするクラスタでのみ必要です。1つのネットワークアダプタのみを使用してパブリックネットワークにアクセスする単一サーバクラスタでは、このアダプタの固定 IP アドレスを使用できません。

4. これは、Security Manager 仮想 IP アドレス/サブネットマスクと同じ値です。

5. 冗長性を確保するためにパブリックネットワークへのアクセスに 2 番目の NIC を使用する場合に必要です。

6. 2 台のサーバーを使用するクラスタでのみ必要です。







## 第 4 章

# 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 \(27 ページ\)](#)
- [Microsoft Windows Server のインストール \(28 ページ\)](#)
- [外部ストレージへのサーバの接続 \(29 ページ\)](#)
- [Veritas 製品のインストール \(29 ページ\)](#)
- [ブートディスクのミラーリング \(任意\) \(30 ページ\)](#)
- [Veritas Volume Manager の設定タスク \(30 ページ\)](#)
- [Security Manager のインストール \(33 ページ\)](#)
- [Veritas Volume Replicator タスク \(41 ページ\)](#)
- [作業ボリュームに対する権限の更新 \(43 ページ\)](#)
- [Veritas Cluster Server タスク \(46 ページ\)](#)

## 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 3: シングルノードサイトのイーサネット接続](#)または[図 4: デュアルノードサイトのイーサネット接続とストレージ接続](#)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 チューニング (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 4: デュアルノードサイトのイーサネット接続とストレージ接続](#)に従って、サーバ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 4: Veritas ソフトウェアコンポーネントを参照してください。

表 4: Veritas ソフトウェアコンポーネント

Veritas 製品/コンポーネント	シングルローカルクラスタ	デュアル地理的クラスタ	クラスタリングが不要な複製
Storage Foundation for Windows	—	—	必須
Veritas Storage Foundation HA for Windows version 6.0.1/6.0.2/6.1/7.4/7.4.2 Veritas InfoScale 7.0/7.2/7.4/7.4.2	必須	必須	—
Volume Replicator Option	不要	必須	必須
Global Cluster Option	不要	必須	—
Dynamic Multipathing Option	(注) を参照 <sup>17</sup>	(注) を参照	(注) を参照
Veritas Enterprise Administrator (GUI) <sup>18</sup>	必須	必須	必須
Cluster Manager (GUI) 2	オプション	オプション	—

<sup>17</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。

<sup>18</sup> 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 アプリケーションに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 \(複製なし\) \(30 ページ\)](#)
- [プライマリサーバ \(複製あり\) \(31 ページ\)](#)
- [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 \(32 ページ\)](#)

### 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ー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ー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ー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ー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 \(34 ページ\)](#)
- [セカンダリサーバへの Security Manager のインストール \(37 ページ\)](#)

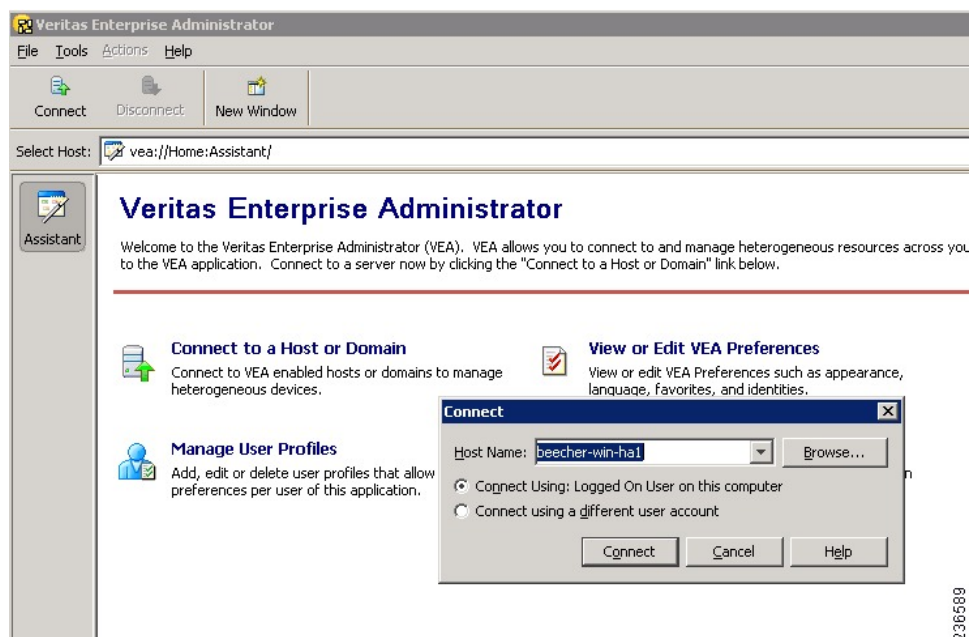
## プライマリサーバへの Security Manager のインストール

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。

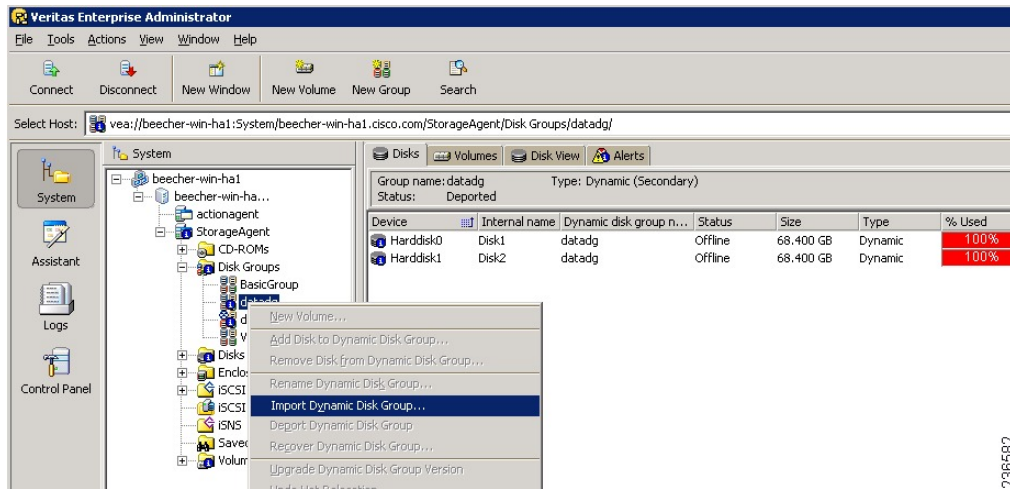
図 236589



236589

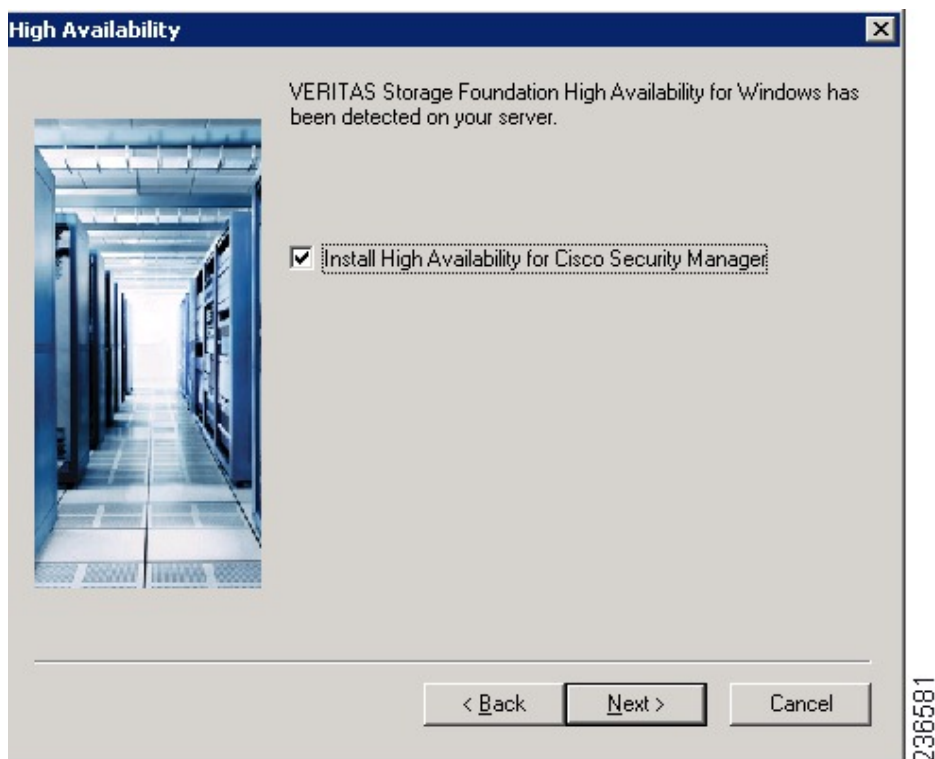
- ステップ 2** datadg ディスクグループを右クリックし、[ダイナミックディスクグループのインポート (Import Dynamic Disk Group)] を選択します。





236582

- 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 \(22 ページ\)](#) または [地理的冗長性 \(DR\) 設定ワークシート \(24 ページ\)](#) を参照してください。
- ステップ 7** 次の HA 固有の項目に注意しながら『Security Manager Installation Guide』[英語] に従って Security Manager をインストールします。
- a) HA 用に Security Manager をインストールするかどうかを尋ねるプロンプトが表示されたら、ボックスをオンにして yes を指定します。



- b) インストールディレクトリの入力を求められたら、[<選択されたドライブ文字>:\Program Files\CSCOpX] を指定します。
- c) データベースパスワードの指定を求められたら、適切なパスワードを選択し、忘れないようにします。HA/DR 構成のすべての Security Manager サーバーにこのパスワードを使用します。

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

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

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

**ステップ 10** online.pl スクリプトを使用して Security Manager を起動します。詳細については、[Security Manager の手動での起動、停止、フェールオーバー \(67 ページ\)](#) 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 \(67 ページ\)](#) 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に関連付けられ、Security Manager をアップグレードまたはアンインストールする場合に限り、再利用されます。このスペアボリュームには、空のデータベース (~2 GB) で Security Manager アプリケーションを保持するのに十分な容量が必要です。十分な領域が (可能であれば別のディスク グループで) 使用可能な場合は、**datadg** ディスクグループにスペアボリュームを作成できます。

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

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

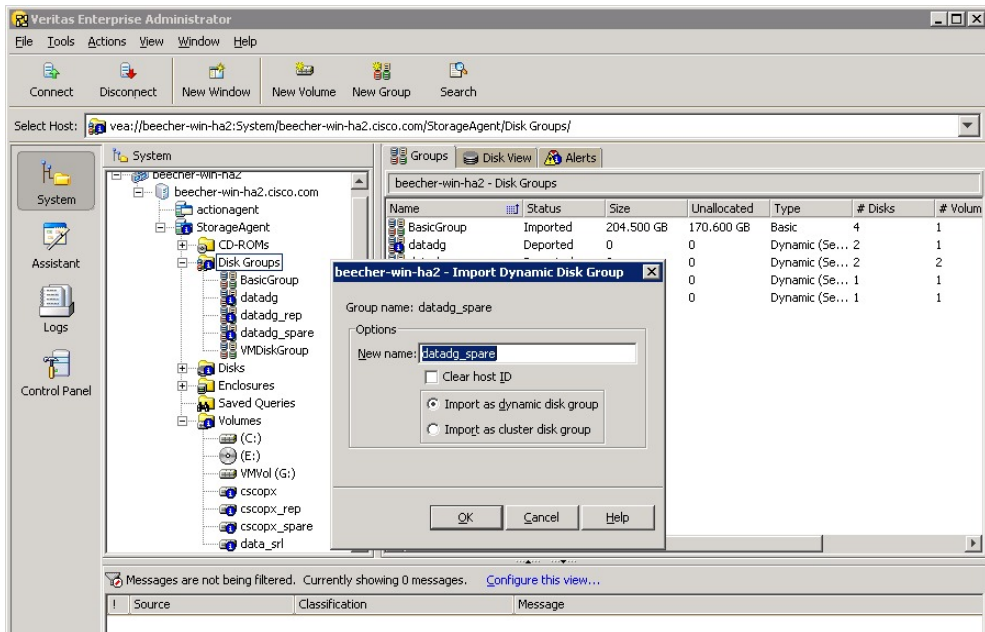
図 236588



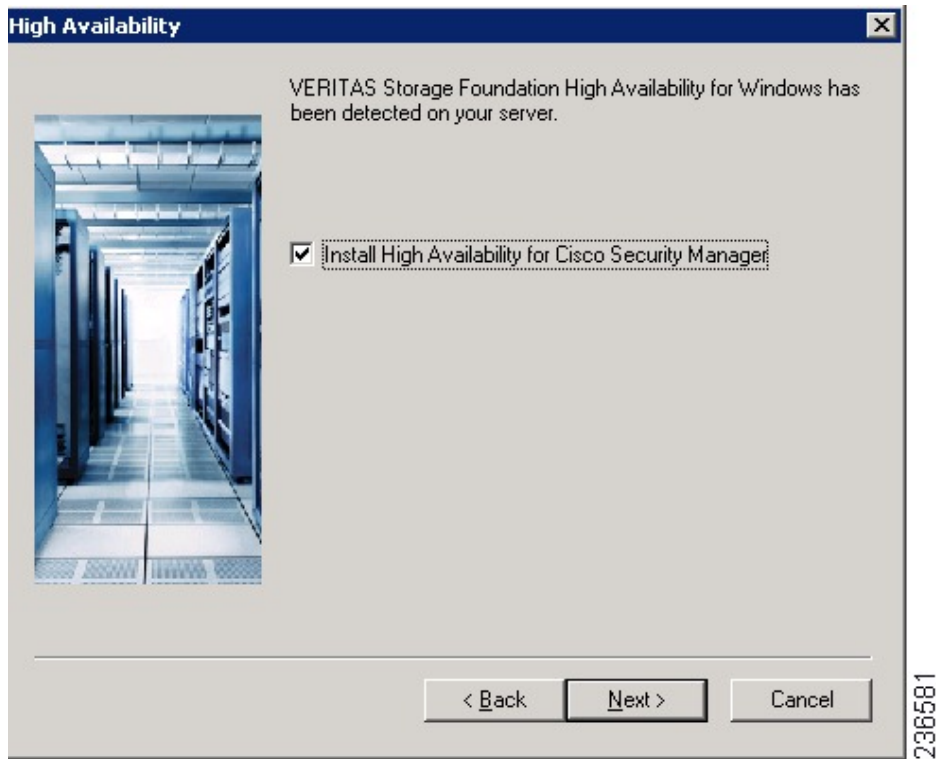
- ステップ 2** **datadg\_spare** ディスクグループを右クリックし、[ダイナミックディスクグループのインポート (Import Dynamic Disk Group)] を選択します。

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

図 236583



- ステップ 4** [システム (System) ] の [ボリューム (Volumes) ] フォルダを展開します。
- ステップ 5** cscopx\_spare ボリュームを右クリックし、[ファイルシステム (File System) ] > [ドライブ文字とパスの変更 (Change Drive Letter and Path) ] を選択します。
- ステップ 6** 目的のドライブ文字を cscopx\_spare ボリュームに割り当て、[OK (OK) ] をクリックします。ドライブの割り当てについては、[ローカル冗長性構成のワークシート \(22 ページ\)](#) または [地理的冗長性 \(DR\) 設定ワークシート \(24 ページ\)](#) を参照してください。
- ステップ 7** 次の HA 固有の項目に注意しながら『Security Manager Installation Guide』[英語]に従って Security Manager をインストールします。
- a) HA 用に Security Manager をインストールするかどうかを尋ねるプロンプトが表示されたら、ボックスをオンにして yes を指定します。



- b) インストールディレクトリの入力を求められたら、[<選択されたドライブ文字>\Program Files\CSCOpX] を指定します。
- c) データベースパスワードの指定を求められたら、プライマリ サーバに選択したのと同じパスワードを選択します。

(注) Security Manager のインストールの終了に近づくとき、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 \(67 ページ\)](#) 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>: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 \(67 ページ\)](#) を参照してください。

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

## セカンダリ HA サーバーでの手動によるサービスの開始

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

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

```
<NMSROOT>\setup\support\resetcasuser.exe
```

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

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

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

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

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

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

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

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

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

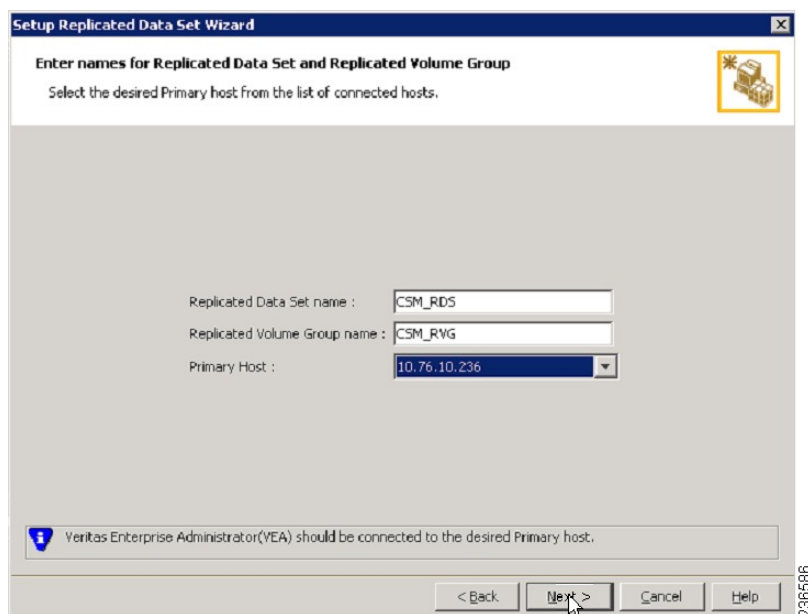
例 : C:\Progra~2\CSCOpX\bin\perl C:\Progra~2\CSCOpX\bin\ChangeService2Casuser.pl casuser admin123

# Veritas Volume Replicator タスク

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

複製を設定するには、次の手順に従います。

- ステップ 1 VEA GUI を使用して、プライマリおよびセカンダリ ホストに接続します。
- ステップ 2 *datadg* ディスクグループがプライマリサーバーとセカンダリサーバーの両方にインポートされていることを確認します。
- ステップ 3 [表示 (View)] > [接続 (Connection)] > [複製ネットワーク (Replication Network)] を選択します。
- ステップ 4 ツリーから [複製ネットワーク (Replication Network)] を選択し、ツールバーから [複製したデータセットを設定 (Setup Replicated Data Set)] ウィザードを選択します。ウィザードの最初のパネルで次の項目を指定します。
  - [複製データセット名 (Replicated Data Set Name)] : **CSM\_RDS**
  - [複製ボリュームグループ名 (Replicated Volume Group name)] : **CSM\_RVG**
  - ドロップダウンリストからプライマリホストを選択します。



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

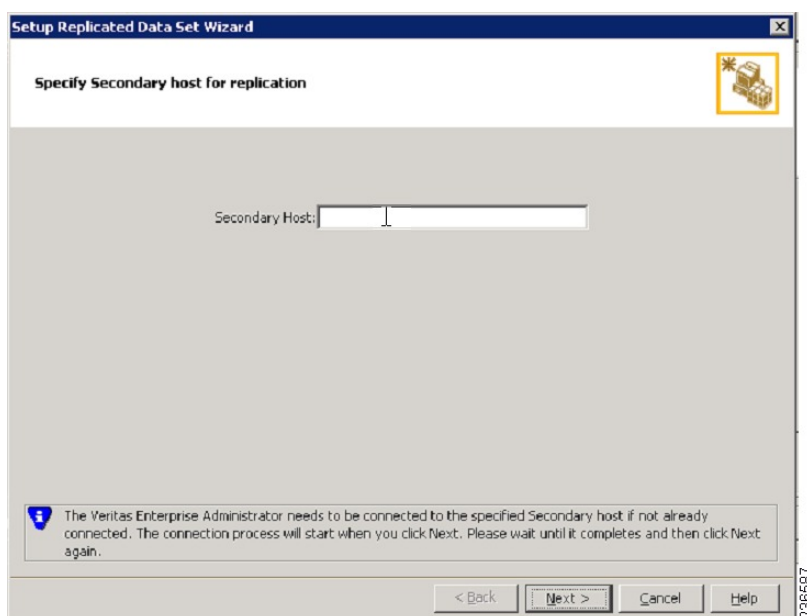
**ステップ 6** [次へ (Next) ] をクリックします。data\_srl が他に利用できる唯一のボリュームの場合、レプリケーターログのストレージボリュームとして自動的に認識されます。複数の追加ボリュームを使用できる場合、[ストレージレプリケーターログ (Storage Replicator Log) ] パネルが表示されます。次を指定します。

- [レプリケーターログのボリューム (Volume for the Replicator Log) ] : data\_srl

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

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

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



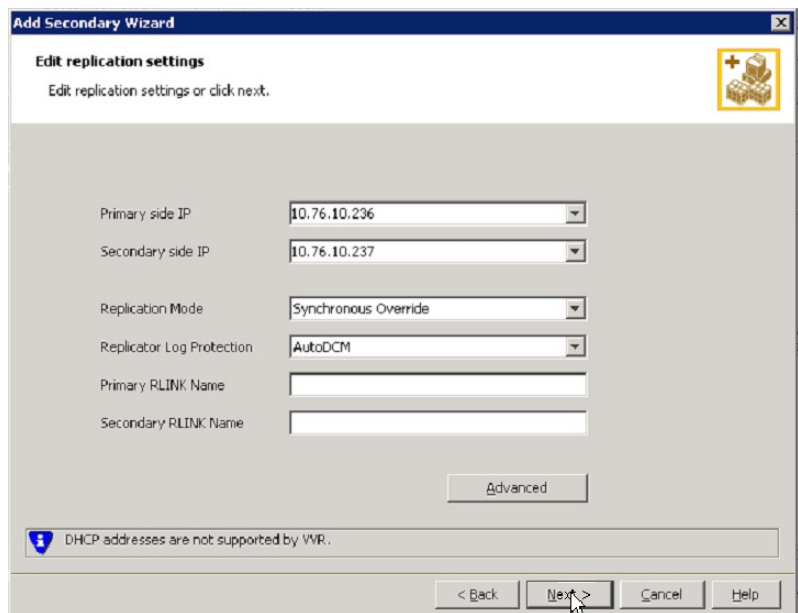
**ステップ 10** [次へ (Next) ] をクリックし、[レプリケーション設定の編集 (Edit replication settings) ] パネルで次の項目を指定します。

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

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



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



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

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

## 作業ボリュームに対する権限の更新

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

ここでは、次の内容について説明します。

- [共有ストレージを使用する場合の権限の更新 \(43 ページ\)](#)
- [複製を使用する場合の権限の更新 \(44 ページ\)](#)

### 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 \(67 ページ\)](#) 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、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 \(67 ページ\)](#) 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（46 ページ）](#)

[デュアル地理的クラスタ構成（50 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（46 ページ）](#)
- [アプリケーションサービス グループの作成（47 ページ）](#)
- [ClusterService グループの作成（49 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、CSManager リソースタイプをインポートします。\$VCS\_ROOT\cluster server\conf\config の下にある CSManagerTypes.cf ファイルを参照し、[インポート (Import)] をクリックします。

---

## アプリケーション サービス グループの作成

アプリケーション サービス グループを作成するには、次の手順に従います。



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

**ステップ 1** APP というサービスグループを追加します。

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

RVG プライマリ リソースを追加します。

- [リソース名 (Resource name) ] = **APP\_RVGPrimary**
- [リソースタイプ (Resource Type) ] = **RVGPrimary**
- [RvgResourceName (RvgResourceName) ] = **APP\_RVG**

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

MountV リソースを追加します。

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

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

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

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

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

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

Proxy リソースを追加します。

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

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

IP リソースを追加します。

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

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

CSManager リソースを追加します。

- [リソース名 (Resource name) ] = **APP\_CSManager**
- [リソースタイプ (Resource Type) ] = **CSManager**
- [PathName (PathName) ] = <選択されたドライブ文字>:\Program Files\CSCOpX
- [EventIPAddress (EventIPAddress) ] = APP\_IP で使用されているものと同じ IP アドレス
- [CertificateDir (CertificateDir) ] = この属性の説明については、[SSL 用のセキュリティ証明書 \(66 ページ\)](#) 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 (図 12: リソースビュー: APP グループ (デュアルクラスター、シングルノード) (93 ページ) を参照)。

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

リソースをリンクするには、次の手順に従います。

- a) 親リソースを右クリックし、[リンク (Link)] を選択します。  
[リンクリソース (Link Resources)] ダイアログボックスが表示されます。
- b) 子リソースを選択し、[OK (OK)] をクリックします。  
選択したリソースがリンクされます。

## ClusterService グループの作成

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



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



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

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

**ClusterService** というサービスグループを追加します。

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

NIC リソースを追加します。

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

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

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

IP リソースを追加します

- [リソース名 (Resource name)] = **VCS\_IP**

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

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

wac リソースを追加します。

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

**ステップ 5** 次の表の定義に従ってリソースをリンクします (図 12: 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) (93 ページ) 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。

- 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。
- 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](#) (51 ページ)
- [ClusterService グループの作成](#) (49 ページ)
- [複製サービスグループの作成](#) (53 ページ)
- [アプリケーション サービス グループの作成](#) (47 ページ)
- [クラスタレベル設定の作成](#) (62 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** ClusterManager を使用し、[ファイル (File)] > [インポートタイプ (Import Types)] を選択して、CSManager リソースタイプをインポートします。\$VCS\_ROOT\cluster server\conf\config の下にある CSManagerTypes.cf ファイルを参照し、[インポート (Import)] をクリックします。
- ステップ 5** セカンダリクラスタに対してステップ 3 と 4 を繰り返します。

## ClusterService グループの作成

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



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



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

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

**ClusterService** というサービスグループを追加します。

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

NIC リソースを追加します。

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

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

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

IP リソースを追加します

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

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

wac リソースを追加します。

- [リソース名 (Resource name) ] = **wac**

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

**ステップ 5** 次の表の定義に従ってリソースをリンクします (図 12: リソースビュー: APP グループ (デュアルクラスター、シングルノード) (93 ページ) 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。

- 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。
- 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ーとセカンダリクラスターの両方で次の手順を実行します。

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

APPRep というサービスグループを追加します。

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

Proxy リソースを追加します。

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

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

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

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

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

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

- [リソース名 (Resource name)] = **APP\_RVG**
- [リソースタイプ (Resource Type)] = **VvrRvg**
- [RVG (RVG)] = **CSM\_RVG**
- [VMDGResName (VMDGResName)] = **datadg**
- [IPResName (IPResName)] = **VVR\_IP**

**ステップ 6** 次の表の定義に従ってリソースをリンクします (図 13: 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) (94 ページ) を参照)。

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

リソースをリンクするには、次の手順に従います。

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

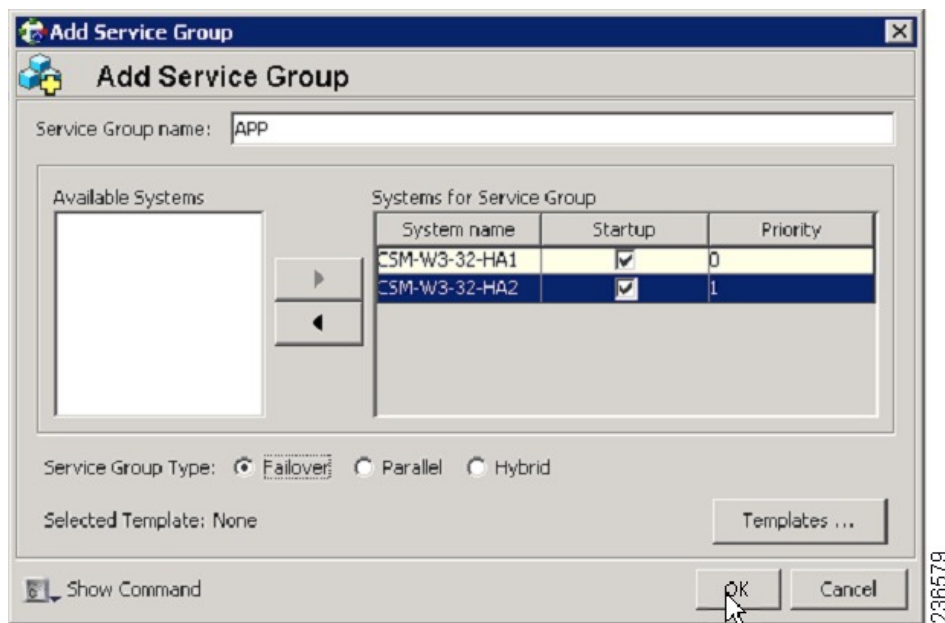
- b) 子リソースを選択し、[OK (OK)] をクリックします。  
 選択したリソースがリンクされます。

## アプリケーション サービス グループの作成

アプリケーション サービス グループを作成するには、次の手順に従います。

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

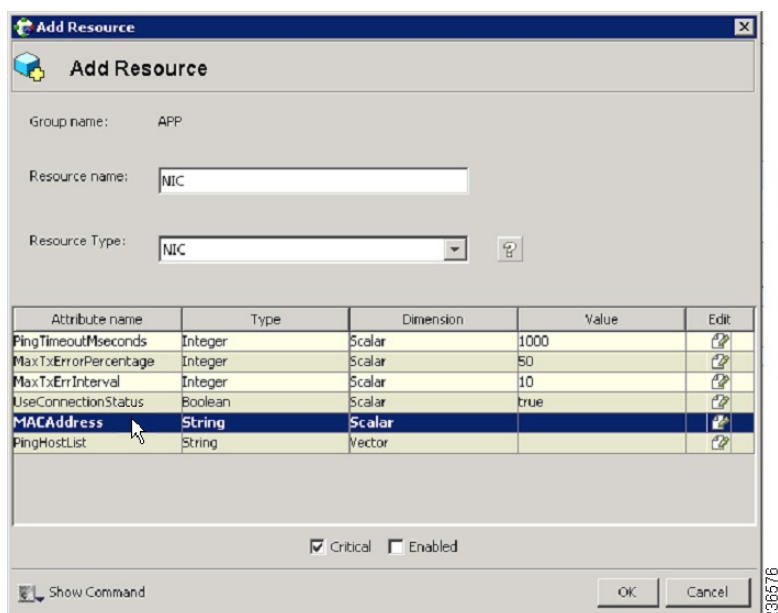
APP というサービスグループを追加し、このサービスグループの両方のサーバを含めて（各サーバの [スタートアップ (Startup)] オプションをオンにする）、サービスグループタイプを [フェールオーバー (Failover)] にします。



- ステップ 2** [APP (APP)] サービスグループを右クリックし、[リソースの追加 (Add Resource)] を選択します。  
 NIC リソースを追加し、[クリティカル (Critical)] および [有効 (Enabled)] チェックボックスをオンにします。

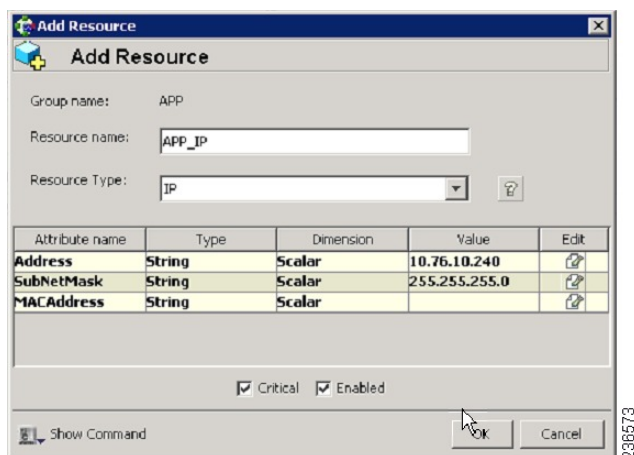
- [リソース名 (Resource name)] = NIC
- [リソースタイプ (Resource Type)] = NIC
- [MACAddress (MACAddress)] = <Security Manager アプリケーションにアクセスするために使用する NIC の MAC アドレス> (クラスタ内のサーバーごとに一意に定義されます)。

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



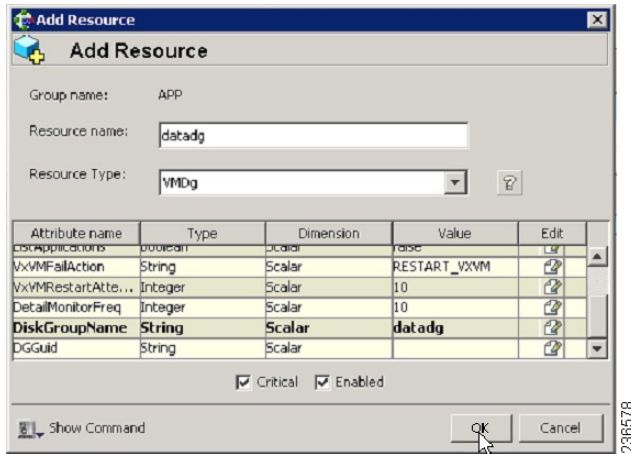
**ステップ 3** [APP (APP) ] サービスグループを右クリックし、[リソースの追加 (Add Resource) ] を選択します。  
IP リソースを追加し、[クリティカル (Critical) ] および [有効 (Enabled) ] チェックボックスをオンにします。

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



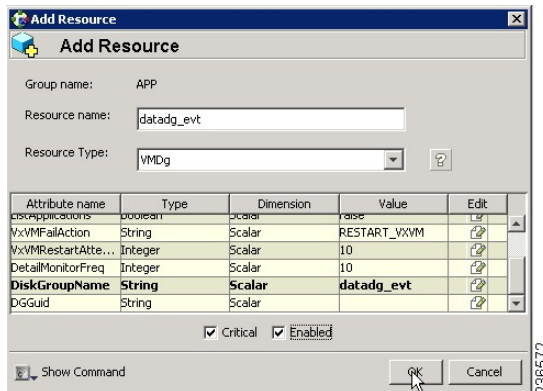
**ステップ 4** [APP (APP) ] サービスグループを右クリックし、[リソースの追加 (Add Resource) ] を選択します。  
VMDg リソースを追加し、[クリティカル (Critical) ] および [有効 (Enabled) ] チェックボックスをオンにします。

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



**ステップ 5** [VMDg (VMDg) ] リソースグループを右クリックし、[リソースの追加 (Add Resource) ] を選択します。  
datadg\_evt リソースを追加し、[クリティカル (Critical) ] および [有効 (Enabled) ] チェックボックスをオンにします。

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



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

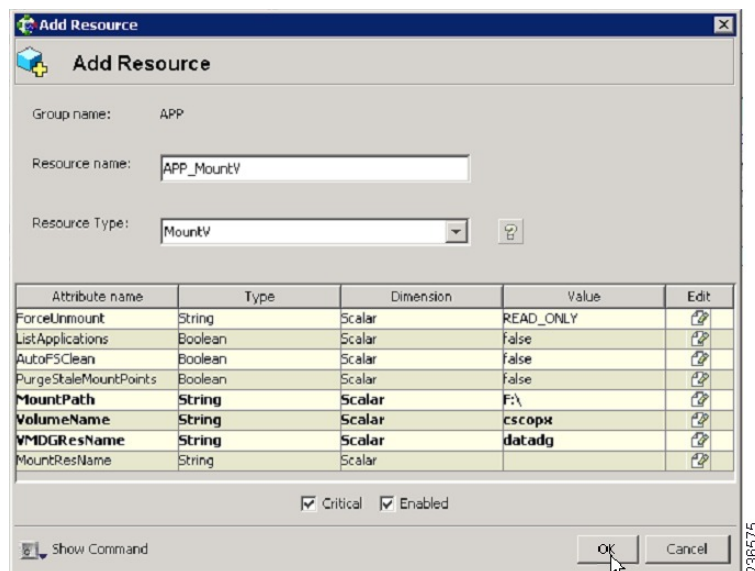
MountV リソースを追加し、[クリティカル (Critical)] および [有効 (Enabled)] チェックボックスをオンにします。

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

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

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

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



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



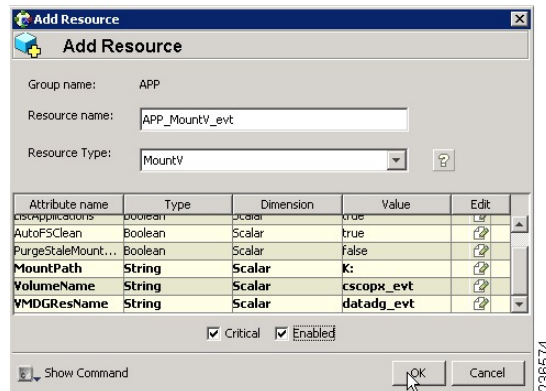
MountV\_evt リソースを追加し、[クリティカル (Critical)] および [有効 (Enabled)] チェックボックスをオンにします。

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

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

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

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

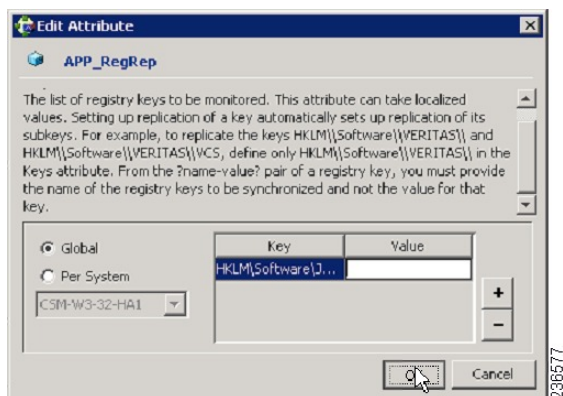


**ステップ 8** [APP (APP)] サービスグループを右クリックし、[リソースの追加 (Add Resource)] を選択します。

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

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

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

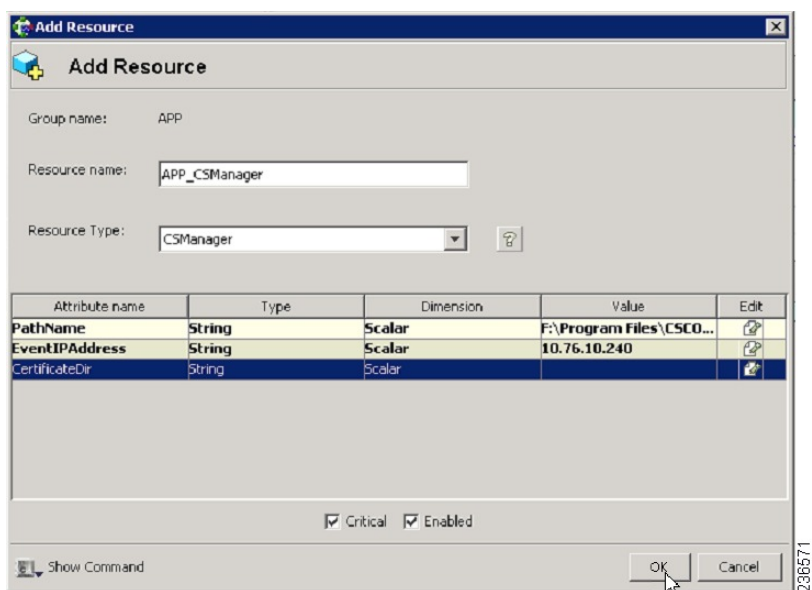


- (注) Security Manager は、サーバーレジストリの HKEY\_LOCAL\_MACHINE\SOFTWARE\JavaSoft\Prefs\vms の下にクライアント ユーザー プリファレンスを保存します。レジストリ複製エージェント (RegRep) は、アクティブサーバの指定レジストリの場所の変更をモニタし、フェールオーバーの発生時にセカンダリサーバにこれらの変更を同期化します。

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

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

- [リソース名 (Resource name) ] = APP\_CSManager
- [リソースタイプ (Resource Type) ] = CSManager
- [PathName (PathName) ] = <選択されたドライブ文字>:\Program Files\CSCOPx\ (グローバル属性として定義)
- [EventIPAddress (EventIPAddress) ] = APP\_IP で使用されているものと同じ IP アドレス (グローバル属性として定義)
- [CertificateDir (CertificateDir) ] = この属性の説明については、[SSL 用のセキュリティ証明書 \(66 ページ\)](#) を参照してください。

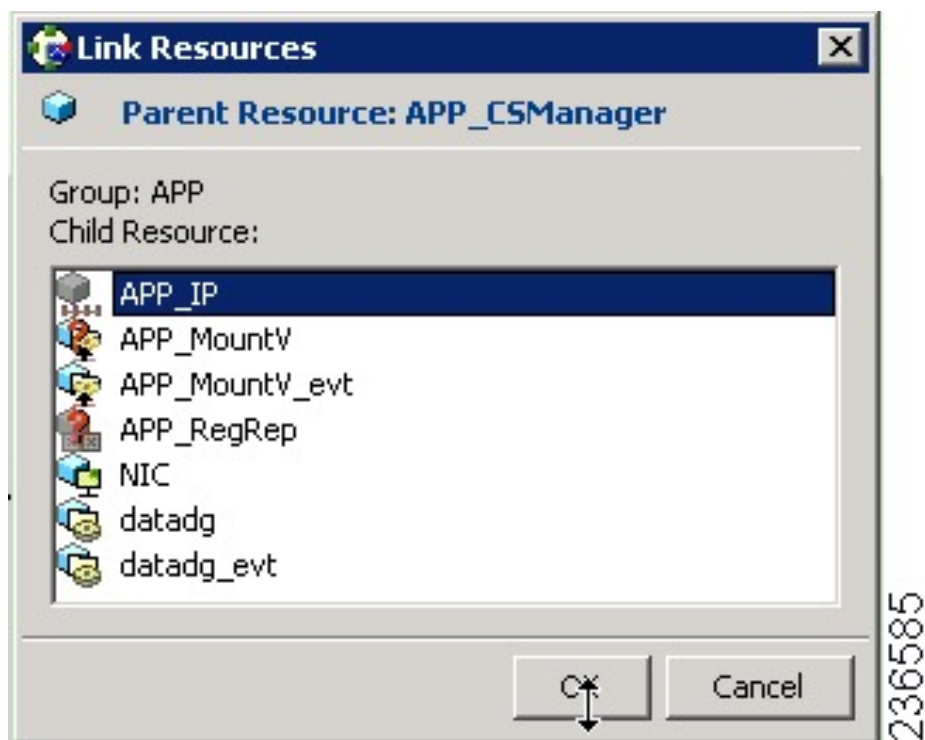


**ステップ 10** 次の表の定義に従ってリソースをリンクします (図 12: リソースビュー: APP グループ (デュアルクラスタ、シングルノード) (93 ページ) を参照)。

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。

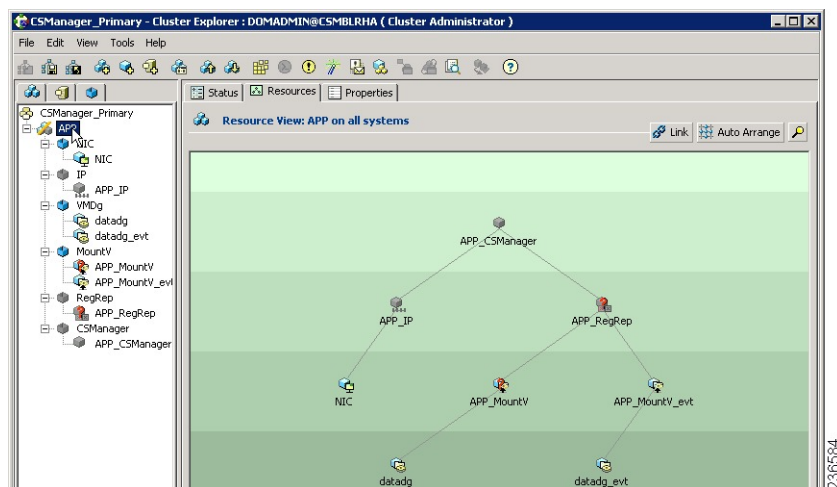
- 親リソースを右クリックし、[リンク (Link)] を選択します。  
[リンクリソース (Link Resources)] ダイアログボックスが表示されます。



- b) 子リソースを選択し、[OK (OK)] をクリックします。

選択したリソースがリンクされます。

すべてのリンクが作成されると、リソースビューは次のように表示されます。



## クラスタレベル設定の作成

クラスタレベル設定を作成するには、次の手順に従います。

- 
- ステップ 1** APPrep サービスグループの親として APP サービスグループをオンライン ローカル ファーム依存関係にリンクします。プライマリクラスタとセカンダリクラスタの両方でこの手順を実行します。
- ステップ 2** クラスタプロパティで、VCS\_IP リソースで使ったのと同じ 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。

[図 15: サービスグループビュー \(デュアルクラスタ、シングルノード\) \(96 ページ\)](#) を参照してください。

---





## 第 5 章

# メンテナンス作業

この章では、HA/DR 構成で使用される Security Manager に関連するメンテナンス作業について説明します。この章は、次の内容で構成されています。

- [VCS 動作のカスタマイズ \(65 ページ\)](#)
- [SSL 用のセキュリティ証明書 \(66 ページ\)](#)
- [Security Manager の手動での起動、停止、フェールオーバー \(67 ページ\)](#)
- [Cisco Secure ACS と Security Manager の統合 \(70 ページ\)](#)
- [Security Manager のアップグレード \(71 ページ\)](#)
- [Security Manager のバックアップ \(72 ページ\)](#)
- [Security Manager のアンインストール \(72 ページ\)](#)
- [非 HA Security Manager の HA への移行 \(73 ページ\)](#)

## VCS 動作のカスタマイズ

VCS では、リソース障害への対応など、VCS 動作を制御するための大量の変数をサポートします。ここでは、このマニュアルの説明に従ってデフォルトインストールを行った場合のフェールオーバー動作の一部を示します。『*Veritas Cluster Server User's Guide*』[英語]の説明に従って、このような動作の制御を確認する必要があります。

- Security Manager が失敗すると、VCS は同じサーバー上でアプリケーションを再起動しようとしません。代わりに、VCS は、クラスタ内のスタンバイサーバーにフェールオーバーします。ただし、リソースレベル属性 `RestartLimit` を使用して、エージェントがリソースの障害状態として宣言する前にリソースを再起動しようとする回数を制御できます。
- 特定のサーバーで最初に Security Manager アプリケーションをオンラインにしようとする時、VCS はリソースを一度だけオンラインにしようとします。 `OnlineRetryLimit` リソースレベル属性では、最初の試行が失敗した場合にオンラインエントリーポイントを再試行する回数を指定します。
- デフォルトでは、VCS は 60 秒ごとに Security Manager アプリケーション モニター スクリプトを実行します。これは、アプリケーションの障害を検出するのに最大 60 秒かかる可能性があることを意味します。 `MonitorInterval` は調整できるリソースレベル属性です。

- デュアルクラスタを使用する場合、クラスタ間のフェールオーバーは、デフォルトでは手動操作です。これは、両方のクラスタで同時にアプリケーションを実行するのを回避します。クラスタ間の通信が失われた場合（冗長パスが地理的に離れたデータセンター間にならない場合に発生しやすくなります）、VCSはリモートクラスタに障害が発生したかどうか、または通信に問題があるかどうかを判断できません。クラスタ間の自動フェールオーバーが必要な場合は、APP サービス グループの ClusterFailOverPolicy 属性で設定できます。

## SSL用のセキュリティ証明書

Security Manager では、サーバーおよびクライアントブラウザまたはアプリケーション間における Secure Socket Layer (SSL) の暗号化の使用を設定できます。SSL暗号化には、サーバにおけるデジタル証明書の作成と配置が必要です。デジタル証明書に含まれている ID 情報の一部は、Common Services Web GUI に表示される Common Name (CN) または「Host Name」です。複数のサーバおよび対応するホスト名が存在する HA/DR 構成では、アプリケーションへのアクセスに使用されるホスト名または IP アドレスに一致する証明書を保持するために、特別な手順が必要になることがあります。

シングルクラスタの場合、単一の仮想 IP アドレスまたは仮想ホスト名でアプリケーションにアクセスします。この場合は、仮想 IP アドレスまたは仮想ホスト名と同じ CN で証明書を作成する必要があります。仮想 IP または仮想ホスト名のアドレスはアプリケーションを実行するクラスタ内のサーバに関係なく有効であるため、フェールオーバーの発生時にデジタル証明書ファイルを更新する必要はありません。

ただし、デュアル地理的クラスタ構成の場合、各クラスタにアプリケーションに関連付けられた独自の IP アドレスまたはホスト名があります。そのため、デジタル証明書ファイルがあるクラスタと一致するように作成されている場合、アプリケーションが他のクラスタにフェールオーバーすると一致しなくなります。この場合は、クラスタ間のフェールオーバーの発生時に、他のクラスタに一致するようにデジタル証明書ファイルを更新する必要があります。



- (注) アプリケーションにアクセスするために仮想ホスト名を使用する場合は、代わりに DNS 更新を使用すると、クラスタ間フェールオーバーのために証明書を更新する必要がなくなります。クラスタ間フェールオーバーが発生すると、DNS は仮想ホスト名に関連付けられた新しい IP アドレスで更新されます。クライアントは常に同じ仮想ホスト名を使用してアプリケーションにアクセスするため、証明書ファイルを更新する必要はありません。

VCS 用の Security Manager エージェントは、アプリケーションを開始する前に非共有の複製されていないローカルディレクトリに保存されているデジタル証明書ファイルを自動的にコピーできます。ただし、クラスタ内の各サーバでこのディレクトリに適切なファイルを配置する必要があります。ディレクトリは CertificateDir パラメータを使用してエージェントに指定されます。

各サイトにサーバが 1 台ある地理的冗長性 (DR) 構成の場合は、よりシンプルなオプションを使用できます。サーバのホスト名に基づいて証明書ファイルを再生成するようにエージェントを設定できます。これは、仮想 IP アドレスまたは仮想ホスト名がないため動作します。エー



ジェントをこのように動作するように設定するには、CertificateDir パラメータの値にキーワード regen を指定します。

Security Manager をインストールすると、サーバのローカルホスト名に一致する自己署名証明書がデフォルトで作成されます。構成に応じて、仮想 IP アドレスまたは仮想ホスト名に一致する自己署名証明書を生成するには、次の手順に従います。

- 
- ステップ 1** サーバー (<http://<ホスト名または IP アドレス>:1741>) の Web ブラウザインターフェイスにログインします。
- ステップ 2** 次のように自己署名証明書セットアップ画面にアクセスします。
- Cisco Security Management Suite のホームページで、[サーバー管理 (Server Administration)] をクリックします。
  - [サーバー管理 (Server Admin)] ページのメニューから、[サーバー (Server)] > [単一サーバー管理 (Single Server Management)] > [証明書の設定 (Certificate Setup)] を選択します。
- ステップ 3** 証明書のフィールドに入力し、[CN (CN)] フィールドで仮想 IP アドレスまたは仮想ホスト名を指定し、[適用 (Apply)] をクリックします。

次の証明書関連ファイルは、NMSROOT\MDC\Apache\conf\ssl ディレクトリに生成されます。

- server.key
- server.crt
- server.pk8
- server.csr
- openssl.conf
- chain.cer

シングルクラスタを使用する場合は、これ以上の処理は必要ありません。ただし、各クラスタ内に複数のサーバが配置されたデュアル地理的クラスタ構成を使用する場合は、クラスタ内の各サーバでこれらの証明書関連ファイルを非共有の複製されていないローカルディレクトリにコピーする必要があります。次に、セカンダリクラスタに対して同じ手順を実行します。ただし、今度はセカンダリクラスタの仮想 IP アドレスまたは仮想ホスト名を指定します。CSManager リソースを定義する場合、選択された非共有の複製されていないローカルディレクトリを **CertificateDir** 属性に指定します。エージェントは、フェールオーバー後、アプリケーションを開始する前に適切な作業ディレクトリに自動的に証明書ファイルをコピーします。

---

## Security Manager の手動での起動、停止、フェールオーバー

非 HA/DR 構成では、通常、Windows Services アプリケーションまたはコマンドラインのそれに相当する net start および net stop を使用して Security Manager を起動および停止します。ただ

し、HA/DR 構成では、この方法を使用しないでください。HA/DR 構成では、Security Manager を起動および停止するための特定のスクリプトが提供されています。これらのスクリプトでは、異なるサーバで Security Manager を起動する場合に必要な追加手順を実行します。これらのスクリプトおよびその他のスクリプトは VCS 用の Security Manager エージェントを構成します。エージェントを使用すると、VCS で Security Manager を制御およびモニタできます。VCS を使用しない場合は、これらのスクリプトを使用して、Security Manager を手動で起動および停止できます。

この項では、次のトピックを扱います。

- [VCS の場合 \(68 ページ\)](#)
- [VCS 以外の場合 \(68 ページ\)](#)

## VCS の場合

VCS を使用する場合、VCS コントロールを使用して、Security Manager サービスグループ (APP) を手動で起動、停止、およびフェールオーバーする必要があります。VCS 用語では、起動および停止はそれぞれオンラインおよびオフラインと呼ばれます。VCS GUI または VCS コマンドライン インターフェイスを使用して、Security Manager サービスグループをオンラインにしたり、オフラインにしたり、フェールオーバーしたりできます。付録 B [ハイ アベイラビリティおよびディザスタ リカバリ 証明テスト計画 \(97 ページ\)](#) に、このような操作の実行例があります。




---

**注意** VCS の外部で Security Manager を手動で (net stop を使用するなどして) を停止すると、VCS はこれをアプリケーション障害として認識し、リカバリの開始を試行します。

---

## VCS 以外の場合

VCS を使用しない場合は、Security Manager に付属の online および offline スクリプトを使用して Security Manager を起動および停止できます。これらのスクリプトは次の場所にあります。

\$NMSROOT\MDC\athena\ha\agent\Veritas60 (Veritas 6.0.1 用)

\$NMSROOT\MDC\athena\ha\agent\VERITAS602 (VERITAS 6.0.2 用)

\$NMSROOT\MDC\athena\ha\agent\Veritas61 (Veritas 6.1 用)

\$NMSROOT\MDC\athena\ha\agent\Veritas70 (Veritas 7.0 用)

\$NMSROOT\MDC\athena\ha\agent\Veritas72 (Veritas 7.2 用)

\$NMSROOT\MDC\athena\ha\agent\Veritas74 (Veritas 7.4 用)

---

Veritas 6.0.1、Veritas 6.0.2、Veritas 6.1、Veritas 7.0、Veritas 7.2、Veritas 7.4、および Veritas 7.4.2 の Windows Server 2012、2012R2 構文：

```
perl online.pl CSManager <PathName> <EventIPAddress> [ <CertificateDir>|regen ]
```

次に例を示します。

```
perl online.pl CSManager F:\Progra~1\CSCOpX 192.0.2.1
```

(注) コマンドプロンプトを開くときに [管理者として実行 (Run as administrator) ] オプションを選択する必要があります。

構文	説明
<PathName>	Security Manager のインストールパス (たとえば、「F:\Program Files\CSCOpX」)。インストールパスにスペースが含まれる場合、引用符で引数を囲みます。
<EventIPAddress>	Security Manager アプリケーションがクライアント/サーバーとサーバー/デバイスの通信に使用する IP アドレス。
<CertificateDir>	オプション。SSL 証明書ファイルが保管される、非共有の複製されていないローカルディレクトリを指定できます。指定した場合、スクリプトは、アプリケーションが使用するインストールディレクトリの下の適切なディレクトリにこれらのファイルをコピーします。regen キーワードが使用されている場合、スクリプトは、サーバーのローカルホスト名に基づいて SSL 証明書を再生成します。このパラメータに使用される値に関係なく、サーバーのホスト名が Security Manager アプリケーションファイルのホスト名と一致する場合は、証明書に対して行う処理はありません。 <a href="#">SSL 用のセキュリティ証明書 (66 ページ)</a> も参照してください。

Windows Server 2012、2012R2 用の offline スクリプトの構文は次のとおりです。

Veritas 6.0.1、Veritas 6.0.2、Veritas 6.1、Veritas 7.4、および Veritas 7.4.2 の Windows Server 2012、2012R2 構文：

```
perl offline.pl CSManager <PathName> <EventIPAddress>
```

次に例を示します。

```
perl offline.pl CSManager F:\Progra~1\CSCOpX 192.0.2.1
```

(注) コマンドプロンプトを開くときに [管理者として実行 (Run as administrator) ] オプションを選択する必要があります。

構文	説明
<PathName>	Security Manager のインストールパス（たとえば、「F:\Program Files\CSCOpX」）。インストールパスにスペースが含まれる場合、引用符で引数を囲みます。
<EventIPAddress>	Security Manager アプリケーションがクライアント/サーバーとサーバー/デバイスの通信に使用する IP アドレス。

使いやすさのために、構成に適した属性を含むオンラインおよびオフラインバッチファイル（online.bat、offline.bat など）を作成する必要がある場合があります。

手動フェールオーバーを実行するには、VEA またはコマンドラインを使用して、複製されたボリュームグループ内でプライマリロールを転送できます。プライマリサーバとセカンダリサーバの両方が動作している場合、プライマリロールをセカンダリに移行（複製の方向を効果的に逆に）できます。または、プライマリサーバに障害が発生して使用できない場合は、（高速フェールバックの有無に関係なく）セカンダリサーバにプライマリロールを引き継がせることができます。詳細については、『Veritas Volume Replicator Administrator's Guide』[英語]を参照してください。

次は、2 台のサーバ間で複製を使用するディザスタリカバリ構成の手動フェールオーバー手順の概要です。

- 
- ステップ 1** offline.pl スクリプトを使用してプライマリサーバで Security Manager を停止します。
- ステップ 2** プライマリサーバ上の Security Manager に使用される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** VEA GUI を使用してプライマリサーバからセカンダリサーバに所有権を移行します。
- ステップ 4** セカンダリサーバの Security Manager に使用されるボリュームにドライブ文字を割り当てます。
- ステップ 5** online.pl スクリプトを使用してセカンダリサーバの Security Manager を起動します。
- (注) セカンダリサーバへの移行またはフェールオーバーが初めての場合、casusers グループのファイル権限をアップグレードする必要があります。これは、ワнтаイムアクティビティです。詳細については、[作業ボリュームに対する権限の更新 \(43 ページ\)](#) を参照してください。
- 

## Cisco Secure ACS と Security Manager の統合

『Installation Guide for Cisco Security Manager』[英語]で説明されているように、Cisco Secure ACS を Security Manager に統合して、Security Manager ユーザーに高度な許可を付与できます。HA/DR 構成では、ACS の AAA クライアントとして設定に関連する各 Security Manager サーバーを追加する必要があります。ACS でサーバーを指定した場合、サーバーの物理ホスト名に関連付けられた固定 IP アドレスを指定します。

ACS 統合で Security Manager に HA/DR 構成を使用する場合は、複数の ACS サーバーを展開して、ACS がシングルポイント障害になるのを回避する必要があります。ACS サーバーが 1 台

だけあり、そのサーバーで障害が発生した場合は、修正措置を行って ACS を復元するかローカル認証を使用するように Security Manager サーバーをリセットしなければ、Security Manager にログインできません。ACS は、プライマリ ACS とのセカンダリ ACS の同期を維持するためにデータベース複製が使用される、プライマリ ACS と複数のセカンダリ ACS の展開をサポートします。Security Manager では、最大 3 つの ACS の指定をサポートするため、最初の ACS が使用できない場合は、必要に応じて 2 台目を試行し、最後に 3 台目を試行します。



(注) Cisco Security Manager 4.21 以降では、以前の ACS サーバーの代わりに Cisco Identity Services Engine (ISE) を認証に使用できます。

## Security Manager のアップグレード

Security Manager のアップグレードには、さまざまな形態があります。

- メジャーリリース (リリースの最初の数字の変更。たとえば、3.x から 4.x に変更)
- マイナーリリース (リリースの 2 桁目の数字の変更。たとえば、3.1 から 3.2 に変更)
- メンテナンスリリース (リリースの 3 桁目の数字の変更。たとえば、3.1 から 3.1.1 に変更)
- サービスパック (Security Manager 3.1 用の SP2 など、サービスパック ID で識別される)

HA/DR 構成の Security Manager をアップグレードする場合、主な違いは、Security Manager のアクティブインスタンスでプライマリサーバーのみをアップグレードする必要があるのか、または Security Manager をサーバー上で実行するために必要な正しいレジストリ設定を行うために、Security Manager のスペアコピーのみが存在するセカンダリサーバーもアップグレードする必要があるかということです。アップグレードによってレジストリが変更される場合、HA/DR 構成のすべてのサーバでアップグレードを実行する必要があります。通常、サービスパックはレジストリに影響しないため、プライマリサーバだけにサービスパックをインストールするだけで十分です。メジャー、マイナー、またはメンテナンスリリースでは、通常、すべてのサーバをアップグレードする必要があります。ただし、`readme` ファイルまたはリリースノートでこれらのガイドラインの例外を確認してください。

セカンダリサーバーをアップグレードする場合は、Security Manager サーバーのスペアコピーを構成内のすべてのサーバーで使用される標準の `$NMSROOT` (F:\Program Files\CSCOpX など) パスにマウントして、定期的なアップグレードをインストールする必要があります。これにより、セカンダリサーバーで Security Manager のアップグレードバージョンを実行するために正しいレジストリ設定が行われます。

アップグレードする前に、すべてのサーバーで VCS を停止します (クラスタ内の任意のサーバーで `hastop -all -force` を使用すると、クラスタ内のすべてのサーバーで VCS が停止し、アプリケーションとリソースは動作可能なままになります)。すべてのサーバでアップグレードし、構成で複製が使用されている場合は、アップグレード時に複製を一時停止するか停止し、アップグレードの完了後にセカンダリサーバを同期する必要があります。

## Security Manager のバックアップ

Security Manager の HA/DR 展開構成によって、Security Manager の定期的なバックアップが不要になるわけではありません。HA/DR 構成により、ハードウェア障害によるデータ損失やアプリケーションのダウンタイムから保護されます。ただし、Security Manager に保持されている重要な情報を誤って、または悪意を持って変更または削除されるなどのユーザーアクションからは保護されません。したがって、Security Manager データベースおよび情報ファイルを引き続きバックアップする必要があります。Security Manager のバックアップ機能を使用できます。

セカンダリサーバーに関連付けられているスペアインスタンスではなく、Security Manager のプライマリアクティブインスタンスのみをバックアップする必要があります。Security Manager は、HA/DR 構成内のサーバーまたは互換性のある Security Manager アプリケーションがインストールされているサーバーで復元できます。

## Security Manager のアンインストール

HA/DR 構成のすべてのサーバーから Security Manager をアンインストールするには、次の手順に従います。

- ステップ 1 プライマリクラスタ内のプライマリサーバーで Security Manager が実行されていることを確認します。
- ステップ 2 Cluster Explorer を使用して、**APP\_CSManager** リソースを右クリックし、[クリティカル (critical)] チェックボックスをオフにします。読み取り/書き込みモードに切り替えるよう求められるため、このダイアログボックスが表示されたら、[はい (Yes)] をクリックします。
- ステップ 3 [APP\_CSManager (APP\_CSManager)] リソースを右クリックし、プライマリサーバーで [オフライン (Offline)] を選択します。Security Manager がオフラインになるまで待ちます。
- ステップ 4 必要に応じて、必要なメンテナンス作業を実行します。
- ステップ 5 **net start crmdmgt** コマンドを使用して、サーバーでデーモンマネージャを手動で起動します。
- ステップ 6 APP\_CSManager がオンラインになります。[クリティカル (Critical)] チェックボックスをオンにします。
- ステップ 7 APP\_CSManager リソースを削除し、VCS 設定を保存します。
- ステップ 8 複製を利用する場合は、VEA GUI を使用して複製を停止します。
- ステップ 9 プライマリサーバーで Security Manager をアンインストールするには、[スタート (Start)] > [すべてのプログラム (All Programs)] > [Cisco Security Manager (Cisco Security Manager)] > [Cisco Security Manager のアンインストール (Uninstall Cisco Security Manager)] を選択します。
- ステップ 10 セカンダリサーバで、VEA GUI またはコマンドラインを使用して、cscopx\_spare ボリュームを含むディスクグループをインポートします (まだインポートしていない場合)。
- ステップ 11 VEA GUI またはコマンドラインを使用して、cscopx\_spare 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 12** プライマリサーバーで Security Manager をアンインストールするには、[スタート (Start)] > [すべてのプログラム (All Programs)] > [Cisco Security Manager (Cisco Security Manager)] > [Cisco Security Manager のアンインストール (Uninstall Cisco Security Manager)] を選択します。
- ステップ 13** 他のセカンダリサーバーまたはセカンダリクラスタ内のプライマリサーバーでステップ 10 ~ 12 を繰り返します。
- (注) Security Manager を再インストールする予定がない場合は、Security Manager に関連付けられた VCS 内のサービスグループおよび複製を使用している場合は複製されたボリュームグループを削除する必要があります。不要なボリュームおよびディスクグループも削除する必要があります。

## 非 HA Security Manager の HA への移行

通常の非 HA 構成に既存の Security Manager がインストールされている場合は、このセクションで HA 構成にそのインスタンスを移行する方法について説明します。移行を実行するには、次の手順を使用します。

- ステップ 1** 『*User Guide for CiscoWorks Common Services 3.2*』 [英語] の説明に従って、既存の Security Manager インスタンスのバックアップを実行します。「*Configuring the Server*」の章の「*Backing Up Data*」 ([http://www.cisco.com/en/US/docs/net\\_mgmt/cisoworks\\_common\\_services\\_software/3.2/user/guide/admin.html](http://www.cisco.com/en/US/docs/net_mgmt/cisoworks_common_services_software/3.2/user/guide/admin.html)) [英語] を参照してください。
- ステップ 2** このマニュアルの説明に従って、目的の Security Manager HA または DR 導入環境を作成します。
- ステップ 3** 『*User Guide for CiscoWorks Common Services 3.2*』 [英語] の説明に従って、元の Security Manager インスタンスから作成したバックアップを HA または DR 導入環境のプライマリサーバーに復元します。上記のリンクにある「*Restoring Data*」という項を参照してください。
- ステップ 4** セカンダリサーバーのレジストリ内のデータベースパスワードをプライマリサーバーのパスワードと手動で同期します。プライマリサーバーで、レジストリエディタ ([スタート (Start)] > [ファイル名を指定して実行 (Run)] > [regedit (regedit)]) を使用して、HKEY\_LOCAL\_MACHINE\SOFTWARE\OBDC\OBDC.INI の cmf、vms、rmeng フォルダにある CWEPWD レジストリエントリの値を探して書き留めます。セカンダリマシンの CWEPWD レジストリ値をプライマリの値と一致するように編集します。







## 第 6 章

# 仮想マシンの高可用性とディザスタリカバリ

このマニュアルでは、VMware ベースの高可用性 (HA) 環境やディザスタリカバリ (DR) 環境に Cisco Security Management Suite (Security Manager) をインストールする方法について説明します。Security Manager は、次のシナリオをサポートしています。

- [ホストベースのフェールオーバー \(ローカル HA\) \(75 ページ\)](#)
- [フォールトトレランス \(77 ページ\)](#)
- [ディザスタカバリ \(81 ページ\)](#)

上記のシナリオで Security Manager を設定する手順は次のとおりです。

- [ホストベースのフェールオーバー \(ローカル HA\) \(75 ページ\)](#)
- [フォールトトレランス \(77 ページ\)](#)
- [ディザスタカバリ \(81 ページ\)](#)

## ホストベースのフェールオーバー (ローカル HA)

この設定では、Security Manager は VMware クラスタ内の ESXi ホスト上の仮想マシンにインストールされます。既存の ESXi ホストでハードウェア障害が発生した場合、ホストベースのフェールオーバー設定により、VMware クラスタ内の別のホストで同じ仮想マシン (VM) が自動的に起動します。

VMware HA エージェントは、プライマリホストとセカンダリホスト間で 1 秒ごと (デフォルト) に送信されるハートビートをモニターして、ホストの障害を検出します。冗長ハートビートネットワークを設定することをお勧めします。これにより、信頼性の高い障害検出が可能になり、隔離状態の発生を防ぐことができます。

同じオペレーティングシステムとアプリケーションボリュームを持つ同じプライマリ VM が、別の ESXi ホストで起動されます。ホストベースのフェールオーバー設定では、ホスト名と IP アドレスは同じままです。この設定は、物理ホスト間の共有 SAN インフラストラクチャで機能します。別のホストへのフェールオーバーのこのプロセスには数分かかる場合があります。



- (注) 次の設定は参照目的でのみ使用されます。VMware インフラストラクチャを設定するための特定の手順については、VMware のドキュメントを参照する必要があります。この章で説明する手順は、Security Manager 固有の手順ではありません。

## VMware HA クラスタ作成の前提条件

VMware クラスタを作成するには、次の前提条件を満たす必要があります。

- すべての仮想マシンとその構成ファイルは、ストレージエリア ネットワーク (SAN) などの共有ストレージに存在する必要があります。
- ESXi ホストは、同じ仮想マシンネットワークにアクセスできるように設定する必要があります。
- VMware HA クラスタ内の各ホストには、ホスト名と静的 IP アドレスが割り当てられている必要があります。
- ホスト間に CPU の互換性が必要です。理想的なクラスタは、ハードウェアとメモリのサイズが完全に一致するクラスタです。
- 冗長なサービスコンソールと VMkernel ネットワーク設定を使用することをお勧めします。

## ホストベースのフェールオーバー用 Security Manager の設定

ホストベースのフェールオーバー用に Security Manager を設定するには、次の手順を実行します。

- ステップ 1** 『*Deployment Planning Guide for Cisco Security Manager 4.27*』 [英語] で説明されている要件を満たす 2 つの物理ホストを設定します。
- (注) 各ホストの CPU には互換性がある必要があります。
- ステップ 2** ステップ 1 で作成した各ホストに VMware ESXi をインストールします。
- ステップ 3** vCenter でクラスタを作成し、ESXi ホストをクラスタに追加します。
- ステップ 4** ESXi ホストで vSphere HA 設定を構成します。詳細については、VMware のマニュアルを参照してください。
- ステップ 5** ESXi ホストの 1 つに VM を作成します。詳細については、『*Deployment Planning Guide for Cisco Security Manager 4.27*』 [英語] を参照してください。
- ステップ 6** ステップ 5 で作成した VM に Security Manager をインストールします。詳細については、『*Installation Guide for Cisco Security Manager 4.27*』 [英語] を参照してください。
- ステップ 7** Security Manager を起動します。

Security Manager が VM にインストールされている ESXi ホストでハードウェア障害が発生した場合、VM はクラスタ内の他の ESXi ホストに移動され、VM が起動します。この移動は完了するまでに数分かかるため、ダウンタイムが発生します。

## 制限事項

ホストベースのフェールオーバー設定には、次の制限があります。

- 障害が発生したホストで仮想マシンを手動で再起動する必要があります。
- 障害が発生したホスト上の VM でアプリケーションの稼働が停止し、アプリケーションデータが破損した場合、フェールオーバー後に VM を手動で再起動しても、アプリケーションは使用できないままになる可能性があります。
- VMware クラスタ内のホストがハートビートネットワークへの接続を失っても、ホスト自体が実行されている場合、そのホストはクラスタから分離されます。この場合、VMware High Availability ソリューションは、ホストがクラスタから分離されていると判断する前に 12 秒間待機します。



(注) アプリケーションベースのモニタリングは、Security Manager ではサポートされていません。つまり、Security Manager プロセスが実行を停止しても、自動的に再起動されません。手動で問題を解決し、プロセスを再起動してから、手動で Security Manager を再起動する必要があります。

## フォールトトレランス

VMware Fault Tolerance 設定では、ホストでハードウェア障害が検出されると、別のホストに 2 番目の VM が作成され、サービスを中断することなく、2 番目の VM で Security Manager の実行が開始されます。VMware Fault Tolerance は、新しいレベルのゲスト冗長性を実現します。VMware Fault Tolerance では、VM の 2 つのコピーがそれぞれ別のホストに保持されます。この機能は、Security Manager がインストールされている VM で耐障害性をオンにすることで有効にできます。

VMware Fault Tolerance とホストベースのフェールオーバー (HA) ソリューションの主な違いは、ESX/ESXi ホストに障害が発生した場合に VM の動作が中断されることです。耐障害性システムは新しいホストに即座に移行しますが、高可用性システムは別のホストで再起動する前にホストで VM に障害が発生したことを確認します。障害が発生したホスト上の VM はプライマリ VM と呼ばれ、引き継ぐ VM はセカンダリ VM と呼ばれます。プライマリ VM からセカンダリ VM へのフェールオーバーは動的で、セカンダリ VM はプライマリ VM が終了した正確なポイントから実行を継続します。このプロセスは自動的に実行され、データの損失、ダウンタイム、またはサービスの中断は発生しません。動的なフェールオーバーの後、セカンダリ VM が新しいプライマリ VM になり、新しいセカンダリ VM が自動的に生成されます。



(注) 次の設定は参照目的でのみ使用されます。VMware インフラストラクチャを設定するための特定の手順については、VMware のドキュメントを参照する必要があります。この章で説明する手順は、Security Manager 固有の手順ではありません。

## 耐障害性システムの作成

### 前提条件

耐障害性システムを作成するには、次の前提条件を満たす必要があります。

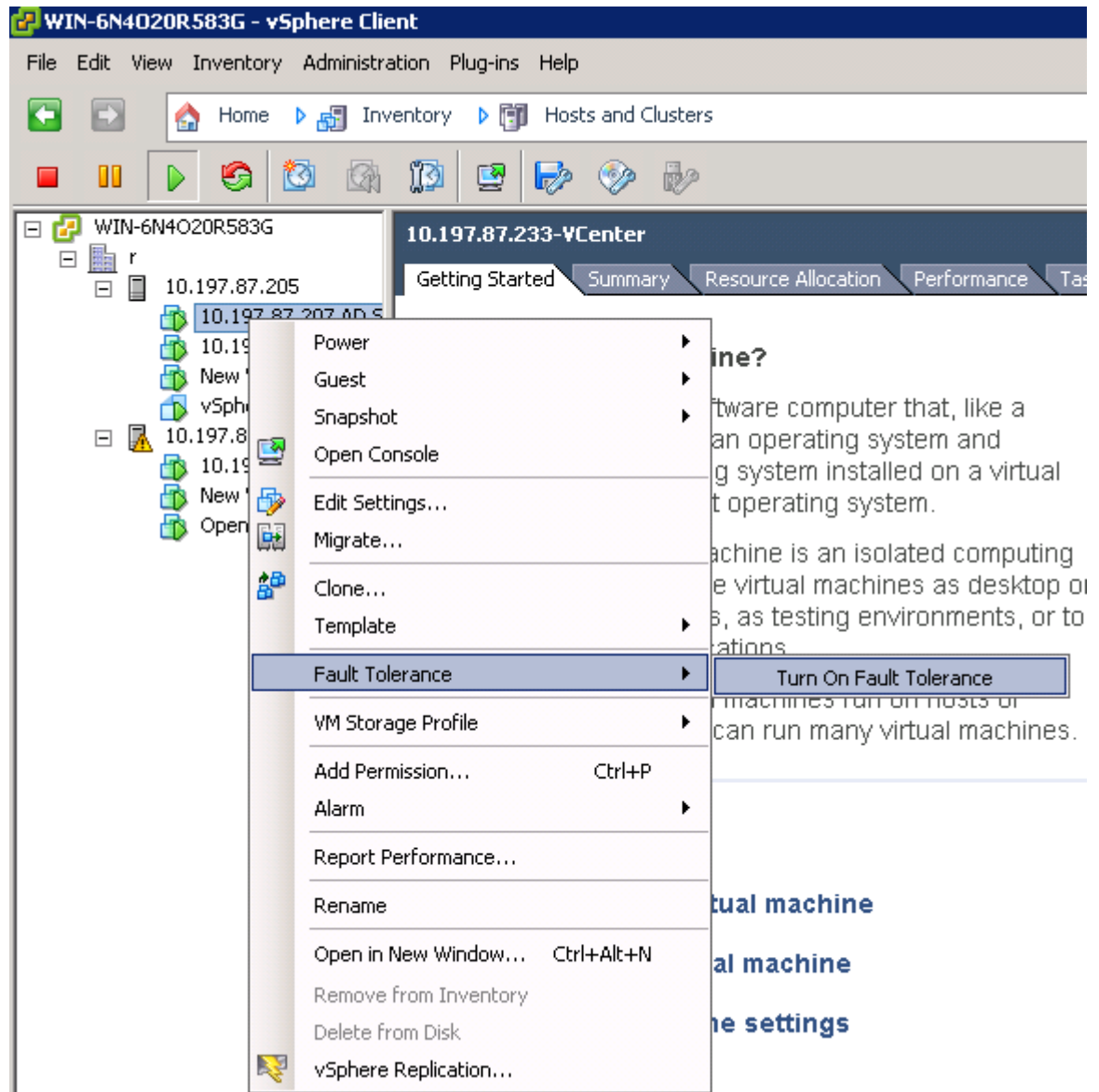
- 耐障害性環境で使用される VMware ソフトウェアのすべてのバージョンが、vSphere 互換性マトリックスのリストに従って互換性があることを確認します。詳細については、『[VMware Compatibility Guide](#)』を参照してください。
- ハードウェアおよびゲスト オペレーティング システム レベルでは、特定のプロセッサとオペレーティングシステムのみがサポートされます。サポートの詳細については、『[VMware Guest OS Compatibility Guide](#)』 (<http://www.vmware.com>) [英語] を参照してください。さらに、既存の VMware 設定がフォールトトレランスに適しているかどうかを確認するには、[https://www.vmware.com/support/shared\\_utilities](https://www.vmware.com/support/shared_utilities) [英語] でサイト調査を実行します。
- クラスタ内の各ホストの BIOS でハードウェア仮想化を有効にします。ハードウェア仮想化を有効にするプロセスは BIOS ごとに異なるため、ハードウェア仮想化を有効にする具体的な手順については、ハードウェアベンダーにお問い合わせください。
- VMware Fault Tolerance で使用されるすべての ESX ホストが VMware High Availability (HA) クラスタのメンバーであることを確認します。VMware Fault Tolerance を機能させるには、VMware HA を有効にする必要があります。VMware HA の有効化については、『[vSphere Availability Guide](#)』 (<http://www.vmware.com>) [英語] を参照してください。
- プライマリおよびセカンダリ耐障害性ノードを実行する ESX ホストが同じビルドの ESX を実行していることを確認します。さらに、パッチには VMware 耐障害性機能の改善が含まれているため、リリースされたパッチを必ず適用してください。
- VMware Fault Tolerance を有効にするには、使用している環境で次のように設定されていることを確認します。
  - 仮想マシンは、共有ストレージ、つまり、クラスタ内のすべての ESX ホストに表示されるストレージに存在する必要があります。
  - ストレージは、ローカルストレージではなく、FCSAN、iSCSI、または NFS である必要があります。
  - 仮想マシンにはスナップショットを含めることはできません。スナップショットがある場合は、続行する前にコミットする必要があります。
- 耐障害性環境でネットワーキングを設定するには、次のタスクを実行してください。

- 耐障害性ロギング用に別の VMkernel ポートグループを定義します。ポートグループを作成する手順については、『ESX Configuration Guide』[英語]を参照してください。
- 耐障害性ロギングおよび VMotion ポートグループを定義し、アップリンク用の物理ネットワークカードを割り当てます。このネットワークカードのサイズは 1GB 以上である必要があります。10GB のネットワークカードを使用することをお勧めします。
- 耐障害性ロギングでのジャンボフレームの使用を有効にします。詳細な手順については、『ESX Configuration Guide』の「Advanced Networking」のセクション [英語]を参照してください。
- VMware では、可用性を確保するために完全な冗長 NIC を有効にすることを推奨していますが、耐障害性は冗長 NIC がなくても機能できます。

前提条件のリストに従って環境を設定したら、次の図に示すように、耐障害性をオンにします。

図 423485

図 5: 耐障害性オン設定



(注) VMware ESXi バージョン 5.102 から ESXi バージョン 6.0 までの小規模展開では、Security Manager に少なくとも 6 つの仮想 CPU が必要です。詳細については、『Cisco Security Manager Deployment Planning Guide』[英語]を参照してください。



- (注) vCenter Server バージョン 5.x の耐障害性仮想マシンは、保護された仮想マシンごとに1つの仮想 CPU をサポートします。vCenter Server バージョン 6.0 は、ライセンスに応じて最大4つの仮想 CPU をサポートします。

## ディザスタ カバリ

Security Manager は、VMware vCenter Site Recovery Manager ツールを VMware vSphere Replication とともに使用して、ディザスタリカバリと管理を行います。

Site Recovery Manager は、VMware vSphere Replication とネイティブに統合され、ビジネス要件に応じてサイト間で仮想マシンを確実にコピーするために、さまざまな高性能アレイベースのレプリケーション製品をサポートします。Site Recovery Manager は、仮想マシンのリカバリの計画、テスト、および実行に役立つディザスタリカバリ ソリューションを提供する VMware vCenter Server の拡張機能です。Site Recovery Manager は、複製されたデータストアを検出して管理し、vCenter Server インスタンス間のインベントリの移行を自動化できます。

## システム要件

### ハードウェア要件

ハードウェア要件については、*VMware Site Recovery Manager 6.1 Documentation Center* (<http://www.vmware.com>) [英語] を参照してください。

### ソフトウェア要件

次に、ディザスタリカバリ用の VMware Site Recovery Manager ソリューションを設定するためのソフトウェア要件の概要を示します。

- Virtual Center 6.0 ライセンスがプライマリ（保護された）サイトとリカバリサイトの両方に適用されている。
- ESXi Server 6.0 ライセンスがプライマリサイトとリカバリサイトの両方に適用されている。
- vSphere SRM 6.0 ライセンスがプライマリサイトとリカバリサイトの両方に適用されている。
- Site Recovery Manager 用の SQL Server データベースがプライマリサイトとリカバリサイトの両方にインストールされている。



- (注) すべての VMware ツールがバージョン 6.0 である必要があります。



(注) VMware Disaster Recovery ソリューションは VMware Site Recovery Manager でテスト済みです。ただし、他の VMware ソリューションも Security Manager で動作する場合があります。

## VMware Site Recovery Manager の設定

vCenter サーバーに Site Recovery Manager をインストールするには、次の手順を実行します。

- ステップ 1 **install.exe** をクリックして、Site Recovery Manager のインストールを開始します。
- ステップ 2 VMware エンドユーザーライセンス契約書に同意します。
- ステップ 3 [VMware vCenter Site Recovery Manager—vSphere Replication (VMware vCenter Site Recovery Manager—vSphere Replication)] ウィンドウで、[vSphere Replicationのインストール (Install vSphere Replication)] を選択し、[次へ (Next)] をクリックします。
- ステップ 4 vCenter サーバーのアドレス、ポート (デフォルトでは 81)、ユーザー名、およびパスワードを入力します。
- ステップ 5 セキュリティ警告を受け入れます。
- ステップ 6 [VMware vCenter Site Recovery Manager : 証明書タイプの選択 (VMware vCenter Site Recovery Manager—Certificate Type Selection)] ウィンドウで、[証明書ソース (Certificate Source)] として [証明書の自動生成 (Automatically Generate a Certificate)] を選択します。
- ステップ 7 vCenter サーバー情報を入力します。

[VMware vCenter Site Recovery Manager エクステンション (VMware vCenter Site Recovery Manager Extension)] ウィンドウで、次のように入力します。

- [ローカルサイト名 (Local Site name)] : vCenter サイトの完全修飾ドメイン名。
- [管理者の電子メール (Administrator Email)] : 組織の要件に応じた管理者の電子メール。
- [追加の電子メール (Additional Email)] : 入力する追加の電子メール ID。
- [ローカルホスト (Local Host)] : 現在のホストの IP アドレス。これは自動的に入力されます。
- リスナーポート
  - [SOAPポート (SOAP Port)] : デフォルトは 8095 です。
  - [HTTPポート (HTTP Port)] : デフォルトは 9085 です。
- [APIリスナーポート (API Listener Port)] : デフォルトは 9007 です。

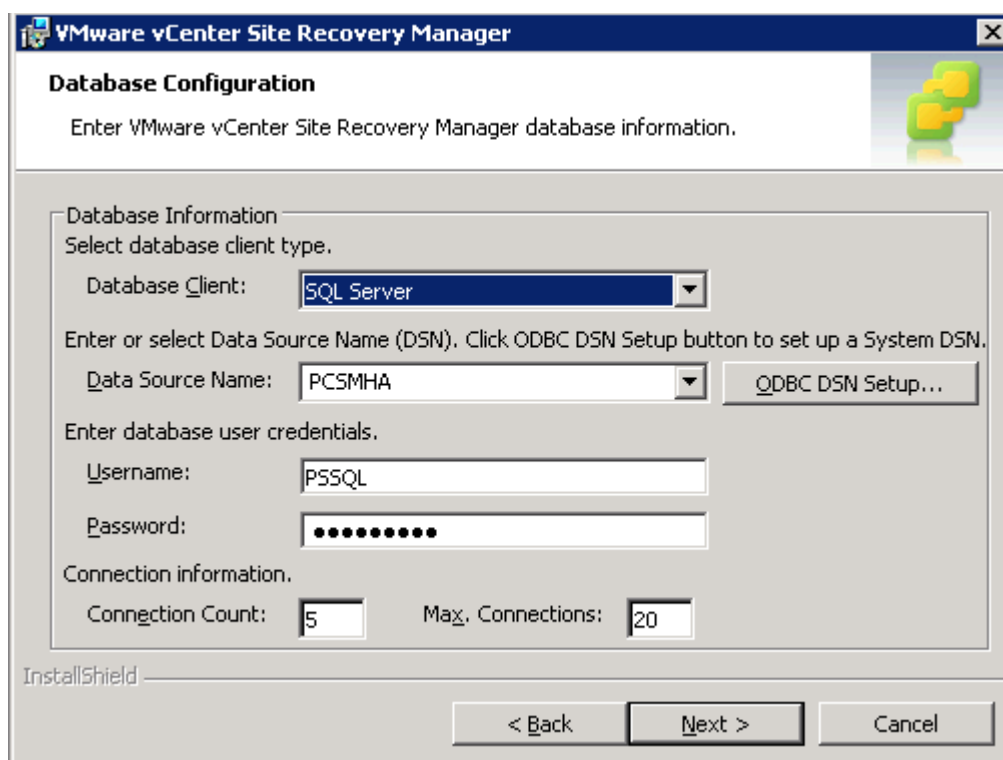
- ステップ 8 Site Recovery Manager サーバーには、リカバリ計画やインベントリ情報などのデータを保存するために使用する独自のデータベースが必要です。Site Recovery Manager データベースは、Site Recovery Manager インストールの重要な部分です。Site Recovery Manager をインストールする前に、Site Recovery Manager データベースを作成し、データベース接続を確立する必要があります。



[VMware vCenter Site Recovery Manager—データベース設定 (VMware vCenter Site Recovery Manager—Database Configuration)] ウィンドウで、次のように入力し、[次へ (Next)] をクリックします。

- ドロップダウンリストから、[データベースクライアントタイプ (Database Client type)] を選択します。
- [データソース名 (Data Source Name)] を入力します。[ODBC DSN設定 (ODBC DSN Setup)] をクリックして、システム DSN を設定します。
- [データベースユーザー名 (Database Username)] と [パスワード (password)] を入力します。
- [接続数 (Connection Count)] と [最大接続数 (Maximum Connections)] を入力します。

図 6: データベースの設定



VMware vCenter Site Recovery Manager

**Database Configuration**

Enter VMware vCenter Site Recovery Manager database information.

Database Information  
Select database client type.

Database Client:

Enter or select Data Source Name (DSN). Click ODBC DSN Setup button to set up a System DSN.

Data Source Name:

Enter database user credentials.

Username:

Password:

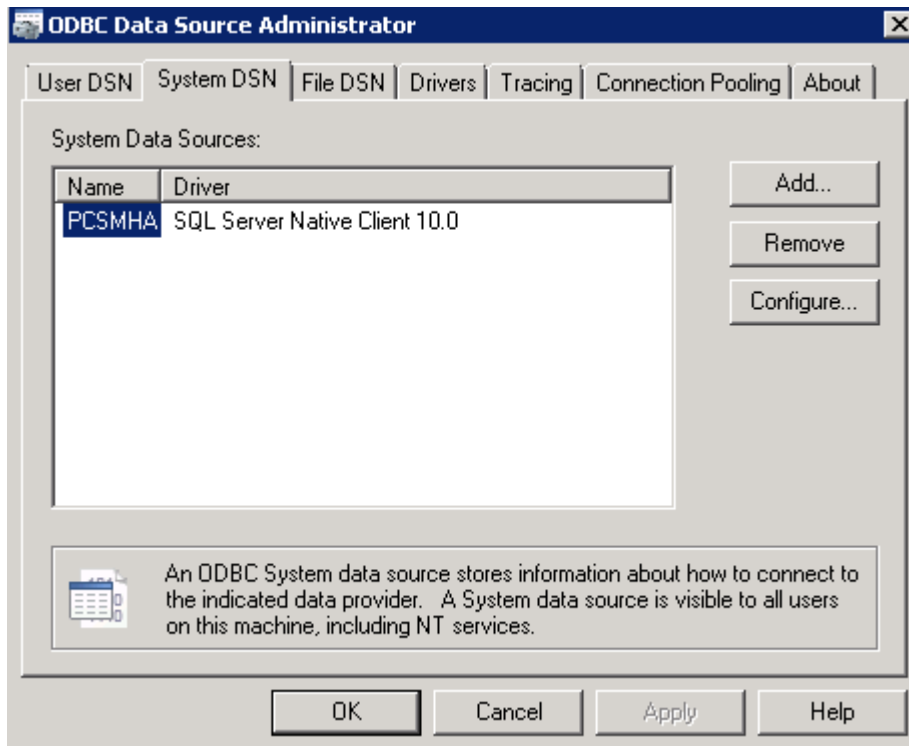
Connection information.

Connection Count:  Max. Connections:

InstallShield

< Back    Next >    Cancel

図 7: ODBC DSN の設定



**ステップ 9** [次へ (Next)] をクリックして、Site Recovery Manager のインストールを完了します。

- (注) 各 Site Recovery Manager サイトには、Site Recovery Manager データベースの独自のインスタンスが必要です。サイトごとに個別の Site Recovery Manager データベースを実行するには、異なるデータベース サーバー インスタンスを使用します。同じデータベース サーバー インスタンスを使用して両方のサイトのデータベースを実行する場合や、データベースサーバーで問題が発生すると、Site Recovery Manager サイトは機能せず、リカバリを実行できなくなります。

## vCenter の設定

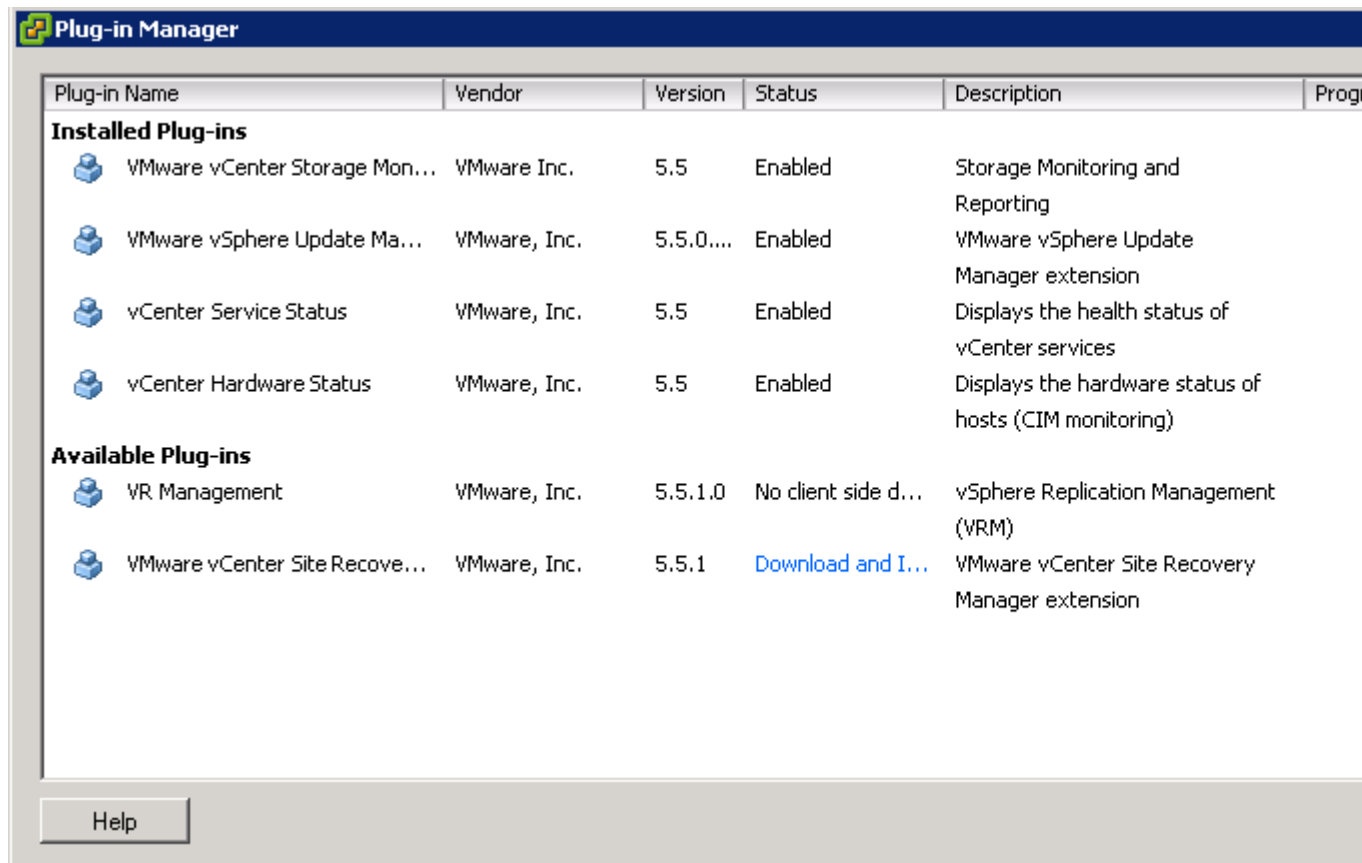
保護サイトで vCenter を設定するには、次の手順を実行します。

vCenter サーバーの詳細は、[ステップ 7](#) で指定したものです。vCenter サーバー情報を入力すると、Site Recovery Manager 5.5 プラグインマネージャが有効になります。

**ステップ 1** プラグインマネージャから、VMware vCenter Site Recovery Manager 拡張機能をダウンロードしてインストールします。

- (注) 上記の手順は、Site Recovery Manager バージョン 5.5 にのみ適用されます。Site Recovery Manager バージョン 6.0 では、vSphere Web クライアントをサポートしているため、プラグインをインストールする必要はありません。

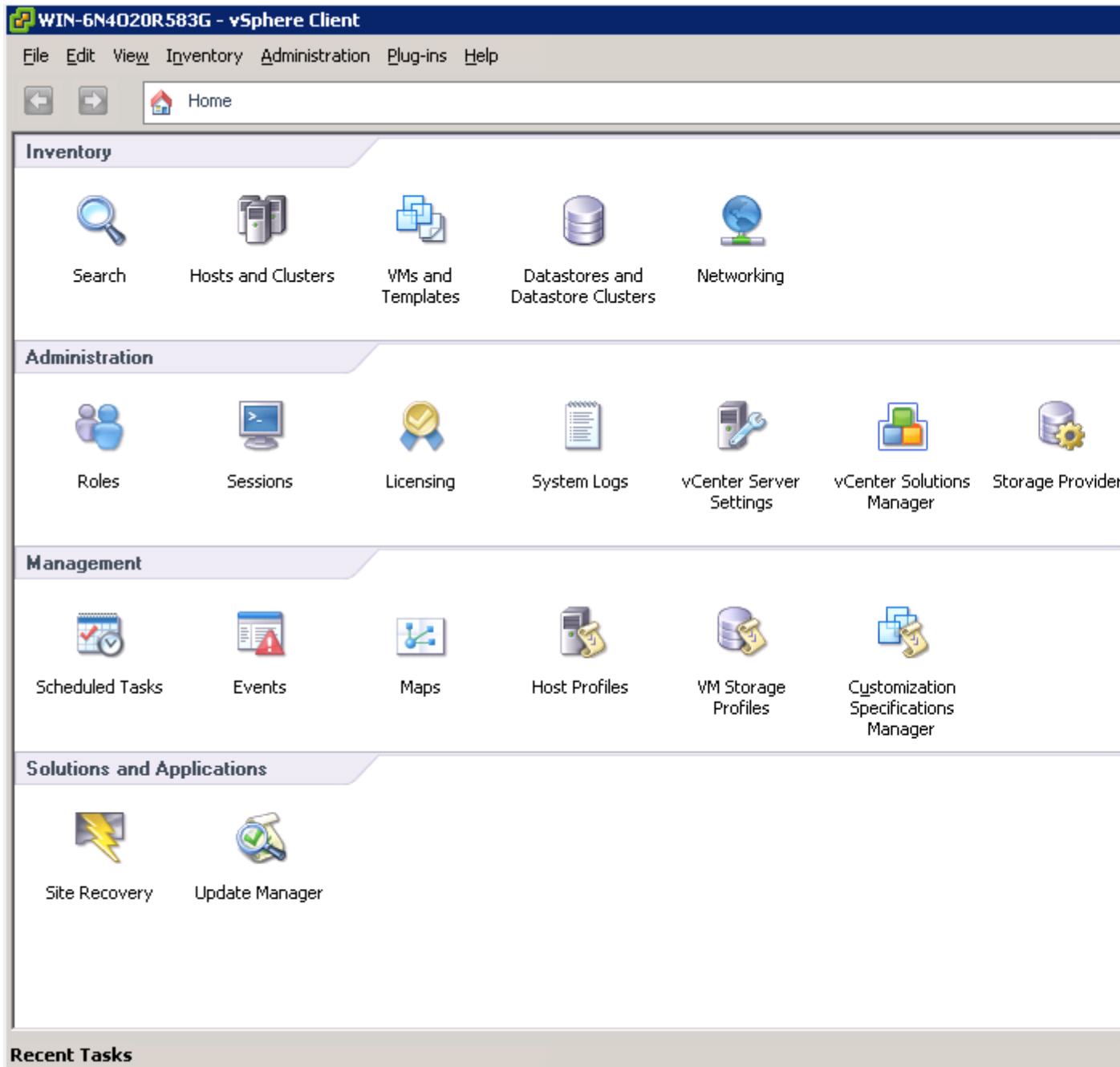
図 8: プラグインマネージャ



**ステップ 2** Site Recovery Manager を設定および管理するには、ホームページで [サイトのリカバリ (Site Recovery)] をクリックします。

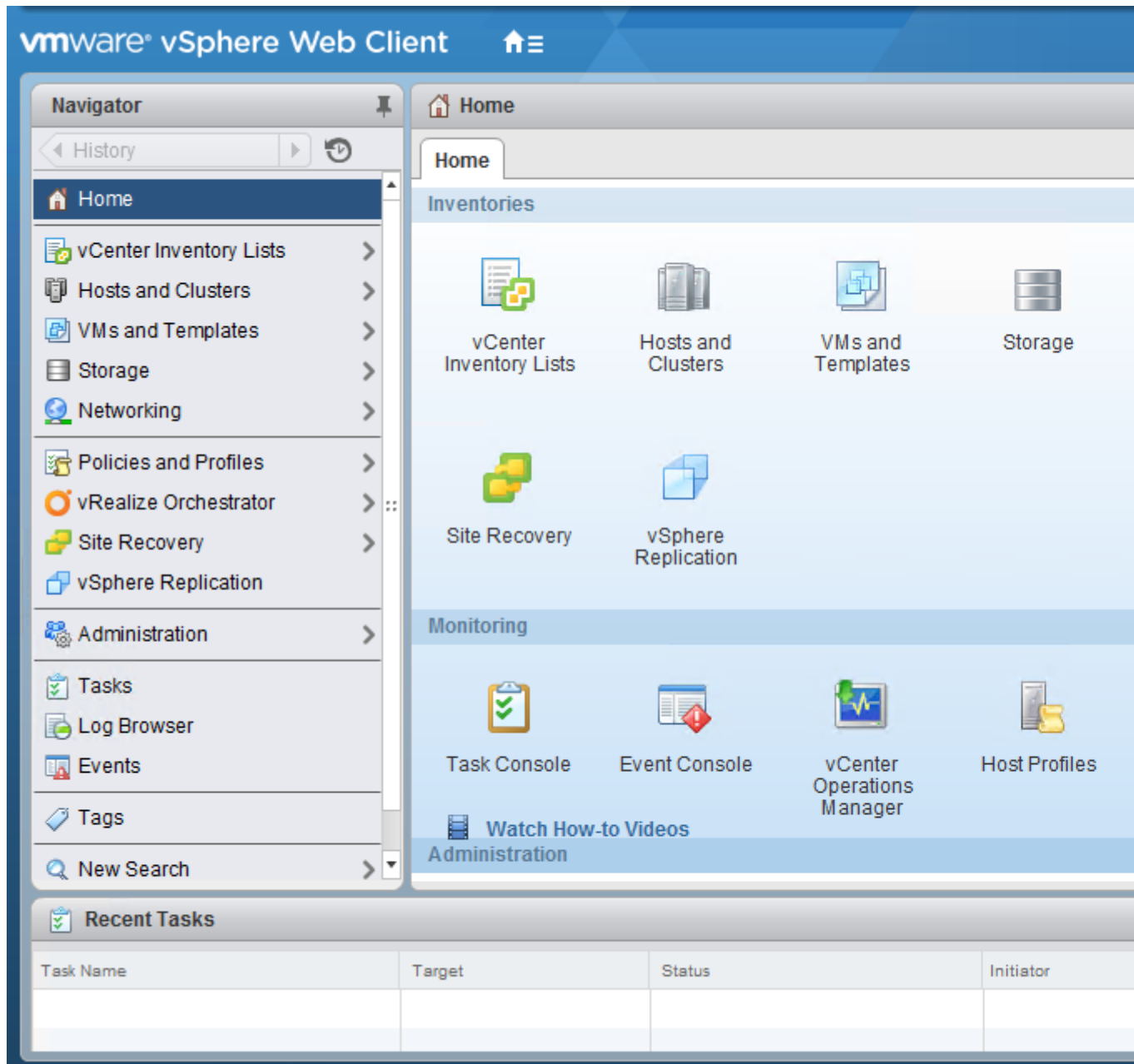
(注) 上記の手順は、Site Recovery Manager バージョン 5.5 にのみ適用されます。Site Recovery Manager バージョン 6.0 では、vSphere Web クライアントをサポートしているため、プラグインをインストールする必要はありません。

図 9 : Site Recovery Manager 5.5



次の図は、Site Recovery Manager バージョン 6.0 へのアクセスに使用できる vSphere Web クライアントを示しています。

図 10: VMware vSphere Web クライアント



## リカバリサイトの設定

VMware Site Recovery Manager の設定 (82 ページ) と vCenter の設定 (84 ページ) で説明されているタスクをリカバリサイトで実行します。

## 複製の設定

保護サイトとリカバリサイトで次のタスクを実行します。次の手順は、Site Recovery Manager バージョン 5.5 および 6.0 に適用されます。

- 保護サイトとレプリケーションサイトの設定
- インベントリの設定
- vSphere Replication のインストールと設定
- 保護グループの設定
- リカバリプランの設定

詳細については、VMware vCenter Site Recovery Manager バージョン 5.5 および 6.0 ドキュメント センターにある『VMware User Guide』 [英語] を参照してください。

## ディザスタリカバリ環境での Security Manager のインストール

保護サイトとリカバリサイトの両方で Site Recovery Manager を設定した後、保護サイトの VM に Security Manager をインストールする必要があります。Security Manager をインストールするには、『*Installation Guide for Cisco Security Manager 4.27*』 [英語] を参照してください。

VMware Site Recovery Manager ツールは、リカバリサイトにインストールを複製します。保護サイトとリカバリサイト間の同期は、保護サイトの帯域幅とデータサイズに基づいて実行されます。保護サイトホストで Site Recovery Manager を有効にすると、vSphere Replication は、ソースの VM とそのレプリカのリカバリサイトへの最初の完全同期を実行します。

完全同期が初めて完了すると、Site Recovery Manager で設定された目標復旧時点（RPO）の時間間隔に基づいて vSphere レプリケーションが実行されます。



(注) 環境、つまり帯域幅とデータサイズに基づいて RPO 時間間隔を設定する必要があります。



**注意** アプリケーションでの作業を開始する前に、Security Manager サービスがリカバリサイトで起動するまで少なくとも 15 分の猶予時間を確保することをお勧めします。猶予時間が許可されていない場合、Security Manager は正常に起動せず、アプリケーションの再インストールが必要になる可能性があります。



(注) Security Manager が Access Control Server (ACS) と統合されている場合は、認証のために、(Security Manager がインストールされている) 保護サイトとリカバリサイトの両方の IP アドレスを AAA クライアントとして ACS サーバーに提供する必要があります。



---

(注) Cisco Security Manager 4.21 以降では、以前の ACS サーバーの代わりに Cisco Identity Services Engine (ISE) を認証に使用できます。

---







## 付録 **A**

# 参照構成の VCS リソース ビュー

ここでは、このマニュアルで説明されている HA/DR Security Manager 構成の Veritas Cluster Server (VCS) リソースビューとサービスグループビューに関する情報を提供します。図 A-1～図 A-5 に、サービスグループのリソース間の依存関係およびサービスグループ間の依存関係を示します。この図では、2つのリソース間の線は、依存関係、つまり親子関係を表します。リソースの依存関係は、リソースをオンラインおよびオフラインにする順序を指定します。フェールオーバー中は、図の上部に最も近いリソースをオフラインにする必要があり、その後、そのリソースにリンクされているリソースがオフラインになります。同様に、図の下部に最も近いリソースをオンラインにする必要があり、その後、そのリソースにリンクされているリソースをオンラインになります。他のリソースに依存するリソースは親リソースです。図では、親リソースのアイコンをその下にある子リソースのアイコンにリンクしています。

ここでは、次の内容について説明します。

- [参照構成の VCS リソースビュー \(91 ページ\)](#)

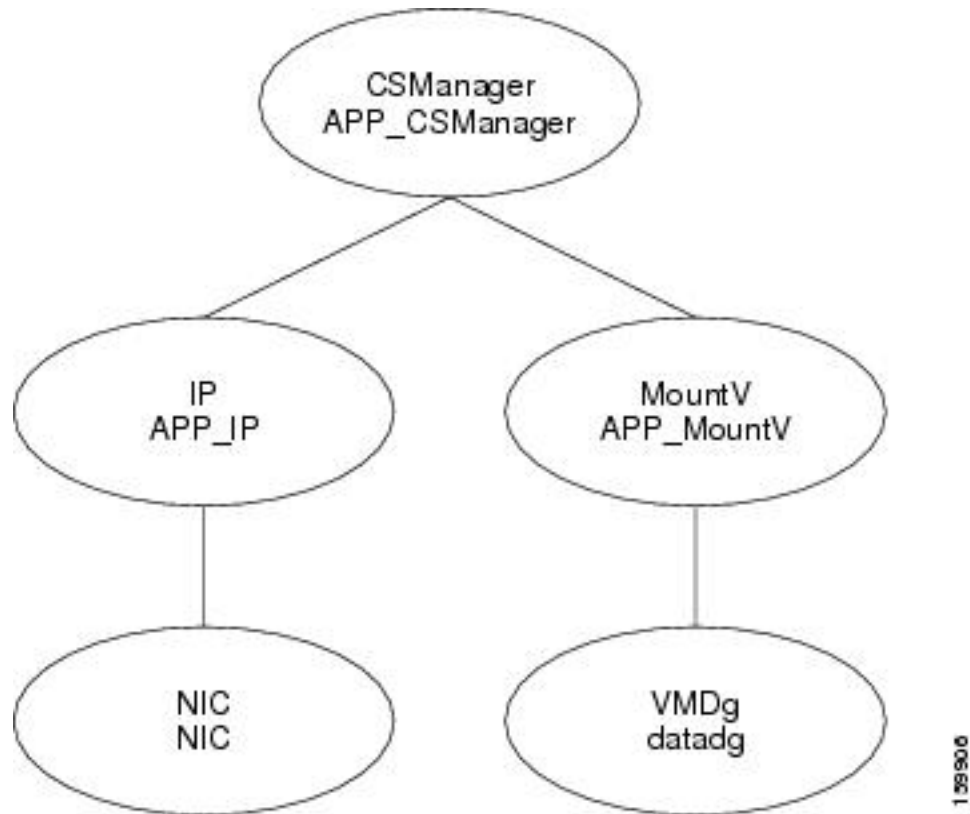
## 参照構成の VCS リソースビュー

ここでは、このマニュアルで説明されている HA/DR Security Manager 構成の Veritas Cluster Server (VCS) リソースビューとサービスグループビューに関する情報を提供します。図 A-1～図 A-5 に、サービスグループのリソース間の依存関係およびサービスグループ間の依存関係を示します。この図では、2つのリソース間の線は、依存関係、つまり親子関係を表します。リソースの依存関係は、リソースをオンラインおよびオフラインにする順序を指定します。フェールオーバー中は、図の上部に最も近いリソースをオフラインにする必要があり、その後、そのリソースにリンクされているリソースがオフラインになります。同様に、図の下部に最も近いリソースをオンラインにする必要があり、その後、そのリソースにリンクされているリソースをオンラインになります。他のリソースに依存するリソースは親リソースです。図では、親リソースのアイコンをその下にある子リソースのアイコンにリンクしています。

## シングルローカルクラスタ（デュアルノード）構成

図 A-1 に、クラスタ内に 2 台のサーバを持つシングルクラスタの Veritas Cluster Server (VCS) リソースビューを示します。

図 11: リソースビュー：APPグループ（シングルクラスタ、デュアルノード）



1 25 90 0

## デュアル地理的クラスタ（シングルノード）構成

図 12: 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）～図 13: リソースビュー：APPprepグループ（デュアルクラスタ、シングルノード）に、クラスタ内に1台のサーバーを持つデュアルクラスタ構成の Veritas Cluster Server（VCS）リソースビューを示します。

図 12: 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)

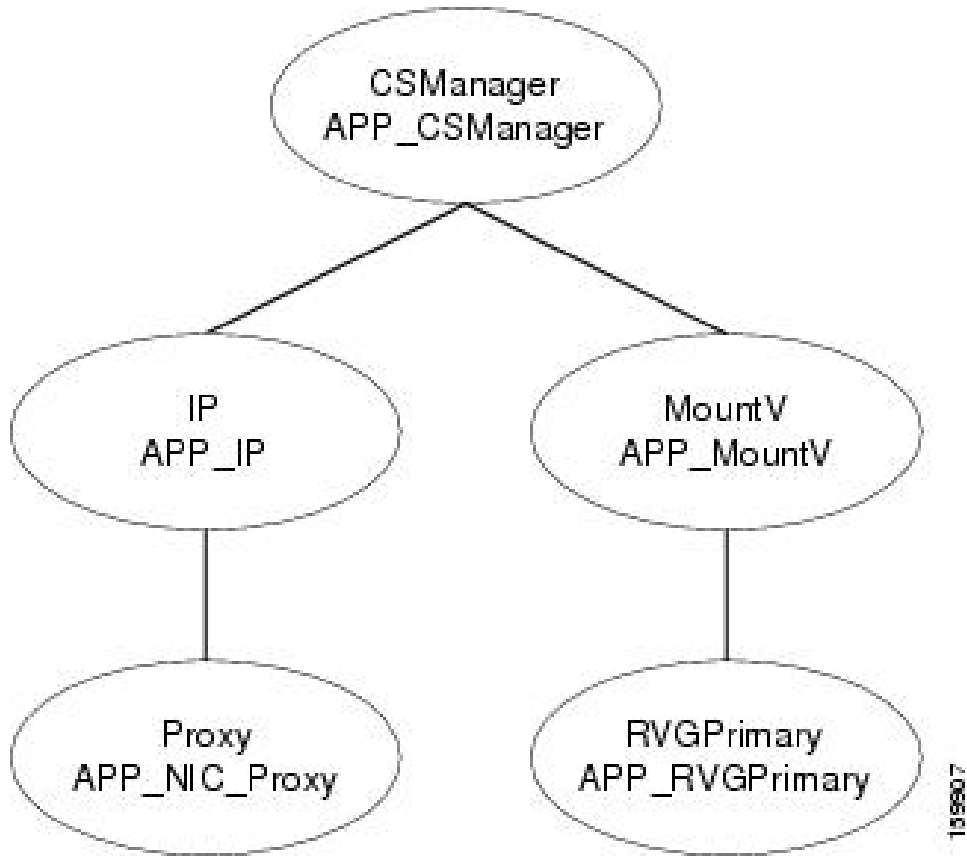
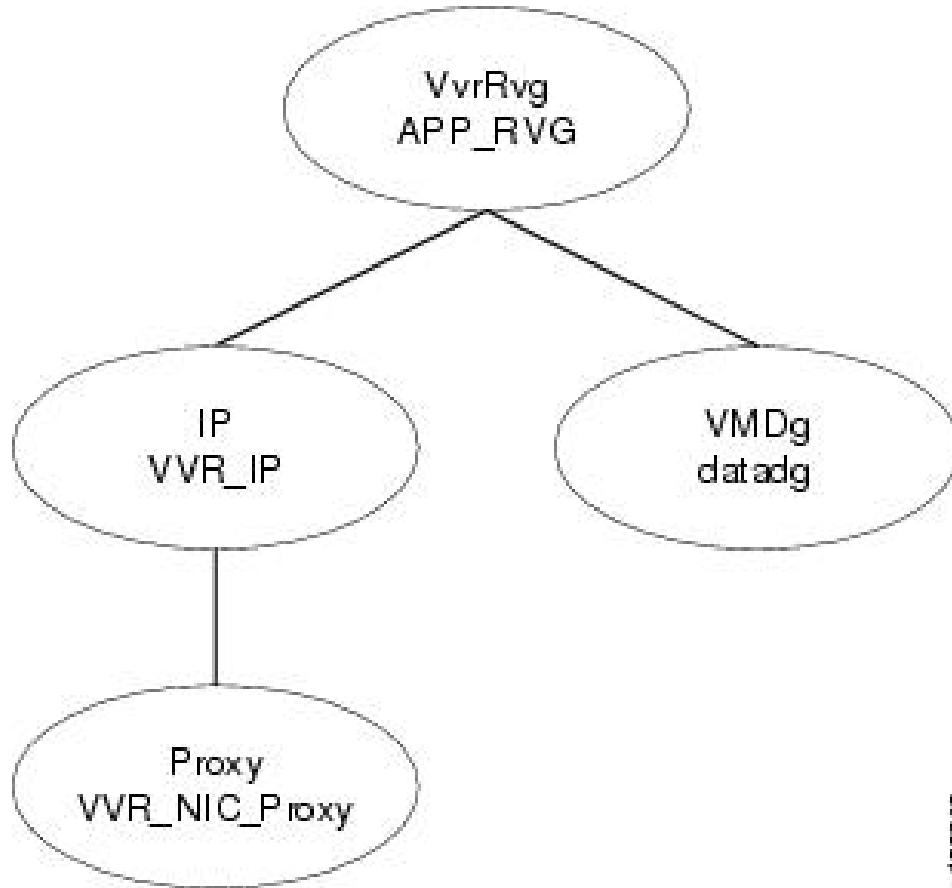


図 13: リソースビュー : APPrep グループ (デュアルクラスタ、シングルノード)



139908

図 14: リソースビュー : *ClusterService* グループ (デュアルクラスタ、シングルノード)

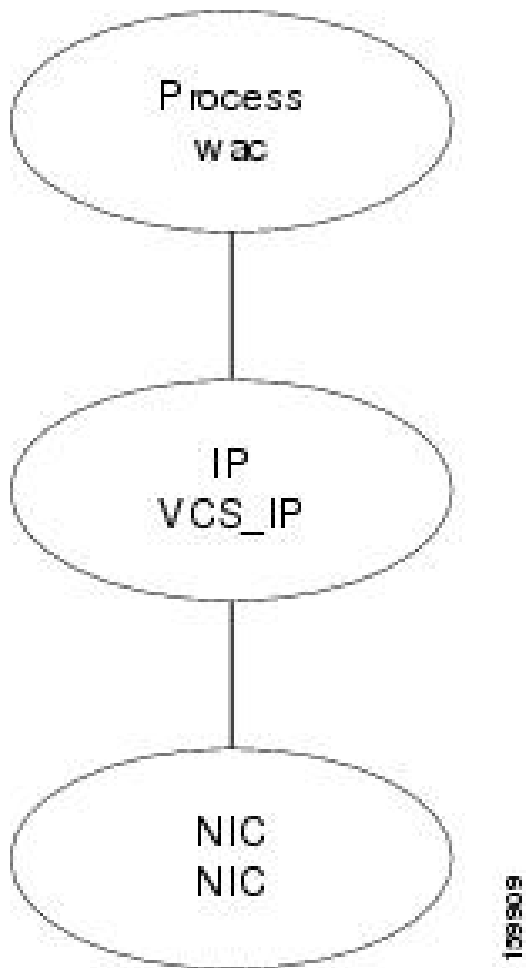
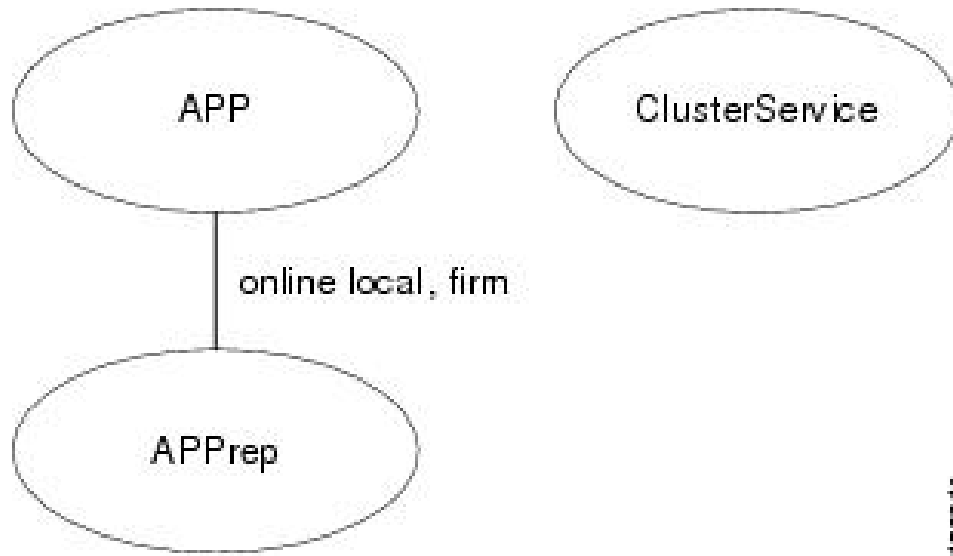


図 15: サービスグループビュー (デュアルクラスタ、シングルノード)



150810



## 付録 **B**

# ハイ アベイラビリティおよびディザスタリカバリ証明テスト計画

HA/DR 証明テスト計画では、Security Manager アプリケーションが高可用性を備え、さまざまなハードウェア障害やソフトウェア障害に対応できることを検証します。テスト計画には、サーバ間でのアプリケーションの手動切り替えなど、メンテナンス作業も含まれます。



- (注) Security Manager クライアントセッションでは、アクティブユーザーがアプリケーションのフェールオーバー後に再度ログインする必要があります。この動作は、サーバーで実行されている Security Manager サービスの停止および開始と同じです。

この付録には、次のテストケースカテゴリがあります。

- [手動切り替え \(97 ページ\)](#)
- [イーサネット/ネットワーク障害 \(99 ページ\)](#)
- [サーバの障害 \(107 ページ\)](#)
- [アプリケーションの障害 \(114 ページ\)](#)

## 手動切り替え

ここでは、2 種類の手動切り替えについて説明します。2 台のサーバを持つシングルクラスタでは、クラスタ内で2台のサーバを切り替えることができます (クラスタ内切り替え)。各クラスタ内に1台のサーバが配置されたデュアルクラスタ構成では、クラスタを切り替えることができます (クラスタ間切り替え)。

ここでは、次の内容について説明します。

- [クラスタ内切り替え \(98 ページ\)](#)
- [クラスタ間切り替え \(98 ページ\)](#)

## クラスタ内切り替え

テストケースタイトル：クラスタ内の手動アプリケーション切り替え。

説明：アプリケーションは、VCSを使用して、同じクラスタ内の別のサーバーに手動で切り替えられます。

テストセットアップ：シングルクラスタ構成内のデュアルノードクラスタ (図)。

**ステップ 1** APP サービスグループがプライマリサーバで実行されていることを確認します。VCS Cluster Explorer を使用して、[APP (APP)] サービスグループを選択します。ショートカットメニューから [切り替え (Switch To)] を選択し、セカンダリサーバを選択します。または、次のコマンドを発行します。

例：

```
C:\> hagr -switch APP -to secondary_server_name
```

**ステップ 2** APP サービスグループのリソースビューで、サービスグループのリソースがプライマリサーバでオフラインになり、その後セカンダリサーバでオンラインになることを確認します。または、次のコマンドを発行して、APP サービスグループのステータスを確認します。

例：

```
C:\> hagr -state APP
```

**ステップ 3** クライアントマシンから、ログインダイアログボックスで [サーバー名 (Server Name)] フィールドに仮想ホスト名または IP アドレスを使用して Security Manager クライアントを起動します。アプリケーションに正常にログインできることを確認します。

## クラスタ間切り替え

テストケースタイトル：クラスタ間の手動アプリケーション切り替え。

説明：アプリケーションは、VCSを使用して、異なるクラスタ内のサーバに手動で切り替えられます。

テストセットアップ：各クラスタ内に 1 台のノードが配置された 図 に示すデュアルクラスタ構成。

**ステップ 1** VCS Cluster Explorer を使用して、[APP (APP)] サービスグループを選択します。ショートカットメニューから、[切り替え (Switch To)]、[リモート切り替え (...)] (Remote Switch(...)) の順に選択して [グローバルに切り替え (Switch global)] ダイアログボックスを開きます。ダイアログボックスで、リモートクラスタと、必要に応じてリモートクラスタ内の特定のサーバを指定します。または、次のコマンドを発行します。

例：



```
C:\> hagr -switch APP -any -clus secondary_cluster_name
```

**ステップ 2** APP サービスグループのリソースビューで、サービスグループのリソースがプライマリクラスタでオフラインになることを確認します。ツリーでルートクラスタノードを選択し、[リモートクラスタステータス (Remote Cluster Status)] ビューを使用して、APP サービスグループがリモートクラスタでオンラインになることを確認します。または、次のコマンドを発行して、APP サービスグループのステータスを確認します。

例：

```
C:\> hagr -state APP
#Group      Attribute      System      Value
APP         State          csm_primary:<Primary Server> |OFFLINE|
APP         State          localclus:<Secondary Server> |ONLINE|
```

**ステップ 3** クライアントマシンから、[ログイン (Login)] ダイアログボックスで [サーバー名 (ServerName)] フィールドにセカンダリクラスタで使用されている適切なホスト名またはアプリケーション IP アドレスを入力して Security Manager クライアントを起動します。アプリケーションに正常にログインできることを確認します。

**ステップ 4** Security Manager クライアントからログアウトし、VCS Cluster Explorer または次のコマンドを使用して、APP サービスグループをプライマリクラスタに切り替えます。

例：

```
C:\> hagr -switch APP -any -clus primary_cluster_name
```

## イーサネット/ネットワーク障害

HA/DR 構成には、2つのタイプのサーバイーサネット接続があります。1つ目はネットワーク通信に使用されるイーサネット接続です (パブリックインターフェイス)。2つ目は、クラスタ内通信専用のイーサネットインターフェイスです (プライベートインターフェイス)。ここでは、イーサネットインターフェイスの各タイプの障害テストケースについて説明します。

- [ネットワーク通信障害 \(99 ページ\)](#)
- [クラスタ通信障害 \(105 ページ\)](#)

## ネットワーク通信障害

ここでは、VCS がネットワーク通信に使用されているネットワークイーサネットポートの障害を検出できることを確認するために使用するテストを示します。ここでは、次の内容について説明します。

- [セカンダリサーバ、シングルクラスタにおけるネットワークイーサネット障害 \(100 ページ\)](#)

- [プライマリサーバ、シングルクラスタにおけるネットワークイーサネット障害 \(101 ページ\)](#)
- [セカンダリサーバ、デュアルクラスタにおけるネットワークイーサネット障害 \(102 ページ\)](#)
- [プライマリサーバ、デュアルクラスタにおけるネットワークイーサネット障害 \(104 ページ\)](#)

## セカンダリサーバ、シングルクラスタにおけるネットワークイーサネット障害

テストケースタイトル：シングルクラスタ構成内のセカンダリサーバのネットワークイーサネット接続で障害が発生しました。

説明：このテストケースでは、VCS がセカンダリサーバのネットワーク イーサネット ポートの障害を検出し、障害の修復後に回復できることを確認します。

テストセットアップ：サーバーごとに1本のネットワーク接続を備えたシングルクラスタ構成内のデュアルノードクラスタ (図)。

**ステップ1** アプリケーションがプライマリサーバで実行されていることを確認します。

**ステップ2** クライアントマシンからアプリケーションにログインします。

**ステップ3** セカンダリサーバのネットワークポートからイーサネットケーブルを取り外して、スイッチ/ルータネットワークとの通信からサーバを分離します。VCS がネットワークポート障害を検出するまで少なくとも 60 秒間待機します。次のコマンドを実行して、VCS がセカンダリサーバの NIC リソースの障害を検出することを確認します。

例：

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System          State          Frozen
A <PrimaryServer>  RUNNING      0
A <SecondaryServer> RUNNING      0
-- GROUP STATE
-- Group           System          Probed    AutoDisabled  State
B APP              <PrimaryServer> Y         N             ONLINE
B APP              <SecondaryServer> Y         N             OFFLINE | FAULTED
-- RESOURCES FAILED
-- Group           Type           Resource   System
C APP              NIC            NIC        <SecondaryServer>
```

**ステップ4** セカンダリサーバのネットワークポートにイーサネットケーブルを戻します。次のコマンドを実行して、障害の解消を VCS が検出することを確認します。

例：

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System          State          Frozen
A <PrimaryServer>  RUNNING      0
A <SecondaryServer> RUNNING      0
-- GROUP STATE
```

-- Group	System	Probed	AutoDisabled	State
B APP	<PrimaryServer>	Y	N	ONLINE
B APP	<SecondaryServer>	Y	N	OFFLINE

## プライマリサーバ、シングルクラスタにおけるネットワークイーサネット障害

テストケースタイトル：シングルクラスタ構成内のプライマリサーバのネットワークイーサネット接続で障害が発生しました。

説明：このテストケースでは、VCSがプライマリサーバのネットワークイーサネットポートの障害を検出し、アプリケーションを自動的にセカンダリサーバに切り替えることができることを確認します。問題が修正された後、アプリケーションを再びプライマリサーバに手動で切り替えることができます。

テストセットアップ：サーバーごとに1本のネットワーク接続を備えたデュアルノードクラスタ（[図 4: デュアルノードサイトのイーサネット接続とストレージ接続（19 ページ）](#)）。

**ステップ 1** アプリケーションがプライマリサーバで実行されていることを確認します。

**ステップ 2** プライマリサーバのネットワークポートからイーサネットケーブルを取り外して、スイッチ/ルータネットワークとの通信からサーバを分離します。VCSがNICリソースの障害を検出し、自動的にセカンダリサーバにAPPサービスグループを切り替えることを確認します。

例：

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System          State          Frozen
A <PrimaryServer>  RUNNING      0
A <SecondaryServer> RUNNING      0
-- GROUP STATE
-- Group          System          Probed    AutoDisabled  State
B APP            <PrimaryServer> Y         N             OFFLINE | FAULTED
B APP            <SecondaryServer> Y         N             ONLINE
-- RESOURCES FAILED
-- Group          Type           Resource   System
C APP            NIC            NIC        <PrimaryServer>
C APP            IP             APP_IP     <PrimaryServer>
```

**ステップ 3** セカンダリサーバで実行中のアプリケーションにログインできることを確認します。

**ステップ 4** プライマリサーバのネットワークポートのイーサネットケーブルを交換し、プライマリサーバの障害が発生しているIPリソースを手動でクリアします。

例：

```
C:\> hares -clear APP_IP -sys primary_server_name
```

**ステップ 5** APPサービスグループを再びプライマリサーバに手動で切り替えます。

例：

```
C:\> hagr -switch APP -to primary_server_name
```

## セカンダリサーバ、デュアルクラスタにおけるネットワークイーサネット障害

テストケースタイトル：デュアルクラスタ構成内のセカンダリサーバのネットワークイーサネット接続で障害が発生しました。

説明：このテストケースでは、VCSがネットワークイーサネットポートの障害を検出し、障害の修復後に回復できることを確認します。

テストセットアップ：クラスタごとにシングルノード、およびサーバごとに1本のイーサネットネットワーク接続を備えたデュアルクラスタ構成 (図)。

**ステップ1** APP サービスグループがプライマリクラスタ/サーバで実行されていることを確認します。

**ステップ2** クライアントマシンから Security Manager にログインします。

**ステップ3** セカンダリクラスタ内のサーバのネットワークポートからイーサネットケーブルを取り外します。これにより、スイッチ/ルータネットワークとの通信からサーバが分離され、複製が中断されます。プライマリサーバで、次のコマンドを実行して、複製が中断（切断）されたことを確認します。

例：

```
C:\> vxprint -Pl
Diskgroup = datadg
Rlink      : rlk_172_6037
info       : timeout=500 packet_size=1400
            latency_high_mark=10000 latency_low_mark=9950
            bandwidth_limit=none
state      : state=ACTIVE
            synchronous=off latencyprot=off srlprot=off
assoc     : rvg=CSM_RVG
            remote_host=172.25.84.34
            remote_dg=datadg
            remote_rlink=rlk_172_32481
            local_host=172.25.84.33
protocol   : UDP/IP
flags     : write attached consistent disconnected
```

**ステップ4** プライマリサーバから次のコマンドを実行して、セカンダリクラスタとの通信が失われたことを確認します。

例：

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System          State          Frozen
A <PrimaryServer>  RUNNING       0
-- GROUP STATE
-- Group           System          Probed    AutoDisabled  State
B APP              <PrimaryServer> Y         N             ONLINE
B APPrep           <PrimaryServer> Y         N             ONLINE
B ClusterService  <PrimaryServer> Y         N             ONLINE
-- WAN HEARTBEAT STATE
```

```

-- Heartbeat      To      State
L Icmp           csm_secondary  ALIVE
-- REMOTE CLUSTER STATE
-- Cluster       State
M csm_secondary  LOST_CONN
-- REMOTE SYSTEM STATE
-- cluster:system      State      Frozen
N csm_secondary:<SecondaryServer>  RUNNING  0
-- REMOTE GROUP STATE
-- Group           cluster:system      Probed      AutoDisabled  State
O APP csm_secondary:<SecondaryServer>  Y           N           OFFLINE

```

**ステップ5** ネットワークイーサネットケーブルをセカンダリサーバに再接続し、複製が再開されたことを確認します。

例：

```

C:\> vxprint -Pl
Diskgroup = datadg
Rlink      : rlk_172_6037
info       : timeout=29 packet_size=1400
            latency_high_mark=10000 latency_low_mark=9950
            bandwidth_limit=none
state      : state=ACTIVE
            synchronous=off latencyprot=off srlprot=off
assoc      : rvg=CSM_RVG
            remote_host=172.25.84.34
            remote_dg=datadg
            remote_rlink=rlk_172_32481
            local_host=172.25.84.33
protocol   : UDP/IP
flags      : write attached consistent connected

```

**ステップ6** セカンダリクラスタへの通信が復元されたことを確認します。

例：

```

C:\> hastatus -sum
-- SYSTEM STATE
-- System      State      Frozen
A <PrimaryServer>  RUNNING  0
-- GROUP STATE
-- Group       System      Probed      AutoDisabled  State
B APP          <PrimaryServer>  Y           N           ONLINE
B APPrep       <PrimaryServer>  Y           N           ONLINE
B ClusterService <PrimaryServer>  Y           N           ONLINE
-- WAN HEARTBEAT STATE
-- Heartbeat   To      State
L Icmp         csm_secondary  ALIVE
-- REMOTE CLUSTER STATE
-- Cluster     State
M csm_secondary  RUNNING
-- REMOTE SYSTEM STATE
-- cluster:system      State      Frozen
N csm_secondary:<SecondaryServer>  RUNNING  0
-- REMOTE GROUP STATE
-- Group           cluster:system      Probed      AutoDisabled  State
O APP csm_secondary:<SecondaryServer>  Y           N           OFFLINE

```

**ステップ7** 複製が回復しない場合は、次のように障害が発生したIPリソースを手動でクリアし、次にセカンダリでAPPrepサービスグループを開始する必要があります。

例：

```
C:\> hares -clear APP_IP
C:\> hagrpr -online APPprep -sys secondary_server_name
```

## プライマリサーバ、デュアルクラスタにおけるネットワークイーサネット障害

テストケースタイトル：プライマリサーバのネットワークイーサネット接続で障害が発生しました。

説明：このテストケースでは、VCSがプライマリサーバのネットワークイーサネットポートの障害を検出し、セカンダリサーバでアプリケーションを起動して回復できることを確認します。イーサネット接続の復元後、元のプライマリサーバに手動でフェールオーバーし、セカンダリでの実行中に行われたデータ変更を保持します。

テストセットアップ：各クラスタ内に1台のノードが配置されたデュアルクラスタ構成 (図)。

**ステップ1** APP サービスグループがプライマリクラスタで実行されていることを確認します。

**ステップ2** プライマリクラスタ内のサーバのポートからイーサネットケーブルを取り外して、スイッチ/ルータネットワークとの通信からサーバを分離します。VCSは、IPおよびNICリソースの障害としてこれを検出する必要があります。VCSが障害を検出し、APP サービスグループを停止したことを確認します。

例：

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System          State          Frozen
A <PrimaryServer>  RUNNING      0
-- GROUP STATE
-- Group           System        Probed    AutoDisabled  State
B APP              <PrimaryServer> Y         N           OFFLINE
B APPprep         <PrimaryServer> Y         N           OFFLINE | FAULTED
B ClusterService <PrimaryServer> Y         N           ONLINE
-- RESOURCES FAILED
-- Group           Type          Resource   System
C APPprep         IP            APP_IP    <PrimaryServer>
C APPprep         NIC          NIC       <PrimaryServer>
-- WAN HEARTBEAT STATE
-- Heartbeat      To           State
L Icmp            csm_secondary DOWN
-- REMOTE CLUSTER STATE
-- Cluster        State
M csm_secondary  FAULTED
-- REMOTE SYSTEM STATE
-- cluster:system State          Frozen
N csm_secondary:<SecondaryServer> FAULTED      0
-- REMOTE GROUP STATE
-- Group          cluster:system Probed    AutoDisabled  State
O APP            csm_secondary:<SecondaryServer> Y         N           OFFLINE
```

**ステップ3** セカンダリサーバで次のコマンドを使用して、セカンダリクラスタの APP サービスグループを開始します。

例：

```
C:\> hagr -online -force APP -sys secondary_server_name
```

**ステップ4** クライアントマシンから、Security Manager にログインして Security Manager が動作していることを確認します。プライマリサーバに切り替えたときに変更が維持されることを確認できるように、データを変更します。

**ステップ5** プライマリクラスタサーバにネットワークイーサネットケーブルを再接続します。

**ステップ6** IP リソースの障害を取り除き、プライマリサーバから APPrep サービスをオンにします。

例：

```
C:\> hares -clear APP_IP  
C:\> hagr -online APPrep -sys primary_server_name
```

**ステップ7** 元のプライマリ RVG をセカンダリに変換し、高速フェールバック機能を使用して、元のプライマリ RVG のデータボリュームを新しいプライマリ RVG のデータボリュームと同期します。セカンダリクラスタの Cluster Explorer を使用して、RVGPrimary リソース (APP\_RVGPrimary) を右クリックし、[アクション (actions)] を選択して [アクション (Actions)] ダイアログボックスから [fbsync (fbsync)] を選択し、[OK (OK)] をクリックします。または、次のコマンドを発行できます。

例：

```
C:\> hares -action APP_RVGPrimary fbsync 0 -sys secondary_server_name
```

**ステップ8** セカンダリクラスタで VCS Cluster Explorer を使用して、[APP (APP)] サービスグループを選択します。ショートカットメニューから、[切り替え (Switch To)]、[リモート切り替え (...)] (Remote Switch(...)) ] の順に選択して [Switch global] ダイアログボックスを開きます。ダイアログボックスで、プライマリクラスタとプライマリサーバを指定します。または、次のコマンドを発行します。

例：

```
C:\> hagr -switch APP -any -clus primarycluster
```

**ステップ9** アプリケーションにログインして、セカンダリサーバに加えた変更が保持されていることを確認します。

## クラスタ通信障害

テストケースタイトル：クラスタ通信に使用されるイーサネットで障害が発生しました。

説明：クラスタ内通信のためにクラスタ内のサーバ間で使用されている専用のイーサネット接続で障害が発生しました。テストでは、3本のうち最大2本の冗長通信パスが失われた場合でも、クラスタ通信が継続されることを確認します。

テストセットアップ：2本の専用クラスタ通信イーサネット接続、およびネットワークイーサネット接続に設定されたプライオリティの低いクラスタ通信接続を備えた、シングルクラスタ構成のデュアルノードクラスタ (☒)。



(注) このテストケースで指定されたコマンドに加えて、Cluster Explorer からツリーでルートノードを選択し、[システムの接続性 (System Connectivity)] タブを選択することによってクラスタ通信のステータスをモニタできます。

**ステップ 1** 次のコマンドを発行して、すべてのシステムが GAB を介して通信していることを確認します。

(注) Group Membership Services/Atomic Broadcast (GAB) は、クラスタメンバーシップやクラスタ通信を担当する VCS プロトコルです。

例 :

```
# gabconfig -a
GAB Port Memberships
=====
Port a gen e8cc02 membership 01
Port h gen e8cc01 membership 01
```

**ステップ 2** プライマリサーバでクラスタ通信に使用される最初の専用イーサネットポートからイーサネットケーブルを取り外します。

**ステップ 3** 次のコマンドを発行して、クラスタ通信に使用されるリンクの詳細なステータスを表示し、最初の専用クラスタ通信ポートがダウンしていることを確認します。

(注) 出力のアスタリスク (\*) は、コマンドが実行されるサーバを示します。コマンドが実行されるサーバは、これらのポートの 1 つ以上が物理的に切断されている場合でも、常にリンクがアップしていることを示します。

例 :

```
# lltstat -nvv
LLT node information:
  Node          State  Link  Status  Address
  * 0 <PrimaryServer> OPEN
                Adapter0  UP    00:14:5E:28:52:9C
                Adapter1  UP    00:14:5E:28:52:9D
                Adapter2  UP    00:0E:0C:9C:20:FE
  1 <SecondaryServer> OPEN
                Adapter0  DOWN
                Adapter1  UP    00:14:5E:28:27:17
                Adapter2  UP    00:0E:0C:9C:21:C2
  ...
```

**ステップ 4** ネットワークインターフェイスにプライオリティの低いハートビートリンクを設定した場合は、プライマリサーバのクラスタ通信に使用される 2 本目の専用イーサネットポートからイーサネットケーブルを取り外します。

**ステップ 5** 次のコマンドを発行して、すべてのシステムが GAB を介して通信していることを確認します。各サーバではハートビートが 1 つだけ動作しているため、クラスタ内の両方のサーバが Jeopardy 状態になったことも確認します。

例 :



```
# gabconfig -a
GAB Port Memberships
=====
Port a gen e8cc02 membership 01
Port a gen e8cc02 jeopardy ;1
Port h gen e8cc01 membership 01
Port h gen e8cc01 jeopardy ;1
```

**ステップ6** 次のコマンドを発行して、クラスタ通信に使用されるリンクの詳細なステータスを表示し、プライマリサーバ上のクラスタ通信に使用される2つ目の専用イーサネットポートがダウンしていることを確認します。

例：

```
# llstat -nv
LLT node information:
Node          State   Link  Status  Address
* 0 <PrimaryServer> OPEN
              Adapter0  UP    00:14:5E:28:52:9C
              Adapter1  UP    00:14:5E:28:52:9D
              Adapter2  UP    00:0E:0C:9C:20:FE
1 <SecondaryServer> OPEN
              Adapter0  DOWN
              Adapter1  UP    00:14:5E:28:27:17
              Adapter2  DOWN
```

**ステップ7** プライマリサーバでクラスタ通信に使用される2つ目の専用イーサネットポートのイーサネットケーブルを交換します。

**ステップ8** 次のコマンドを発行して、Jeopardy 状態が解消されたことを確認します。

例：

```
# gabconfig -a
GAB Port Memberships
=====
Port a gen e8cc02 membership 01
Port h gen e8cc01 membership 01
```

**ステップ9** プライマリサーバでクラスタ通信に使用される最初の専用イーサネットポートのイーサネットケーブルを交換します。

## サーバの障害

ここでは、サーバから電源を取り外してサーバ障害を引き起こします。4つのケースについて説明します。

- [スタンバイサーバの障害、シングルクラスタ \(108 ページ\)](#)
- [プライマリサーバの障害、シングルクラスタ \(108 ページ\)](#)
- [スタンバイサーバの障害、デュアルクラスタ \(109 ページ\)](#)
- [プライマリサーバの障害、デュアルクラスタ \(111 ページ\)](#)

## スタンバイサーバの障害、シングルクラスタ

テストケースタイトル：シングルクラスタ構成のスタンバイサーバで障害が発生しました。

説明：このテストケースでは、プライマリサーバで稼働しているアプリケーションが影響を受けないことと、スタンバイサーバが修復された後、アプリケーションが正常にクラスタ構成に再度参加できることを確認します。

テストセットアップ：2本の専用クラスタ通信イーサネット接続、およびネットワークイーサネット接続のプライオリティの低いクラスタ通信接続を備えた、デュアルノードクラスタ（[図4：デュアルノードサイトのイーサネット接続とストレージ接続（19ページ）](#)）。

**ステップ1** アプリケーションがクラスタ内のプライマリサーバで実行されていることを確認します。

例：

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System          State          Frozen
A <PrimaryServer>  RUNNING       0
A <SecondaryServer> RUNNING       0
-- GROUP STATE
-- Group           System          Probed    AutoDisabled  State
B APP              <PrimaryServer> Y         N             ONLINE
B APP              <SecondaryServer> Y         N             OFFLINE
```

**ステップ2** セカンダリサーバの電源を取り外し、VCSが障害を検出し、アプリケーションがプライマリサーバで実行し続けることを確認します。

例：

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System          State          Frozen
A <PrimaryServer>  RUNNING       0
A <SecondaryServer> FAULTED       0
-- GROUP STATE
-- Group           System          Probed    AutoDisabled  State
B APP              <PrimaryServer> Y         N             ONLINE
```

**ステップ3** 電源を再度適用し、セカンダリサーバをブートします。サーバが回復したら、次のコマンドを実行して、正常な状態でクラスタに再接続されていることを確認します。出力はステップ1の出力と同一である必要があります。

例：

```
C:\> hastatus -sum
```

## プライマリサーバの障害、シングルクラスタ

テストケースタイトル：シングルクラスタ内のプライマリサーバで障害が発生しました。

説明：このテストケースでは、プライマリサーバーで障害が発生するとセカンダリサーバーでアプリケーションが実行を開始することと、プライマリサーバーが修復された後、アプリケーションをプライマリサーバーで再設定できることを確認します。

テストセットアップ：デュアルノードクラスタ (図)。

**ステップ 1** 次のコマンドの出力を調べて、APP サービスグループがクラスタ内のプライマリサーバで実行されていることを確認します。

例：

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System          State          Frozen
A <PrimaryServer>  RUNNING       0
A <SecondaryServer> RUNNING       0
-- GROUP STATE
-- Group           System          Probed      AutoDisabled  State
B APP              <PrimaryServer> Y           N             ONLINE
B APP              <SecondaryServer> Y           N             OFFLINE
```

**ステップ 2** プライマリサーバの電源を取り外し、VCS が障害を検出し、APP サービスグループがセカンダリサーバに正常に移行されることを確認します。

例：

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System          State          Frozen
A <PrimaryServer>  FAULTED       0
A <SecondaryServer> RUNNING       0
-- GROUP STATE
-- Group           System          Probed      AutoDisabled  State
B APP              <SecondaryServer> Y           N             ONLINE
```

**ステップ 3** クライアントマシンから Security Manager に正常にログインできることを確認します。

**ステップ 4** 電源をプライマリサーバに復元し、サーバが正常な状態でクラスタに再参加できることを確認します。次のコマンドを実行します。出力はステップ 1 の出力と同一である必要があります。

例：

```
C:\> hastatus -sum
```

**ステップ 5** APP サービスグループを再びプライマリサーバに手動で切り替えます。

例：

```
C:\> hagrps -switch APP -to primary_server_name
```

## スタンバイサーバの障害、デュアルクラスタ

テストケースタイトル：デュアルクラスタ構成のスタンバイサーバーで障害が発生しました。

説明：このテストケースでは、プライマリクラスタで稼働しているアプリケーションがスタンバイサーバーの障害の影響を受けないことと、スタンバイサーバーが修復された後、アプリケーションが正常にデュアルクラスタ構成に再度参加できることを確認します。

テストセットアップ：各クラスタ内に複製が行われる1台のノードが配置されたデュアルクラスタ構成 (図)。

**ステップ1** プライマリサーバで次のコマンドを実行して、APPおよびClusterService サービスグループがプライマリクラスタで動作していることを確認します。

例：

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System          State          Frozen
A <PrimaryServer>  RUNNING      0
-- GROUP STATE
-- Group           System          Probed    AutoDisabled  State
B APP              <PrimaryServer> Y         N           ONLINE
B APPPrep          <PrimaryServer> Y         N           ONLINE
B ClusterService  <PrimaryServer> Y         N           ONLINE
-- WAN HEARTBEAT STATE
-- Heartbeat       To              State
L Icmp             csm_secondary  ALIVE
-- REMOTE CLUSTER STATE
-- Cluster         State
M csm_secondary   RUNNING
-- REMOTE SYSTEM STATE
-- cluster:system  State          Frozen
N csm_secondary:<SecondaryServer> RUNNING      0
-- REMOTE GROUP STATE
-- Group           cluster:system  Probed    AutoDisabled  State
O APP              csm_secondary:<SecondaryServer> Y         N           OFFLINE
```

**ステップ2** 電源をセカンダリサーバから取り外し、プライマリクラスタがセカンダリクラスタとの通信の喪失を検出することを確認します。

例：

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System          State          Frozen
A <PrimaryServer>  RUNNING      0
-- GROUP STATE
-- Group           System          Probed    AutoDisabled  State
B APP              <PrimaryServer> Y         N           ONLINE
B APPPrep          <PrimaryServer> Y         N           ONLINE
B ClusterService  <PrimaryServer> Y         N           ONLINE
-- WAN HEARTBEAT STATE
-- Heartbeat       To              State
L Icmp             csm_secondary  ALIVE
-- REMOTE CLUSTER STATE
-- Cluster         State
M csm_secondary   LOST_CONN
-- REMOTE SYSTEM STATE
-- cluster:system  State          Frozen
N csm_secondary:<SecondaryServer> RUNNING      0
-- REMOTE GROUP STATE
```

```
-- Group          cluster:system          Probed      AutoDisabled      State
0 APP            csm_secondary:<SecondaryServer> Y           N            OFFLINE
```

**ステップ3** セカンダリサーバに電源を戻します。サーバの再起動後、プライマリクラスタで次のコマンドを実行して、セカンダリクラスタとの通信を再確立したことを確認します。出力はステップ1の出力と同一である必要があります。

例：

```
C:\> hastatus -sum
```

**ステップ4** 次のコマンドを実行して、複製が機能し、矛盾していないことを確認します。

例：

```
C:\> vxprint -Pl
Diskgroup = BasicGroup
Diskgroup = datadg
Rlink      : rlk_172_6037
info       : timeout=16 packet_size=1400
            latency_high_mark=10000 latency_low_mark=9950
            bandwidth_limit=none
state      : state=ACTIVE
            synchronous=off latencyprot=off srlprot=off
assoc      : rvg=CSM_RVG
            remote_host=172.25.84.34
            remote_dg=datadg
            remote_rlink=rlk_172_32481
            local_host=172.25.84.33
protocol   : UDP/IP
flags      : write attached consistent connected
```

## プライマリサーバの障害、デュアルクラスタ

テストケースタイトル：デュアルクラスタ構成のプライマリサーバで障害が発生しました。

説明：このテストケースでは、プライマリサーバで障害が発生するとセカンダリサーバでアプリケーションが実行を開始することと、プライマリサーバが修復された後、アプリケーションをプライマリサーバで再設定できることを確認します。

テストセットアップ：各クラスタ内に複製が行われる1台のノードが配置されたデュアルクラスタ構成 (図)。

**ステップ1** セカンダリサーバから次のコマンドを実行して、APPおよびClusterService サービスグループがプライマリクラスタで動作していることを確認します。

例：

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System          State          Frozen
A <SecondaryServer>  RUNNING       0
-- GROUP STATE
```

```

-- Group          System          Probed    AutoDisabled    State
B APP             <SecondaryServer> Y          N               OFFLINE
B APPrep         <SecondaryServer> Y          N               ONLINE
B ClusterService <SecondaryServer> Y          N               ONLINE
-- WAN HEARTBEAT STATE
-- Heartbeat      To          State
L Icmp           csm_primary ALIVE
-- REMOTE CLUSTER STATE
-- Cluster        State
M csm_primary    RUNNING
-- REMOTE SYSTEM STATE
-- cluster:system State          Frozen
N csm_primary:<PrimaryServer> RUNNING 0
-- REMOTE GROUP STATE
-- Group          cluster:system Probed    AutoDisabled    State
O APP            csm_primary:<PrimaryServer> Y          N          ONLINE

```

**ステップ2** プライマリサーバから電源を取り外してサーバ障害を引き起こします。セカンダリクラスタがプライマリクラスタへの接続の喪失を報告したことを確認します。

例：

```

C:\> hastatus -sum
-- SYSTEM STATE
-- System          State          Frozen
A <SecondaryServer> RUNNING       0
-- GROUP STATE
-- Group          System          Probed    AutoDisabled    State
B APP             <SecondaryServer> Y          N               OFFLINE
B APPrep         <SecondaryServer> Y          N               ONLINE
B ClusterService <SecondaryServer> Y          N               ONLINE
-- WAN HEARTBEAT STATE
-- Heartbeat      To          State
L Icmp           csm_primary ALIVE
-- REMOTE CLUSTER STATE
-- Cluster        State
M csm_primary    LOST_CONN
-- REMOTE SYSTEM STATE
-- cluster:system State          Frozen
N csm_primary:<PrimaryServer> RUNNING 0
-- REMOTE GROUP STATE
-- Group          cluster:system Probed    AutoDisabled    State
O APP            csm_primary:<PrimaryServer> Y          N          ONLINE

```

**ステップ3** 複製の状態が **disconnected** であることを確認します。次のコマンド出力の **flags** パラメータからこの状態を確認できます。

例：

```

C:\> vxprint -Pl
Diskgroup = BasicGroup
Diskgroup = datadg
Rlink      : rlk_172_32481
info       : timeout=500 packet_size=1400
            latency_high_mark=10000 latency_low_mark=9950
            bandwidth_limit=none
state      : state=ACTIVE
            synchronous=off latencyprot=off srlprot=off
assoc     : rvg=CSM_RVG
            remote_host=172.25.84.33
            remote_dg=datadg
            remote_rlink=rlk_172_6037

```

```

        local_host=172.25.84.34
protocol   : UDP/IP
flags      : write attached consistent disconnected

```

**ステップ4** 次のコマンドを使用してセカンダリサーバでアプリケーションを起動します。

例：

```
C:\> hagr -online -force APP -sys secondary_server_name
```

**ステップ5** アプリケーションにログインし、プライマリサーバに戻っても、アプリケーションがセカンダリサーバ上で稼働している間に行われた変更を保持できることを後で確認できるように、データを変更します。

**ステップ6** 電源をプライマリサーバに戻し、サーバが完全に起動できるようにします。

**ステップ7** 複製が **connected** であることを示す複製のステータスを確認します。ただし、両側が同期していません。

例：

```

C:\> vxprint -Pl
Diskgroup = BasicGroup
Diskgroup = datadg
Rlink      : rlk_172_32481
info       : timeout=500 packet_size=1400
            latency_high_mark=10000 latency_low_mark=9950
            bandwidth_limit=none
state      : state=ACTIVE
            synchronous=off latencyprot=off srlprot=off
assoc      : rvg=CSM_RVG
            remote_host=172.25.84.33
            remote_dg=datadg
            remote_rlink=rlk_172_6037
            local_host=172.25.84.34
protocol   : UDP/IP
flags      : write attached consistent connected dcm_logging failback_logging

```

**ステップ8** 元のプライマリ RVG をセカンダリに変換し、高速フェールバック機能を使用して、元のプライマリ RVG のデータボリュームを新しいプライマリ RVG のデータボリュームと同期します。セカンダリクラスタの Cluster Explorer を使用して、RVGPrimary リソース (APP\_RVGPrimary) を右クリックし、[アクション (actions)] を選択して [アクション (Actions)] ダイアログボックスから [fbsync (fbsync)] を選択し、[OK (OK)] をクリックします。または、次のコマンドを発行できます。

例：

```
C:\> hares -action APP_RVGPrimary fbsync 0 -sys secondary_server_name
```

**ステップ9** 次のコマンド出力の **flags** パラメータの **consistent** キーワードを調べて、現在のセカンダリ (以前のプライマリ) が現在のプライマリ (以前のセカンダリ) と同期していることを確認します。

例：

```

C:\> vxprint -Pl
Diskgroup = BasicGroup
Diskgroup = datadg
Rlink      : rlk_172_32481
info       : timeout=29 packet_size=1400
            latency_high_mark=10000 latency_low_mark=9950
            bandwidth_limit=none
state      : state=ACTIVE

```

```

synchronous=off latencyprot=off srlprot=off
assoc      : rvg=CSM_RVG
            remote_host=172.25.84.33
            remote_dg=datadg
            remote_rlink=rlk_172_6037
            local_host=172.25.84.34
protocol   : UDP/IP
flags      : write attached consistent connected

```

**ステップ 10** セカンダリクラスタで VCS Cluster Explorer を使用して、[APP (APP)] サービスグループを選択します。ショートカットメニューから、[切り替え (Switch To)]、[リモート切り替え (...)] (Remote Switch(...)) の順に選択して [グローバルに切り替え (Switch global)] ダイアログボックスを開きます。ダイアログボックスで、プライマリクラスタとプライマリサーバを指定します。または、次のコマンドを発行します。primarycluster はプライマリクラスタの名前です。

例：

```
C:\> hagr -switch APP -any -clus primarycluster
```

**ステップ 11** アプリケーションにログインして、セカンダリサーバに加えた変更が保持されていることを確認します。

## アプリケーションの障害

ここでは、Security Manager アプリケーションで障害が発生した場合のテストケースについて説明します。シングルクラスタ構成とデュアルクラスタ構成の2つのケース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。

- [アプリケーションの障害、シングルクラスタ \(114 ページ\)](#)
- [アプリケーションの障害、デュアルクラスタ \(115 ページ\)](#)

### アプリケーションの障害、シングルクラスタ

テストケースタイトル：シングルクラスタ構成内のプライマリサーバでアプリケーションの障害が発生しました。

説明：このテストケースでは、VCS がアプリケーションの障害を検出し、アプリケーションを自動的にセカンダリサーバに移行することを確認します。

テストセットアップ：デフォルトのアプリケーションフェールオーバー動作を使用するデュアルノードクラスタ (☒)。

**ステップ 1** 次のコマンドを実行して、APP サービスグループがクラスタ内のプライマリサーバで実行されていることを確認します。

例：

```
C:\> hastatus -sum
```



```

-- SYSTEM STATE
-- System          State          Frozen
A <PrimaryServer>  RUNNING      0
A <SecondaryServer>  RUNNING      0
-- GROUP STATE
-- Group           System          Probed    AutoDisabled  State
B APP              <PrimaryServer>  Y         N              ONLINE
B APP              <SecondaryServer> Y         N              OFFLINE

```

**ステップ 2** Security Manager が実行されているサーバーで、次のコマンドを発行してアプリケーションを停止します。

例：

```
C:\> net stop crmdmgt
```

**ステップ 3** VCS がプライマリサーバーで Security Manager が失敗したことを検出し、アプリケーションをセカンダリサーバーで開始することを確認します。

例：

```

# hastatus -sum
-- SYSTEM STATE
-- System          State          Frozen
A <PrimaryServer>  RUNNING      0
A <SecondaryServer>  RUNNING      0
-- GROUP STATE
-- Group           System          Probed    AutoDisabled  State
B APP              <PrimaryServer>  Y         N              OFFLINE | FAULTED
B APP              <SecondaryServer> Y         N              ONLINE
-- RESOURCES FAILED
-- Group           Type            Resource          System
C APP              CSManager       APP_CSManager    <PrimaryServer>

```

**ステップ 4** APP サービスグループの障害を手動で解決します。

例：

```
C:\> hagr -clear APP -sys primary_server_name
```

**ステップ 5** APP サービスグループを再びプライマリサーバに手動で切り替えます。

例：

```
C:\> hagr -switch APP -to primary_server_name
```

## アプリケーションの障害、デュアルクラスタ

テストケースタイトル：デュアルクラスタ構成内のプライマリサーバでアプリケーションの障害が発生しました。

説明：このテストケースでは、VCSがアプリケーションの障害を検出することを確認します。

テストセットアップ：各クラスタ内に複製が行われる1台のノードが配置されたデュアルクラスタ構成 (図)。同様に、デフォルトのアプリケーションフェールオーバー動作が変更されて

いない（つまり、クラスタ間のフェールオーバーに手動による介入が必要である）ことを前提とします。

**ステップ 1** プライマリサーバで次のコマンドを実行して、APP および ClusterService サービスグループがプライマリクラスタで動作していることを確認します。

例：

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System          State          Frozen
A <SecondaryServer>  RUNNING      0
-- GROUP STATE
-- Group           System          Probed    AutoDisabled  State
B APP              <SecondaryServer> Y         N            OFFLINE
B APPrep           <SecondaryServer> Y         N            ONLINE
B ClusterService  <SecondaryServer> Y         N            ONLINE
-- WAN HEARTBEAT STATE
-- Heartbeat       To              State
L Icmp             csm_primary    ALIVE
-- REMOTE CLUSTER STATE
-- Cluster         State
M csm_primary      RUNNING
-- REMOTE SYSTEM STATE
-- cluster:system  State          Frozen
N csm_primary:<PrimaryServer> RUNNING      0
-- REMOTE GROUP STATE
-- Group           cluster:system  Probed    AutoDisabled  State
O APP              csm_primary:<PrimaryServer> Y         N            ONLINE
```

**ステップ 2** Security Manager が実行されているサーバで、次のコマンドを発行してアプリケーションを停止します。

例：

```
C:\> net stop crmdmgtd
```

**ステップ 3** VCS がアプリケーションの障害を検出し、APP サービスグループを停止したことを確認します。次のコマンドを発行し、出力を確認します。

例：

```
# hastatus -sum
-- SYSTEM STATE
-- System          State          Frozen
A <PrimaryServer>  RUNNING      0
-- GROUP STATE
-- Group           System          Probed    AutoDisabled  State
B APP              <PrimaryServer> Y         N            OFFLINE|FAULTED
B APPrep           <PrimaryServer> Y         N            ONLINE
B ClusterService  <PrimaryServer> Y         N            ONLINE
-- RESOURCES FAILED
-- Group           Type            Resource   System
C APP              CSManager      APP_CSManager  <PrimaryServer>
-- WAN HEARTBEAT STATE
-- Heartbeat       To              State
L Icmp             csm_secondary  ALIVE
-- REMOTE CLUSTER STATE
-- Cluster         State
M csm_secondary   RUNNING
```

```
-- REMOTE SYSTEM STATE
-- cluster:system          State          Frozen
N csm_secondary:<SecondaryServer> RUNNING 0
-- REMOTE GROUP STATE
-- Group                    cluster:system    Probed    AutoDisabled    State
O APP                       csm_secondary:<SecondaryServer> Y         N          OFFLINE
```

**ステップ4** APP サービスグループの障害を手動で解決します。

例：

```
C:\> hagr -clear APP
```

**ステップ5** APP サービスグループをプライマリサーバでオンラインにしてアプリケーションを再起動します。

例：

```
C:\> hagr -online APP -sys primary_server_name
```

---



## 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。