

vSphere のアップグレード

Update 2

変更日：2020 年 8 月 11 日

VMware vSphere 6.0

VMware ESXi 6.0

vCenter Server 6.0

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>)

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴィエムウェア株式会社
〒108-0023 東京都港区芝浦 3-1-1
田町ステーションタワー N 18 階
www.vmware.com/jp

Copyright © 2009-2021 VMware, Inc. All rights reserved. 著作権および商標情報。

目次

『vSphere のアップグレード』について 8

更新情報 9

1 vSphere のアップグレードの概要 11

- vCenter Server のコンポーネントおよびサービス 12
- vSphere 6.0 と vSphere 5.x の違い 14
- vCenter Server のデプロイ モデル 16
- vSphere アップグレード プロセス 19
 - vCenter Server のアップグレード時のバージョン混在の移行環境 21
 - vSphere ライセンス サービスへのアップグレード 26
 - vSphere のアップグレードとアップデートの違い 27
- vCenter Single Sign-On がアップグレードに与える影響 27
- vSphere セキュリティ証明書の概要 29
- 拡張リンク モードの概要 30
- vCenter Server のアップグレード パスの例 30

2 アップグレード要件 35

- vCenter Server アップグレード互換性 35
- Windows 版 vCenter Server の要件 36
 - Windows 版 vCenter Server の Pre-Upgrade Checker 37
 - Windows 用 vCenter Server のストレージ要件 38
 - Windows 版 vCenter Server のハードウェア要件 38
 - Windows 版 vCenter Server のソフトウェア要件 39
 - Windows 版 vCenter Server データベースの要件 39
- vCenter Server Appliance の要件 40
 - vCenter Server Appliance のハードウェア要件 40
 - vCenter Server Appliance のストレージ要件 40
 - vCenter Server Appliance に含まれるソフトウェア 41
 - vCenter Server Appliance のソフトウェア要件 41
 - vCenter Server Appliance データベースの要件 41
- vCenter Server および Platform Services Controller に必要なポート 42
- vCenter Server データベースの構成に関する注意事項 47
- ESXi の要件 48
 - ESXi のハードウェア要件 48
 - サポートされているリモート管理のサーバ モデルとファームウェア バージョン 50
 - ESXi のパフォーマンスを改善するための推奨事項 51
 - ESXi ホストの発着信ファイアウォール ポート 52

- vSphere DNS の要件 54
- vSphere Web Client のソフトウェア要件 55
- クライアント統合プラグインのソフトウェア要件 55
- vSphere Client の要件 56
 - vSphere Client のハードウェア要件 56
 - vSphere Client のソフトウェア要件 57
 - vSphere Client の TCP および UDP ポート 57
- システム ログに必要な空き容量 57

3 vCenter Server をアップグレードする前に行う作業 59

- vCenter Server をアップグレードする前の基本的な互換性の確認 59
- vCenter Server データベースの準備 60
 - vCenter Server 6.0 へアップグレードする前の Oracle データベースの準備 60
 - vCenter Server 6.0 へのアップグレード前に Microsoft SQL Server データベースを準備する 62
 - Microsoft SQL Server データベース スキーマおよびロールの作成と適用を行うためのスクリプトの使用 64
 - vCenter Server 6.0 にアップグレードする前の PostgreSQL データベースの準備 66
 - vCenter Server のデータベース権限の要件 66
 - vCenter Server がローカル データベースと通信できることの確認 69
- アップグレード前のネットワークの前提条件の確認 70
- vCenter Server をアップグレードする前のロード バランサの確認 71
- vCenter Server のアップグレードのための ESXi ホストの準備 71
 - ホストのアップグレードと証明書 72
 - 証明書モードの変更 73
- vCenter Server のアップグレード準備が完了したことの確認 74
 - vSphere ネットワーク上の時計の同期 75
 - vCenter Server のアップグレード中のダウンタイム 76
 - vCenter Server を実行するための、ユーザー アカウントの使用 77
- Windows 版 vCenter Server のアップグレードに必要な情報 77
- vCenter Server Appliance のアップグレードに必要な情報 78

4 Windows 版 vCenter Server のアップグレードおよび更新 81

- Windows 版 vCenter Server 6.0 のアップグレード プロセスについて 81
- vCenter Server 6.0 へのアップグレード中の Windows サービス用の分散 vCenter Server の移行 83
- Windows 版 vCenter Server のインストーラのダウンロード 85
- 外部デプロイの vCenter Single Sign-On 5.1 のアップグレード 86
- 外部デプロイの vCenter Single Sign-On 5.5 のアップグレード 89
- vCenter Server 5.0 のアップグレード 92
- Windows 版 vCenter Server 5.1 のアップグレード 94
- Windows 版 vCenter Server 5.5 のアップグレード 97
- VIMPatch での Java コンポーネントと vCenter Server tc Server の更新 100

5 vCenter Server Appliance および Platform Services Controller アプライアンスのアップグレードとパッチ適用 101

vCenter Server Appliance のアップグレード 102

vCenter Server Appliance のアップグレード プロセスについて 102

vCenter Server Appliance のインストーラのダウンロード 105

クライアント統合プラグインのインストール 105

vCenter Single Sign-On が組み込まれた vCenter Server Appliance のアップグレード 106

外部 vCenter Single Sign-On 環境の vCenter Server Appliance のアップグレード 110

vCenter Server Appliance および Platform Services Controller アプライアンスのパッチ適用 115

アプライアンス管理インターフェイスを使用した vCenter Server Appliance へのパッチ適用 116

アプライアンス シェルを使用した vCenter Server Appliance へのパッチ適用 119

6 vCenter Server のアップグレード後 126

vCenter Server アップグレード後のコンポーネントの構成 127

アップグレード後の移行された vCenter Server サービスの再構成 127

vSphere Authentication Proxy のインストールまたはアップグレード 128

vSphere Client へのアップグレード 130

vCenter Server での VMware vCenter Server - tc Server 設定の構成 131

vCenter Server のアップグレード後の最大データベース接続数の設定 133

vCenter Server 管理者ユーザーの設定 133

vCenter Server 環境への認証 134

vCenter Single Sign-On による vCenter Server の ID ソース 134

ESXi 証明書とキー ファイルのリストア 136

別の外部 Platform Services Controller への vCenter Server の再ポイント 136

組み込み Platform Services Controller を使用するスタンドアロン vCenter Server の、外部 Platform Services Controller を使用する vCenter Server への再構成 138

組み込み Platform Services Controller を使用する vCenter Server の複数の参加済みインスタンスの、外部 Platform Services Controller を使用する vCenter Server への再構成 141

組み込み Platform Services Controller インスタンスのサービスが実行されていることの確認 143

すべての外部 Platform Services Controller インスタンスの間のレプリケーション関係の構成 144

各 vCenter Server インスタンスの再構成と組み込みから外部 Platform Services Controller インスタンスへの再ポイント 147

7 Update Manager のアップグレード 151

Update Manager サーバのアップグレード 152

8 ホストをアップグレードする前に行う作業 154

ESXi アップグレードのベスト プラクティス 154

ESXi 6.0 のアップグレード オプション 155

サードパーティ製のカスタム VIB があるホストのアップグレード 157

vSphere Update Manager で実行されるアップグレードには、手動で割り当てられた IP アドレスを使用する 157

ESXi インストーラを起動するためのメディア オプション	157
ESXi インストーラ ISO イメージのダウンロードおよび CD または DVD への書き込み	158
USB フラッシュ ドライブのフォーマットによる ESXi インストールまたはアップグレードの起動	158
USB フラッシュ ドライブを作成して、ESXi インストール スクリプトまたはアップグレード スクリプトを保存する	160
カスタムのインストールまたはアップグレード スクリプトを含む、インストーラ ISO イメージの作成	162
ESXi インストーラの PXE 起動	163
ソフトウェア FCoE による ESXi のインストールおよび起動	171
リモート管理アプリケーションの使用	171
ESXi インストーラのダウンロード	172

9 ホストのアップグレード 173

vSphere Update Manager を使用した、ホストの組織的なアップグレード	173
[]ホストおよびクラスタの設定の構成	174
vSphere Update Manager を使用した、ホストの組織的なアップグレードの実行	175
スクリプトを使用した、ホストのインストールまたはアップグレード	193
インストール スクリプトまたはアップグレード スクリプトを開始するための起動オプションの入力	193
起動オプション	194
インストール スクリプトおよびアップグレード スクリプトについて	195
スクリプトを使用した、CD または DVD からの ESXi のインストールまたはアップグレード	206
スクリプトを使用した、USB フラッシュ ドライブからの ESXi のインストールまたはアップグレード	207
インストーラの PXE 起動による、スクリプトを使用した ESXi のインストールまたはアップグレードの実行	208
vSphere Auto Deploy を使用した、ホストの再プロビジョニング	208
ホストの再プロビジョニング	208
シンプルな再起動操作によるホストの再プロビジョニング	209
新しいイメージ プロファイルを使用したホストの再プロビジョニング	210
ルールの記述とホストへのホスト プロファイルの割り当て	211
ルールのコンプライアンスのテストおよび修復	212
esxcli コマンドを使用した、ホストのアップグレード	213
VIB、イメージ プロファイル、およびソフトウェア デポ	214
VIB およびホストの許容レベルについて	214
更新するためにホストをメンテナンス モードにする必要があるか、再起動する必要があるかの確認	217
ホストをメンテナンス モードに切り替える	218
個々の VIB によるホストの更新	219
イメージ プロファイルによるホストのアップグレードまたは更新	220
Zip ファイルを使用した ESXi ホストのアップデート	223
ホストからの VIB の削除	223
esxcli コマンドを使用した、ホストへのサードパーティ製拡張機能の追加	225
esxcli インストールまたはアップグレードのドライ ランの実行	225
次回ホストを再起動したあとでアクティブになるインストール済み VIB およびプロファイルの表示	226
ホストのイメージ プロファイルと許容レベルの表示	226

ホストの対話型アップグレード 227

10 ESXi ホストをアップグレードした後に行う作業 229

ESXi の評価モードとライセンス モードについて 229

ESXi 6.0 へのアップグレード後の、ライセンスの適用 230

システム ログに必要な空き容量 230

ESXi ホストでの syslog の構成 231

11 仮想マシンと VMware Tools のアップグレード 233

12 vSphere のアップグレードのトラブルシューティング 234

vCenter Server のインストールまたはアップグレードのトラブルシューティングのためのログの収集 234

インストール ウィザードを使用したインストール ログの収集 235

インストール ログの手動による収集 235

vCenter Server Appliance のインストール ログの収集 235

データベース アップグレード ログの収集 236

ESXi ホストをトラブルシューティングするためのログの収集 237

インストールおよびアップグレードの事前チェック スクリプトで返されるエラーおよび警告 237

アップグレードが失敗した場合の vCenter Server サービスのリストア 240

vCenter Server Appliance のアップグレード後の起動中の VMware Component Manager のエラー 240

サポートされていない互換モードに設定されている Microsoft SQL データベースを原因とする vCenter Server のインストールまたはアップグレードの失敗 241

『vSphere のアップグレード』 について

『vSphere のアップグレード』では、VMware vSphere™ を最新のバージョンにアップグレードする方法を説明します。

既存の構成を保持しないフレッシュ インストールを実行して最新バージョンの vSphere に移行するには、『vSphere のインストールとセットアップ』ドキュメントを参照してください。

対象読者

『vSphere のアップグレード』は、vSphere の以前のバージョンからアップグレードする必要があるすべてのユーザーを対象にしています。これらのトピックは、Microsoft Windows または Linux のシステム管理者としての経験があり、仮想マシン テクノロジーおよびデータ センターの運用に詳しい方を対象としています。

更新情報

『vSphere アップグレード』は、製品のリリースごとに、または必要に応じて更新されます。

『vSphere アップグレード』の更新履歴については、次の表をご確認ください。

リビジョン	説明
2021 年 4 月 2 日	VMware は、My VMware ポータルの名称を VMware Customer Connect に変更しました。この名称変更を反映するように『vSphere のアップグレード』ドキュメントを更新しました。
2020 年 8 月 11 日	VMware では、多様性の受け入れを尊重しています。弊社のお客様、パートナー、内部コミュニティにおいてこの原則を推進するため、弊社のコンテンツに含まれている用語の見直しを行っています。不適切な表現を削除するため、このガイドを更新しました。
EN-001989-08	vCenter Server および Platform Services Controller に必要なポートにポート 5480 を追加しました。
EN-001989-07	vCenter Server および Platform Services Controller に必要なポートで、ポート 22 から UDP を削除しました。
JA-001989-06	<ul style="list-style-type: none">■ vCenter Server および Platform Services Controller に必要なポートのポート 514 に関する情報を更新。■ vSphere Update Manager を使用した、ホストの組織的なアップグレード：不要な /boot パーティション容量の要件を削除。
JP-001989-05	<ul style="list-style-type: none">■ boot.cfg ファイルについて：例の参照を追加。■ vSphere Client の TCP および UDP ポート：ポート 903 を削除。■ 別の外部 Platform Services Controller への vCenter Server の再ポイント：タスクのコンテキストと前提条件の情報を改訂。
JA-001989-04	<ul style="list-style-type: none">■ Platform Services Controller が組み込まれた vCenter Server と外部 Platform Services Controller を使用する vCenter Server のハードウェア要件が同じであることを説明するように Windows 版 vCenter Server のハードウェア要件 と vCenter Server Appliance のハードウェア要件 を更新。■ 組み込みと外部の Platform Services Controller インスタンスの間に直接のレプリケーション関係を作成するため、存在しない場合はステップを追加するように、各 vCenter Server インスタンスの再構成と組み込みから外部 Platform Services Controller インスタンスへの再ポイントを更新。
JA-001989-03	<ul style="list-style-type: none">■ vCenter Server および Platform Services Controller に必要なポート のポート 22 の情報を更新。■ トピック vCenter Single Sign-On が組み込まれた vCenter Server Appliance のアップグレード および 外部 vCenter Single Sign-On 環境の vCenter Server Appliance のアップグレード に、アプライアンスのアップグレード中にオープンである必要のあるポートの前提条件を記載。■ 実行ファイルの場所に関する情報を直すため、クライアント統合プラグインのインストール を更新。■ USB フラッシュ ドライブのフォーマットによる ESXi インストールまたはアップグレードの起動 の前提条件と手順を修正。
JA-001989-02	<ul style="list-style-type: none">■ vCenter Server および Platform Services Controller に必要なポート のポート 389、636、11711、11712 の情報を更新。■ カスタムのインストールまたはアップグレード スクリプトを含む、インストーラ ISO イメージの作成 と 起動オプション の例を少し修正。

リビジョン	説明
JA-001989-01	<ul style="list-style-type: none">■ vCenter Single Sign-On がアップグレードに与える影響 内の vCenter Server インスタンス数に関する情報を更新。■ Platform Services Controller を組み込んだ vCenter Server のスタンドアロン インスタンスおよび複数インスタンスを再構成する情報を改善するため、トピック「組み込み Platform Services Controller を使用するスタンドアロン vCenter Server の、外部 Platform Services Controller を使用する vCenter Server への再構成」を更新し、トピック「組み込み Platform Services Controller を使用する vCenter Server の複数の参加済みインスタンスの、外部 Platform Services Controller を使用する vCenter Server への再構成」を追加。■ 必要なくなった APJ ポート 8009 を削除するためトピック vCenter Server での VMware vCenter Server - tc Server 設定の構成 を更新。
JA-001989-00	初期リリース。

vSphere のアップグレードの概要

1

vSphere 6.0 には、vSphere デプロイをアップグレードするためのオプションが数多くあります。vSphere のアップグレードを成功させるには、アップグレード オプション、アップグレード プロセスに影響を与える構成の詳細、タスクの順序を理解しておく必要があります。

vSphere の 2 つの主要なコンポーネントは、VMware ESXi™ と VMware vCenter Server™ です。{ESXi は、仮想マシンおよび仮想アプライアンスを作成および実行できる仮想プラットフォームです。vCenter Server は、ネットワーク内で接続された ESXi ホストを一元的に管理する機能を果たすサービスです。vCenter Server システムを使用して、複数のホストのリソースをリソース プールにまとめて管理できます。

Windows 仮想マシンまたは物理サーバ上の vCenter Server システムをアップグレードするか、vCenter Server Appliance をアップグレードできます。vCenter Server Appliance は、vCenter Server システムおよび vCenter Server コンポーネントの実行用に最適化された、事前構成済みの Linux ベースの仮想マシンです。

vSphere 6.0 からは、vCenter Server および vCenter Server コンポーネントを実行するために事前に必要なすべてのサービスが Platform Services Controller にバンドルされています。既存の vCenter Server 構成の詳細に応じて、組み込みまたは外部の Platform Services Controller を使用する vCenter Server システムにアップグレードできます。vCenter Server 6.0 のアップグレード オプションの詳細については、[Windows 版 vCenter Server 6.0 のアップグレード プロセス](#)についておよび [vCenter Server Appliance のアップグレード プロセス](#)についてを参照してください。

ESXi のアップグレード サポートの詳細については、[ESXi 6.0 のアップグレード オプション](#)を参照してください。

vSphere 6.0 にアップグレードするとき、発生する可能性があるデータの損失を防ぎ、ダウンタイムを最小限するため、すべての手順を順番通りに実行する必要があります。各コンポーネントのアップグレード プロセスは、1 方向にしか実行できません。たとえば、vCenter Server 6.0 へのアップグレード後に vCenter Server 5.x に戻すことはできません。バックアップおよび計画を行うことで、元のソフトウェア レコードをリストアできます。

vSphere 全体のアップグレード順序については、[vSphere アップグレード プロセス](#)を参照してください。

この章には、次のトピックが含まれています。

- [vCenter Server のコンポーネントおよびサービス](#)
- [vSphere 6.0 と vSphere 5.x の違い](#)
- [vCenter Server のデプロイ モデル](#)
- [vSphere アップグレード プロセス](#)
- [vCenter Single Sign-On がアップグレードに与える影響](#)
- [vSphere セキュリティ証明書の概要](#)

- 拡張リンク モードの概要
- vCenter Server のアップグレード パスの例

vCenter Server のコンポーネントおよびサービス

vCenter Server には、仮想マシンおよびホストの管理、操作、リソース プロビジョニング、パフォーマンス評価を行うための一元化されたプラットフォームがあります。

vCenter Server と組み込み Platform Services Controller または vCenter Server Appliance と組み込み Platform Services Controller にアップグレードする場合、vCenter Server、vCenter Server コンポーネント、および Platform Services Controller に含まれるサービスは同じシステムにデプロイされます。

vCenter Server と外部 Platform Services Controller にアップグレードする場合や、vCenter Server Appliance と外部 Platform Services Controller をデプロイする場合、vCenter Server および vCenter Server コンポーネントは一方のシステムにデプロイされ、Platform Services Controller に含まれるサービスは他方のシステムにデプロイされます。

次のコンポーネントは、vCenter Server および vCenter Server Appliance インストールに含まれます。

- インフラストラクチャ サービスの VMware Platform Services Controller グループには、vCenter Single Sign-On、ライセンス サービス、Lookup Service、および VMware 認証局が含まれます。
- サービスの vCenter Server グループには、vCenter Server、vSphere Web Client、Inventory Service、vSphere Auto Deploy、vSphere ESXi Dump Collector、VMware vSphere Syslog Collector (Windows)、および vCenter Server Appliance 用の VMware Sphere Syslog サービスが含まれます。

VMware Platform Services Controller とともにインストールされるサービス

vCenter Single Sign-On

vCenter Single Sign-On 認証サービスは、安全な認証サービスを vSphere ソフトウェア コンポーネントに提供します。vCenter Single Sign-On を使用することで、Active Directory などのディレクトリ サービスで各コンポーネントがユーザーを個別に認証するのではなく、安全なトークン交換メカニズムを介して vSphere コンポーネントが互いに通信できます。vCenter Single Sign-On は、インストールまたはアップグレード プロセス中に vSphere ソリューションおよびコンポーネントが登録される内部セキュリティ ドメイン (vsphere.local など) を構築し、インフラストラクチャ リソースを提供します。vCenter Single Sign-On は、独自の内部ユーザーおよびグループでユーザーを認証したり、Microsoft Active Directory などの信頼できる外部ディレクトリ サービスに接続したりできます。その後、vSphere 環境内で登録されたソリューションベースのアクセス許可またはロールを、認証されたユーザーに割り当てることができます。

vCenter Server 5.1.x 以降では、vCenter Single Sign-On が使用可能であるとともに必要です。

vSphere ライセンス サービス

vSphere ライセンス サービスでは、1 つの Platform Services Controller または複数のリンクされた Platform Services Controller に接続されているすべての vCenter Server システムに、共通のライセンス インベントリおよび管理機能を提供します。

VMware 認証局

VMware 認証局 (VMCA) により、VMCA をデフォルトでルート認証局とする署名証明書を使用して、各 ESXi ホストをプロビジョニングします。プロビジョニングは、ESXi ホストが vCenter Server に明示的に追加される場合に、または ESXi ホストのインストール プロセスの一環として実行されます。すべての ESXi 証明書は、ホストにローカルに保存されます。

vCenter Server とともにインストールされるサービス

これらの追加コンポーネントは、vCenter Server のインストール時にサイレント インストールされます。これらのコンポーネントには独自のインストーラがないため、個別にインストールすることはできません。

vCenter Inventory Service

Inventory Service には vCenter Server 構成とインベントリ データが格納されており、vCenter Server インスタンス全体でインベントリ オブジェクトを検索してアクセスすることができます。

PostgreSQL

vSphere および vCloud Hybrid Service 用にバンドルされた PostgreSQL データベースの VMware ディストリビューション。

vSphere Web Client

vSphere Web Client を使用すると、Web ブラウザを使用して vCenter Server インスタンスに接続し、vSphere インフラストラクチャを管理できます。

vSphere ESXi Dump Collector

vCenter Server のサポート ツール。システムに重大なエラーが発生した場合にディスクではなくネットワーク サーバに VMkernel メモリを保存するように、ESXi を構成できます。vSphere ESXi Dump Collector は、ネットワーク全体でこのようなメモリ ダンプを収集します。

VMware vSphere Syslog Collector

ネットワーク ログと、複数のホストからのログの結合を有効にする Windows 上の vCenter Server のサポート ツール。vSphere Syslog Collector を使用して、ESXi システム ログをローカル ディスクではなくネットワーク上のサーバに送信できます。ログの収集元となるサポート対象ホストの推奨最大数は 30 です。vSphere Syslog Collector の構成については、<http://kb.vmware.com/kb/2021652> を参照してください。

VMware Syslog サービス

システム ログやネットワーク ログ、およびホストからのログの収集のための統合アーキテクチャを提供する vCenter Server Appliance のサポート ツール。VMware Syslog サービスを使用して、ESXi システム ログをローカル ディスクではなくネットワーク上のサーバに送信できます。ログの収集元となるサポート対象ホ

ホストの推奨最大数は 30 です。VMware Syslog サービスの構成については、『vCenter Server Appliance の構成』を参照してください。

vSphere Auto Deploy

ESXi ソフトウェア搭載の物理ホストを大量にプロビジョニングできる vCenter Server のサポート ツール。デプロイするイメージと、そのイメージを使用してプロビジョニングするホストを指定できます。任意で、ホストに適用するホスト プロファイルと、各ホストの vCenter Server の場所（フォルダまたはクラスター）を指定できます。

vSphere 6.0 と vSphere 5.x の違い

vSphere 5.x から vSphere 6.0 への変更の中には、vCenter Server アップグレード プロセスに影響を与えるものがあります。vSphere 6.0 の新機能の包括的な一覧については、バージョン 6.0 リリースのリリース ノートを参照してください。

新機能の VMware Platform Services Controller

VMware Platform Services Controller には、vCenter Single Sign-On、VMware 認証局、ライセンス管理、サーバ予約と登録サービスなどの共通インフラストラクチャ サービスが含まれます。

Platform Services Controller インスタンスは、vCenter Server と同じ仮想マシン (VM) または物理サーバ（組み込み Platform Services Controller インスタンスを使用する vCenter Server）にデプロイできます。このほか、Platform Services Controller インスタンスを別のマシンまたは物理サーバ（外部の Platform Services Controller インスタンスを使用する vCenter Server）にデプロイすることも可能です。[vCenter Server のデプロイ モデル](#)を参照してください。

拡張リンク モード

vSphere 6.0 から、リンク モードの実装が変更されました。vCenter Server インスタンスをリンク モードグループに参加させる必要がなくなりました。複数の vCenter Server インスタンスを同じ Platform Services Controller に登録するか、または Platform Services Controller インスタンスを同じ vCenter Single Sign-On ドメインに参加させることにより、vSphere 5.5 でリンク モードで提供されるレプリケーション機能にアクセスできます。

単一の vCenter Single Sign-On ドメイン内の vCenter Server インスタンス間で高可用性を有効にするには、vCenter Server インスタンスで同一のサイト名を使用する必要があります。

これまでのリンク モードとは異なり、拡張リンク モードは Windows 上と vCenter Server Appliance 上の vCenter Server で使用可能であり、サポートされます。

vCenter Server コンポーネント サービスのデプロイ

vSphere 6.0 から、vCenter Server コンポーネント サービスは、vCenter Server、Platform Services Controller のいずれかのサービスのグループでデプロイされます。vCenter Server 6.0 では、vSphere 共通サービスを個別にアップグレードすることはできなくなります。

vCenter Server アップグレード ソフトウェアでは、必要に応じて既存の vCenter Server 5.1 または vCenter Server 5.5 サービスの移行、アップグレード、および構成が行われます。アップグレード プロセスでは、個々にデプロイされている vCenter Server 5.0 または vCenter Server 5.1 サービスが適切なサービスグループに移行されます。

- 現在、vCenter Single Sign-On の認証情報、証明書、およびポートは Platform Services Controller インスタンスの一部になっています。
- タグ付けデータとライセンスは、Platform Services Controller インスタンスの一部です。
- その他のサービスは vCenter Server インスタンスの一部です。詳細については、[vCenter Server 6.0 へのアップグレード中の Windows サービス用の分散 vCenter Server の移行](#)を参照してください。
- これで、アップグレード ソフトウェアが使用するターゲット フォルダを選択できます。

サービス デプロイの詳細については、[Windows 版 vCenter Server 6.0 のアップグレード プロセスについて](#)を参照してください。

シンプル アップグレード プロセスの後継機能

vCenter Server 5.1 または vCenter Server 5.5 シンプル アップグレード プロセスは、組み込み Platform Services Controller インスタンスを使用する vCenter Server 6.0 へのアップグレードに置き換えられます。このアップグレード プロセスにより、vCenter Server 5.1 または vCenter Server 5.5 サービスは、組み込み Platform Services Controller インスタンスを使用する vCenter Server 6.0 デプロイに移行されます。

カスタム アップグレード プロセスの後継機能

vCenter Server 5.1 または 5.5 カスタム アップグレード プロセスまたは個別アップグレード プロセスは、外部 Platform Services Controller インスタンスを使用する vCenter Server 6.0 へのアップグレードに置き換えられます。カスタムまたは分散 vCenter Server 5.1 または 5.5 インスタンスをアップグレードする場合、vCenter Server から別途デプロイされる vCenter Server 5.1 または 5.5 サービスがあれば、それらもアップグレード プロセスに含まれます。それらを個別にアップグレードする必要はありません。

外部 Platform Services Controller デプロイを使用する vCenter Server 6.0 へのアップグレード プロセスでは、vCenter Server から個別の仮想マシンまたは物理サーバにデプロイされる vCenter Server 5.1 または 5.5 のサービスは、vCenter Server インスタンスと同じ仮想マシンまたは物理サーバに移行されます。vCenter Server コンポーネントは個別にデプロイできなくなりました。アップグレード時のサービス移行の詳細については、[vCenter Server 6.0 へのアップグレード中の Windows サービス用の分散 vCenter Server の移行](#)を参照してください。

アップグレード中、Platform Services Controller のデプロイ モデルを変更できない

vCenter Server 6.0 へのアップグレード中、デプロイ モデルを変更することはできません。たとえば、組み込み Platform Services Controller インスタンスを使用する vCenter Server をデプロイする場合、外部 Platform Services Controller インスタンスを使用する vCenter Server に切り替えることはできません。実行できるのは、Platform Services Controller インスタンスの削除だけです。

アップグレード後、vCenter Server と Platform Services Controller 間の接続を再ポイントすることによって vCenter Server デプロイを更新できます。また、組み込み Platform Services Controller デプロイを外部 Platform Services Controller デプロイに変換することもできます。

データベースの変更

vCenter Server 5.x に組み込みの Microsoft SQL Server Express データベースは、vCenter Server 6.0 へのアップグレードによって組み込みの PostgreSQL データベースに置き換えられます。Microsoft SQL Server Express に適用されているインベントリの最大サイズが PostgreSQL にも適用されます。

VMware vSphere Syslog Collector

vSphere Syslog Collector は、Windows 版 vCenter Server 6.0 の場合、vCenter Server サービス グループに含められ、引き続き vCenter Server 5.5 の場合とまったく同じように機能しますが、vCenter Server Appliance 6.0 では使用されません。

VMware Syslog Service

vCenter Server Appliance 6.0 の場合、vSphere Syslog サービスは vCenter Server サービス グループに含められる、ロギング用のサポート ツールです。vCenter Server のコンポーネントおよびサービスを参照してください。

vCenter Server のデプロイ モデル

Microsoft Windows Server 2008 SP2 以降が実行されている仮想マシンまたは物理サーバに vCenter Server をインストールするか、vCenter Server Appliance をデプロイすることができます。vCenter Server Appliance は事前構成された Linux ベースの仮想マシンで、vCenter Server の実行用に最適化されています。

vSphere 6.0 では、Platform Services Controller が組み込まれている vCenter Server と外部 Platform Services Controller を使用する vCenter Server が導入されています。

重要： このドキュメントでは、基本デプロイ モデルについて説明します。推奨するトポロジについては、「[List of recommended topologies for vSphere 6.0.x](#)」を参照してください。

vCenter Server と組み込み Platform Services Controller

Platform Services Controller にバンドルされているすべてのサービスは、vCenter Server と同じ仮想マシンまたは物理サーバにデプロイされます。

vCenter Server と外部 Platform Services Controller

Platform Services Controller と vCenter Server にバンドルされているサービスは、別々の仮想マシンまたは物理サーバにデプロイされます。

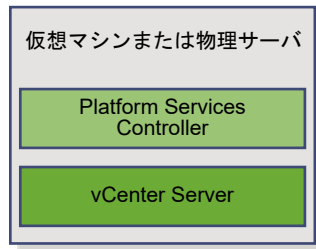
まず、1 つの仮想マシンまたは物理サーバに Platform Services Controller をデプロイし、その後別の仮想マシンまたは物理サーバに vCenter Server をデプロイする必要があります。

注： 組み込み Platform Services Controller を使用する vCenter Server をデプロイしたら、トポロジを再構成して、外部 Platform Services Controller を使用する vCenter Server に切り替えることができます。これは一方向のプロセスで、後で組み込み Platform Services Controller を使用する vCenter Server に戻すことはできません。vCenter Server インスタンスは、同じドメイン内のインフラストラクチャ データをレプリケートするように構成された外部 Platform Services Controller にのみ再ポイントできます。

vCenter Server と組み込みの Platform Services Controller

vCenter Server と Platform Services Controller は、単一の仮想マシンまたは物理サーバにデプロイされます。

図 1-1. Platform Services Controller が組み込まれている vCenter Server



Platform Services Controller が組み込まれている vCenter Server をインストールすることには、次のようなメリットがあります。

- vCenter Server と Platform Services Controller がネットワークを介して接続されておらず、vCenter Server と Platform Services Controller の間での接続性問題や名前解決問題のために vCenter Server が停止することがなくなります。
- Windows 仮想マシンまたは物理サーバに vCenter Server をインストールする場合、必要な Windows ライセンスの数が少なくて済みます。
- 管理する必要がある仮想マシンや物理サーバの数が減ります。
- ロード バランサーを使用して複数の Platform Services Controller に負荷を分散する必要がなくなります。

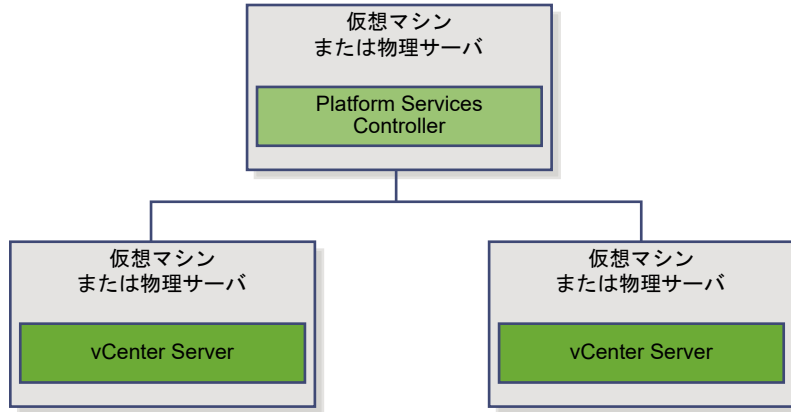
Platform Services Controller を組み込んでのインストールには、次のようなデメリットがあります。

- 製品ごとに Platform Services Controller がインストールされますが、これは必要以上です。これにより、リソースの使用量が増えます。
- このモデルは、小規模な環境に適しています。

vCenter Server と外部の Platform Services Controller

vCenter Server と Platform Services Controller は、別々の仮想マシンまたは物理サーバにデプロイします。Platform Services Controller は、いくつかの vCenter Server インスタンス間で共有できます。Platform Services Controller をインストールし、次にいくつかの vCenter Server インスタンスをインストールして、それらを Platform Services Controller に登録することができます。次に、別の Platform Services Controller をインストールして、最初の Platform Services Controller に関するデータをレプリケートするようにそのコントローラを構成し、それから vCenter Server インスタンスをインストールして、それらのインスタンスを 2 番目の Platform Services Controller に登録することができます。

図 1-2. 外部 Platform Services Controller を使用する vCenter Server



外部 Platform Services Controller を使用する vCenter Server をインストールすることには、次のようなメリットがあります。

- Platform Services Controller でのサービスを合わせた場合の消費リソース量が少なくなるため、フットプリントとメンテナンスの負担を軽減できます。
- より多くの vCenter Server インスタンスで使用環境を構成できます。

外部 Platform Services Controller を使用する vCenter Server をインストールすることには、次のようなデメリットがあります。

- vCenter Server と Platform Services Controller がネットワークを介して接続され、接続問題と名前解決問題が発生しやすくなります。
- Windows 仮想マシンまたは物理サーバに vCenter Server をインストールする場合、必要な Windows ライセンスの数が多くなります。
- 多くの仮想マシンまたは物理サーバを管理する必要があります。

オペレーティング システムの混在環境

Windows 上にインストールされた vCenter Server インスタンスは、Windows 上にインストールされた Platform Services Controller または Platform Services Controller アプライアンスに登録することができます。vCenter Server Appliance は、Windows 上にインストールされた Platform Services Controller または Platform Services Controller アプライアンスに登録することができます。vCenter Server と vCenter Server Appliance の両方は、同じドメイン内の同じ Platform Services Controller に登録することができます。

図 1-3. Windows 上の外部 Platform Services Controller との混在オペレーティング システム環境の例

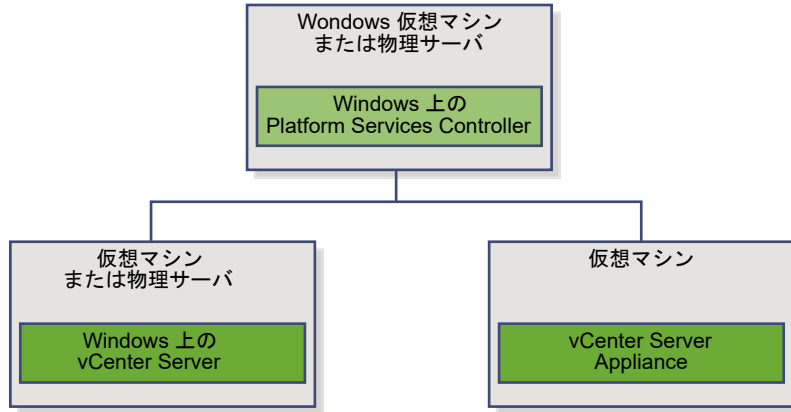
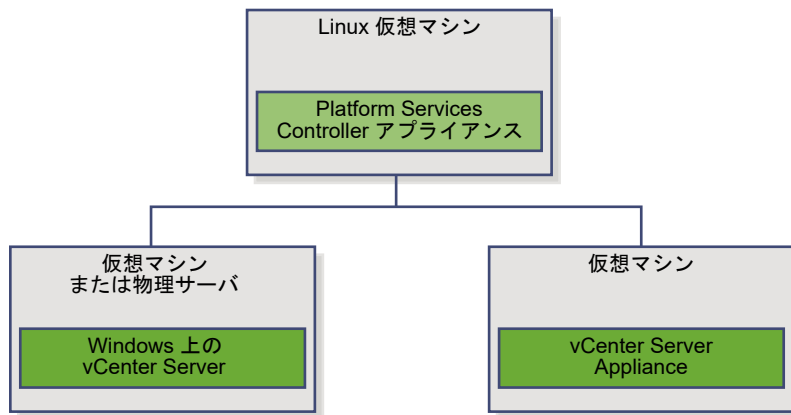


図 1-4. 外部 Platform Services Controller アプライアンスとの混在オペレーティング システム環境の例



インフラストラクチャ データをレプリケートする Platform Services Controller を多くすることにより、システムの可用性を高めることができます。

vCenter Server インスタンスまたは vCenter Server Appliance を最初に登録した外部 Platform Services Controller が応答を停止した場合は、vCenter Server または vCenter Server Appliance の接続先を、ドメイン内の別の外部 Platform Services Controller に再ポイントすることができます。詳細については、[別の外部 Platform Services Controller への vCenter Server の再ポイント](#) を参照してください。

vSphere アップグレード プロセス

vSphere は、アップグレードされる複数のコンポーネントを備えた高機能な製品です。vSphere を正しくアップグレードするために必要となる一連のタスクについて理解する必要があります。

vSphere のアップグレードには次のタスクが含まれます。

- 1 vSphere リリース ノートを参照します。
- 2 システムが vSphere のハードウェア要件およびソフトウェア要件を満たしていることを確認します。[2 章 アップグレード要件](#) を参照してください。
- 3 構成をバックアップしたことを確認します。

- 4 vSphere システムに VMware ソリューションまたはプラグインが含まれる場合は、それらが、アップグレードしている vCenter Server または vCenter Server Appliance のバージョンと互換性があることを確認します。http://www.vmware.com/resources/compatibility/sim/interop_matrix.php に掲載されている『VMware 製品の相互運用性マトリックス』を参照してください。

- 5 vCenter Server をアップグレードします。

vCenter Server インスタンスと外部の Platform Services Controller インスタンスを拡張リンク モード構成で接続できます。

重要： vCenter Single Sign-On ドメインへの参加を選択できますが、Platform Services Controller が組み込まれた vCenter Server はスタンドアロンのインストールと見なし、インフラストラクチャ データのレプリケーションには使用しないでください。

同時アップグレードはサポートされません。アップグレードは順に行う必要があります。vCenter Server インスタンスと同じ物理サーバまたは仮想マシン (VM) にインストールされていない vCenter Server インスタンスまたはサービスが複数存在する場合は、[vCenter Server 6.0 へのアップグレード中の Windows サービス用の分散 vCenter Server の移行および vCenter Server のアップグレード時のバージョン混在の移行環境](#)を参照してください。

Windows 仮想マシンまたは物理サーバ上で vCenter Server をアップグレードするか、または vCenter Server Appliance をアップグレードします。Windows 版 vCenter Server のアップグレード ワークフローについては、[Windows 版 vCenter Server 6.0 のアップグレード プロセスについて](#)を参照してください。vCenter Server Appliance のワークフローについては、[vCenter Server Appliance のアップグレード プロセスについて](#)を参照してください。

- a vCenter Server をアップグレードするためのハードウェア要件およびソフトウェア要件をシステムが満たしていることを確認します。[Windows 版 vCenter Server の要件](#) または [vCenter Server Appliance の要件](#) を参照してください。
- b アップグレードに備えて環境を整えます。を参照してください。[3 章 vCenter Server をアップグレードする前に行う作業](#)
- c アップグレードに必要な情報をまとめたワークシートを作成します。[Windows 版 vCenter Server のアップグレードに必要な情報](#) または [vCenter Server Appliance のアップグレードに必要な情報](#) を参照してください。
- d vCenter Server をアップグレードします。[4 章 Windows 版 vCenter Server のアップグレードおよび更新](#) または [5 章 vCenter Server Appliance および Platform Services Controller アプライアンスのアップグレードとパッチ適用](#) を参照してください。

vCenter Server 5.0 は、組み込みまたは外部 Platform Services Controller デプロイにアップグレードすることができます。vCenter Server 5.1 または 5.5 アップグレードの場合、アップグレード後のデプロイの結果は初期のデプロイによって決まります。デプロイの詳細とデプロイがアップグレードに与える影響については、[Windows 版 vCenter Server 6.0 のアップグレード プロセスについて](#)、[vCenter Server Appliance のアップグレード](#)、[vCenter Server Appliance および Platform Services Controller アプライアンスのパッチ適用](#)、[vCenter Server のアップグレード パスの例](#)を参照してください。

- 6 vCenter Server をアップグレードした後、アップグレード後のタスクを完了します。アップグレード前の構成詳細によっては、再構成タスクをいくつか完了しなければならないことがあります。[6 章 vCenter Server のアップグレード後](#) を参照してください。
- 7 vSphere Update Manager を使用している場合は、これをアップグレードします。[7 章 Update Manager のアップグレード](#) を参照してください。
- 8 ESXi ホストをアップグレードします。
 - a アップグレードのためのベスト プラクティスに目を通し、システムがアップグレード要件を満たしていることを確認します。[ESXi アップグレードのベスト プラクティス](#) および [ESXi の要件](#) を参照してください。
 - b 使用する ESXi アップグレード オプションを決定します。[ESXi 6.0 のアップグレード オプション](#) を参照してください。
 - c ESXi インストーラを配置および起動する場所を決定します。[ESXi インストーラを起動するためのメディア オプション](#) を参照してください。インストーラを PXE 起動する場合は、ネットワークの PXE インフラストラクチャが正しく設定されていることを確認します。[ESXi インストーラの PXE 起動](#) を参照してください。
 - d ESXi をアップグレードします。
 - [vSphere Update Manager を使用した、ホストの組織的なアップグレード](#)
 - [スクリプトを使用した、ホストのインストールまたはアップグレード](#)
 - [vSphere Auto Deploy を使用した、ホストの再プロビジョニング](#)
 - [esxcli コマンドを使用した、ホストのアップグレード](#)
 - [ホストの対話型アップグレード](#)
- 9 ESXi ホストをアップグレードした後、このホストを vCenter Server に再接続し、ライセンスを適用し直す必要があります。[10 章 ESXi ホストをアップグレードした後に行う作業](#) を参照してください。
- 10 ログ ファイルに十分なディスク ストレージを確保するため、リモート ログ機能用の syslog サーバの設定を検討します。リモート ホスト上のログ機能を設定することは、ローカル ストレージが不十分なホストで特に重要です。[システム ログに必要な空き容量](#) および [ESXi ホストでの syslog の構成](#) を参照してください。
- 11 仮想マシンと仮想アプライアンスを、手動でアップグレードするか、または vSphere Update Manager を使用して組織的にアップグレードします。[11 章 仮想マシンと VMware Tools のアップグレード](#) を参照してください。

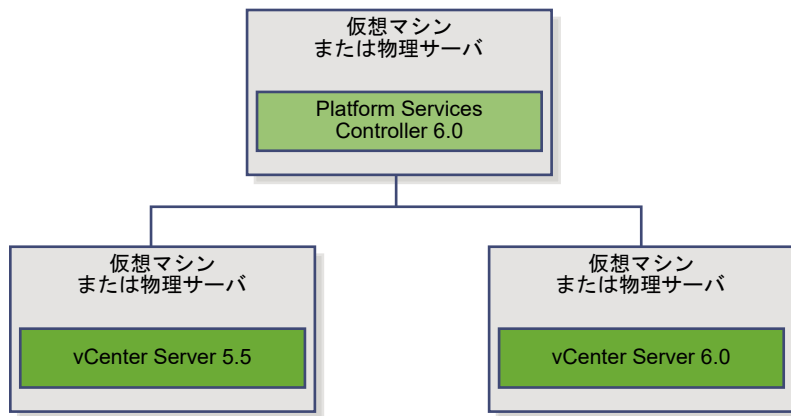
vCenter Server のアップグレード時のバージョン混在の移行環境

vCenter Server とは別の仮想マシンまたは物理サーバにデプロイされている vCenter Single Sign-On インスタンスを、バージョン 5.5 で使用している vCenter Server インスタンスを残したまま、外部でデプロイされた Platform Services Controller 6.0 にアップグレードすることができます。

外部でデプロイされた vCenter Single Sign-On インスタンスを外部でデプロイされた Platform Services Controller 6.0 にアップグレードする場合、その vCenter Single Sign-On インスタンスを使用していた vCenter Server 5.5 インスタンスは影響を受けません。vCenter Server 5.5 インスタンスは、アップグレード前と同様、アップグレードされた Platform Services Controller と連携し続け、問題が発生したり、再構成が必要になったりすることはありません。vCenter Server 5.5 インスタンスは引き続き vSphere Web Client 5.5 に表示されますが、vCenter Server 6.0 インスタンスは vSphere Web Client 5.5 に表示されません。

バージョン混在の移行動作は、vCenter Single Sign-On インスタンスが Windows 環境の vCenter Server 5.5 にデプロイされている場合と、vCenter Server Appliance 環境にデプロイされている場合とで同じです。

図 1-5. バージョン混在環境



注： バージョン混在環境は、本番環境ではサポートされません。vCenter Server のバージョンを移行する時以外は、そのような環境はお勧めできません。

外部の vCenter Single Sign-On をアップグレードする場合、および他の vCenter Server インスタンスをバージョン 5.5 にしたままで少なくとも 1 つの vCenter Server インスタンスをバージョン 6.0 にアップグレードする場合は、次のような結果になります。

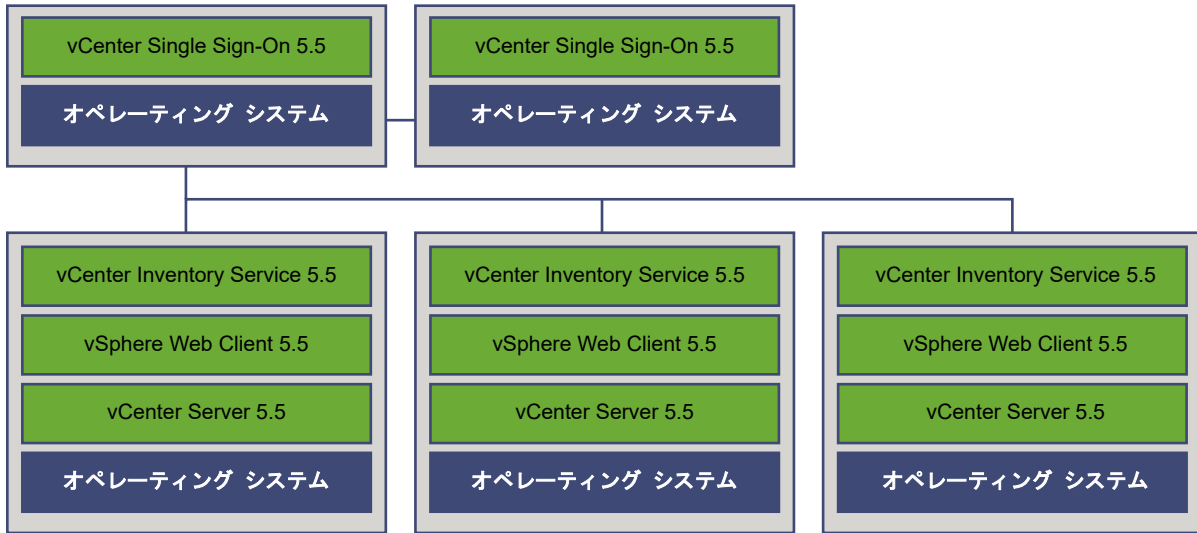
- リンク モードが機能しなくなります。
- vCenter Server 5.5 インスタンスは、アップグレード前と同様、アップグレードされた Platform Services Controller と連携し続け、問題が発生したり、再構成が必要になったりすることはありません。
- vCenter Server バージョン 5.5 と 6.0 が混在する環境の場合、vSphere Web Client 6.0 インスタンスには、vCenter Server 5.5 インスタンスが表示されます。
- vSphere Web Client 5.5 には、vCenter Server インスタンスのみが表示され、6.0 インスタンスは表示されません。

すべての vCenter Server 5.5 インスタンスを 6.0 にアップグレードし、分散した vCenter Single Sign-On インスタンスを外部の Platform Services Controller にアップグレードする場合、vCenter Server インスタンスはどれも影響を受けません。それらのインスタンスは、アップグレード前と同様に、Platform Services Controller と連携し続け、問題が発生したり、アクションが必要になったりすることはありません。

バージョン 5.5 と 6.0 が混在する環境でアップグレード後に必要とされるアクションは、まだアップグレードされていない vCenter Server 5.5 インスタンスを表示するために使用する場合に、すべてのレガシー vSphere Web Client インスタンスを再起動することのみです。

図 1-6. アップグレード開始前のデプロイの例

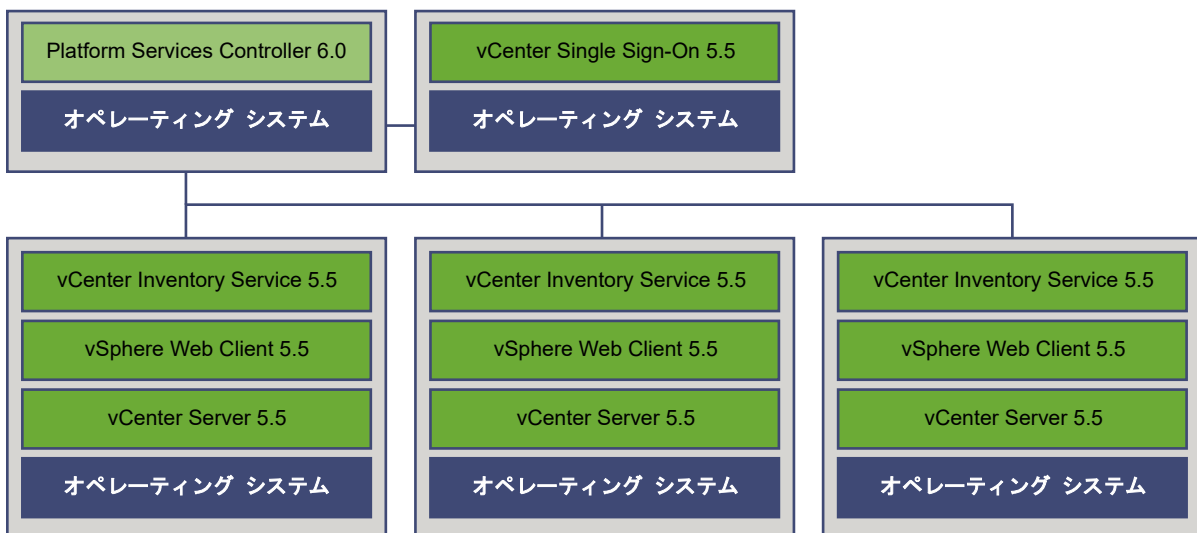
暫定のアップグレード環境：構成の開始



たとえば、3 つの vCenter Server 5.5 インスタンスおよび 2 つの外部 vCenter Single Sign-On インスタンスを使用するデプロイでは、1 つのインスタンスずつバージョン 6.0 にアップグレードする必要があります。

図 1-7. 手順 1 の移行でのデプロイ例

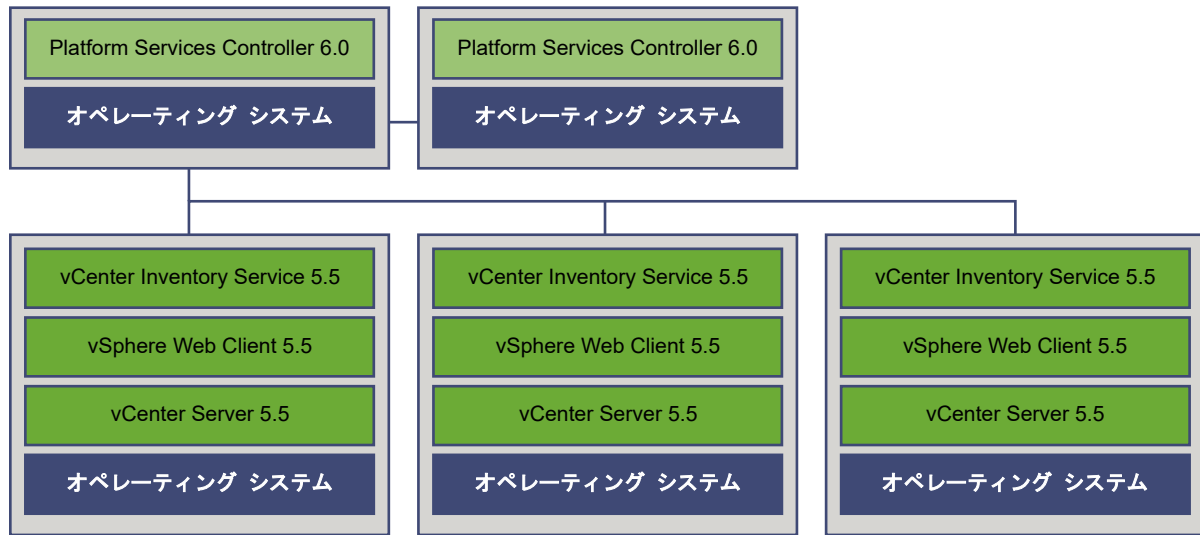
暫定のアップグレード環境：ステップ 1



最初の外部 vCenter Single Sign-On インスタンスを外部 Platform Services Controller にアップグレードしても、リンク モードが機能しなくなる以外は、vCenter Server 5.5 インスタンスに影響はありません。

図 1-8. 手順 2 の移行でのデプロイ例

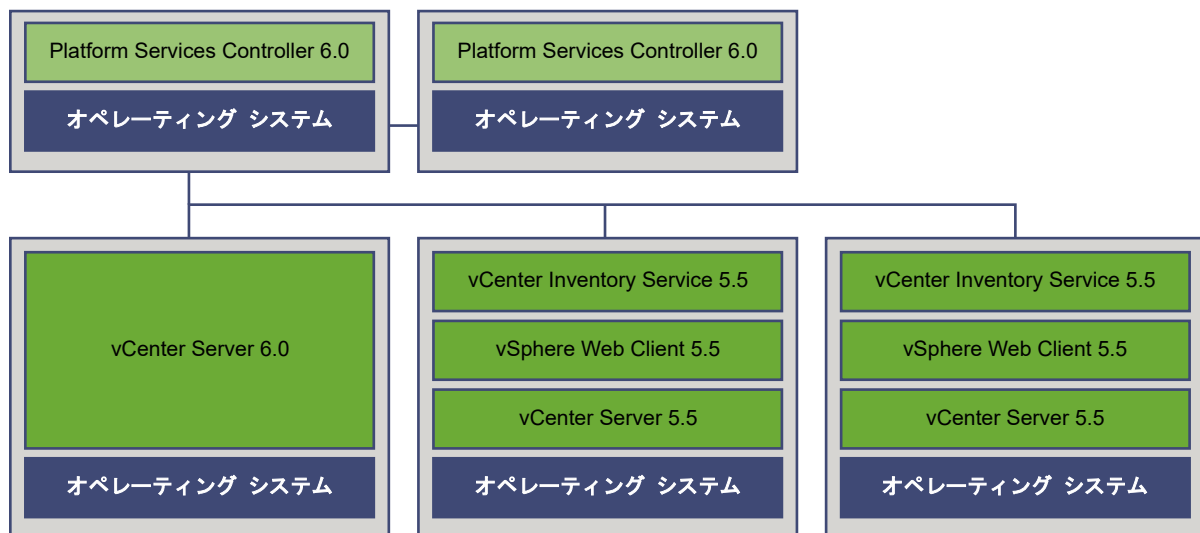
暫定のアップグレード環境：ステップ 2



2 つ目の外部 vCenter Single Sign-On インスタンスを外部 Platform Services Controller にアップグレードしても、vCenter Server 5.5 インスタンスの動作に影響はありません。

図 1-9. 手順 3 の移行でのデプロイ例

暫定のアップグレード環境：ステップ 3



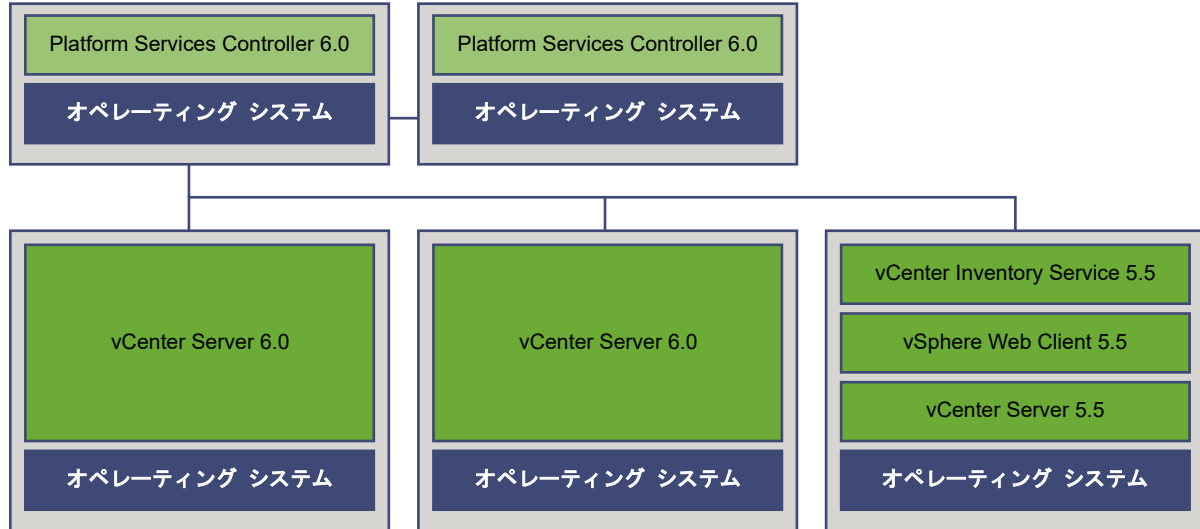
最初の vCenter Server インスタンスを 6.0 にアップグレードした後、vCenter Server インスタンス間の接続に変更が発生します。

- 残りの 2 つの vSphere Web Client 5.5 インスタンスは、新しくアップグレードされた vCenter Server 6.0 インスタンスが Platform Services Controller インスタンスに参加した後は、新しくアップグレードされたそのインスタンスを表示できなくなります。
- vSphere Web Client 5.5 インスタンスは、vSphere Web Client 5.5 インスタンスの再起動後も vCenter Server 5.5 インスタンスを表示できます。

- 新しくアップグレードされた vCenter Server 6.0 インスタンスの一部である vSphere Web Client 6.0 インスタンスは、vCenter Server 5.5 および vCenter Server 6.0 のインスタンスを表示できます。

図 1-10. 手順 4 の移行でのデプロイ例

暫定のアップグレード環境：ステップ 4

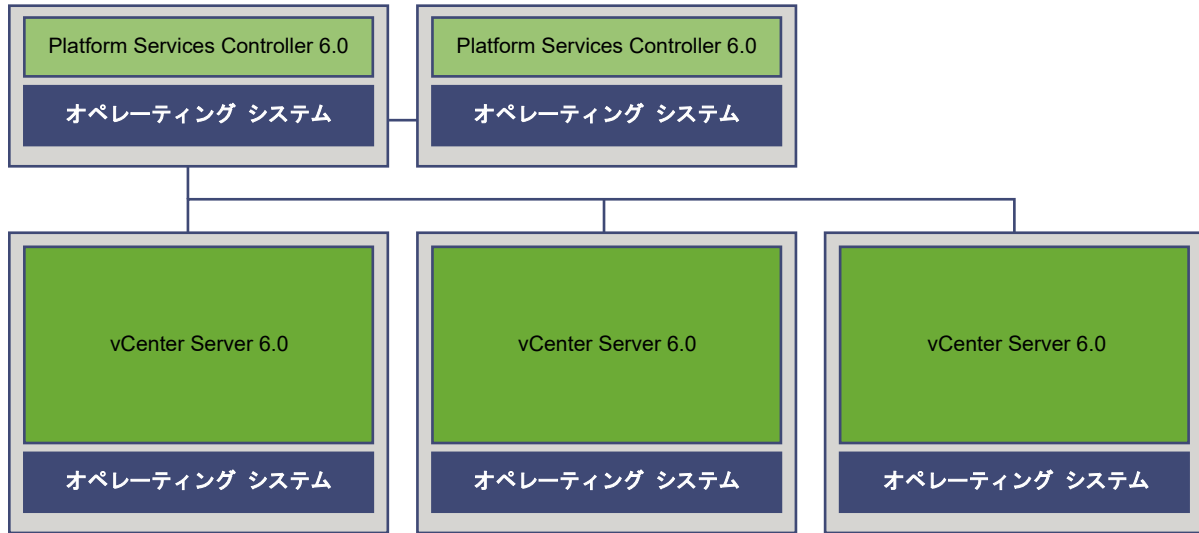


2 つ目の vCenter Server インスタンスを 6.0 にアップグレードした後、vCenter Server インスタンス間の接続にさらに変更が発生します。

- リンク モード機能は、新しくアップグレードされた vCenter Server 6.0 インスタンスが Platform Services Controller に参加した後に、それらのインスタンス間で拡張リンク モード機能に置き換えられます。
- 残りの vSphere Web Client 5.5 インスタンスでは、vCenter Server 6.0 インスタンスを表示できなくなります。
- vSphere Web Client 5.5 インスタンスは、vSphere Web Client 5.5 インスタンスの再起動後も vCenter Server 5.5 インスタンスを表示できます。
- 新しくアップグレードされた vCenter Server 6.0 インスタンスの一部である vSphere Web Client 6.0 インスタンスは、vCenter Server 5.5 および vCenter Server 6.0 のインスタンスを表示できます。

図 1-11. アップグレードが完了した手順 5 の移行でのデプロイ例

暫定のアップグレード環境: ステップ 5



3 つ目と最後の vCenter Server インスタンスを 6.0 にアップグレードした後、すべての vCenter Server インスタンスが vCenter Server 6.0 の機能に接続されます。

- リンク モード機能は、すべての vCenter Server 6.0 インスタンスが Platform Services Controller に参加した後に、それらのすべてのインスタンス間で拡張リンク モード機能に置き換えられます。
- vSphere Web Client 6.0 インスタンスは、すべての vCenter Server 6.0 インスタンスを表示できます。



vCenter Server 5.5 から 6.0 への移行アップグレード環境

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_orp6ck9v/uiConfId/49694343/)

vSphere ライセンス サービスへのアップグレード

vSphere 5.x では、ライセンス管理およびレポート機能は、個々の vCenter Server システムにあります。

vSphere 6.0 では、Platform Services Controller に含まれるライセンス サービスが導入されています。ライセンス サービスでは、1 つの Platform Services Controller、または 1 つの vCenter Single Sign-On ドメインに参加している複数の Platform Services Controller に登録されている vCenter Server システムに、共通のライセンス インベントリおよび管理機能を提供します。

ライセンス データは、Platform Services Controller に接続されている vCenter Server システムのアップグレード時にライセンス サービスに転送されます。ライセンス データには、ホスト、vCenter Server システム、Virtual SAN クラスタ、および vSphere で使用するその他の製品の使用可能なライセンスやライセンス割り当てが含まれます。

vCenter Server システムのアップグレードが完了したら、ライセンス サービスによって使用可能なライセンスが保存され、vSphere 環境全体のライセンス割り当てが管理されます。vSphere 環境が、1 つの vCenter Single Sign-On ドメインに参加している複数の Platform Services Controller で構成されている場合、すべての Platform Services Controller のライセンス サービスに、環境全体のライセンス データのレプリカが格納されます。

ライセンス サービスおよび vSphere でのライセンスの管理の詳細については、『vCenter Server およびホスト管理』を参照してください。

vSphere のアップグレードとアップデートの違い

vSphere 製品では、アップグレード（ソフトウェアの大きな変更）とアップデート（ソフトウェアの小さな変更）を区別しています。

VMware の製品バージョンには、vSphere 6.0 など、2 桁の番号が振られます。たとえば 5.5 から 6.0 へ、または 5.1 から 5.5 へと数字が変わっているリリースは、ソフトウェアの大幅な変更を含んでおり、以前のバージョンからのアップグレードが必要になります。変更が小さく、アップデートだけで済むリリースは、vSphere 6.0 Update 1 のようにアップデート番号で示されます。

ESXi ホストをアップグレードする場合には、一部のホスト構成情報がアップグレード後のバージョンに保存されます。アップグレードされたホストは、再起動後、同じレベルにアップグレードされている vCenter Server インスタンスに参加できます。アップデートとパッチにはソフトウェアの大きな変更が含まれないため、ホスト構成は影響を受けません。詳細については、次を参照してください。[イメージ プロファイルによるホストのアップグレードまたは更新](#)

vCenter Single Sign-On がアップグレードに与える影響

シンプル インストール環境を vCenter Server 6 の組み込みデプロイにアップグレードする場合、アップグレードはシームレスになります。カスタム インストールをアップグレードする場合、vCenter Single Sign-On サービスは、アップグレード後に Platform Services Controller の一部になります。アップグレード後に vCenter Server にログインできるユーザーは、アップグレード前のバージョンとデプロイ構成によって異なります。

アップグレードの一環として、vsphere.local の代わりに別の vCenter Single Sign-On ドメイン名を使用するように定義できます。

アップグレード パス

アップグレードの結果は、選択したインストール オプションおよびアップグレード先のデプロイ モデルによって異なります。

表 1-1. アップグレード パス

ソース	結果
vSphere 5.5 以前のシンプル インストール	Platform Services Controller が組み込まれた vCenter Server。
vSphere 5.5 以前のカスタム インストール	<p>vCenter Single Sign-On が vCenter Server とは異なるノードにあった場合、外部 Platform Services Controller を使用する環境になります。</p> <p>vCenter Single Sign-On が vCenter Server と同じノードにあった場合で、他のサービスが別のノードにある場合、組み込み Platform Services Controller を使用する環境になります。</p> <p>カスタム インストールに複数のレプリケーション vCenter Single Sign-On サーバが含まれていた場合、複数のレプリケーション Platform Services Controller インスタンスを使用する環境になります。</p>

シンプル インストールのアップグレード後にログイン可能なユーザー

シンプル インストール オプションを使用してプロビジョニングされた環境をアップグレードする場合、結果は常に組み込み Platform Services Controller を使用するインストールになります。ログインを許可されるユーザーは、ソースの環境が vCenter Single Sign-On を含むかどうかにより異なります。

表 1-2. シンプル インストール環境のアップグレード後のログイン権限

ソースのバージョン	ログイン アクセス権限	メモ
vSphere 5.0	ローカル オペレーティング システム ユーザー administrator@vsphere.local	ユーザー ストアの変更により、インストール中に vSphere インベントリ階層のルート フォルダの管理者情報を求められることがあります。 以前のインストールで Active Directory をサポートしていた場合は、その Active Directory ドメインを ID ソースとして追加できます。
vSphere 5.1	ローカル オペレーティング システム ユーザー administrator@vsphere.local Admin@SystemDomain	vSphere 5.5 からは、vCenter Single Sign-On では 1 つのデフォルトの ID ソースのみをサポートします。デフォルトの ID ソースは設定可能です。 『vSphere セキュリティ』ドキュメントを参照してください。 デフォルト以外のドメインのユーザーは、ログイン時にドメインを指定できます (<i>DOMAIN\user</i> または <i>user@DOMAIN</i>)。
vSphere 5.5	administrator@vsphere.local またはアップグレード中に指定したドメインの管理者。 すべての ID ソースのすべてのユーザーが以前と同様にログインできます。	

vCenter Single Sign-On を含まない vSphere 5.0 から vCenter Single Sign-On を含むバージョンにアップグレードする場合、ローカル オペレーティング システム ユーザーの重要度は、Active Directory などのディレクトリ サービスのユーザーよりもかなり低くなります。このため、ローカル オペレーティング システム ユーザーを認証済みユーザーにしておくことができない場合や、望ましくない場合もあります。

カスタム インストールのアップグレード後にログイン可能なユーザー

カスタム インストール オプションを使用してプロビジョニングした環境をアップグレードする場合、結果は最初の選択によって異なります。

- vCenter Single Sign-On が vCenter Server システムと同じノードにあった場合、結果は組み込み Platform Services Controller を使用するインストールになります。
- vCenter Single Sign-On が vCenter Server システムとは別のノードにあった場合、結果は外部 Platform Services Controller を使用するインストールになります。
- vSphere 5.0 からアップグレードする場合、アップグレード プロセスの一環として、外部または組み込みの Platform Services Controller を選択できます。

アップグレード後のログイン権限は、いくつかの要因により異なります。

表 1-3. カスタム インストール環境のアップグレード後のログイン権限

ソースのバージョン	ログイン アクセス権限	メモ
vSphere 5.0	<p>vCenter Single Sign-On は、Platform Services Controller がインストールされたマシンのローカル オペレーティング システムのユーザーを認識しますが、vCenter Server がインストールされたマシンについては認識しません。</p> <p>注： 特に統合された環境では、管理にローカル オペレーティング システムのユーザーを使用することはお勧めしません。</p> <p>administrator@vsphere.local は、管理者ユーザーとして、vCenter Single Sign-On および各 vCenter Server インスタンスにログインすることができます。</p>	<p>5.0 のインストールが Active Directory ユーザーをサポートしていた場合、これらのユーザーはアップグレード後はアクセス権がなくなります。ID ソースとして Active Directory ドメインを追加できます。</p>
vSphere 5.1 または vSphere 5.5	<p>vCenter Single Sign-On は、Platform Services Controller がインストールされたマシンのローカル オペレーティング システムのユーザーを認識しますが、vCenter Server がインストールされたマシンについては認識しません。</p> <p>注： 特に統合された環境では、管理にローカル オペレーティング システムのユーザーを使用することはお勧めしません。</p> <p>administrator@vsphere.local は、管理者ユーザーとして、vCenter Single Sign-On および各 vCenter Server インスタンスにログインできます。</p> <p>vSphere 5.1 からのアップグレードでは、Admin@SystemDomain は administrator@vsphere.local と同じ権限を持ちます。</p>	<p>vSphere 5.5 からは、vCenter Single Sign-On では 1 つのデフォルトの ID ソースのみをサポートします。デフォルトの ID ソースは設定可能です。</p> <p>『vSphere セキュリティ』ドキュメントを参照してください。</p> <p>デフォルト以外のドメインのユーザーは、ログイン時にドメインを指定できます (<i>DOMAIN\user</i> または <i>user@DOMAIN</i>)。</p>

vSphere セキュリティ証明書の概要

ESXi ホストと vCenter Server は、SSL 経由で安全に通信し、機密性、データの整合性、および認証を保証します。

vSphere 6.0 では、VMware 認証局 (VMCA) により、VMCA をデフォルトでルート認証局とする署名付き証明書を使用して、各 ESXi ホストをプロビジョニングします。プロビジョニングは、ESXi ホストが vCenter Server に明示的に追加されるときに実行されるか、ESXi ホストのインストールの一環として実行されます。すべての ESXi 証明書は、ホストにローカルに保存されます。

別のルート認証局 (CA) によるカスタム証明書を使用することもできます。ESXi ホストの証明書の管理の詳細については、『vSphere セキュリティ』ドキュメントを参照してください。

vCenter Server および vCenter Server のサービスのすべての証明書は、VMware Endpoint 証明書ストア (VECS) に保存されます。

vCenter Server の VMCA 証明書は、任意の CA によって署名された別の証明書で置き換えることができます。サードパーティの証明書を使用する場合は、Platform Services Controller をインストールし、新しい CA 署名付きルート証明書を VMCA に追加して、vCenter Server をインストールします。vCenter Server の証明書の管理の詳細については、『vSphere セキュリティ』ドキュメントを参照してください。

拡張リンク モードの概要

拡張リンク モードでは、1 つ以上の Platform Services Controller を使用して、複数の vCenter Server システムを接続します。

拡張リンク モードを使用することにより、リンクされたすべての vCenter Server システムを表示し、まとめて検索することができ、ロール、アクセス許可、ライセンス、ポリシー、およびタグを複製できます。

外部の Platform Services Controller を使用して vCenter Server のインストールまたは vCenter Server Appliance のデプロイを行う場合、まず Platform Services Controller をインストールする必要があります。Platform Services Controller のインストール中に、新しい vCenter Single Sign-On ドメインを作成するか、既存のドメインに参加するかを選択できます。すでに Platform Services Controller がインストールまたはデプロイされていて、vCenter Single Sign-On ドメインが作成されている場合、既存の vCenter Single Sign-On ドメインに参加することを選択できます。既存の vCenter Single Sign-On ドメインに参加する場合、既存の Platform Services Controller と新しい Platform Services Controller 間でデータが複製されます。また、インフラストラクチャ データも 2 つの Platform Services Controller 間で複製されます。

拡張リンク モードでは、Windows 上で実行されている vCenter Server システムだけでなく、多数の vCenter Server Appliance も接続できます。また、複数の vCenter Server システムと vCenter Server Appliance がリンクされている環境を設定することもできます。

vCenter Server と外部 Platform Services Controller をインストールする場合、まず Platform Services Controller を一方の仮想マシンまたは物理サーバにデプロイしてから、vCenter Server を別の仮想マシンまたは物理サーバにデプロイします。vCenter Server のインストール時に、外部 Platform Services Controller を選択する必要があります。選択する Platform Services Controller がスタンドアロンの外部 Platform Services Controller であることを確認します。組み込みインストールの一部である既存の Platform Services Controller を選択することはできません。また、デプロイ後に再構成することもできません。推奨されるトポロジの詳細については、<http://kb.vmware.com/kb/2108548> 参照してください。

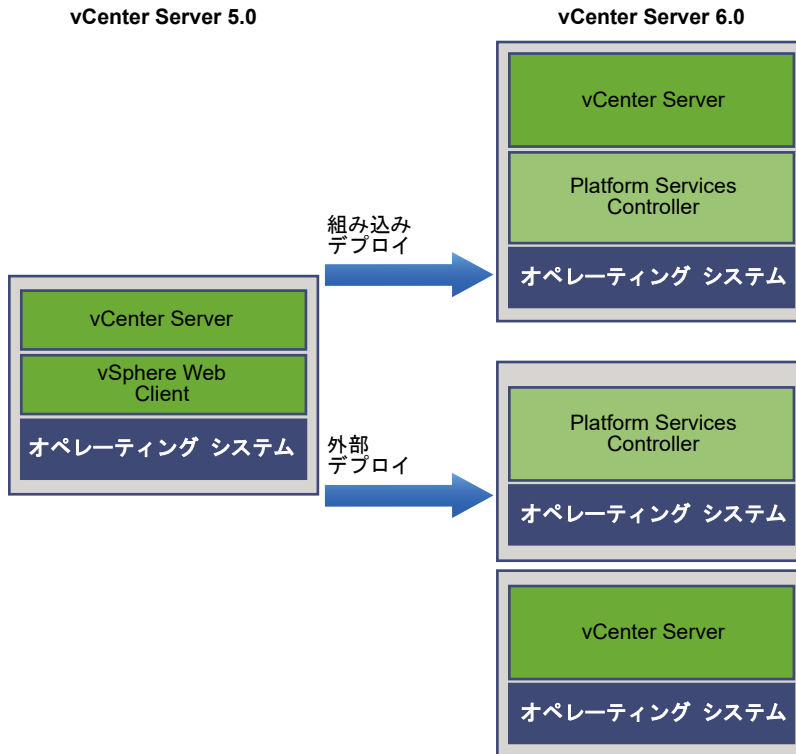
vCenter Server のアップグレード パスの例

最初の vCenter Server 5.x 構成により、アップグレードと 6.0 構成のオプションが決定します。

アップグレード パスの例では、vCenter Server アップグレード前の一般的な初期構成と、vCenter Server アップグレード後に予想される構成結果をいくつか示します。

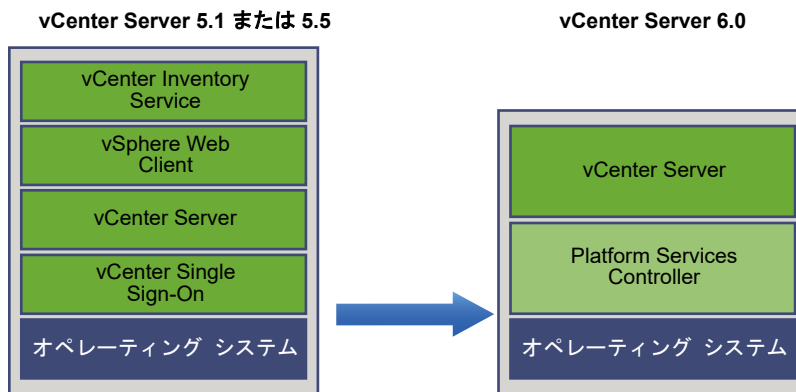
現在 vCenter Server 5.0 を使用している場合は、構成する共通サービスはありません。Platform Services Controller が組み込まれた vCenter Server にアップグレードするか、外部に Platform Services Controller がある vCenter Server にアップグレードするかを選択できます。

図 1-12. vCenter Server 5.0 デプロイのアップグレードの選択肢



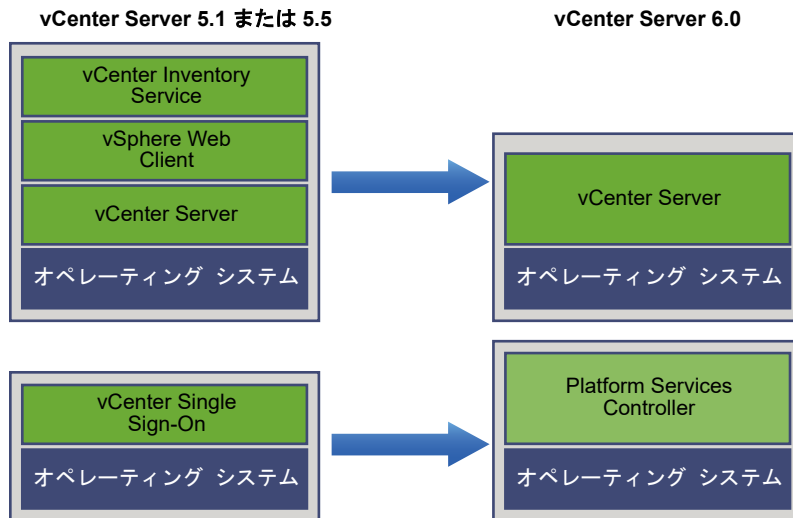
vCenter Server 5.1 または 5.5 のすべてのコンポーネントが同じシステムに配置される単純なインストールの場合、vCenter Server 6.0 ソフトウェアは、組み込み Platform Services Controller インスタンスを使用する vCenter Server にシステムをアップグレードします。このソフトウェアは、vCenter Server などの vCenter Single Sign-On の共通サービスを Platform Services Controller インスタンスにアップグレードします。vSphere Web Client、Inventory Service などの他の vCenter Server コンポーネントは、vCenter Server のサービス グループの一部として 6.0 にアップグレードされます。ソフトウェアは、vCenter Server とそのすべてのサービスを、正しい順序で同じバージョンにアップグレードします。

図 1-13. アップグレード前後の、vCenter Single Sign-On デプロイが組み込まれた vCenter Server 5.1 または 5.5



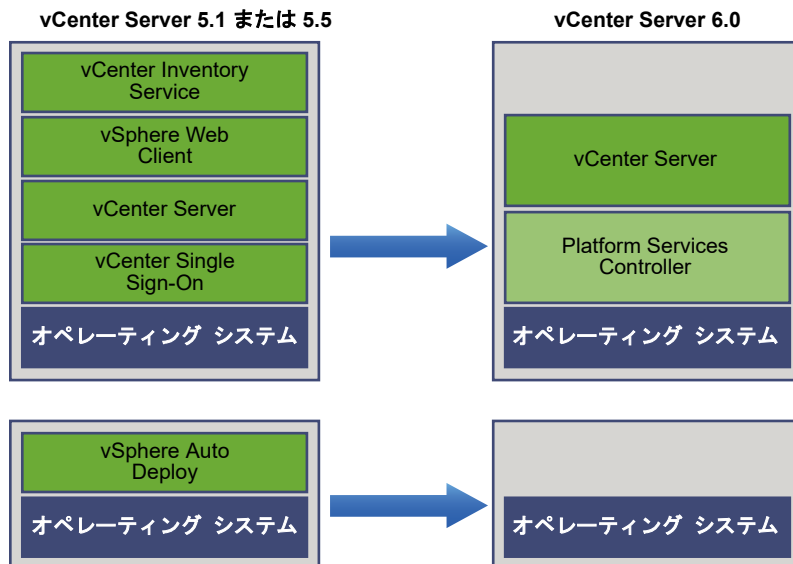
vCenter Single Sign-On が外部にデプロイされているカスタムの vCenter Server 5.1 または 5.5 環境の場合、vCenter Server 6.0 ソフトウェアは、デプロイを外部 Platform Services Controller インスタンスを使用する vCenter Server にアップグレードします。

図 1-14. アップグレード前後の、vCenter Single Sign-On が外部にデプロイされている vCenter Server 5.1 または 5.5



使用中の構成に vSphere Auto Deploy サーバが含まれている場合、アップグレード プロセスは、関連付けられている vCenter Server インスタンスのアップグレード時に、Auto Deploy サーバをアップグレードします。以前のバージョンの製品に含まれていた vSphere Auto Deploy サーバを vCenter Server 6.0 と併用することはできません。vSphere Auto Deploy サーバがリモート システムで実行されている場合は、アップグレード プロセスでアップグレードされ、vCenter Server と同じシステムに移行されます。

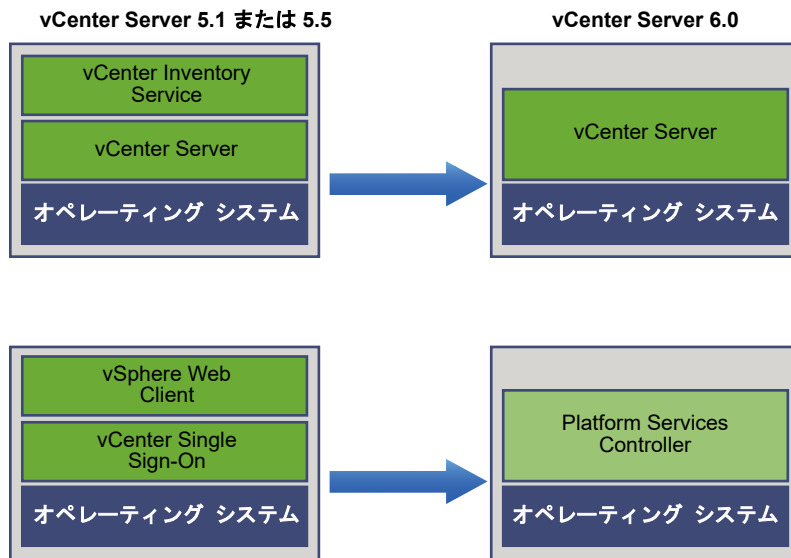
図 1-15. アップグレード前後の、リモート vSphere Auto Deploy サーバがある vCenter Server 5.1 または 5.5



たとえば、使用中の vCenter Server が vCenter Server Appliance に所属しており、vSphere Auto Deploy サーバを Windows マシンにインストールした場合は、アップグレード プロセスにより、vSphere Auto Deploy サーバは vCenter Server Appliance と同じ場所に移行されます。すべての設定が新しい場所に移行されます。ただし、新しい vSphere Auto Deploy の場所を参照するように ESXi ホストを再構成する必要があります。[アップグレード後の移行された vCenter Server サービスの再構成](#)を参照してください。

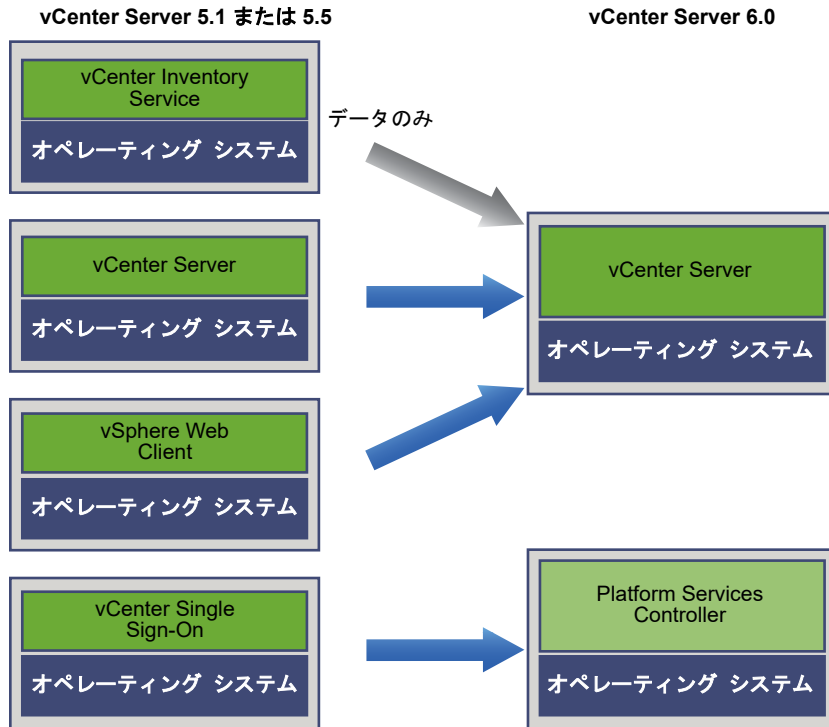
使用中の構成に、リモートにデプロイされている vSphere Web Client が含まれている場合は、vSphere Web Client は登録先の vCenter Server インスタンスとともにアップグレードされ、vCenter Server インスタンスと同じ場所に移行されます。

図 1-16. アップグレード前後の、リモート vSphere Web Client とリモート vCenter Single Sign-On がある vCenter Server 5.1 または 5.5



vCenter Server 6.0 にアップグレードした後、vCenter Single Sign-On インスタンスのみが、Platform Services Controller インスタンスの一部としてリモートでデプロイされたままになります。すべての vCenter Server コンポーネントがリモートでデプロイされている場合は、アップグレード中に vCenter Single Sign-On を除くすべてのコンポーネントが vCenter Server の場所に移行されます。Inventory Service データは vCenter Server の場所に移行されますが、レガシー バージョンは使用されなくなり、手動でアンインストールする必要があります。[vCenter Server 6.0 へのアップグレード中の Windows サービス用の分散 vCenter Server の移行](#)を参照してください。

図 1-17. アップグレード前後の、すべてのリモート コンポーネントがある vCenter Server 5.1 または 5.5



高可用性を実現するために複数のシステムを構成している場合、vCenter Server では、アップグレード プロセスの一環として、共通サービスを外部の Platform Services Controller 構成に組み込むことができます。

複製により複数サイトのセットアップを構成する場合、vCenter Server を使用して、アップグレード プロセスの一環として、共通サービスを外部 Platform Services Controller 構成に組み込むことができます。



5.0 から 6.0 への vCenter Server のアップグレード

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_1h7nmi18/uiConfId/49694343/)



5.1 または 5.5 から 6.0 への vCenter Server のアップグレード

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_vs0qr73b/uiConfId/49694343/)

バージョンが混在する移行環境の詳細については、vCenter Server のアップグレード時のバージョン混在の移行環境を参照してください。

アップグレード要件

2

vCenter Server および ESXi インスタンスをアップグレードするには、システムが特定の要件を満たしている必要があります。

この章には、次のトピックが含まれています。

- vCenter Server アップグレード互換性
- Windows 版 vCenter Server の要件
- vCenter Server Appliance の要件
- vCenter Server および Platform Services Controller に必要なポート
- vCenter Server データベースの構成に関する注意事項
- ESXi の要件
- vSphere DNS の要件
- vSphere Web Client のソフトウェア要件
- クライアント統合プラグインのソフトウェア要件
- vSphere Client の要件
- システム ログに必要な空き容量

vCenter Server アップグレード互換性

vCenter Server 6.0 へのアップグレードは、データセンターのその他のソフトウェア コンポーネントに影響を与えます。

表 2-1. vCenter Server および関連する VMware 製品とコンポーネントのアップグレードでは、vCenter Server のアップグレードがデータセンターのコンポーネントに及ぼす影響について概説します。

vCenter Server 6.0 は、ESXi 6.0 ホストのあるクラスタ内の ESXi 5.x ホストを管理できますが、ESX 4.x または ESXi 4.x ホストは管理できません。

vCenter Server 4.x 以前から vCenter Server 6.0 にアップグレードすることはできません。まず vCenter Server 5.x にアップグレードする必要があります。

表 2-1. vCenter Server および関連する VMware 製品とコンポーネントのアップグレード

製品またはコンポーネント	互換性
vCenter Server	vCenter Server の既存のバージョンから、アップグレード予定のバージョンへのアップグレードパスがサポートされていることを確認します。VMware 製品の相互運用性マトリックスを参照してください。 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php
vCenter Server データベース	データベースが、アップグレード後の vCenter Server バージョンでサポートされていることを確認します。必要に応じてデータベースをアップグレードします。VMware 製品の相互運用性マトリックスを参照してください。 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php 注： vCenter Server Appliance for vCenter Server 6.0 では、組み込みデータベースに PostgreSQL を使用します。外部データベースについては、vCenter Server Appliance では「VMware 製品の相互運用性マトリックス」に示されている、アップグレード後の vCenter Server バージョン用と同じバージョンの Oracle データベースのみをサポートします。
vSphere Web Client	vSphere Web Client がアップグレード後の vCenter Server バージョンと連携することを確認します。最高のパフォーマンスと互換性を実現するには、vSphere Web Client を vCenter Server と同じバージョンにアップグレードします。VMware 製品の相互運用性マトリックスを参照してください。 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php
ESX ホストおよび ESXi ホスト	ESX または ESXi が、アップグレード後の vCenter Server バージョンと連携することを確認します。必要に応じてアップグレードします。VMware 製品の相互運用性マトリックスを参照してください。 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php
VMware 仮想マシン ファイル システム (VMFS) のボリューム	既存の VMFS3 データストアは引き続き使用できますが、新しい VMFS3 データストアを作成することはできません。VMFS3 データストアを使用している場合、VMFS5 にアップグレードします。VMFS ボリュームのアップグレードの詳細については、『vSphere ストレージ』ドキュメントを参照してください。
仮想マシン	現在の使用バージョンによってアップグレード オプションが異なります。11 章 仮想マシンと VMware Tools のアップグレードを参照してください。
VMware Tools	現在の使用バージョンによってアップグレード オプションが異なります。VMware Tools のアップグレードについては、11 章 仮想マシンと VMware Tools のアップグレードを参照してください。
Auto Deploy	互換性と最高のパフォーマンスを確保するには、vCenter Server 6.0 にアップグレードするときに、Auto Deploy を使用して ESXi ホストを同じバージョンにアップグレードします。

Windows 版 vCenter Server の要件

Windows の仮想マシンまたは物理サーバの vCenter Server をアップグレードするには、システムが固有のハードウェアおよびソフトウェア要件を満たしている必要があります。

- vCenter Server 5.x サービスが実行されているすべての仮想マシンのクロックを同期します。[vSphere ネットワーク上の時計の同期](#) を参照してください。
- vCenter Server 5.x のサービスが実行されているマシンのシステム ネットワーク名が有効で、ネットワークの他のマシンから到達可能なことを確認します。
- vCenter Server をインストールまたはアップグレードする仮想マシンまたは物理サーバのホスト名が、RFC 1123 ガイドラインに準拠していることを確認します。

- vCenter Server サービスがローカル システム アカウント以外のユーザー アカウントで実行されている場合は、vCenter Server サービスを実行しているユーザー アカウントに次のアクセス許可があることを確認します。
 - システム管理者グループのメンバー
 - サービスとしてログオン
 - オペレーティング システムの一部として動作（ユーザーがドメイン ユーザーである場合）
- LOCAL SERVICE アカウントに、vCenter Server がインストールされるフォルダおよび HKLM レジストリに対する読み取りアクセス許可があることを確認します。
- 仮想マシンや物理サーバとドメイン コントローラ間の接続が機能していることを確認します。

Windows 版 vCenter Server の Pre-Upgrade Checker

vCenter Server および Platform Services Controller のアップグレード時、インストーラは、vCenter Server をアップグレードする仮想マシンまたは物理サーバに十分な領域があるかどうかの検証などのアップグレード前チェックを実行し、外部データベース（使用する場合）に正常にアクセスできるかどうかを検証します。

組み込み Platform Services Controller または外部 Platform Services Controller を使用する vCenter Server をデプロイすると、vCenter Single Sign-On が Platform Services Controller の一部としてインストールされます。アップグレード時に、インストーラによって、既存の vCenter Single Sign-On サーバドメインに参加するためのオプションが提示されます。他の vCenter Single Sign-On サービスに関する情報を指定すると、インストーラは、管理者アカウントを使用してホスト名とパスワードを確認し、指定された vCenter Single Sign-On サーバの詳細情報で認証されるかどうかを確認してから、アップグレード プロセスを続行します。

Pre-Upgrade Checker は、環境の次の点を確認します。

- Windows のバージョン
- プロセッサ最小要件
- メモリ最小要件
- ディスク領域最小要件
- 選択したインストールおよびデータ ディレクトリでのアクセス許可
- 内部および外部ポートの可用性
- 外部データベースのバージョン
- 外部データベースとの接続
- Windows マシン上の管理者権限
- 入力するすべての認証情報
- vCenter Server 5.x サービス

最小ストレージ要件の詳細については、[Windows 用 vCenter Server のストレージ要件](#)を参照してください。最小ハードウェア要件の詳細については、[Windows 版 vCenter Server のハードウェア要件](#)を参照してください。

Windows 用 vCenter Server のストレージ要件

vCenter Server をアップグレードする場合は、システムが最小限のストレージ要件を満たしている必要があります。

フォルダごとのストレージ要件は、マシンにデプロイされる vCenter Server 5.x サービス、アップグレードのデプロイ モデル、および vSphere 5.x インベントリのサイズによって異なります。インストーラは、アップグレード中にストレージ要件を動的に計算し、マシンに十分なディスク空き領域があることを確認してから、アップグレードの処理を進めます。

インストール時には、デフォルトの C:\Program Files\VMware フォルダ以外のフォルダを選択して vCenter Server と Platform Services Controller をインストールすることもできます。データを保存するデフォルトの C:\ProgramData\VMware\vCenterServer\ 以外のフォルダを選択することもできます。次の表に、デプロイ モデルごとの絶対的な最小ディスク領域要件の一覧を示します。各要件は、インストールされる vCenter Server 5.x サービスと vSphere 5.x のインベントリ サイズによって異なります。

表 2-2. デプロイ モデルに応じた vCenter Server の最小ストレージ要件

デフォルトのフォルダ	vCenter Server と組み込みの Platform Services Controller	vCenter Server と外部の Platform Services Controller	外部 Platform Services Controller
プログラム ファイル	6 GB	6 GB	1 GB
ProgramData	8 GB	8 GB	2 GB
システム フォルダ (MSI インストーラをキャッシュ)	3 GB	3 GB	1 GB

Windows 版 vCenter Server のハードウェア要件

Microsoft Windows で実行している仮想マシンまたは物理サーバに vCenter Server をインストールするときには、システムが固有のハードウェア要件を満たしている必要があります。

vCenter Server と Platform Services Controller は、同一の仮想マシンまたは物理サーバにインストールすることも、異なる仮想マシンまたは物理サーバにインストールすることもできます。vCenter Server と組み込みの Platform Services Controller をインストールする場合は、vCenter Server と Platform Services Controller を同一の仮想マシンまたは物理サーバにインストールします。vCenter Server と外部の Platform Services Controller をインストールする場合は、最初に、ある仮想マシンまたは物理サーバに必要なサービスをすべて含む Platform Services Controller をインストールしてから、vCenter Server と各種 vCenter Server コンポーネントを別の仮想マシンまたは物理サーバにインストールします。

注： ネットワーク ドライブまたは USB フラッシュ ドライブに vCenter Server をインストールすることはサポートされていません。

表 2-3. Windows での vCenter Server および Platform Services Controller インストールの最小推奨ハードウェア要件

Platform Services Controller		極めて小さな環境 (最大 10 ホスト、 100 仮想マシン) のための組み込み または外部 Platform Services Controller 実装 vCenter Server	小さな環境 (最大 100 ホスト、1000 仮想マシン) のため の組み込みまたは 外部 Platform Services Controller 実装 vCenter Server	中程度の環境 (最大 400 ホスト、 4,000 仮想マシ ン) のための組み込 みまたは外部 Platform Services Controller 実装 vCenter Server	大きな環境 (最大 1,000 ホスト、 10,000 仮想マシ ン) のための組み込 みまたは外部 Platform Services Controller 実装 vCenter Server
CPU の数	2	2	4	8	16
メモリ	2 GB RAM	8 GB RAM	16 GB RAM	24 GB RAM	32 GB RAM

使用中のデータベースのハードウェア要件については、データベースのドキュメントを参照してください。データベースと vCenter Server を同一のマシン上で実行する場合は、データベースの要件を vCenter Server の要件に追加する必要があります。

Windows 版 vCenter Server のソフトウェア要件

使用するオペレーティング システムが vCenter Server をサポートしていることを確認します。

vCenter Server には 64 ビットのオペレーティング システムが必要であり、vCenter Server を外部データベースに接続するには 64 ビットのシステム DSN が必要です。

vCenter Server をサポートしている最も古い Windows Server のバージョンは、Windows Server 2008 SP2 です。Windows Server には、最新のアップデートおよびパッチがインストールされている必要があります。サポートされているオペレーティング システムの完全なリストについては、<http://kb.vmware.com/kb/2091273> を参照してください。

Windows 版 vCenter Server データベースの要件

vCenter Server には、サーバ データを格納および編成するためのデータベースが必要です。

各 vCenter Server インスタンスには、独自のデータベースがある必要があります。ホスト 20 台、仮想マシン 200 台までの環境では、バンドルされている PostgreSQL データベースを使用できます。PostgreSQL データベースは、vCenter Server のインストール時に、vCenter Server インストーラによってインストールおよび設定されます。大規模インストールの場合、環境のサイズに対応できる外部データベースがサポートされている必要があります。

vCenter Server のインストールまたはアップグレード時に、組み込みのデータベースをインストールするか、既存のサポートされているデータベースを使用するように vCenter Server システムを設定するかを選択する必要があります。vCenter Server では、Oracle および Microsoft SQL Server データベースをサポートしています。サポートされているデータベース サーバのバージョンの詳細については、http://www.vmware.com/resources/compatibility/sim/interop_matrix.php で「VMware 製品の相互運用性マトリックス」を参照してください。

vCenter Server Appliance の要件

vCenter Server Appliance は、ESXi ホスト 5.0 以降でアップグレードできます。また、システムは、固有のソフトウェアおよびハードウェア要件を満たしている必要があります。

完全修飾ドメイン名を使用する場合は、vCenter Server Appliance のデプロイに使用するマシンと ESXi ホストが同じ DNS サーバに存在することを確認します。

vCenter Server Appliance をデプロイする前に、vSphere ネットワーク上のすべての仮想マシンの時刻を同期させてください。時刻が同期されていないと認証の問題が発生して、インストールに失敗したり、vCenter Server サービスを起動できなくなることがあります。[vSphere ネットワーク上の時計の同期](#) を参照してください。

vCenter Server Appliance のハードウェア要件

vCenter Server Appliance をデプロイする場合は、vSphere 環境のサイズに合ったアプライアンスをデプロイするように選択できます。選択したオプションによって、アプライアンスに搭載される CPU の数とメモリ容量が決まります。

CPU の数やメモリなどのハードウェア要件は、vSphere インベントリのサイズによって異なります。

表 2-4. VMware vCenter Server Appliance および Platform Services Controller アプライアンスのハードウェア要件

リソース	Platform Services Controller アプライアンス	極めて小さな環境 (最大 10 ホスト、 100 仮想マシン) のための組み込み または外部	小さな環境 (最大 100 ホスト、 1,000 仮想マシ ン) のための組み込 みまたは外部	中程度の環境 (最大 400 ホスト、 4,000 仮想マシ ン) のための組み込 みまたは外部	大きな環境 (最大 1,000 ホスト、 10,000 仮想マシ ン) のための組み込 みまたは外部
		Platform Services Controller 実装 vCenter Server Appliance	Platform Services Controller 実装 vCenter Server Appliance	Platform Services Controller 実装 vCenter Server Appliance	Platform Services Controller 実装 vCenter Server Appliance
CPU の数	2	2	4	8	16
メモリ	2 GB RAM	8 GB RAM	16 GB RAM	24 GB RAM	32 GB RAM

vCenter Server Appliance のストレージ要件

vCenter Server Appliance をデプロイする場合、アプライアンスをデプロイするホストが最小ストレージ要件を満たしている必要があります。必要なストレージ容量は、vSphere 環境のサイズだけでなく、ディスク プロビジョニングモードによっても異なります。

ストレージ要件は、デプロイで選択するデプロイ モデルによって異なります。

表 2-5. デプロイ モデルに応じた vCenter Server の最小ストレージ要件

	Platform Services Controller が組み込まれた vCenter Server Appliance	外部 Platform Services Controller を備えた vCenter Server Appliance	外部 Platform Services Controller アプライアンス
極小規模環境（最大ホスト 10 台、 仮想マシン 100 台）	120 GB	86 GB	30 GB
小規模環境（最大ホスト 100 台、 仮想マシン 1,000 台）	150 GB	108 GB	30 GB
中規模環境（最大ホスト 400 台、 仮想マシン 4,000 台）	300 GB	220 GB	30 GB
大規模環境（最大ホスト 1,000 台、仮想マシン 10,000 台）	450 GB	280 GB	30 GB

vCenter Server Appliance に含まれるソフトウェア

vCenter Server Appliance は事前に構成された Linux ベースの仮想マシンであり、vCenter Server および関連サービスの実行に最適化されています。

vCenter Server Appliance パッケージには、次のソフトウェアが含まれています。

- VMware 用 SUSE Linux Enterprise Server 11 Update 3（64 ビット エディション）
- PostgreSQL
- vCenter Server 6.0 および vCenter Server 6.0 コンポーネント。

vCenter Server Appliance のソフトウェア要件

VMware vCenter Server Appliance は、ESXi バージョン 5.0 以降を実行しているホストでのみアップグレードできます。

vCenter Server Appliance をアップグレードするには、クライアント統合プラグインを使用する以外に方法はありません。Windows で動作する HTML インストーラであるクライアント統合プラグインを使用して、ESXi 5.0.x、ESXi 5.1.x、ESXi 5.5.x、または ESXi 6.0 ホストに直接接続し、そのホストに vCenter Server Appliance をデプロイできます。

重要： vCenter Server Appliance は、vSphere Client または vSphere Web Client を使用してデプロイすることはできません。vCenter Server Appliance のデプロイ時には、オペレーティング システム、vCenter Single Sign-On のパスワードなど、さまざまな入力を行う必要があります。vSphere Client または vSphere Web Client を使用してアプライアンスをデプロイしようとする、このような入力は要求されず、デプロイに失敗します。

vCenter Server Appliance データベースの要件

vCenter Server Appliance には、サーバ データを格納および編成するためにデータベースが必要です。

各 vCenter Server Appliance インスタンスには、固有のデータベースが必要です。vCenter Server Appliance にバンドルされている PostgreSQL データベースを使用する場合は、ホスト 1,000 台までと仮想マシン 10,000 台までがサポートされます。

外部データベースの場合、vCenter Server Appliance によってサポートされるのは Oracle データベースのみです。サポートされている Oracle データベースは、インストールする vCenter Server の VMware 製品の相互運用性マトリクスに記載されているのと同じバージョンです。VMware 製品の相互運用性マトリクス (http://www.vmware.com/resources/compatibility/sim/interop_matrix.php) を参照してください。

外部データベースを使用する場合は、vCenter Server が Oracle データベースに接続できるよう、64 ビット DSN が作成されていることを確認します。

vCenter Server および Platform Services Controller に必要なポート

Windows 上とアプライアンスの両方に存在する vCenter Server システムでは、すべての管理対象ホストにデータを送信し、vSphere Web Client サービスと Platform Services Controller サービスからデータを受信できるようになっている必要があります。管理対象ホスト間での移行アクティビティやプロビジョニングアクティビティを有効にするには、送信元ホストと送信先ホスト間でデータの送受信が可能である必要があります。

ポートが使用中であるか、拒否リストに登録されている場合は、vCenter Server インストーラによってエラーメッセージが表示されます。インストールを続行するには別のポート番号を使用する必要があります。プロセス間通信でのみ使用される内部ポートがあります。

VMware では、通信に指定のポートが使用されます。また、管理対象ホストでは、vCenter Server からのデータが指定ポートで監視されます。これらのいずれかの構成要素の間にファイアウォールが存在する場合は、インストールまたはアップグレード処理中にインストーラによってポートが開かれます。カスタマイズされたファイアウォールの場合は、必要なポートを手動で開く必要があります。管理対象ホスト 2 台の間にファイアウォールが存在し、移行、クローン作成など、送信元または送信先のアクティビティを実行する場合、管理対象ホストがデータを受信できるように構成する必要があります。

注： Microsoft Windows Server 2008 以降では、デフォルトでファイアウォールが有効になっています。

表 2-6. コンポーネント間の通信に必要なポート

ポート	プロトコル	説明	目的	ノード間通信での使用
22	TCP	<p>SSHD のシステム ポート。</p> <p>重要： アプライアンスのアップグレード中はこのポートを開放しておく必要があります。アップグレード プロセスによって、既存のアプライアンスから新しいアプライアンスにデータを転送するための SSH 接続が確立されます。</p>	<p>次のアプライアンスのデプロイ</p> <ul style="list-style-type: none"> ■ vCenter Server ■ Platform Services Controller 	なし
80	TCP	<p>vCenter Server では、直接 HTTP 接続用にポート 80 が必要です。ポート 80 では、要求が HTTPS ポート 443 にリダイレクトされます。このリダイレクトは、https://server ではなく、誤って http://server を使用した場合に有効です。</p> <p>WS-Management (ポート 443 が開いていることも必要)</p> <p>vCenter Server と同じ仮想マシンまたは物理サーバに格納されている Microsoft SQL データベースを使用する場合は、SQL Reporting Service によってポート 80 が使用されます。vCenter Server をインストールまたはアップグレードする際、インストーラによって、vCenter Server 用の HTTP ポートの変更を求めるメッセージが表示されます。インストールまたはアップグレードを正常に実行するため、vCenter Server の HTTP ポートをカスタムの値に変更します。</p> <p>重要： このポート番号は、vCenter Server および Platform Services Controller の Windows へのインストール時に変更できません。</p>	<p>Windows へのインストールとアプライアンスのデプロイ</p> <ul style="list-style-type: none"> ■ vCenter Server ■ Platform Services Controller 	なし
88	TCP	<p>Active Directory サーバ。Active Directory に参加するため、このポートはホストに対して開放しておく必要があります。ネイティブの Active Directory を使用する場合、ポートは vCenter Server と Platform Services Controller の両方で開放する必要があります。</p>	<p>Windows のインストールと、Platform Services Controller のアプライアンスのデプロイ</p>	なし

表 2-6. コンポーネント間の通信に必要なポート（続き）

ポート	プロトコル	説明	目的	ノード間通信での使用
389	TCP/UDP	<p>このポートは、vCenter Server のローカル インスタンスとすべてのリモート インスタンスで開いている必要があります。これは、vCenter Server グループのディレクトリ サービス用の LDAP ポート番号です。このポートで別のサービスが実行されている場合は、そのサービスを削除するか、別のポートに変更することをお勧めします。LDAP サービスを 1025 ～ 65535 の任意のポートで実行できます。</p> <p>このインスタンスを Microsoft Windows Active Directory として使用する場合は、ポート番号を 389 から、1025 ～ 65535 の範囲内の使用可能なポートに変更します。</p>	Windows のインストールと、Platform Services Controller のアプライアンスのデプロイ	<ul style="list-style-type: none"> ■ vCenter Server から Platform Services Controller へ ■ Platform Services Controller から Platform Services Controller へ
443	TCP	<p>vCenter Server システムが、vSphere Web Client からの接続を待機するデフォルトのポートです。vCenter Server システムが vSphere Web Client からデータを受信できるようにするには、ファイアウォールでポート 443 を開きます。</p> <p>vCenter Server システムでは、SDK クライアントからのデータ転送を監視する場合にもポート 443 が使用されます。</p> <p>このポートは、次のサービスでも使用されます。</p> <ul style="list-style-type: none"> ■ WS-Management（ポート 80 の開放が必要） ■ サードパーティ製ネットワーク管理クライアントから vCenter Server への接続 ■ サードパーティ製ネットワーク管理クライアントからホストへのアクセス <p>重要： このポート番号は、vCenter Server および Platform Services Controller の Windows へのインストール時に変更できません。</p>	<p>Windows へのインストールとアプライアンスのデプロイ</p> <ul style="list-style-type: none"> ■ vCenter Server ■ Platform Services Controller 	<ul style="list-style-type: none"> ■ vCenter Server から vCenter Server へ ■ vCenter Server から Platform Services Controller へ ■ Platform Services Controller から vCenter Server へ
514	TCP/UDP	<p>Windows 上の vCenter Server 用の vSphere Syslog Collector ポートと、vCenter Server Appliance 用の vSphere Syslog Service ポート</p> <p>重要： このポート番号は、vCenter Server および Platform Services Controller の Windows へのインストール時に変更できません。</p>	<p>Windows へのインストールとアプライアンスのデプロイ</p> <ul style="list-style-type: none"> ■ vCenter Server ■ Platform Services Controller 	なし

表 2-6. コンポーネント間の通信に必要なポート（続き）

ポート	プロトコル	説明	目的	ノード間通信での使用
636	TCP	vCenter Single Sign-On LDAPS	Windows のインストールと、Platform Services Controller のアプライアンスのデプロイ	vCenter Server から Platform Services Controller へ
902	TCP/UDP	<p>vCenter Server システムが、管理対象ホストへのデータ送信に使用するデフォルトのポートです。管理対象ホストは、UDP ポート 902 を使用して、vCenter Server システムに定期的なハートビートも送信します。このポートは、サーバとホスト間、またはホスト間のファイアウォールによってブロックされないようにする必要があります。</p> <p>ポート 902 は vSphere Client とホストの間でブロックされないようにする必要があります。vSphere Client は、このポートを使用して仮想マシンのコンソールを表示します。</p> <p>重要： このポート番号は、vCenter Server の Windows へのインストール時に変更できません。</p>	Windows のインストールと、vCenter Server のアプライアンスのデプロイ	なし
1514	TCP/UDP	<p>Windows 上の vCenter Server 用の vSphere Syslog Collector TLS ポートと、vCenter Server Appliance 用の vSphere Syslog Service TLS ポート</p> <p>重要： このポート番号は、vCenter Server および Platform Services Controller の Windows へのインストール時に変更できません。</p>	<p>Windows へのインストールとアプライアンスのデプロイ</p> <ul style="list-style-type: none"> ■ vCenter Server ■ Platform Services Controller 	なし
2012	TCP	vCenter Single Sign-On の制御インターフェイス RPC	Windows のインストールと、Platform Services Controller のアプライアンスのデプロイ	<ul style="list-style-type: none"> ■ vCenter Server から Platform Services Controller へ ■ Platform Services Controller から vCenter Server へ ■ Platform Services Controller から Platform Services Controller へ
2014	TCP	<p>すべての VMCA（VMware 認証局）API の RPC ポート</p> <p>重要： このポート番号は、Platform Services Controller の Windows へのインストール時に変更できます。</p>	Windows のインストールと、Platform Services Controller のアプライアンスのデプロイ	<ul style="list-style-type: none"> ■ vCenter Server から Platform Services Controller へ ■ Platform Services Controller から vCenter Server へ

表 2-6. コンポーネント間の通信に必要なポート（続き）

ポート	プロトコル	説明	目的	ノード間通信での使用
2020	TCP/UDP	認証フレームワーク管理 重要： このポート番号は、vCenter Server および Platform Services Controller の Windows へのインストール時に変更できます。	Windows へのインストールとアプライアンスのデプロイ ■ vCenter Server ■ Platform Services Controller	■ vCenter Server から Platform Services Controller へ ■ Platform Services Controller から vCenter Server へ
5480	TCP	アプライアンス管理インターフェイス HTTPS、XMLRPS、JSON-RPC のすべてのリクエストに HTTPS 経由で対応するエンドポイントを開放します。	次のアプライアンスのデプロイ ■ vCenter Server ■ Platform Services Controller	なし
6500	TCP/UDP	ESXi Dump Collector ポート 重要： このポート番号は、vCenter Server の Windows へのインストール時に変更できます。	Windows のインストールと、vCenter Server のアプライアンスのデプロイ	なし
6501	TCP	Auto Deploy サービス 重要： このポート番号は、vCenter Server の Windows へのインストール時に変更できます。	Windows のインストールと、vCenter Server のアプライアンスのデプロイ	なし
6502	TCP	Auto Deploy 管理 重要： このポート番号は、vCenter Server の Windows へのインストール時に変更できます。	Windows のインストールと、vCenter Server のアプライアンスのデプロイ	なし
7444	TCP	Secure Token Service	Windows のインストールと、Platform Services Controller のアプライアンスのデプロイ	■ vCenter Server から Platform Services Controller へ ■ Platform Services Controller から vCenter Server へ
9443	TCP	vSphere Web Client HTTPS	Windows のインストールと、vCenter Server のアプライアンスのデプロイ	なし

表 2-6. コンポーネント間の通信に必要なポート（続き）

ポート	プロトコル	説明	目的	ノード間通信での使用
11711	TCP	vCenter Single Sign-On LDAP	-	vSphere 5.5 との下位互換性のためのみ。 vCenter Single Sign-On 5.5 から Platform Services Controller 6.0
11712	TCP	vCenter Single Sign-On LDAPS	-	vSphere 5.5 との下位互換性のためのみ。 vCenter Single Sign-On 5.5 から Platform Services Controller 6.0

別のポートを使用して vSphere Web Client データを受信するように vCenter Server システムを構成するには、『vCenter Server およびホスト管理』を参照してください。

ファイアウォールの構成の詳細については、『vSphere セキュリティ』を参照してください。

vCenter Server データベースの構成に関する注意事項

サポートされているデータベース タイプを選択したら、特殊な構成要件をすべて把握していることを確認してください。

表 2-7. vCenter Server でサポートされるデータベースの構成メモ は、vCenter Server および vCenter Server Appliance でサポートされているデータベースの完全なリストではありません。vCenter Server でサポートされる特定のデータベース バージョンおよびサービス パック構成の詳細については、『VMware 製品の相互運用性マトリックス』を参照してください。vCenter Server Appliance では、vCenter Server と同じバージョンの Oracle データベースがサポートされています。表 2-7. vCenter Server でサポートされるデータベースの構成メモ には、製品相互運用性マトリックスには含まれていない特殊なデータベース構成メモだけが掲載されています。

注： vSphere Update Manager にもデータベースが必要です。vCenter Server と vSphere Update Manager には、異なるデータベースを使用してください。

vCenter Server データベースでは UTF コード セットが必要です。

表 2-7. vCenter Server でサポートされるデータベースの構成メモ

データベース タイプ	構成メモ
PostgreSQL	<p>vCenter Server 6.0 の場合、ホスト 20 台、仮想マシン 200 台までの環境では、バンドルされている PostgreSQL データベースが適しています。vCenter Server Appliance の場合、ホスト 1,000 台、仮想マシン 10,000 台までの環境では、組み込みの PostgreSQL データベースを使用できます。</p> <p>重要： 組み込みの PostgreSQL データベースを使用する場合は、Windows で vCenter Server をアンインストールすると、組み込みのデータベースもアンインストールされ、すべてのデータが消失します。</p> <p>vCenter Server 5.x を vCenter Server 6.0 にアップグレードすると、バンドルされている Microsoft SQL Server Express データベースが PostgreSQL に移行されます。</p>
Microsoft SQL Server 2008 R2 SP2 以上	<p>マシンに有効な ODBC DSN エントリがあることを確認します。</p> <p>注： このデータベースは、vCenter Server アプライアンスではサポートされません。</p>
Microsoft SQL Server 2012	<p>マシンに有効な ODBC DSN エントリがあることを確認します。</p> <p>注： このデータベースは、vCenter Server アプライアンスではサポートされません。</p>
Microsoft SQL Server 2014	<p>マシンに有効な ODBC DSN エントリがあることを確認します。</p> <p>注： このデータベースは、vCenter Server アプライアンスではサポートされません。</p>
Oracle 11g および Oracle 12c	<p>マシンに有効な ODBC DSN エントリがあることを確認します。</p> <p>vCenter Server のインストールが完了したら、Oracle クライアントおよびサーバに最新のパッチを適用します。</p>

ESXi の要件

ESXi 6.0 をインストールするか、ESXi 6.0 にアップグレードするには、システムが固有のハードウェアおよびソフトウェア要件を満たしている必要があります。

ESXi のハードウェア要件

ESXi 6.0 でサポートされるハードウェアの最小構成を満たしていることを確認します。

ハードウェアおよびシステム リソース

ESXi 6.0 をインストールまたはアップグレードするには、ハードウェアとシステムのリソースが次の要件を満たしている必要があります。

- サポートされているサーバ プラットフォーム。サポートされているプラットフォームについては、<http://www.vmware.com/resources/compatibility> の『VMware 互換性ガイド』を参照してください。
- ESXi 6.0 では、少なくとも 2 つの CPU コアを持つホスト マシンが必要です。
- ESXi 6.0 は、2006 年 9 月以降にリリースされた 64 ビット x86 プロセッサをサポートしています。これには、広範なマルチコア プロセッサが含まれます。サポートされるプロセッサの詳細なリストについては、『VMware 互換性ガイド』(<http://www.vmware.com/resources/compatibility>) を参照してください。
- ESXi 6.0 では、BIOS で CPU の NX/XD ビットを有効にする必要があります。
- ESXi には、少なくとも 4GB の物理 RAM が必要です。一般的な本番環境で仮想マシンを実行するためには、少なくとも 8 GB の RAM を用意することをお勧めします。

- 64 ビット仮想マシンをサポートするには、ハードウェア仮想化のサポート (Intel VT-x または AMD RVI) を x64 CPU で有効にする必要があります。
- 1 つ以上のギガビットまたはより高速なイーサネット コントローラ。サポートされているネットワーク アダプタ モデルについては、<http://www.vmware.com/resources/compatibility> の『VMware 互換性ガイド』を参照してください。
- 仮想マシン用にパーティショニングされていない領域がある SCSI ディスクまたはローカル (ネットワークに接続されていない) RAID LUN。
- SATA (Serial ATA) の場合、サポート対象の SAS コントローラまたはオンボード SATA コントローラを介して接続されるディスク。SATA ディスクは、ローカルではなくリモートと見なされます。これらのディスクは、リモートと見なされるため、デフォルトではスクラッチ パーティションとして使用されません。

注： ESXi 6.0 ホストにある仮想マシンに SATA CD-ROM デバイスを接続することはできません。SATA CD-ROM デバイスを使用するには、IDE エミュレーション モードを使用する必要があります。

ストレージ システム

サポートされるストレージ システムについては、<http://www.vmware.com/resources/compatibility> で『VMware 互換性ガイド』を参照してください。ソフトウェア ファイバ チャネル オーバー イーサネット (FCoE) については、[ソフトウェア FCoE による ESXi のインストールおよび起動](#)を参照してください。

ESXi 起動要件

vSphere 6.0 では、統合拡張ファームウェア インターフェイス (UEFI) から ESXi ホストを起動できます。UEFI を使用すると、ハード ドライブ、CD-ROM ドライブ、または USB メディアからシステムを起動できます。VMware Auto Deploy を使用したネットワークの起動またはプロビジョニングでは、レガシーの BIOS ファームウェアが必要ですが、UEFI では使用できません。

ESXi は、2TB を超える大きさのディスクから起動できます (使用しているシステム ファームウェアおよびアドインカード上のファームウェアでサポートされている場合)。ベンダーのドキュメントを参照してください。

注： ESXi 6.0 のインストール後に、起動タイプをレガシーの BIOS から UEFI に変更すると、ホストの起動に失敗する可能性があります。その場合は、ホストに、VMware の起動バンクではないことを示すエラー メッセージが表示されます。ESXi 6.0 のインストール後に、レガシーの BIOS と UEFI の間で起動タイプを変更することはできません。

ESXi 6.0 をインストールまたはアップグレードするためのストレージ要件

ESXi 6.0 のインストールまたは ESXi 6.0 へのアップグレードには、最低 1GB の起動デバイスが必要です。ローカル ディスク、SAN、または iSCSI LUN から起動する場合、VMFS ボリュームと 4GB のスクラッチ パーティションを起動デバイスに作成するには、5.2GB のディスクが必要です。これより小さいディスクまたは LUN が使用されている場合、インストーラは別個のローカル ディスク上にスクラッチ領域を割り当てようとします。ローカル ディスクが見つからない場合、スクラッチ パーティション /scratch が ESXi ホスト RAM ディスクに置かれ、/tmp/scratch にリンクされます。別のディスクまたは LUN を使用するように /scratch を再設定できます。最適なパフォーマンスとメモリーの最適化を実現するために、/scratch を ESXi ホスト RAM ディスク上に置かないでください。

/scratch を再設定するには、『vSphere のインストールとセットアップ』ドキュメントのトピック「vSphere Web Client からのスクラッチ パーティションの設定」を参照してください。

USB および SD デバイスの I/O 感度により、インストーラはこれらのデバイス上にはスクラッチ パーティションを作成しません。USB または SD デバイスでインストールまたはアップグレードする場合、インストーラはスクラッチ領域を使用可能なローカル ディスクまたはデータストアに割り当てようとします。ローカル ディスクまたはデータストアが見つからない場合、/scratch は RAM ディスクに置かれます。インストールまたはアップグレード後、永続データストアを使用するように、/scratch を再設定する必要があります。最小構成のインストールには 1GB の USB または SD デバイスがあれば十分ですが、4GB 以上のデバイスを使用するようにしてください。余分なスペースは、USB/SD デバイス上の拡張コアダンプ パーティションに使用されます。フラッシュ セルが余分にあれば起動メディア長持ちさせることができるため、16 GB 以上の高品質な USB フラッシュ ドライブを使用してください。ただし、4 GB 以上の高品質なドライブであれば、コアダンプの拡張パーティションを保持するには十分です。詳細は、ナレッジ ペースの記事 <http://kb.vmware.com/kb/2004784> を参照してください。

Auto Deploy インストールの場合、インストーラはスクラッチ領域を使用可能なローカル ディスクまたはデータストアに割り当てようとします。ローカル ディスクまたはデータストアが見つからない場合、/scratch は RAM ディスクに置かれます。インストールの後に永続データストアを使用するように、/scratch を再設定する必要があります。

SAN から起動する環境または Auto Deploy を使用する環境では、ESXi ホストごとに別個の LUN を割り当てる必要はありません。多数の ESXi ホスト用のスクラッチ領域を単一の LUN に一緒に置くことができます。単一の LUN に割り当てるホスト数は、LUN のサイズと仮想マシンの I/O 動作を考慮して比較検討する必要があります。

サポートされているリモート管理のサーバ モデルとファームウェア バージョン

リモート管理アプリケーションを使用して、ESXi のインストールまたはアップグレード、またはホストのリモート管理を実行できます。

表 2-8. サポートされているリモート管理のサーバ モデルとファームウェアの最小バージョン

リモート管理サーバ モデル	ファームウェアのバージョン	Java
Dell DRAC 7	1.30.30 (ビルド 43)	1.7.0_60-b19
Dell DRAC 6	1.54 (ビルド 15)、1.70 (ビルド 21)	1.6.0_24
Dell DRAC 5	1.0、1.45、1.51	1.6.0_20、1.6.0_203
Dell DRAC 4	1.75	1.6.0_23
HP iLO	1.81、1.92	1.6.0_22、1.6.0_23
HP iLO 2	1.8、1.81	1.6.0_20、1.6.0_23
HP iLO 3	1.28	1.7.0_60-b19
HP iLO 4	1.13	1.7.0_60-b19
IBM RSA 2	1.03、1.2	1.6.0_22

ESXi のパフォーマンスを改善するための推奨事項

パフォーマンスを向上させるには、必要最小限以上の容量を持つ RAM と複数の物理ディスクがある堅牢なシステムで ESXi をインストールまたはアップグレードします。

ESXi システムの要件については、[ESXi のハードウェア要件](https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-perfbest-practices-vsphere6-0-white-paper.pdf)を参照してください。vSphere のパフォーマンスに関するテクニカル ペーパー (<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-perfbest-practices-vsphere6-0-white-paper.pdf>) も参照してください。

表 2-9. パフォーマンス向上に関する推奨事項

システム要素	推奨
RAM	<p>ESXi ホストには、一般的なサーバよりも多くの RAM が必要です。ESXi の機能を十分に活用し、一般的な本番環境で仮想マシンを実行するために、少なくとも 8 GB の RAM を提供します。ESXi ホストに、複数の仮想マシンを同時に実行するのに十分な容量の RAM が必要です。次の例を使用して、ESXi ホストで実行されている仮想マシンが必要とする RAM の計算方法を示します。</p> <p>Red Hat Enterprise Linux または Windows XP がインストールされた 4 台の仮想マシンが動作するには、ベースライン パフォーマンスを保つだけでも最低 3 GB の RAM が必要です。この数値には、仮想マシン用の約 1,024 MB、オペレーティング システムごとに最小限必要な 256 MB（ベンダーが推奨する値）が含まれます。</p> <p>これらの 4 台の仮想マシンを 512 MB の RAM で実行するには、ESXi ホストに約 4 GB の RAM が必要です（仮想マシン用の 2,048 MB を含む）。</p> <p>これらの計算値には、各仮想マシンに可変オーバーヘッド メモリを使用することで節約できるメモリ容量は考慮されていません。『vSphere リソース管理』を参照してください。</p>
仮想マシン専用のファスト イーサネット アダプタ	<p>管理ネットワークと仮想マシン ネットワークを異なる物理ネットワーク カードに配置します。Intel PRO 1000 アダプタなど仮想マシン専用のギガビット イーサネット カードを使用すると、高ネットワークトラフィックでの仮想マシンへのスループットが向上します。ディスクの場所：</p>
ディスクの場所	<p>仮想マシンで使用されるすべてのデータを仮想マシンに割り当てられている物理ディスク上に配置します。ESXi の起動イメージがあるディスクに仮想マシンを配置しないほうが、パフォーマンスが向上します。物理ディスクは、すべての仮想マシンによって使用されるディスク イメージを保存できる大きさを備えている必要があります。</p>
VMFS5 パーティショニング	<p>ESXi インストーラでは、最初に検出された空のローカル ディスク上に初期 VMFS ボリュームが作成されます。ディスクを追加するか、元の構成を変更するには、vSphere Web Client を使用します。この方法では、パーティションの開始セクタが 64K セクタごとの割り当てになるため、ストレージ パフォーマンスが改善されます。</p> <p>注： SAS のみの環境では、インストーラがディスクをフォーマットしない場合があります。一部の SAS ディスクは、ディスクがローカルかリモートかを識別することができません。インストール後、vSphere Web Client を使用して VMFS を設定できます。</p>

表 2-9. パフォーマンス向上に関する推奨事項（続き）

システム要素	推奨
プロセッサ	プロセッサの処理速度が速いほど、ESXi のパフォーマンスが向上します。特定のワークロードでは、キャッシュが大きい方が ESXi のパフォーマンスが向上します。
ハードウェア互換性	サーバ内で、ESXi 6.0 ドライバのサポート対象になっているデバイスを使用します。 http://www.vmware.com/resources/compatibility の『ハードウェア互換性ガイド』を参照してください。

ESXi ホストの発着信ファイアウォール ポート

vSphere Web Client では、各サービスのファイアウォール ポートを開閉したり、選択した IP アドレスからのトラフィックを許可したりできます。

次の表に、通常インストールされるサービスのファイアウォールを一覧表示します。他の VIB をホストにインストールすると、追加のサービスおよびファイアウォール ポートが使用可能になる場合があります。

表 2-10. 着信ファイアウォール接続

サービス	ポート	コメント
CIM サーバ	5988 (TCP)	CIM (Common Information Model) のサーバ。
CIM セキュア サーバ	5989 (TCP)	CIM のセキュア サーバ。
CIM SLP	427 (TCP、UDP)	CIM クライアントは、サービス ロケーション プロトコル バージョン 2 (SLPv2) を使用して、CIM サーバを検索します。
DHCPv6	546 (TCP、UDP)	IPv6 の DHCP クライアント。
DVSSync	8301、8302 (UDP)	DVSSync ポートは、VMware FT の記録/再生が有効になっているホスト間で分散仮想ポートの状態を同期するために使用されます。これらのポートは、プライマリまたはバックアップ仮想マシンを実行しているホストでのみ開いている必要があります。VMware FT を使用していないホストでは、これらのポートが開いている必要はありません。
NFC	902 (TCP)	NFC (ネットワーク ファイル コピー) によって、vSphere コンポーネントでファイル タイプに対応した FTP サービスを使用できます。ESXi は、データストア間のデータのコピーや移動などの操作にデフォルトで NFC を使用します。
Virtual SAN クラスタリング サービス	12345、23451 (UDP)	Virtual SAN クラスタ監視およびメンバーシップ ディレトリ サービス。UDP ベースの IP マルチキャストを使用してクラスタ メンバーを確立し、Virtual SAN メタデータをすべてのクラスタ メンバーに配布します。無効になっている場合、Virtual SAN は機能しません。
DHCP クライアント	68 (UDP)	IPv4 の DHCP クライアント。
DNS クライアント	53 (UDP)	DNS クライアント。
Fault Tolerance	8200、8100、8300 (TCP、UDP)	vSphere Fault Tolerance (FT) 用のホスト間のトラフィック。

表 2-10. 着信ファイアウォール接続（続き）

サービス	ポート	コメント
NSX 分散論理ルータ サービス	6999 (UDP)	NSX 仮想分散ルータ サービス。NSX VIB がインストールされていて、VDR モジュールが作成されている場合、このサービスに関連付けられているファイアウォール ポートが開きます。VDR インスタンスがホストに関連付けられていない場合、ポートが開いている必要はありません。 このサービスは、この製品の以前のバージョンでは NSX 分散論理ルータと呼ばれていました。
Virtual SAN 転送	2233 (TCP)	Virtual SAN の信頼性の高いデータグラム転送。TCP を使用し、Virtual SAN ストレージ IO で使用されます。無効になっている場合、Virtual SAN は機能しません。
SNMP サーバ	161 (UDP)	ホストから SNMP サーバに接続できます。
SSH サーバ	22 (TCP)	SSH アクセスに必要です。
vMotion	8000 (TCP)	vMotion を使用した仮想マシンの移行に必要です。
vSphere Web Client	902, 443 (TCP)	クライアント接続
vsanvp	8080 (TCP)	VSAN VASA ベンダー プロバイダ。Virtual SAN ストレージのプロファイル、機能、およびコンプライアンスに関する情報にアクセスするために、vCenter の一部であるストレージ管理サービス (SMS) で使用されます。無効になっている場合、Virtual SAN ストレージ プロファイル ベース管理 (SPBM) は機能しません。
vSphere Web Access	80 (TCP)	別のインターフェイスのダウンロード リンクがある [ようこそ] ページ。

表 2-11. 発信ファイアウォール接続

サービス	ポート	コメント
CIM SLP	427 (TCP, UDP)	CIM クライアントは、サービス ロケーション プロトコル バージョン 2 (SLPv2) を使用して、CIM サーバを検索します。
DHCPv6	547 (TCP, UDP)	IPv6 の DHCP クライアント。
DVSSync	8301, 8302 (UDP)	DVSSync ポートは、VMware FT の記録/再生が有効になっているホスト間で分散仮想ポートの状態を同期するために使用されます。これらのポートは、プライマリまたはバックアップ仮想マシンを実行しているホストでのみ開いている必要があります。VMware FT を使用していないホストでは、これらのポートが開いている必要はありません。
HBR	44046, 31031 (TCP)	vSphere Replication および VMware Site Recovery Manager によって、実行中のレプリケーション トラフィックで使用されます。
NFC	902 (TCP)	NFC (ネットワーク ファイル コピー) によって、vSphere コンポーネントでファイル タイプに対応した FTP サービスを使用できます。ESXi は、データストア間のデータのコピーや移動などの操作にデフォルトで NFC を使用します。

表 2-11. 発信ファイアウォール接続（続き）

サービス	ポート	コメント
WOL	9 (UDP)	Wake-on-LAN によって使用されます。
Virtual SAN クラスタリング サービス	12345、23451 (UDP)	Virtual SAN で使用されるクラスタ監視、メンバーシップ、およびディレクトリ サービス。
DHCP クライアント	68 (UDP)	DHCP クライアント。
DNS クライアント	53 (TCP、UDP)	DNS クライアント。
Fault Tolerance	80、8200、8100、8300 (TCP、UDP)	VMware Fault Tolerance に対応します。
ソフトウェア iSCSI クライアント	3260 (TCP)	ソフトウェア iSCSI に対応します。
NSX 分散論理ルータ サービス	6999 (UDP)	NSX VIB がインストールされていて、VDR モジュールが作成されている場合、このサービスに関連付けられているファイアウォール ポートが開きます。VDR インスタンスがホストに関連付けられていない場合、ポートが開いている必要はありません。
rabbitmqproxy	5671 (TCP)	仮想マシン内で実行されるアプリケーションと、vCenter ネットワーク ドメインで実行される AMQP ブローカが通信できるようにする、ESXi ホストで実行されるプロキシ。仮想マシンはネットワーク上に存在している必要はありません。つまり、NIC は必要ありません。プロキシは、vCenter ネットワーク ドメインのブローカに接続します。そのため、発信接続 IP アドレスには、少なくとも現在使用中のブローカまたは後で使用するブローカが含まれている必要があります。拡張が必要な場合にブローカを追加できます。
Virtual SAN 転送	2233 (TCP)	Virtual SAN ノード間の RDT トラフィック（ピア ツー ピアのユニキャスト通信）で使用されます。
vMotion	8000 (TCP)	vMotion を使用した仮想マシンの移行に必要です。
VMware vCenter Agent	902 (UDP)	vCenter Server エージェント。
vsanvp	8080 (TCP)	Virtual SAN ベンダー プロバイダ トラフィックで使用されます。

vSphere DNS の要件

vCenter Server は、ほかのネットワーク サーバと同様に、固定 IP アドレスと既知の DNS 名を持つマシンにインストールまたはアップグレードし、クライアントが確実にサービスにアクセスできるようにします。

vCenter Server システムを導入する Windows サーバに、固定 IP アドレスとホスト名を割り当てること。この IP アドレスは、有効な（内部）ドメイン名システム（DNS）に登録されている必要があります。vCenter Server と Platform Services Controller をインストールする場合は、インストールまたはアップグレードが実行されるホスト マシンの完全修飾ドメイン名 (FQDN) または固定 IP アドレスを指定する必要があります。FQDN を使用することを推奨します。

vCenter Server Appliance をデプロイする際に、アプライアンスに固定 IP アドレスを割り当てることができます。固定 IP アドレスを割り当てれば、システムが再起動された場合でも、vCenter Server Appliance の IP アドレスは変わりません。

DNS のリバース ルックアップで、vCenter Server がインストールされているホスト マシンの IP アドレスを指定して問い合わせたときに、FQDN が返されることを確認します。vCenter Server のインストールまたはアップグレード時に、インストーラが vCenter Server ホスト マシンの IP アドレスからその完全修飾ドメイン名をルックアップできないと、vSphere Web Client をサポートする Web サーバ コンポーネントのインストールまたはアップグレードに失敗します。リバース ルックアップは PTR レコードを使用して実装されます。

vCenter Server の固定 IP アドレスではなく DHCP を使用する場合は、vCenter Server のコンピュータ名がドメイン名システム (DNS) 内で更新されていることを確認します。コンピュータ名を ping 送信すると、その名前が DNS でアップデートされます。

ESXi ホスト管理インターフェイスで、vCenter Server とすべての vSphere Web Client インスタンスから有効に DNS 解決されることを確認してください。vCenter Server で、すべての ESXi ホストとすべての vSphere Web Client が、DNS で正しく名前解決されることを確認してください。

vSphere Web Client のソフトウェア要件

使用するブラウザが vSphere Web Client をサポートしていることを確認します。

vSphere Web Client 6.0 には、Adobe Flash Player 16 以降が必要です。Linux システム用の Adobe Flash Player の最新バージョンは 11.2 です。したがって、vSphere Web Client を Linux プラットフォームで実行することはできません。

次のゲスト OS とブラウザ バージョンはテスト済みであり、vSphere Web Client でサポートされています。最高のパフォーマンスを得るには、Google Chrome を使用してください。

表 2-12. vSphere Web Client でサポートされるゲスト OS およびブラウザの最小バージョン

オペレーティング システム	ブラウザ
Windows	Microsoft Internet Explorer 10.0.19 以降。 Mozilla Firefox 34 以降。 Google Chrome 39 以降。
Mac OS	Mozilla Firefox 34 以降。 Google Chrome 39 以降。

クライアント統合プラグインのソフトウェア要件

ESXi ホストに接続して vCenter Server Appliance をデプロイまたはアップグレードできるように、vSphere Web Client から個別にクライアント統合プラグインをインストールする場合、ブラウザでクライアント統合プラグインがサポートされていることを確認します。

クライアント統合プラグインを使用するには、いずれかのサポート対象 Web ブラウザがあることを確認します。

表 2-13. サポート対象 Web ブラウザ

ブラウザ	サポートされているバージョン
Microsoft Internet Explorer	バージョン 10 および 11
Mozilla Firefox	バージョン 30 以降
Google Chrome	バージョン 35 以降

vSphere Client の要件

vSphere Client をインストールして単一の ESXi ホストを管理できます。vSphere Client をインストールする Windows システムは、特定のハードウェア要件とソフトウェア要件を満たしている必要があります。

vSphere Client のハードウェア要件

vSphere Client のハードウェアが最小要件を満たしていることを確認します。

vSphere Client のハードウェア最小要件および推奨事項

表 2-14. vSphere Client のハードウェア最小要件および推奨事項

vSphere Client ハードウェア	要件および推奨事項
CPU	1 つの CPU
プロセッサ	500MHz 以上の Intel または AMD プロセッサ (1GHz を推奨)
メモリ	500MB (1GB を推奨)
ディスク ストレージ	<p>次のコンポーネントを含むフル インストールでは 1.5GB の空きディスク容量</p> <ul style="list-style-type: none"> ■ Microsoft .NET 2.0 SP2 ■ Microsoft .NET 3.0 SP2 ■ Microsoft .NET 3.5 SP1 ■ Microsoft Visual J# <p>vSphere Client をインストールするシステム上にある Microsoft Visual J# のインストール済みのバージョンをすべて削除します。</p> <ul style="list-style-type: none"> ■ vSphere Client <p>これらのコンポーネントがいずれもインストールされていない場合、%temp% ディレクトリがあるドライブに 400MB の空き容量が必要です。</p> <p>コンポーネントがすべてインストールされている場合は、%temp% ディレクトリがあるドライブに 300MB の空き容量が必要であり、vSphere Client には 450MB の空き容量が必要です。</p>
ネットワーク	ギガビット接続を推奨

vSphere Client のソフトウェア要件

使用するオペレーティング システムが vSphere Client をサポートしていることを確認します。

vSphere Client でサポートされる全オペレーティング システムの最新の一覧については、「[vSphere Client \(Windows\) のインストールがサポートされるホスト オペレーティング システム](#)」を参照してください。

vSphere Client には、Microsoft .NET 3.5 SP1 Framework が必要です。システムにインストールされていない場合は、vSphere Client のインストーラによってインストールされます。ファイルを追加でダウンロードするために、.NET 3.5 SP1 インストールでインターネット接続が必要になる場合があります。

vSphere Client の TCP および UDP ポート

ESXi ホストおよびその他のネットワーク コンポーネントには、あらかじめ定義されている TCP および UDP ポートを使用してアクセスします。ファイアウォールの外からネットワーク コンポーネントを管理する場合、ファイアウォールを再設定して、該当するポートへのアクセスを許可する必要があります。

次の表に、TCP および UDP ポートと、それぞれの目的およびタイプを示します。インストール時にデフォルトで開かれたポートは、「(デフォルト)」で示されます。

表 2-15. TCP および UDP ポート

ポート	目的	トラフィック タイプ
443 (デフォルト)	HTTPS アクセス vSphere Client から vCenter Server へのアクセス vSphere Client から ESXi ホストへのアクセス vSphere Client から vSphere Update Manager へのアクセス	ESXi ホストへの送信 TCP 接続
902 (デフォルト)	vSphere Client から仮想マシン コンソールへのアクセス	ESXi ホストへの受信 TCP 接続、ESXi ホストからの送信 TCP 接続、 ESXi ホストからの送信 UDP 接続

システム ログに必要な空き容量

Auto Deploy を使用して ESXi 6.0 ホストをインストールする場合、または VMFS ボリューム上のスクラッチ ディレクトリ内のデフォルトの場所とは別にログ ディレクトリを設定する場合、システム ログ用の十分な空き領域を用意するため、現在のログ サイズとローテーション設定の変更が必要になることがあります。

vSphere のすべてのコンポーネントではこのインフラストラクチャを使用しています。このインフラストラクチャでのログ容量のデフォルト値は、使用可能なストレージの量、およびシステム ログの構成内容に応じて変わります。Auto Deploy を使用してデプロイしたホストでは、ログが RAM ディスクに保存されます。つまり、ログに使用できる領域はわずかです。

ホストが Auto Deploy を使用してデプロイされている場合は、次のいずれかの方法でログ ストレージを再構成してください。

- ネットワーク経由でリモート コレクタにログをリダイレクトする。
- NAS ストアまたは NFS ストアにログをリダイレクトする。

NAS ストアや NFS ストアなどの非デフォルト ストレージにログをリダイレクトする場合は、ディスクにインストールされたホストのログ サイズとローテーションも再構成できます。

デフォルト構成を使用する ESXi ホストのログ ストレージを再構成する必要はありません。このストレージは、VMFS ボリュームのスクラッチ ディレクトリにログを格納します。これらのホストについては、ESXi 6.0 によって、インストールに最も適した方法でログが構成され、ログ メッセージの保存に十分な空き領域が用意されます。

表 2-16. hostd、vpxa、fdm の各ログに対して推奨される最小サイズとローテーションの構成

ログ	ログ ファイルの最大サイズ	維持するローテーション数	必要な最小ディスク領域
管理エージェント (hostd)	10 MB	10	100 MB
VirtualCenter エージェント (vpxa)	5 MB	10	50 MB
vSphere HA エージェント (フォールト ドメイン マネージャ (fdm))	5 MB	10	50 MB

syslog および syslog サーバの設定と構成、および vSphere Syslog Collector のインストールについては、『vSphere Installation and SetupvSphere のインストールとセットアップ』ドキュメントを参照してください。

vCenter Server をアップグレードする前に行う作業

3

互換性を確認し、必要なデータベース、ネットワークまたはその他の準備タスクを行うことにより、システムで vCenter Server のアップグレードのための準備が完了していることを確認します。

この章には、次のトピックが含まれています。

- vCenter Server をアップグレードする前の基本的な互換性の確認
- vCenter Server データベースの準備
- アップグレード前のネットワークの前提条件の確認
- vCenter Server をアップグレードする前のロード バランサの確認
- vCenter Server のアップグレードのための ESXi ホストの準備
- vCenter Server のアップグレード準備が完了したことの確認
- Windows 版 vCenter Server のアップグレードに必要な情報
- vCenter Server Appliance のアップグレードに必要な情報

vCenter Server をアップグレードする前の基本的な互換性の確認

vCenter Server のアップグレード前に、すべてのコンポーネントが基本的な互換性の要件を満たしていることを確認します。

オペレーティング システムの要件を満たすために vCenter Single Sign-On 5.1 マシンのオペレーティング システムを Windows 2003 から Windows 2008 にアップグレードすると、ナレッジベースの記事 [2036170](#) で説明されている症状と同様の症状が発生する可能性があります。

前提条件

システムがハードウェアとソフトウェアの要件を満たしていることを確認します。[Windows 版 vCenter Server の要件](#) および [vCenter Server Appliance の要件](#) を参照してください。

ソリューションやプラグインがある場合は、VMware 製品の相互運用性マトリックスで調べてください。を参照してください。http://www.vmware.com/resources/compatibility/sim/interop_matrix.php

手順

- 1 前のバージョンの vCenter Server のインストール パスは、ADAM/AD LDS (Microsoft Active Directory Application Mode) のインストール要件に適合する必要があります。

インストール パスには、ASCII 以外の文字、コンマ (,)、ピリオド (.)、感嘆符 (!)、ナンバー記号 (#)、アット記号 (@)、パーセント記号 (%) のいずれの文字も含めることができません。

前のバージョンの vCenter Server がこの要件を満たしていない場合は、vCenter Server を新規インストールする必要があります。

- 2 vCenter Server システムが、プライマリまたはバックアップの Active Directory ドメイン コントローラになっていないことを確認します。
- 3 すべての ESX/ESXi 4.1 ホストをバージョン 5.x に更新します。
- 4 アップグレードしない ESX 4.x ホストがある場合は、そのホストを vCenter Server インベントリから削除する必要があります。
- 5 アップグレードする vCenter Server 4.x 環境に Guided Consolidation 4.x が存在する場合は、Guided Consolidation をアンインストールしてから vCenter Server 6.0 にアップグレードします。

vCenter Server データベースの準備

vCenter Server には、サーバ データを格納および編成するためのデータベースが必要です。デプロイ時に、インストールおよび構成可能なバンドルされている PostgreSQL データベースを使用するか、外部データベースを設定します。

Windows 版 vCenter Server では、Oracle および Microsoft SQL データベースがサポートされていますが、vCenter Server Appliance では、外部データベースとして Oracle データベースのみがサポートされています。

バンドルされているデータベースはインストーラによって自動的に構成されますが、外部データベースは手動でまたはスクリプトを使用して構成できます。また、データ ソース名ユーザーには、特定の権限のリストを付与する必要があります。

データベースのパスワードは、vCenter Server をインストールする Windows 仮想マシンまたは物理ホスト、および vCenter Server Appliance にクリア テキストで保存されます。パスワードが保存されているファイルは、オペレーティング システムの保護機能を使用して保護されます。つまり、これらのファイルにアクセスして読み取るには、Windows のローカル管理者か、Linux の ルート ユーザーである必要があります。

vCenter Server インスタンスは、同じデータベース スキーマを共有できません。複数の vCenter Server データベースは同じデータベース サーバ上に配置することも、複数のデータベース サーバ間で別々に配置することもできます。Oracle データベースには、スキーマ オブジェクトの概念があるため、各 vCenter Server インスタンスのスキーマ所有者が異なる場合、1つのデータベース サーバで複数の vCenter Server インスタンスを実行できます。各 vCenter Server インスタンスで、専用の Oracle データベース サーバを使用することもできます。

vCenter Server 6.0 へアップグレードする前の Oracle データベースの準備

vCenter Server をアップグレードする前に、Oracle データベースが要件を満たしていること、必要な認証情報があること、必要なクリーンアップまたは他の準備が完了していることを確認します。

前提条件

vCenter Server のアップグレード用に Oracle データベースを準備する前に、基本的なアップグレードの相互運用性を確認します。[Windows 版 vCenter Server データベースの要件](#)および[vCenter Server Appliance データベースの要件](#)を参照してください。

データベースをバックアップしたことを確認します。vCenter Server データベースのバックアップの詳細については、Oracle のドキュメントを参照してください。

データベースの権限を正しく設定するには、[vCenter Server のデータベース権限の要件](#)を参照してください。

手順

- 1 データベースがアップグレード要件を満たしていることを確認します。必要に応じて、データベースをサポート対象のバージョンにアップグレードします。

- 2 データベース サーバが vCenter Server でサポートされていない場合、サポート対象バージョンにデータベースをアップグレードするか、サポート対象バージョンにデータベースをインポートします。

- 3 既存のデータベースが Oracle で、Oracle 11g などの新しくサポートされた Oracle データベースにアップグレードする場合、vCenter Server をアップグレードする前に Oracle データベースをアップグレードします。

既存のデータベースが Oracle であれば、vCenter Server の新規インストールは不要です。

たとえば、既存の Oracle 9i データベースを Oracle 11g または Oracle 12c にアップグレードしてから、vCenter Server 5.x を vCenter Server 6.0 にアップグレードできます。

- 4 パスワードが最新であり、十分な有効期限が設定されていることを確認します。
- 5 vCenter Server データベースで使用するログイン認証情報、データベース名、およびデータベース サーバ名があることを確認します。

ODBC システムを検索して、vCenter Server データベースのデータベース ソース名の接続名を探します。

- 6 SID の代わりに Oracle SERVICE_NAME を使用して、Oracle データベース インスタンスが使用可能であることを確認します。

- 次のアラート ログから読み取りを行うデータベース サーバにログインします。`$ORACLE_BASE/diag/rdbms/$instance_name/$INSTANCE_NAME/trace/alert_$INSTANCE_NAME.log`。
- Oracle リスナーのステータス出力から読み取りを行うデータベース サーバにログインします。
- SQL*Plus クライアントがインストールされている場合、vCenter データベース インスタンスに `tnsping` を使用できます。`tnsping` コマンドが最初に機能しない場合、数分待機した後に再試行します。再試行がうまくいかない場合、Oracle サーバ上の vCenter データベース インスタンスを再起動し、`tnsping` を再試行して使用可能であることを確認します。

- 7 JDBC ドライバ ファイルが CLASSPATH 変数に組み込まれていることを確認します。
- 8 アクセス許可が正しく設定されていることを確認します。
- 9 ユーザーに DBA ロールを割り当てるか、必要なアクセス許可を付与します。
- 10 ISO イメージで `cleanup_orphaned_data_Oracle.sql` スクリプトを探し、それを Oracle サーバにコピーします。

11 vCenter Server データベース アカウントで SQL*Plus セッションにログインします。

12 クリーンアップ スクリプトを実行します。

```
@pathcleanup_orphaned_data_Oracle.sql
```

クリーンアップ プロセスにより、どの vCenter Server コンポーネントでも使用されていない不要な、実体のないデータがバージされます。

13 vCenter Server データベースと vCenter Inventory Service データベースのフル バックアップを作成してください。

結果

vCenter Server アップグレードのためのデータベースの準備が整いました。

次のステップ

アップグレードが完了したら、必要に応じてユーザー プロファイルから create any sequence および create any table を削除します。

デフォルトで、RESOURCE ロールには CREATE PROCEDURE、CREATE TABLE、および CREATE SEQUENCE 権限が割り当てられています。RESOURCE ロールにこれらの権限がない場合は、vCenter Server データベースのユーザーに付与します。

vCenter Server 6.0 へのアップグレード前に Microsoft SQL Server データベースを準備する

vCenter Server のアップグレード前に、Microsoft SQL Server データベースが要件を満たしていること、必要な認証情報が揃っていること、および必要なクリーンアップやその他の準備作業が完了していることを確認します。

DBO ロールを削除し、DBO スキーマのすべてのオブジェクトをカスタム スキーマに移行するには、VMware のナレッジベースの記事 <http://kb.vmware.com/kb/1036331> を参照してください。

Microsoft SQL Server Express は、vCenter Server 6.0 ではサポートされません。vCenter Server 5.x の組み込み Microsoft SQL Server Express データベースは、vCenter Server 6.0 へのアップグレード時に、組み込み PostgreSQL データベースで置き換えられます。PostgreSQL データベースへ移行せずにアップグレードする方法については、VMware のナレッジベースの記事 <http://kb.vmware.com/kb/2109321> を参照してください。

Microsoft SQL Express から 完全な Microsoft SQL Server に vCenter Server データベースを移行するには、VMware のナレッジベースの記事 <http://kb.vmware.com/kb/1028601> を参照してください。

重要: vCenter Server サービスが Microsoft Windows のビルトイン システム アカウントで実行されている場合、統合 Windows の認証方法は使用できません。

前提条件

vCenter Server のアップグレード用に Microsoft SQL Server データベースを準備する前に、基本的なアップグレードの相互運用性を確認します。 [Windows 版 vCenter Server データベースの要件](#) および [vCenter Server Appliance データベースの要件](#) を参照してください。

データベースをバックアップしたことを確認します。vCenter Server データベースのバックアップの詳細については、Microsoft SQL Server のドキュメントを参照してください。

データベースの権限を正しく設定するには、[vCenter Server のデータベース権限の要件](#) および [Microsoft SQL Server データベース スキーマおよびロールの作成と適用を行うためのスクリプトの使用](#) を参照してください。

手順

- 1 データベースがアップグレード要件を満たしていることを確認します。必要に応じて、データベースをサポート対象のバージョンにアップグレードします。
- 2 データベース サーバが vCenter Server でサポートされていない場合、サポート対象バージョンにデータベースをアップグレードするか、サポート対象バージョンにデータベースをインポートします。
- 3 既存のデータベースが Microsoft SQL Server であるときに、それを Microsoft SQL Server 2012 などの新しくサポートされる Microsoft SQL Server データベースにアップグレードする場合は、vCenter Server のアップグレード前に Microsoft SQL Server データベースをアップグレードしてください。

既存のデータベースが Microsoft SQL Server の場合、新しい vCenter Server インスタンスをインストールする必要はありません。

たとえば、Microsoft SQL Server 2005 のデータベースを Microsoft SQL Server 2008 R2-SP2、2012、または 2014 データベースにアップグレードし、それから、vCenter Server 5.0 以降を vCenter Server 6.0 にアップグレードすることができます。

Microsoft SQL Server 2005 から Microsoft SQL Server 2008 R2-SP2 以降に移行する際は、データベースの互換性レベルを 100 に設定してください。

- 4 アクセス許可が正しく設定されていることを確認します。
- 5 パスワードが最新であり、十分な有効期限が設定されていることを確認します。
- 6 vCenter Server マシンに JDK 1.6 以降がインストールされていることを確認します。
- 7 vCenter Server をアップグレードするマシンの CLASSPATH 変数に、sqljdbc4.jar ファイルが追加されていることを確認します。

システムに sqljdbc4.jar ファイルがインストールされていない場合は、vCenter Server のインストーラによってインストールされます。

- 8 システム データベース ソース名で Microsoft SQL Server Native Client 10 または 11 のドライバが使用されていることを確認します。
- 9 DBO ロールを削除し、DBO スキーマのすべてのオブジェクトをカスタム スキーマに移行する場合は、必要なアクセス許可を付与する必要があります。
 - a vCenter Server データベースの vCenter Server ユーザーに、必要な権限を付与します。
 - b MSDB データベースのユーザーに、必要なアクセス許可を付与します。
- 10 ISO イメージで cleanup_orphaned_data_MSSQL.sql スクリプトを探し、それを Microsoft SQL サーバにコピーします。

11 データベースにログインします。

- a Microsoft SQL Server Express の場合は、コマンド プロンプトを開きます。
- b Microsoft SQL Server の場合は、vCenter Server データベース ユーザーとして Microsoft SQL Server Management Studio セッションにログインします。

12 Microsoft SQL Server Express の場合は、クリーンアップ スクリプトを実行します。

```
sqlcmd -E -S localhost\VIM_SQLEXP -d VIM_VCDB -i
pathcleanup_orphaned_data_MSSQL.sql
```

13 Microsoft SQL Server の場合は、cleanup_orphaned_data_MSSQL.sql のコンテンツを実行します。

vCenter Server が使用しているデータベースに接続されていることを確認します。

クリーンアップ スクリプトにより、vCenter Server データベース内の不要なデータがクリーンアップされます。

14 vCenter Server データベースと Inventory Service データベースのフル バックアップを作成してください。**結果**

vCenter Server アップグレードのためのデータベースの準備が整いました。

Microsoft SQL Server データベース スキーマおよびロールの作成と適用を行うためのスクリプトの使用

ここで説明する SQL データベースの構成方法では、既存の dbo スキーマを使用する代わりに、カスタムのスキーマ VMW を作成します。vCenter Server と組み込みまたは外部の Platform Services Controller をインストールする場合は、ユーザーのデータベース モニタリングも有効にする必要があります。

この方法では、新しいデータベース ロールの作成と、これらのロールにデータベースの *user* の権限を付与する必要があります。

前提条件

vCenter Server をアップグレードする前に適切なロールおよびアクセス許可があることを確認するには、vCenter Server の SQL Server データベースおよびユーザーを更新します。

手順

- 1 sysadmin として Microsoft SQL Server Management Studio セッションにログインするか、sysadmin の権限を持ったユーザー アカウントとしてログインします。
- 2 次のスクリプトを実行して、ロールの作成と権限の適用を行います。

このスクリプトは、vCenter Server のインストール パッケージの /インストール ディレクトリ/vCenter-Server/dbschema/DB_and_schema_creation_scripts_MSSQL.txt にあります。

```
CREATE SCHEMA [VMW]
go
ALTER USER [vpxuser] WITH DEFAULT_SCHEMA =[VMW]

if not exists (SELECT name FROM sysusers WHERE issqlrole=1 AND name = 'VC_ADMIN_ROLE')
```



```

CREATE ROLE VC_ADMIN_ROLE;
GRANT ALTER ON SCHEMA :: [VMW] to VC_ADMIN_ROLE;
GRANT REFERENCES ON SCHEMA :: [VMW] to VC_ADMIN_ROLE;
GRANT INSERT ON SCHEMA :: [VMW] to VC_ADMIN_ROLE;

GRANT CREATE TABLE to VC_ADMIN_ROLE;
GRANT CREATE VIEW to VC_ADMIN_ROLE;
GRANT CREATE Procedure to VC_ADMIN_ROLE;

if not exists (SELECT name FROM sysusers WHERE issqlrole=1 AND name = 'VC_USER_ROLE')
CREATE ROLE VC_USER_ROLE
go
GRANT SELECT ON SCHEMA :: [VMW] to VC_USER_ROLE
go
GRANT INSERT ON SCHEMA :: [VMW] to VC_USER_ROLE
go
GRANT DELETE ON SCHEMA :: [VMW] to VC_USER_ROLE
go
GRANT UPDATE ON SCHEMA :: [VMW] to VC_USER_ROLE
go
GRANT EXECUTE ON SCHEMA :: [VMW] to VC_USER_ROLE
go
sp_addrolemember VC_USER_ROLE , [vpuser]
go
sp_addrolemember VC_ADMIN_ROLE , [vpuser]
go
use MSDB
go
if not exists (SELECT name FROM sysusers WHERE issqlrole=1 AND name = 'VC_ADMIN_ROLE')
CREATE ROLE VC_ADMIN_ROLE;
go
GRANT SELECT on msdb.dbo.syscategories to VC_ADMIN_ROLE
go
GRANT SELECT on msdb.dbo.sysjobsteps to VC_ADMIN_ROLE
go
GRANT SELECT ON msdb.dbo.sysjobs to VC_ADMIN_ROLE
go
GRANT SELECT ON msdb.dbo.sysjobs_view to VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_delete_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobstep TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_update_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobserver TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobschedule TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_category TO VC_ADMIN_ROLE
go
sp_addrolemember VC_ADMIN_ROLE , [vpuser]
go

```

```
use master
go
grant VIEW SERVER STATE to [vpuser]
go
GRANT VIEW ANY DEFINITION TO [vpuser]
go
```

vCenter Server 6.0 にアップグレードする前の PostgreSQL データベースの準備

vCenter Server をアップグレードする前に、PostgreSQL データベースが要件を満たしていること、必要な認証情報があること、必要なクリーンアップまたは他の準備が完了していることを確認します。

vCenter Server データベースのバックアップ方法の詳細については、PostgreSQL のドキュメントを参照してください。

前提条件

vCenter Server のアップグレード用に PostgreSQL データベースを準備する前に、基本的なアップグレードの相互運用性を確認します。

手順

- 1 パスワードが最新であり、十分な有効期限が設定されていることを確認します。
- 2 ISO イメージ内で `cleanup_orphaned_data_PostgreSQL.sql` スクリプトを探し、それを PostgreSQL サーバにコピーします。
- 3 root ユーザーとして vCenter Server Appliance にログインします。
- 4 クリーンアップ スクリプトを実行します。

```
/opt/vmware/PostgreSQL/1.0/bin/psql -U postgres -d VCDB -f
pathcleanup_orphaned_data_Postgres.sql
```

クリーンアップ スクリプトは、vCenter Server コンポーネントによって使用されていない vCenter Server データベース内の不要なまたは実体のないデータをクリーンアップして消去します。

- 5 vCenter Server データベースと vCenter Inventory Service データベースのフル バックアップを作成してください。

結果

vCenter Server アップグレードのためのデータベースの準備が整いました。

vCenter Server のデータベース権限の要件

vCenter Server にはデータベースが必要です。外部の Oracle または Microsoft SQL Server データベースを使用する場合は、データベースの作成時に、一定の権限をデータベース ユーザーに付与する必要があります。

Microsoft SQL データベースをアップグレードする時は、権限が正しく設定される必要があります。

表 3-1. vCenter Server での Microsoft SQL データベースの権限

権限	説明
GRANT ALTER ON SCHEMA :: [VMW] TO VC_ADMIN_ROLE	SQL Server のカスタム スキーマを使用する場合に必須です。
GRANT REFERENCES ON SCHEMA :: [VMW] TO VC_ADMIN_ROLE	SQL Server のカスタム スキーマを使用する場合に必須です。
GRANT INSERT ON SCHEMA :: [VMW] TO VC_ADMIN_ROLE	SQL Server のカスタム スキーマを使用する場合に必須です。
GRANT CREATE TABLE TO VC_ADMIN_ROLE	テーブルを作成する場合に必要です。
GRANT CREATE VIEW TO VC_ADMIN_ROLE	ビューを作成する場合に必要です。
GRANT CREATE PROCEDURE TO VC_ADMIN_ROLE	ストアド プロシージャを作成する場合に必要です。
GRANT SELECT ON SCHEMA :: [VMW] TO VC_USER_ROLE	VMW スキーマの一部であるテーブルで、SELECT、INSERT、DELETE、UPDATE 操作を実行できるようにする権限です。
GRANT INSERT ON SCHEMA :: [VMW] TO VC_USER_ROLE	
GRANT DELETE ON SCHEMA :: [VMW] TO VC_USER_ROLE	
GRANT UPDATE ON SCHEMA :: [VMW] TO VC_USER_ROLE	
GRANT EXECUTE ON SCHEMA :: [VMW] TO VC_USER_ROLE	db スキーマでストアド プロシージャを実行する場合に必要です。
GRANT SELECT ON msdb.dbo.syscategories TO VC_ADMIN_ROLE	SQL Server のジョブをデプロイする場合に必要です。 これらの権限は、インストールとアップグレードの場合にのみ必須であり、デプロイ後は不要になります。
GRANT SELECT ON msdb.dbo.sysjobsteps TO VC_ADMIN_ROLE	
GRANT SELECT ON msdb.dbo.sysjobs TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_job TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_delete_job TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_jobstep TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_update_job TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_jobserver TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_jobschedule TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_category TO VC_ADMIN_ROLE	

表 3-1. vCenter Server での Microsoft SQL データベースの権限（続き）

権限	説明
GRANT VIEW SERVER STATE TO [vpxuser]	SQL Server DMV ビューおよび sp_lock 実行へのアクセス権を付与します。
GRANT VIEW ANY DEFINITION TO [vpxuser]	SQL Server オブジェクトのメタデータを表示する権限をユーザーに付与する場合に必要です。

Oracle データベースをアップグレードする時は、権限が正しく設定される必要があります。

表 3-2. vCenter Server での Oracle データベースの権限

権限	説明
GRANT CONNECT TO VPXADMIN	Oracle データベースに接続する場合に必要です。
GRANT RESOURCE TO VPXADMIN	トリガー、シーケンス、タイプ、プロシージャなどを作成する場合に必要です。 RESOURCE ロールには、デフォルトで、CREATE PROCEDURE、CREATE TABLE、および CREATE SEQUENCE 権限が割り当てられています。RESOURCE ロールにこれらの権限がない場合は、vCenter Server データベースのユーザーに付与します。
GRANT CREATE VIEW TO VPXADMIN	ビューを作成する場合に必要です。
GRANT CREATE SEQUENCE TO VPXADMIN	シーケンスを作成する場合に必要です。
GRANT CREATE TABLE TO VPXADMIN	テーブルを作成する場合に必要です。
GRANT CREATE MATERIALIZED VIEW TO VPXADMIN	マテリアライズド ビューを作成する場合に必要です。
GRANT EXECUTE ON dbms_lock TO VPXADMIN	vCenter Server データベースが単一の vCenter Server インスタンスによって使用されるよう保証するために必要です。
GRANT EXECUTE ON dbms_job TO VPXADMIN	インストールまたはアップグレード時に SQL ジョブのスケジュール設定と管理を行う場合に必要です。 この権限は、デプロイ後には不要になります。
GRANT SELECT ON dba_lock TO VPXADMIN	vCenter Server データベース上での既存のロックを判別する場合に必要です。
GRANT SELECT ON dba_tablespaces TO VPXADMIN	アップグレード時に必要なディスク領域を判別する場合に必要です。 この権限は、デプロイ後には不要になります。
GRANT SELECT ON dba_temp_files TO VPXADMIN	アップグレード時に必要なディスク領域を判別する場合に必要です。 この権限は、デプロイ後には不要になります。
GRANT SELECT ON dba_data_files TO VPXADMIN	vCenter Server の動作中に空き領域を監視する場合に必要です。
GRANT SELECT ON v_\$session TO VPXADMIN	vCenter Server データベース上での既存のロックを判別するために使用されるビューです。
GRANT UNLIMITED TABLESPACE TO VPXADMIN	vCenter Server データベース ユーザーに無制限のテーブルスペース権限を付与する場合に必要です。
GRANT SELECT ON v_\$system_event TO VPXADMIN	ログ ファイルの切り替えを確認する場合に必要です。
GRANT SELECT ON v_\$sysmetric_history TO VPXADMIN	CPU 使用量を確認する場合に必要です。

表 3-2. vCenter Server での Oracle データベースの権限（続き）

権限	説明
GRANT SELECT ON v_\$sysstat TO VPXADMIN	バッファ キャッシュ ヒット率を判定する場合に必要です。
GRANT SELECT ON dba_data_files TO VPXADMIN	テーブルスペースの使用状況を判別する場合に必要です。
GRANT SELECT ON v_\$loghist TO VPXADMIN	チェックポイントの頻度を確認する場合に必要です。

マスター データベースでの権限は、vCenter Server データベースの監視に使用されます。たとえば、特定のしきい値に到達すると、アラートが表示されます。

vCenter Server がローカル データベースと通信できることの確認

vCenter Server のインストール先と同じマシン上にデータベースがあり、そのマシン名を変更した場合は、構成を確認します。vCenter Server DSN が、新しい名前のマシンと通信するように構成されていることを確認します。

vCenter Server のコンピュータ名を変更すると、データベース サーバが vCenter Server と同じコンピュータ上にある場合、データベース接続に影響を与えます。マシン名を変更した場合、通信が維持されていることを確認できます。

データベースがリモートの場合は、この手順を省略できます。名前を変更しても、リモート データベースとの通信には影響を与えません。

サーバの名前を変更したら、データベースのすべてのコンポーネントが動作していることを、データベース管理者またはデータベースのベンダーに確認してください。

前提条件

- データベース サーバが実行中であることを確認します。
- vCenter Server のコンピュータ名が、ドメイン名サービス (DNS) 内でアップデートされていることを確認します。

手順

- 1 必要に応じて、データ ソースの情報をアップデートします。
- 2 コンピュータ名を指定して ping コマンドを実行し、この接続を確認します。

たとえば、コンピュータ名が `host-1.company.com` の場合、Windows コマンド プロンプトで次のコマンドを実行します。

```
ping host-1.company.com
```

コンピュータ名を ping 送信すると、その名前が DNS でアップデートされます。

結果

vCenter Server の通信が確認されます。使用環境の他のコンポーネントの準備に進むことができます。

アップグレード前のネットワークの前提条件の確認

ネットワークが正しく設定され、vCenter Server をアップグレードするための接続の前提条件を満たしていることを確認します。

PTR レコードの作成の詳細については、vCenter Server ホストのオペレーティング システムのドキュメントを参照してください。

Active Directory の構成の詳細については、Microsoft 社の Web サイトを参照してください。

アップグレード中、vCenter Server の管理者権限が設定された Windows 管理者グループに含まれるドメイン ユーザーを使用して vCenter Server を認証することはできません。また、アップグレード後、これらのユーザーに vCenter Server の権限はありません。

手順

- 1 vCenter Server をアップグレードするシステムの完全修飾ドメイン名 (FQDN) が解決可能かどうか検証します。FQDN が解決可能であることを確認するには、コマンドラインのプロンプトで **[nslookup -nosearch -nodefname your_vCenter_Server_fqdn]** と入力します。

FQDN が解決可能な場合は、**nslookup** コマンドによって、ドメイン コントローラーのマシンの IP と名前が返されます。

- 2 vCenter Server の IP アドレスで照会されたときに、DNS の逆引き参照で完全修飾ドメイン名が返されることを確認します。

vCenter Server をアップグレードすると、インストーラが vCenter Server の完全修飾ドメイン名を IP アドレスから検索できなかった場合、vSphere Web Client をサポートしている Web サーバ コンポーネントのインストールが失敗します。

リバース ルックアップは PTR レコードを使用して実装されます。

- 3 vCenter Server に、手動設定した (固定) IP アドレスではなく DHCP を使用する場合は、vCenter Server のコンピュータ名がドメイン名システム (DNS) 内で更新されていることを確認します。更新をテストするため、コンピュータ名に対して ping を送信します。

たとえば、コンピュータ名が `host-1.company.com` の場合、Windows コマンド プロンプトで次のコマンドを実行します。

```
ping host-1.company.com
```

コンピュータ名を ping 送信すると、その名前が DNS でアップデートされます。

- 4 ESXi ホスト管理インターフェイスに、vCenter Server とすべての vSphere Web Client インスタンスからの有効な DNS 解決があることを確認します。vCenter Server に、すべての ESXi ホストとすべての vSphere Web Client インスタンスからの有効な DNS 解決があることを確認します。

- Active Directory をアイデンティティ ソースとして使用する場合は、正しくセットアップされていることを確認します。vCenter Single Sign-On サーバ ホスト マシンの DNS には、Active Directory のドメイン コントローラのルックアップ エントリとリバース ルックアップ エントリの両方が含まれている必要があります。

たとえば、*mycompany.com* に対する ping 送信では、*mycompany* のドメイン コントローラの IP アドレスが返されます。同様に、その IP アドレスに対する `ping -a` コマンドは、ドメイン コントローラのホスト名を返します。

名前解決の問題をホスト ファイルを編集することによって訂正しようとししないでください。代わりに、DNS サーバが正しくセットアップされていることを確認してください。

- アップグレードの前に、vCenter Server のアップグレードに使用するドメイン ユーザーを選択します。ドメイン ユーザーに、Windows 管理者グループのメンバーとしての管理者権限ではなく、vCenter Server のための専用の管理者権限を付与します。

結果

ネットワークで vCenter Server アップグレードのための準備が整いました。

次のステップ

環境のその他のコンポーネントを準備します。

vCenter Server をアップグレードする前のロード バランサの確認

vCenter Single Sign-On の高可用性にロード バランサを使用する場合、vCenter Server 6.0 にアップグレードする前に、そのロード バランサがサポートされており正常に構成されていることを確認する必要があります。

vCenter Server システムが 4 つ未満の環境では、VMware は通常 1 つの Platform Services Controller インスタンスおよび関連する vCenter Single Sign-On サービスを推奨しています。より大規模な環境では、ネットワーク ロード バランサにより保護された、複数の Platform Services Controller インスタンスの使用を検討してください。この設定については、VMware Web サイトのホワイト ペーパー『vCenter Server 6.0 のデプロイ ガイド』で説明されています。上限の最新情報については、『構成の上限』を参照してください。

vCenter Single Sign-On および Platform Services Controller の高可用性互換性マトリックスについては、VMware ナレッジベースの記事 <http://kb.vmware.com/kb/2112736> を参照してください。

前提条件

手順

- ロード バランシングの詳細は、『vCenter Server 6.0 のデプロイ ガイド』ドキュメントを参照してください。
- ご使用のロード バランサがサポートされていない場合、サポートされているロード バランサと置き換えます。
- ロード バランサが『vCenter Server 6.0 のデプロイ ガイド』の推奨事項に基づいて正しく構成されていることを確認します。

vCenter Server のアップグレードのための ESXi ホストの準備

vCenter Server 6.0 にアップグレードする前に、ESXi ホストを準備する必要があります。

前提条件

- vCenter Server をアップグレードするには、ESXi ホストのバージョンが 5.x である必要があります。ESXi ホストが 5.0 より前のバージョンの場合は、5.x にアップグレードします。ホストを ESXi 5.x にアップグレードする際のベスト プラクティスを確認してそれに従います。
- vCenter Server Appliance をバージョン 6.0 へアップグレードする場合、ターゲットのホストで ESXi 5.1 以降が実行されている必要があります。
- vCenter Server Appliance をバージョン 6.0 へアップグレードする場合、ソースおよびターゲットの ESXi ホストがロックダウン モードまたはメンテナンス モードであってはなりません。

手順

- 1 既存の SSL 証明書を維持するには、vCenter Server 6.0 にアップグレードする前に vCenter Server システムにある SSL 証明書をバックアップします。

SSL 証明書のデフォルトの場所は %allusersprofile%\Application Data\VMware\VMware VirtualCenter です。

- 2 カスタムまたはサムプリントの証明書が存在する場合、[ホストのアップグレードと証明書](#)を参照して、準備手順を決定します。

- 3 vSphere HA クラスタが存在する場合、SSL 証明書の確認を有効にする必要があります。

アップグレード時に証明書のチェックが有効になっていないと、vSphere HA はホスト上で構成に失敗します。

- a インベントリ パネルで vCenter Server インスタンスを選択します。
- b [管理] > [全般] タブの順に選択します。
- c [SSL 設定] フィールドが [vCenter Server には検証済みのホスト SSL 証明書が必要です] に設定されていることを確認します。

結果

ESXi ホストで vCenter Server アップグレードの準備が整いました。

ホストのアップグレードと証明書

ESXi ホストを ESXi 6.0 以降にアップグレードすると、アップグレード プロセスで自己署名証明書が VMCA 署名付き証明書に置き換えられます。このプロセスでは、証明書が有効期限切れまたは無効な場合でもカスタム証明書は保持されます。

推奨されるアップグレード ワークフローは、現在の証明書によって異なります。

サムプリント証明書でプロビジョニングされたホスト

現在、ホストでサムプリント証明書が使用されている場合、アップグレード プロセスの一部として VMCA 証明書が自動的に割り当てられます。

注： VMCA 証明書を使用してレガシー ホストをプロビジョニングすることはできません。ESXi 6.0 以降にアップグレードする必要があります。

カスタム証明書でプロビジョニングされたホスト

カスタム証明書（通常はサードパーティ CA 署名付き証明書）を使用してホストがプロビジョニングされている場合、これらの証明書は有効なままです。証明書モードをカスタムに変更すると、証明書が誤って置き換えられることを回避できます。

注： VMCA モードの環境の場合、vSphere Web Client から証明書を更新すると、既存の証明書が VMCA で署名された証明書に置き換えられます。

その後、vCenter Server によって証明書が監視され、証明書の有効期限などの情報が vSphere Web Client に表示されます。

ホストを vSphere 6.0 以降にアップグレードしない場合、VMCA 証明書を使用する vCenter Server システムによってホストが管理されていても、現在使用している証明書がホストで保持されます。

Auto Deploy でプロビジョニングされるホストには、ESXi 6.0 ソフトウェアを使用して最初に起動したときに常に新しい証明書が割り当てられます。Auto Deploy でプロビジョニングされたホストをアップグレードする場合、Auto Deploy サーバによってホストの証明書署名要求 (CSR) が生成され、VMCA に送信されます。VMCA には、ホストの署名証明書が保存されています。Auto Deploy サーバがホストをプロビジョニングすると、VMCA から証明書を取得し、プロビジョニング プロセスの一部としてその証明書を含めます。

Auto Deploy は、カスタム証明書とともに使用できます。

証明書モードの変更

ほとんどの場合、VMCA を使用して ESXi ホストを使用環境にプロビジョニングすることが最適な解決方法になります。企業のポリシーで、異なるルート CA のカスタム証明書を使用することが求められている場合は、証明書の更新時に VMCA 証明書を使用してホストが自動的にプロビジョニングされないように vCenter Server 詳細オプションを編集できます。その後、ユーザーが使用環境で証明書を管理します。

vCenter Server 詳細設定を使用して、サムプリント モードまたはカスタム CA モードに変更できます。サムプリント モードは、フォールバック オプションとしてのみ使用します。

手順

- 1 ホストを管理する vCenter Server を選択し、[設定] をクリックします。
- 2 [詳細設定] をクリックし、[編集] をクリックします。
- 3 [フィルタ] ボックスに、「certmgmt」と入力し、証明書管理キーのみを表示します。
- 4 独自の証明書を管理する場合は vpxd.certmgmt.mode の値を [custom] に変更し、一時的にサムプリント モードを使用する場合は [thumbprint] に変更して、[OK] をクリックします。
- 5 vCenter Server サービスを再起動します。

vCenter Server のアップグレード準備が完了したことの確認

使用中の環境のすべてのコンポーネントで、vCenter Server をアップグレードする準備が整っていることを確認します。

アップグレード前の vCenter Server サービスの構成は、アップグレード後の vCenter Server サービスのデプロイに影響します。

- vCenter Server 5.0 の場合、アップグレード中に組み込みまたは外部の Platform Services Controller インスタンスのいずれかを構成することを選択できます。 [vCenter Server 5.0 のアップグレード](#) を参照してください。
- vCenter Server 5.1 または 5.5 を使用している場合は、アップグレード中に選択するデプロイ オプションはありません。 [Windows 版 vCenter Server 5.1 のアップグレード](#) または [Windows 版 vCenter Server 5.5 のアップグレード](#) を参照してください。
- vCenter Server 5.1 または 5.5 サービスが同じ仮想マシンまたは物理サーバにデプロイされている場合、インストーラはそれらを組み込みの Platform Services Controller インスタンスを使用する vCenter Server 6.0 にアップグレードします。
- vCenter Single Sign-On 5.1 または 5.5 サービスが vCenter Server とは異なる仮想マシンまたは物理サーバにデプロイされている場合、インストーラはデプロイを外部の Platform Services Controller インスタンスを使用する vCenter Server 6.0 にアップグレードします。アップグレード中の分散サービスの連携については、 [vCenter Server 6.0 へのアップグレード中の Windows サービス用の分散 vCenter Server の移行](#) および [vCenter Server のアップグレード パスの例](#) を参照してください。

注： アップグレード後、vCenter Server サービスのデプロイを変更することはできません。

サービスのアップグレードの詳細については、 [Windows 版 vCenter Server 6.0 のアップグレード プロセスについて](#) を参照してください。外部でデプロイされた vCenter Single Sign-On サーバのアップグレードの詳細については、 [外部デプロイの vCenter Single Sign-On 5.5 のアップグレード](#) を参照してください。

時刻の同期の詳細については、 [vSphere ネットワーク上の時計の同期](#) を参照してください。

インストーラをダウンロードする方法については、 [Windows 版 vCenter Server のインストーラのダウンロード](#) を参照してください。

前提条件

データベース、ネットワーク、ローカル データベース通信、および ESXi ホストの基本的な互換性とアップグレード準備を確認したら、ご使用の環境のアップグレード準備を完了するための最終タスクを実行します。

手順

- 1 ASCII 以外の文字を含んでいないユーザー名を使用して、ホスト マシンに管理者グループのメンバーとしてログインします。
- 2 アップグレード前の構成が、実現したいアップグレード後のデプロイに適していることを確認します。
 - vCenter Server 5.1 または 5.5 で、組み込みの Platform Services Controller デプロイにアップグレードするときは、vCenter Server および vCenter Single Sign-On のインスタンスが単一の仮想マシンまたは物理ホストにデプロイされていることを確認します。

- vCenter Server 5.1 または 5.5 で、外部の Platform Services Controller デプロイにアップグレードするときは、vCenter Single Sign-On が関連する vCenter Server とは別の仮想マシンまたは物理ホストにデプロイされていることを確認します。
 - vCenter Server 5.0 で、組み込みの Platform Services Controller デプロイにアップグレードするときは、アップグレード前の手順を実行する必要はありません。
 - vCenter Server 5.0 で、外部の Platform Services Controller デプロイにアップグレードするときは、vCenter Server をアップグレードする前に、外部の Platform Services Controller インスタンスを構成する必要があります。Platform Services Controller 情報は、外部の Platform Services Controller を vCenter Server に登録するために、アップグレード時に使用されます。
- 3 必要なサービスが開始されていることを確認します。
- vCenter Server を登録する vCenter Single Sign-On インスタンス
 - VMware Certificate Authority
 - VMware Directory Service
 - VMware Identity Manager Service
 - VMware KDC サービス
 - tcruntime-C-ProgramData-VMware-cis-runtime-VMwareSTSService
- 4 vSphere 製品をインストールまたはアップグレードする前に、vSphere ネットワークのすべてのマシンの時刻を同期します。
- 5 vCenter Server 6.0 を評価モードで使わない場合は、購入したすべての機能に有効なライセンス キーがあることを確認します。前のバージョンの vSphere からのライセンス キーでは前のバージョンが引き続きサポートされますが、vCenter Server 6.0 はサポートされません。
- ライセンス キーがない場合は、評価モードでインストールし、vSphere Web Client を使用してあとでライセンス キーを入力できます。
- 6 vSphere Web Client のすべてのインスタンスを閉じます。
- 7 プロセスが競合していないことを確認します。
- 8 インストーラをダウンロードします。

結果

ご使用の環境で vCenter Server をアップグレードするための準備が整いました。

vSphere ネットワーク上の時計の同期

vSphere ネットワーク上のすべてのコンポーネントの時計が同期されていることを確認します。vSphere ネットワーク内のマシンの時計が同期されていないと、ネットワーク マシン間の通信において、時間的な制約を受ける SSL 証明書が有効ではないと認識される場合があります。

時計が同期されていないと認証に問題が発生し、インストールが失敗したり、vCenter Server Appliance の vpxd サービスが起動しないことがあります。

vCenter コンポーネントが実行される Windows ホスト マシンが NTP サーバと同期していることを確認します。詳細は、ナレッジ ベースの記事 <http://kb.vmware.com/kb/1318> を参照してください。

ネットワーク タイム サーバによる ESXi の時計の同期

vCenter Server のインストールまたは vCenter Server Appliance のデプロイの前に、vSphere ネットワーク上のすべてのマシンの時計を確実に同期させてください。

このタスクでは、vSphere Client から NTP をセットアップする方法を説明します。代わりに `vicfg-ntp` vCLI コマンドを使用できます。『vSphere Command-Line Interface Reference』を参照してください。

手順

- 1 vSphere Client を起動し、ESXi ホストに接続します。
- 2 [構成] タブで [時間の構成] をクリックします。
- 3 [プロパティ] をクリックし、[オプション] をクリックします。
- 4 [NTP 設定] を選択します。
- 5 [追加] をクリックします。
- 6 [NTP サーバの追加] ダイアログ ボックスで、同期する NTP サーバの IP アドレスまたは完全修飾ドメイン名を入力します。
- 7 [OK] をクリックします。

ホスト時刻が NTP サーバと同期します。

vCenter Server のアップグレード中のダウンタイム

vCenter Server のアップグレードの際には、vCenter Server のダウンタイムが必要です。

vCenter Server で予期されるダウンタイムは次のとおりです。

- アップグレードの際には、vCenter Server の稼働を最低 40 ～ 50 分停止する必要があります。データベースのサイズに応じて、これ以上停止しなければならないこともあります。データベース スキーマのアップグレードでは、約 10 ～ 15 分停止する必要があります。この時間にはアップグレード後のホスト再接続にかかる時間は含まれません。
- 組み込みデータベースを含む vCenter Server のデプロイの場合は、アップグレードの際に、レガシー vCenter Server データベースから新しいデータベース インスタンスにデータを移行するための余分な時間が必要になる場合があります。
- マシンに Microsoft .NET Framework がインストールされていない場合は、vCenter Server のインストールを開始する前に再起動する必要があります。
- アップグレードの実行中は、vSphere Distributed Resource Scheduler (DRS) を使用できません。vSphere HA は、アップグレード中も使用できます。

vCenter Server が管理している ESXi ホスト、またはそれらのホスト上で実行されている仮想マシンについては、ダウンタイムは不要です。

vCenter Server を実行するための、ユーザー アカウントの使用

vCenter Server の実行には、Microsoft Windows に組み込まれているシステム アカウントか、ユーザー アカウントを使用できます。ユーザー アカウントを使用する場合、SQL Server に Windows 認証を使用でき、セキュリティを高くすることができます。

ユーザー アカウントは、ローカル マシンのシステム管理者である必要があります。インストールのウィザードで、アカウント名を *DomainName\Username* の形式で指定します。ドメイン アカウントに SQL Server へのアクセスを許可するように SQL Server のデータベースを構成する必要があります。

Microsoft Windows に組み込まれているシステム アカウントは、vCenter Server システムが必要とする以上のサーバに対する権限とアクセス権を持つため、セキュリティの問題が発生する可能性があります。

重要： vCenter Server サービスが Microsoft Windows 組み込みシステム アカウントで実行されている場合、Microsoft SQL Server を使用すると、vCenter Server 6.0 は SQL Server 認証によって DSN のみをサポートします。

Windows 認証が付属した SQL Server の DSN の場合、VMware VirtualCenter Management Webservices サービスと DSN ユーザーに同じユーザー アカウントを使用します。

SQL Server に Microsoft Windows 認証を使用しない場合や、Oracle データベースを使用する場合でも、vCenter Server システム用にローカルのユーザー アカウントを設定したほうがよい場合があります。唯一の要件は、ユーザー アカウントはローカル マシンの管理者として、アカウントに サービスとしてログオン 権限を付与する必要があります。

Windows 版 vCenter Server のアップグレードに必要な情報

vCenter Server アップグレード ウィザードには、アップグレード情報の入力を求めるメッセージが表示されます。製品の再インストールが必要になる場合に備えて、ここで入力した値を記録しておくことをお勧めします。

このワークシートを使用して、将来 Windows 版 vCenter Server のアップグレード時に必要となる情報を記録できます。

以下のテーブルにデフォルト値が表示されるのは、ソース vCenter Server インスタンスのインストール時にデフォルト値を残した場合のみです。

表 3-3. Windows 版 vCenter Server のアップグレードに必要な情報。

必要な情報	デフォルト値	入力内容
vCenter Single Sign-On 管理者ユーザー名	administrator@vsphere.local	インストール時にデフォルトのユーザー名を変更することはできません。
vCenter Single Sign-On 管理者パスワード		
vCenter Server の認証情報と同じ認証情報を使用する 設定を有効または無効	デフォルトで有効	
vCenter Server のユーザー名	administrator@vsphere.local	
vCenter Server のパスワード		

表 3-3. Windows 版 vCenter Server のアップグレードに必要な情報。 (続き)

必要な情報	デフォルト値	入力内容
Syslog サービス ポート	514	
Syslog サービス TLS ポート	1514	
Auto Deploy 管理ポート	6502	
Auto Deploy サービス ポート	6501	
ESXi Dump Collector ポート	6500	
ターゲット ディレクトリ フォルダパスには、非 ASCII 文字 (コンマ (,), ピリオド (.), 感嘆符 (!), ナンバー記号 (#), アット記号 (@), パーセ ント記号 (%)) のいずれも含 めることはできません。	vCenter Server のインストール デ ィレクトリ vCenter Server のデータの保存先 ディレクトリ 5.x のデータのエクスポート先ディレ クトリ	C:\Program Files\VMware C:\ProgramData\VM ware C:\ProgramData\VM ware\VMware\vCent erServer\export
VMware カスタマ エクスペリエンス改善プログラム (CEIP) に参加 する、または参加しない CEIP の詳細については、『vCenter Server およびホスト管理』の「カ スタマ エクスペリエンス改善プログラムの構成」セクションを参照して ください。	CEIP に参加する	

vCenter Server Appliance のアップグレードに必要な情報

vCenter Server Appliance のアップグレード ウィザードに、デプロイ情報の入力を求めるメッセージが表示されます。製品の再インストールが必要になる場合に備えて、ここで入力した値を記録しておくことをお勧めします。

重要： vCenter Server Appliance 5.1 Update 3 以降から vCenter Server Appliance 6.0 へのアップグレードがサポートされています。vCenter Server Appliance 5.0 をアップグレードするには、まず vCenter Server Appliance をバージョン 5.1 Update 3 または 5.5 Update 2 にアップグレードしてから、vCenter Server Appliance 6.0 にアップグレードします。vCenter Server Appliance 5.0 からバージョン 5.1 Update 3 へのアップグレードの詳細については、VMware vSphere 5.1 のドキュメントを参照してください。vCenter Server Appliance 5.0 からバージョン 5.5 Update 2 へのアップグレードの詳細については、VMware vSphere 5.5 のドキュメントを参照してください。

このワークシートを使用して、vCenter Server Appliance バージョン 5.1 Update 3 または 5.5.x をアップグレードする場合に必要な情報を記録することができます。

表 3-4. vCenter Server Appliance 5.1.x または 5.5.x のアップグレードに必要な情報

必要な情報	デフォルト値	入力内容
vCenter Server Appliance をアップグレードするターゲット ESXi ホストの IP アドレスまたは FQDN		
ターゲット ESXi ホストで管理権限を持つユーザーの認証情報	ターゲット ESXi ホストのユーザー名 ターゲット ESXi ホストのパスワード	
vCenter Server Appliance 6.0 名		
vCenter Server Appliance 6.0 にアップグレードする vCenter Server Appliance のバージョン		
アップグレードする vCenter Server Appliance のデータ	vCenter Server Appliance の IP アドレスまたは FQDN	
	vCenter Single Sign-On 管理者ユーザー名	vCenter Server Appliance 5.5.x からアップグレードする場合は administrator@vsphere.local
	vCenter Single Sign-On 管理者のパスワード	
	vCenter Server の HTTPS ポート番号	
	root ユーザーのパスワード	
	一時的なアップグレード ファイル パス	/tmp/vmware/cis-export-folder
	パフォーマンスなどの履歴データの移行	デフォルトでは無効
アップグレードする vCenter Server Appliance が存在するソース ESXi ホストの IP アドレスまたは FQDN		
ソース ESXi ホストで管理権限を持つユーザーの認証情報	ソース ESXi ホストのユーザー名	
	ソース ESXi ホストのパスワード	
vCenter Single Sign-On の設定	vCenter Single Sign-On パスワード	
vCenter Server Appliance バージョン 5.1.x をアップグレードしている場合にのみ必要	vCenter Single Sign-On ドメイン名	
	vCenter Single Sign-On サイト名	
vCenter Server Appliance のサイズ。 vSphere 環境のサイズに応じて、次の各オプションがあります。		極小（最大でホスト 20 台、仮想マシン 400 台）
■ 極小（最大でホスト 20 台、仮想マシン 400 台）		
■ 小（最大でホスト 150 台、仮想マシン 3,000 台）		
■ 中（最大でホスト 300 台、仮想マシン 6,000 台）		
■ 大（最大でホスト 1,000 台、仮想マシン 10,000 台）		

表 3-4. vCenter Server Appliance 5.1.x または 5.5.x のアップグレードに必要な情報（続き）

必要な情報	デフォルト値	入力内容
vCenter Server Appliance の新バージョンがデプロイされるデータストアの名前		
シン ディスク モードの有効化または無効化	デフォルトでは無効	
アップグレードする vCenter Server Appliance と新しい vCenter Server Appliance 間の通信に使用する一時的なネットワーク		
IP アドレス バージョン	IPv4	
IP アドレスの割り当て方法	DHCP	
静的割り当ての設定	ネットワーク アドレス	
	サブネット マスク	
	ネットワーク ゲートウェイ	
	ネットワーク DNS サーバ（コンマで区切り）	
SSH の有効化または無効化	デフォルトでは無効	
VMware カスタマ エクスペリエンス改善プログラム (CEIP) に参加する、または参加しない。		
CEIP の詳細については、『vCenter Server およびホスト管理』の「カスタマ エクスペリエンス改善プログラムの構成」セクションを参照してください。		
組み込みの vCenter Single Sign-On を使用する vCenter Server Appliance をアップグレードしている場合にのみ必要		

Windows 版 vCenter Server のアップグレードおよび更新

4

vCenter Server のアップグレードには、データベーススキーマのアップグレード、vCenter Single Sign-On から Platform Services Controller への移行、および vCenter Server ソフトウェアのアップグレードが含まれます。

この章には、次のトピックが含まれています。

- Windows 版 vCenter Server 6.0 のアップグレード プロセスについて
- vCenter Server 6.0 へのアップグレード中の Windows サービス用の分散 vCenter Server の移行
- Windows 版 vCenter Server のインストーラのダウンロード
- 外部デプロイの vCenter Single Sign-On 5.1 のアップグレード
- 外部デプロイの vCenter Single Sign-On 5.5 のアップグレード
- vCenter Server 5.0 のアップグレード
- Windows 版 vCenter Server 5.1 のアップグレード
- Windows 版 vCenter Server 5.5 のアップグレード
- VIMPatch での Java コンポーネントと vCenter Server tc Server の更新

Windows 版 vCenter Server 6.0 のアップグレード プロセスについて

Windows での vCenter Server のアップグレード オプションは、既存の導入環境およびバージョンによって異なります。

Windows 版 vCenter Server のアップグレード プロセスは次のとおりです。

- 1 vCenter Server 5.x 構成のエクスポート
- 2 vCenter Server 5.x 構成のアンインストール
- 3 vCenter Server 6.0 のインストール
- 4 vCenter Server 5.x サービスおよびデータの vCenter Server 6.0 環境への移行と構成

アップグレード後の環境は現在の導入環境によって異なります。

- vCenter Server 5.0 からのアップグレード中に、組み込みまたは外部の Platform Services Controller インスタンスのいずれかを構成できます。

- 単一の仮想マシンまたは物理サーバにサービスがデプロイされている vCenter Server バージョン 5.1 または 5.5 導入環境は、組み込みの Platform Services Controller を使用する vCenter Server にアップグレードされます。
- vCenter Server とは異なる仮想マシンまたは物理サーバにデプロイされた vCenter Single Sign-On を使用する vCenter Server バージョン 5.1 または 5.5 環境は、外部の Platform Services Controller を使用する vCenter Server にアップグレードされます。
- vCenter Server の複数のインスタンスをアップグレードする場合、アップグレードは適切な順序で行う必要があります。アップグレードの順序は重要です。[vCenter Server のアップグレード時のバージョン混在の移行環境](#)を参照してください。

図 4-1. Windows 版 vCenter Server 5.0 のアップグレード ワークフロー

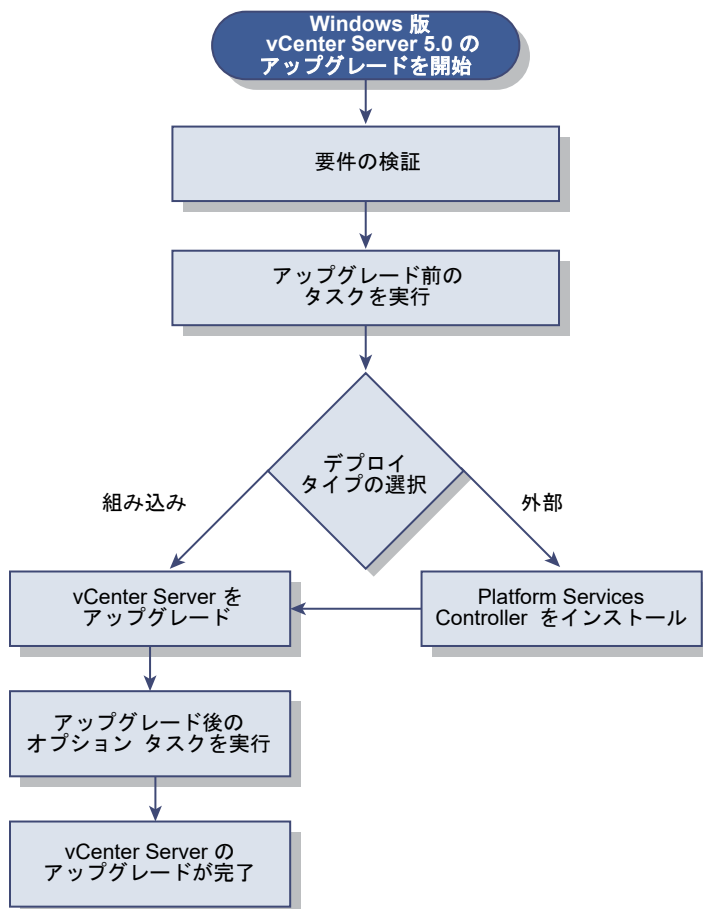
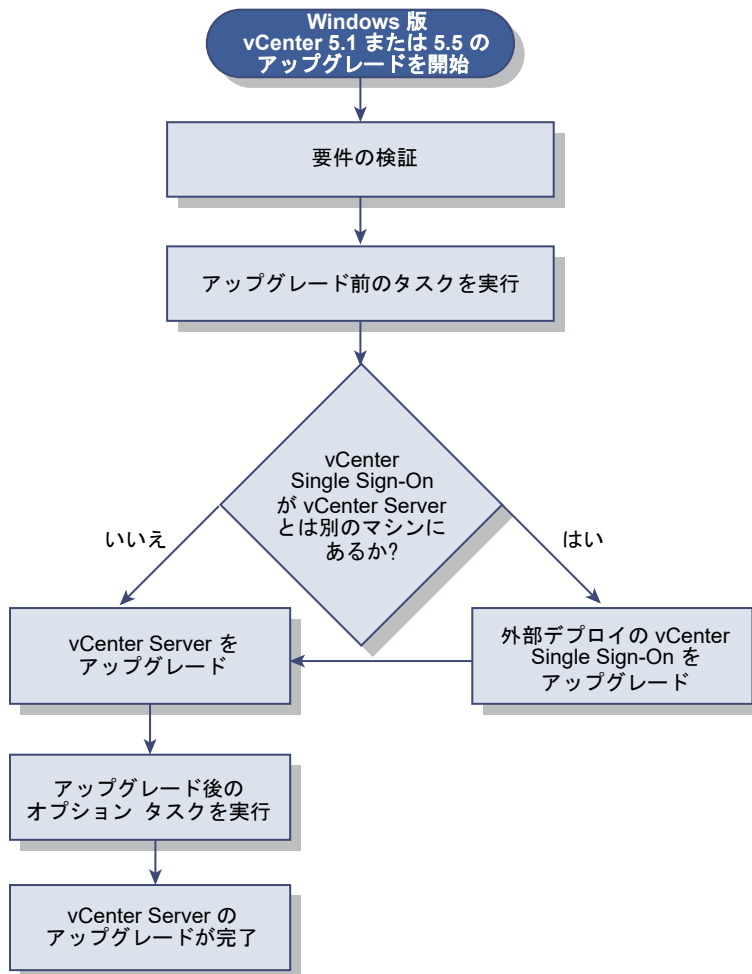


図 4-2. Windows 版 vCenter Server 5.1 または 5.5 のアップグレード ワークフロー



アップグレード プロセスでは、個々のサービスをアンインストールまたは再インストールできません。たとえば、Inventory Service を個別にデプロイすることはできません。これは、vCenter Server 6.0 の vCenter Server のサービス グループの一部となります。

注： アップグレード中は vCenter Server のデプロイ モデルは変更できません。たとえば、組み込みの Platform Services Controller インスタンスを使用する vCenter Server と、外部の Platform Services Controller インスタンスを使用する vCenter Server とを変更することはできません。

vCenter Server 6.0 へのアップグレード中の Windows サービス用の分散 vCenter Server の移行

複数のマシンにサービスが配置される Windows 用の vCenter Server 5.1 または 5.5 のカスタム インストールは、アップグレード プロセス中にアップグレードされ、vCenter Server システムに移行されます（必要な場合）。

すべての vCenter Server 5.x サービスを同じシステムにデプロイする場合、それらのサービスはその場所でアップグレードされ、アップグレード後に構成を行う必要はありません。ただし、1つ以上のサービスをリモートでデプロイする場合は、ソフトウェアにより、アップグレード中に1つ以上のサービスが vCenter Server 仮想マシンまたは物理サーバに移行されます。サービスによっては、アップグレード後に再構成またはその他のアクションを実行する必要があります。アップグレードプロセス中に移行されて vCenter Server サービスグループの一部になる Windows 版 vCenter Server 5.x サービスには次のものがあります。

- インベントリ サービス
- vSphere Web Client
- vSphere Auto Deploy
- vSphere Syslog Collector
- vSphere ESXi Dump Collector

移行されないサービスは vCenter Server と vCenter Single Sign-On だけです。vCenter Single Sign-On インスタンスは、vCenter Server が存在するシステム以外のシステムにデプロイされる場合、その場所でアップグレードされて外部 Platform Services Controller の一部になります。

図 4-3. vCenter Server のサービスグループに移行されるコンポーネント サービス

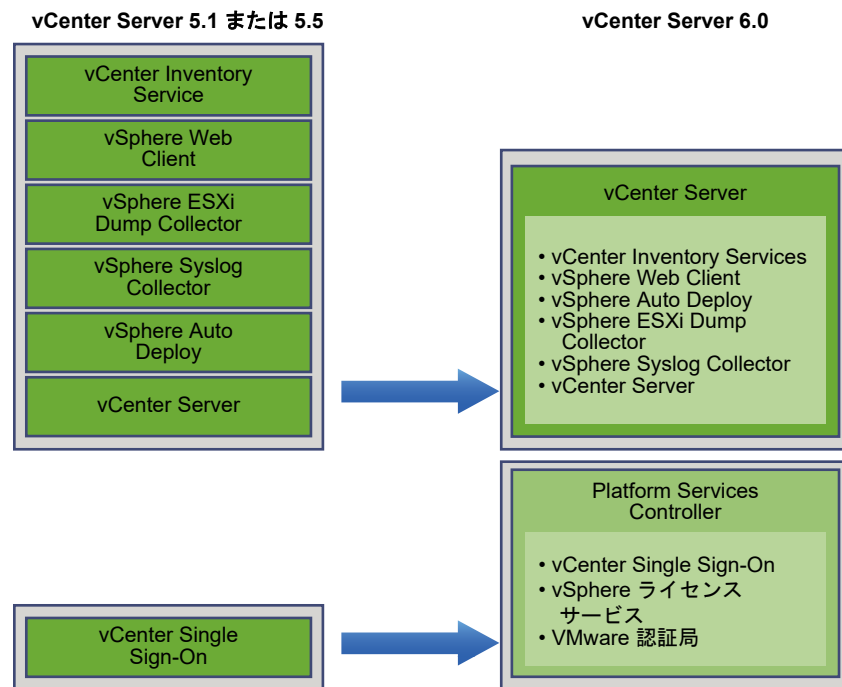


表 4-1. アップグレード中の vCenter Server 5.x 分散サービスの移行

サービス名	アップグレード前のサービスの場所	アップグレード後のサービスの場所	アップグレード後のアクション
vCenter Inventory Service	vCenter Server システムにインストールされない	vCenter Server システムにインストールされる	vCenter Inventory Service 5.x データは、vCenter Server 6.0 と共にインストールされる Inventory Service 6.0 インスタンスにコピーされます。手動でコピーする必要はありません。 vCenter Inventory Service 5.x は実行され続けますが、使用されなくなります。手動で停止して削除する必要があります。
vSphere Web Client	vCenter Server システムにインストールされない	vCenter Server システムにインストールされる	vCenter Server 5.x データは、vCenter Server 6.0 と共にインストールされる vSphere Web Client 6.0 インスタンスにコピーされます。 vSphere Web Client 5.x は実行され続けますが、使用されなくなります。手動で停止して削除する必要があります。
vSphere Auto Deploy	vCenter Server システムにインストールされない	vCenter Server システムに移行される	vSphere Auto Deploy データは、vCenter Server 6.0 と共にインストールされる Auto Deploy 6.0 インスタンスにコピーされます。 vCenter Server DHCP 設定を、移行された vSphere Auto Deploy サービスに再ポイントします。 vCenter Server vSphere Auto Deploy 5.x は実行され続けますが、使用されなくなります。手動で停止して削除する必要があります。
vSphere Syslog Collector	vCenter Server システムにインストールされない	vCenter Server システムにインストールされる データが移行されない。ポート、プロトコル、およびローテーション ログ サイズの構成は維持されます。	<ul style="list-style-type: none"> ■ ESXi システムの情報は、再配置されるまで古いシステム上に残る可能性があります。 ■ ESXi ホストでは、新しい vSphere Syslog Collector サーバを指すように再構成が必要になることがあります。
vSphere ESXi Dump Collector	vCenter Server システムにインストールされない	vCenter Server システムにインストールされる データが移行されない。	<ul style="list-style-type: none"> ■ ESXi コア ダンプ データは、移行されるまで古いシステムに残る可能性があります。 ■ ESXi ホストでは、新しい vSphere ESXi Dump サーバを参照するように再構成が必要になることがあります。

アップグレード シナリオの詳細については、[vCenter Server のアップグレード パスの例](#)を参照してください。アップグレード後に必要なサービス再構成の詳細については、[アップグレード後の移行された vCenter Server サービスの再構成](#)を参照してください。

Windows 版 vCenter Server のインストーラのダウンロード

vCenter Server for Windows、関連付けられた vCenter Server コンポーネント、およびサポート ツールの .iso インストーラをダウンロードします。

前提条件

<https://my.vmware.com/web/vmware/> で Customer Connect アカウントを作成します。

手順

- 1 VMware の Web サイト (<https://my.vmware.com/web/vmware/downloads>) から vCenter Server のインストーラをダウンロードします。

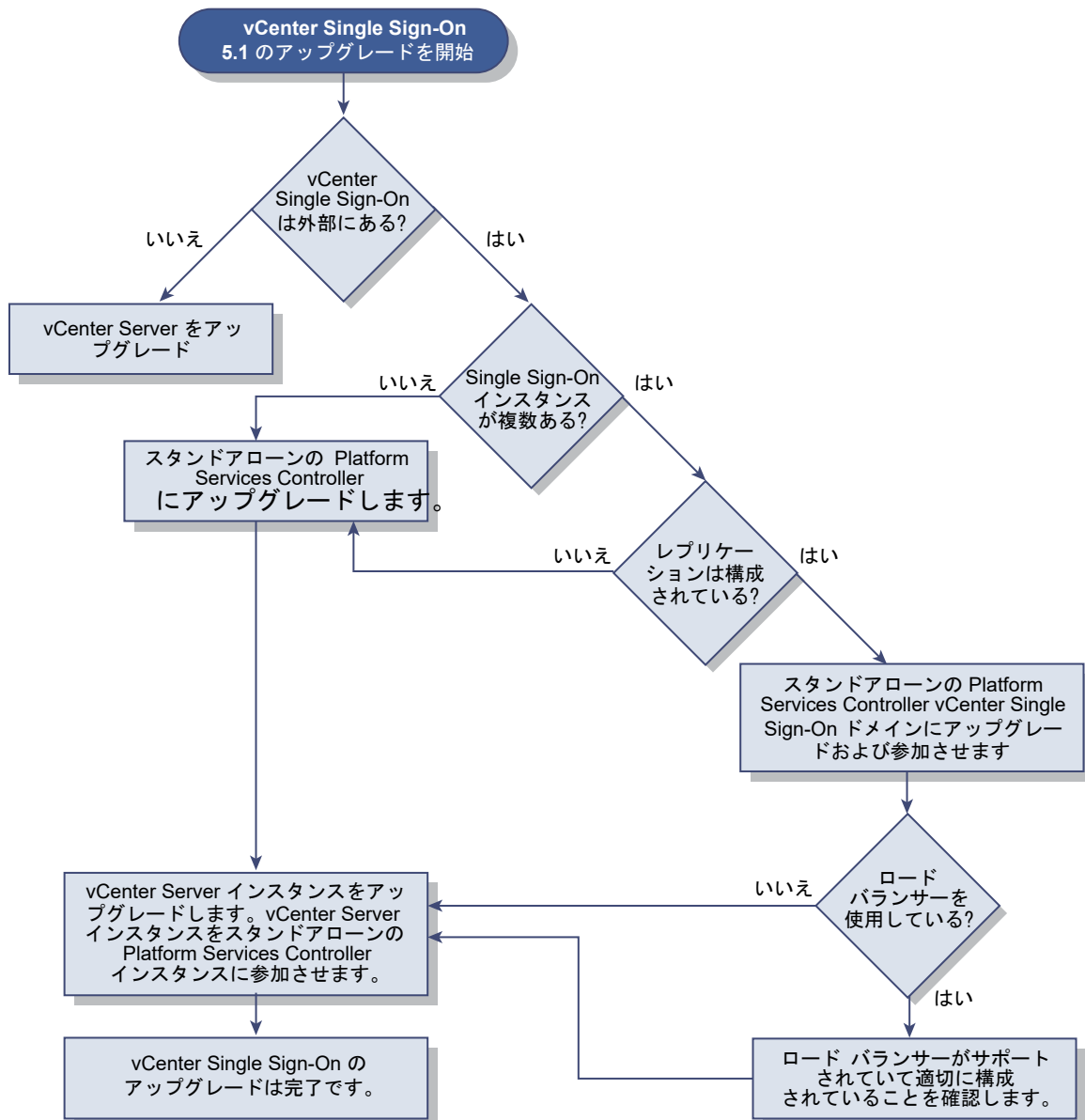
vCenter Server は、VMware vCloud Suite および VMware vSphere の一部であり、データセンターおよびクラウド インフラストラクチャの下に表示されています。
- 2 md5sum が正しいことを確認します。

MD5 チェックサムをの使用については、VMware Web サイトのトピックをご覧ください (<http://www.vmware.com/download/md5.html>)。
- 3 vCenter Server for Windows をインストールする Windows 仮想マシンまたは物理サーバに ISO イメージをマウントします。

外部デプロイの vCenter Single Sign-On 5.1 のアップグレード

Windows 版 vCenter Server のインストーラを使用して、外部でデプロイされている vCenter Single Sign-On 5.1 を外部でデプロイされている Platform Services Controller インスタンスにアップグレードすることができます。

図 4-4. Windows 版の vCenter Single Sign-On 5.1 アップグレード ワークフロー



バージョンが混在した環境で、外部デプロイされている vCenter Single Sign-On 5.1 インスタンスを、外部デプロイされる Platform Services Controller インスタンスにアップグレードする場合、すべての vCenter Server 5.1 インスタンスは、vCenter Single Sign-On と連携していた場合とまったく同じように、アップグレードされた Platform Services Controller と連携し続け、問題が発生したり、アクションが必要になったりすることはありません。

- vCenter Single Sign-On がアップグレードに与える影響の詳細については、[vCenter Single Sign-On がアップグレードに与える影響](#)を参照してください。
- バージョンが混在した環境での vCenter Server の動作の詳細については、[vCenter Server のアップグレード時のバージョン混在の移行環境](#)を参照してください。
- デプロイ オプションについては、[vCenter Server のデプロイ モデル](#)を参照してください。

前提条件

- 既存の vCenter Single Sign-On は、vCenter Server インスタンスとは別の仮想マシンまたは物理サーバにインストールされたものである必要があります。
- 構成がこのアップグレード要件を満たしていることを確認します。 [Windows 版 vCenter Server の要件](#)を参照してください。
- アップグレード タスクの準備を完了します。 [3 章 vCenter Server をアップグレードする前に行う作業](#)を参照してください。
- vCenter Server 構成とデータベースのバックアップが作成済みであることを確認します。
- vCenter Server のインストーラをダウンロードします。 [Windows 版 vCenter Server のインストーラのダウンロード](#)を参照してください。

注: vCenter Server 5.1 と同じ仮想マシンまたは物理サーバにデプロイされた vCenter Single Sign-On 5.1 インスタンスは、vCenter Server 6.0 にアップグレードすると、組み込み Platform Services Controller インスタンスに自動的にアップグレードされます。

手順

- 1 Windows 版 vCenter Server の ISO ファイルをダウンロードします。ISO ファイルをローカルで抽出するか、または ISO ファイルをドライブとしてマウントします。
- 2 ソフトウェア インストーラで、**autorun.exe** ファイルをダブルクリックし、インストーラを起動します。
- 3 Windows 版 vCenter Server を選択し、インストール をクリックします。

インストーラは、バックグラウンドでアップグレード前チェックを実行して既存の vCenter Single Sign-On 設定を検出し、アップグレード プロセスに影響する問題があれば通知します。vCenter Server のインストーラが起動し、画面が開きます。

- 4 検出された情報とアップグレード パスを確認します。

要件が満たされていない場合は、ダイアログ ボックスが表示されます。ダイアログ ボックス内の指示に従ってください。

- 5 画面を確認し、使用許諾契約書に同意します。

インストーラは、バックグラウンドでアップグレード前チェックを行い、アップグレードの失敗の原因となる問題を検出します。古い証明書が現在の VMware のセキュリティ基準を満たさない場合には、警告が表示されます。

- 6 vCenter Single Sign-On インスタンスをアップグレードします。

Platform Services Controller サイトを作成することも、参加することもできます。

- これが最初の、またはプライマリ vCenter Single Sign-On インスタンスである場合は、新しい vCenter Single Sign-On ドメイン名とサイト名を構成することによって、これを新しいスタンドアロン Platform Services Controller インスタンスにアップグレードします。
- 2 つ以上の vCenter Single Sign-On インスタンスが存在し、これが 2 つ目または追加の vCenter Single Sign-On インスタンスである場合は、これをプライマリ Platform Services Controller の vCenter Single Sign-On サイトに参加させて複製できるようにします。

複製情報はアップグレード時に保持されます。

vCenter Single Sign-On 5.1 のドメイン「System-Domain」は、選択する新規ドメインに移行されます。

- 7 ポートを構成し、次へ をクリックします。

インストーラは、選択されたポートの可用性をチェックし、使用できない場合はエラー メッセージを表示します。

- 8 インストール、データ、およびエクスポートの各ディレクトリを構成し、次へ をクリックします。

インストーラは、選択されたディレクトリでディスク容量とアクセス許可のチェックを実行し、選択されたディレクトリが要件を満たさない場合にはエラー メッセージを表示します。

- 9 [VMware カスタマ エクスペリエンス改善プログラム (CEIP)] ページを参照し、プログラムへの参加を希望するかどうかを選択します。

CEIP の詳細については、『vCenter Server およびホスト管理』の「カスタマ エクスペリエンス改善プログラムの構成」セクションを参照してください。

- 10 [サマリ] ページの設定が正しいことを確認します。システムのバックアップを作成したことを確認し、アップグレード をクリックします。

インストーラによってアップグレード プロセスが開始されると、進捗状況インジケータが表示されます。プロセスが完了すると、インストーラがアップグレードの状態を検証します。

- 11 終了 をクリックする前に、アップグレード後の手順を書き留めます。

- 12 終了 をクリックし、アップグレードを完了します。

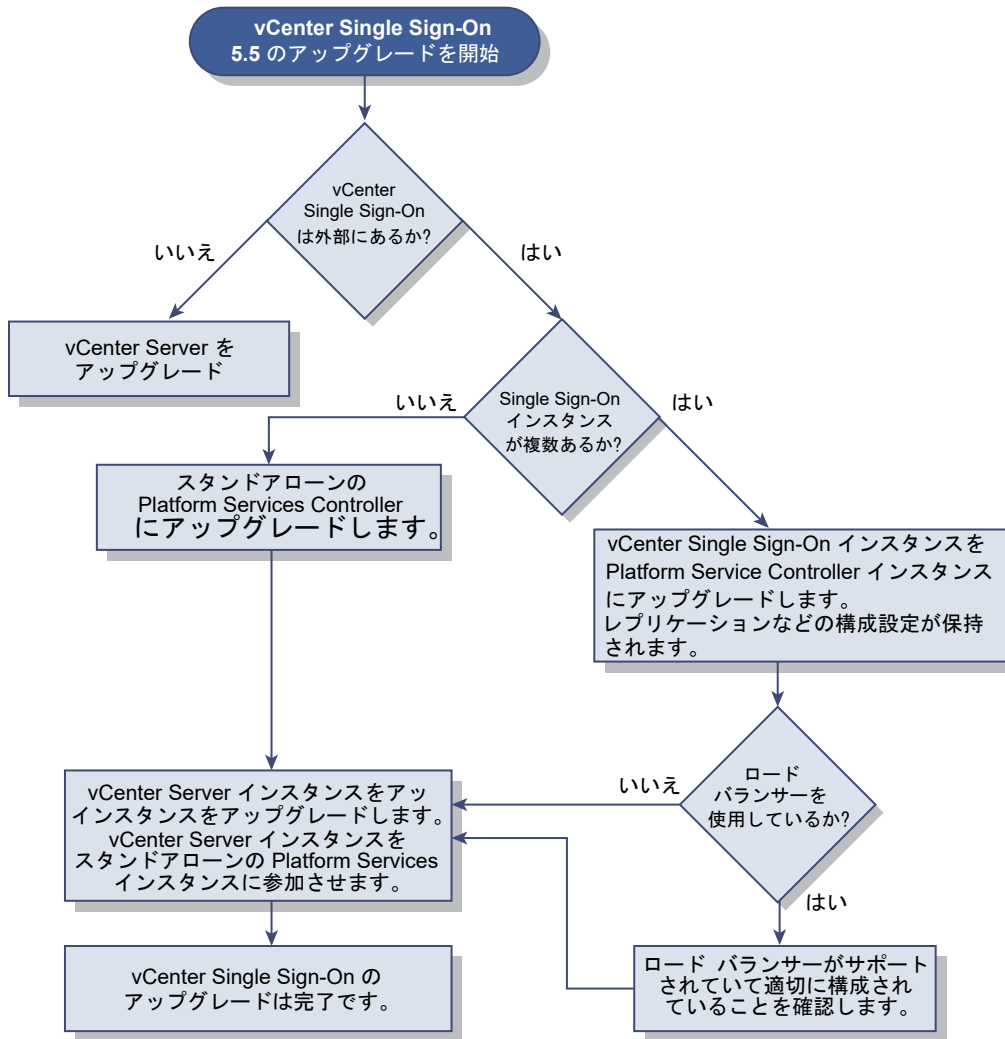
次のステップ

外部の Platform Services Controller インスタンスを構成すれば、vCenter Server を外部デプロイにアップグレードする準備が整います。

外部デプロイの vCenter Single Sign-On 5.5 のアップグレード

Windows 版 vCenter Server のインストーラを使用して、外部でデプロイされている vCenter Single Sign-On 5.5 を外部でデプロイされている Platform Services Controller インスタンスにアップグレードすることができます。

図 4-5. Windows 版の vCenter Single Sign-On 5.5 アップグレード ワークフロー



バージョンが混在した環境で、外部でデプロイされている vCenter Single Sign-On 5.5 を、外部でデプロイされる Platform Services Controller にアップグレードする場合、すべての vCenter Server 5.5 インスタンスは、vCenter Single Sign-On との場合と同様にアップグレードされた Platform Services Controller と問題なく連携し続けます。特定のアクションを取る必要はありません。

注： vCenter Server 5.5 と同じ仮想マシンまたは物理サーバにデプロイされた vCenter Single Sign-On 5.5 を vCenter Server 6.0 にアップグレードすると、組み込みの Platform Services Controller に自動的にアップグレードされます。

- vCenter Single Sign-On がアップグレードに与える影響の詳細については、[vCenter Single Sign-On がアップグレードに与える影響](#)を参照してください。
- バージョンが混在した環境での vCenter Server の動作の詳細については、[vCenter Server のアップグレード時のバージョン混在の移行環境](#)を参照してください。
- デプロイ オプションについては、[vCenter Server のデプロイ モデル](#)を参照してください。

前提条件

- 現在の vCenter Single Sign-On は、vCenter Server インスタンスとは別の仮想マシン (VM) または物理サーバにインストールされたものである必要があります。
- 構成がこのアップグレード要件を満たしていることを確認します。 [Windows 版 vCenter Server の要件](#)を参照してください。
- アップグレード タスクの準備を完了します。 [3 章 vCenter Server をアップグレードする前に行う作業](#)を参照してください。
- vCenter Server 構成とデータベースのバックアップが作成済みであることを確認します。
- VMware ディレクトリ サービスが安定した状態にあり、停止できることを確認するには、このサービスを手動で再起動します。vCenter Server アップグレード ソフトウェアでアップグレード プロセス中に vCenter Single Sign-On をアンインストールするには、VMware ディレクトリ サービスを停止する必要があります。
- vCenter Server のインストーラをダウンロードします。 [Windows 版 vCenter Server のインストーラのダウンロード](#)を参照してください。

手順

- 1 Windows 版 vCenter Server の ISO ファイルをダウンロードします。ISO ファイルをローカルで抽出するか、または ISO ファイルをドライブとしてマウントします。
- 2 ソフトウェア インストーラで、**autorun.exe** ファイルをダブルクリックし、インストーラを起動します。
- 3 Windows 版 vCenter Server を選択し、インストール をクリックします。

インストーラは、バックグラウンドで既存の vCenter Single Sign-On 設定を検索し、アップグレード プロセスに影響する問題があれば通知します。

vCenter Server のインストーラが起動し、画面が開きます。

- 4 検出された情報とアップグレード パスを確認します。
要件が満たされていない場合は、ダイアログ ボックスが表示されます。ダイアログ ボックス内の指示に従ってください。
- 5 画面を確認し、使用許諾契約書に同意します。
- 6 **administrator@vsphere.local** の認証情報を入力します。

インストーラは、バックグラウンドでアップグレード前チェックを行い、アップグレードの失敗の原因となる問題を検出します。古い証明書が現在の VMware のセキュリティ基準を満たさない場合には、警告が表示されます。

- 7 プロンプトに従って、vCenter Single Sign-On インスタンスを Platform Services Controller インスタンスにアップグレードします。

Platform Services Controller インスタンスを作成することも、参加することもできます。

- これが最初の、またはプライマリ vCenter Single Sign-On インスタンスである場合は、新しい vCenter Single Sign-On ドメイン名とサイト名を構成することによって、これを新しいスタンドアロン Platform Services Controller インスタンスにアップグレードします。

- 2 つ以上の vCenter Single Sign-On インスタンスが存在し、これが 2 つ目または追加の vCenter Single Sign-On インスタンスである場合は、これをプライマリ Platform Services Controller の vCenter Single Sign-On サイトに参加させて複製できるようにします。

複製情報はアップグレード時に保持されます。

vCenter Single Sign-On 5.5 のドメイン *System-Domain* は、選択する新規ドメインに移行されます。

- 8 ポートを構成し、次へ をクリックします。

vCenter Single Sign-On がポート 80 と 443 を使用できるようにするため、これらのポートが利用されておらず、占有できることを確認します。そうでない場合、インストール時にはカスタム ポートが使用されます。

インストーラは、選択されたポートの可用性をチェックし、使用できない場合はエラー メッセージを表示します。

- 9 インストール、データ、およびエクスポートの各ディレクトリを構成し、次へ をクリックします。

インストーラは、選択されたディレクトリでディスク容量とアクセス許可のチェックを実行し、選択されたディレクトリが要件を満たさない場合にはエラー メッセージを表示します。

- 10 [VMware カスタマ エクスペリエンス改善プログラム (CEIP)] ページを参照し、プログラムへの参加を希望するかどうかを選択します。

CEIP の詳細については、『vCenter Server およびホスト管理』の「カスタマ エクスペリエンス改善プログラムの構成」セクションを参照してください。

- 11 [サマリ] ページの設定が正しいことを確認します。システムのバックアップを作成したことを確認し、アップグレード をクリックします。

インストーラによってアップグレード プロセスが開始されると、進捗状況インジケータが表示されます。プロセスが完了すると、インストーラがアップグレードの状態を検証します。

- 12 終了 をクリックする前に、アップグレード後の手順を書き留めます。

- 13 終了 をクリックし、アップグレードを完了します。

次のステップ

外部の Platform Services Controller インスタンスを構成すれば、vCenter Server を外部デプロイにアップグレードする準備が整います。

vCenter Server 5.0 のアップグレード

Windows 版 vCenter Server のインストーラを使用して、既存の vCenter Server 5.0 デプロイをアップグレードできます。

vCenter Server 5.0 からアップグレードする際、アップグレード中に組み込みまたは外部の Platform Services Controller のいずれかを構成できます。

- vCenter Server で使用されているポートは保持されます。アップグレード中、ポートを変更することはできません。必要なポートの詳細については、[vCenter Server および Platform Services Controller に必要なポート](#)を参照してください。

- インストーラは、Microsoft SQL Server Express のデータベースを vCenter Server に含まれる PostgreSQL (vPostgres) データベースに自動的に移行します。VC 6.0 へアップグレードする前に Microsoft SQL Server Express から Microsoft SQL Server へ移行する方法については、VMware のナレッジベースの記事 <http://kb.vmware.com/kb/1028601> および Microsoft のドキュメントを参照してください。PostgreSQL データベースへ移行せずにアップグレードする方法については、VMware のナレッジベースのこちらの記事 <http://kb.vmware.com/kb/2109321> を参照してください。
- デプロイ オプションについては、[vCenter Server のデプロイ モデル](#)および [Windows 版 vCenter Server 6.0 のアップグレード プロセス](#)についてを参照してください。
- アップグレード後の手順の詳細については、[6 章 vCenter Server のアップグレード後](#)を参照してください。

前提条件

- 構成がこのアップグレード要件を満たしていることを確認します。[Windows 版 vCenter Server の要件](#)を参照してください。
- アップグレード準備タスクを完了します。[3 章 vCenter Server をアップグレードする前に行う作業](#)を参照してください。
- vCenter Server 構成とデータベースのバックアップが作成済みであることを確認します。
- vCenter Server のインストーラをダウンロードします。[Windows 版 vCenter Server のインストーラのダウンロード](#)を参照してください。

手順

- 1 Windows 版 vCenter Server の ISO ファイルをダウンロードします。ISO ファイルをローカルで抽出するか、または ISO ファイルをドライブとしてマウントします。
- 2 ソフトウェア インストーラで、**autorun.exe** ファイルをダブルクリックし、インストーラを起動します。
- 3 Windows 版 vCenter Server を選択し、インストール をクリックします。

インストーラはバックグラウンドでチェックを実行し、既存の設定を検出して、アップグレード プロセスに影響を与える可能性がある問題を通知します。

vCenter Server のインストーラが起動し、画面が開きます。

- 4 検出された情報およびアップグレード パスが表示されたら、それが正しいことを確認します。
要件が満たされていない場合は、ダイアログ ボックスが表示されます。ダイアログ ボックス内の指示に従ってください。
- 5 インストール ウィザードの手順を完了し、使用許諾契約に同意します。
- 6 vCenter Server 管理者の認証情報を入力します。

インストーラは、バックグラウンドでチェックを行い、アップグレードの失敗の原因になる可能性がある問題を検出します。古い証明書が現在の VMware のセキュリティ基準を満たさない場合には、警告が表示されます。

7 vCenter Server デプロイ モデルを選択します。

- 組み込みの Platform Services Controller を使用する vCenter Server を選択した場合、vCenter Single Sign-On ドメインおよびサイトを作成するか、それらに参加して、次へ をクリックします。

重要： vCenter Single Sign-On ドメインへの参加を選択できますが、Platform Services Controller が組み込まれた vCenter Server はスタンドアロンのインストールと見なし、インフラストラクチャ データのレプリケーションには使用しないでください。

- 外部の Platform Services Controller を使用する vCenter Server を選択した場合、外部の Platform Services Controller の情報を入力し、次へ をクリックします。

組み込みの Platform Services Controller インスタンスの場合、インストーラは vCenter Single Sign-On ドメインの *System-Domain* を Platform Services Controller に対して選択されている新しいドメインに移行させます。外部の Platform Services Controller の場合、インストーラは入力された認証情報を使用して Platform Services Controller インスタンスに接続することによって、入力された情報が正しいことを検証します。

8 ポートを構成し、次へ をクリックします。

インストーラは、選択されたポートが使用できるかどうかをチェックし、それらのポートが使用できない場合はエラー メッセージを表示します。

9 インストール、データ、およびエクスポート データの各ディレクトリを構成し、次へ をクリックします。

インストーラは、選択されたディレクトリでディスク容量とアクセス許可のチェックを実行し、選択されたディレクトリが要件を満たさない場合にはエラー メッセージを表示します。

10 組み込みのデプロイを選択した場合、VMware カスタム エクスペリエンス改善プログラム (CEIP) のページを確認して、プログラムに参加するかどうかを選択します。

CEIP の詳細については、『vCenter Server およびホスト管理』の「カスタム エクスペリエンス改善プログラムの構成」セクションを参照してください。

11 [サマリ] ページを確認して、設定が正しいことを確認します。vCenter Server マシンと vCenter Server データベースのバックアップを作成したことを確認し、アップグレード をクリックします。

インストーラによってアップグレード プロセスが開始されると、進捗状況インジケータが表示されます。プロセスが完了すると、インストーラがアップグレードの状態を検証します。

12 終了 をクリックする前に、アップグレード後の手順を書き留めます。

13 終了 をクリックし、アップグレードを完了します。

結果

Windows 版 vCenter Server のアップグレードが完了します。アップグレード後のタスクの詳細については、[6 章 vCenter Server のアップグレード後](#)を参照してください。

Windows 版 vCenter Server 5.1 のアップグレード

Windows 版 vCenter Server のインストーラを使用して、既存の vCenter Server 5.1 デプロイをアップグレードできます。

vCenter Server 5.1 サービスの構成により、アップグレード後のコンポーネントとサービスのデプロイが決定されます。

- vCenter Server と同じ仮想マシンまたは物理サーバに vCenter Single Sign-On 5.1 が置かれている場合、インストーラは、組み込み Platform Services Controller デプロイを使用する vCenter Server に構成をアップグレードします。
- vCenter Server とは異なる仮想マシンまたは物理サーバに vCenter Single Sign-On 5.1 が置かれている場合、インストーラは構成を外部 Platform Services Controller デプロイを使用する vCenter Server にアップグレードします。
- vCenter Server と vCenter Single Sign-On によって使用されている vCenter Server 5.1 ポートは保持されます。アップグレード中、ポートを変更することはできません。必要なポートの詳細については、[vCenter Server および Platform Services Controller に必要なポート](#)を参照してください。
- vCenter Server サービスは、vCenter Server と別個にデプロイされなくなりました。個別にデプロイされた 5.1 サービスは、アップグレード プロセス中にアップグレードされ、vCenter Server 仮想マシンまたは物理サーバに移行されます。サービス移行の詳細については、[vCenter Server 6.0 へのアップグレード中の Windows サービス用の分散 vCenter Server の移行および vCenter Server のアップグレード パスの例](#)を参照してください。
- インストーラは、Microsoft SQL Server Express のデータベースを vCenter Server に含まれる PostgreSQL データベースに自動的に移行します。VC 6.0 へアップグレードする前に Microsoft SQL Server Express から Microsoft SQL Server へ移行する方法については、当社のナレッジ ベースの記事 (<http://kb.vmware.com/kb/1028601>) および Microsoft のドキュメントを参照してください。PostgreSQL データベースへ移行しないでアップグレードする方法については、当社のナレッジ ベースのこちらの記事 (<http://kb.vmware.com/kb/2109321>) を参照してください。

注: 外部 vCenter Single Sign-On インスタンスを使用している場合は、これを Platform Services Controller 6.0 にアップグレードしてから vCenter Server 5.5 インスタンスを 6.0 にアップグレードする必要があります。[外部デプロイの vCenter Single Sign-On 5.1 のアップグレード](#) を参照してください。

- デプロイ オプションについては、[vCenter Server のデプロイ モデルおよび Windows 版 vCenter Server 6.0 のアップグレード プロセスについて](#)を参照してください。
- バージョンが混在した環境での vCenter Server の動作の詳細については、[vCenter Server のアップグレード時のバージョン混在の移行環境](#)を参照してください。
- vCenter Single Sign-On 5.1 のアップグレードの詳細については、[外部デプロイの vCenter Single Sign-On 5.1 のアップグレード](#)を参照してください。
- アップグレード後の手順の詳細については、[6 章 vCenter Server のアップグレード後](#)を参照してください。

前提条件

- 構成がこのアップグレード要件を満たしていることを確認します。[Windows 版 vCenter Server の要件](#) を参照してください。
- アップグレード タスクの準備を完了します。を参照してください。[3 章 vCenter Server をアップグレードする前に行う作業](#)

- vCenter Server 構成とデータベースのバックアップが作成済みであることを確認します。
- vCenter Server のインストーラをダウンロードします。を参照してください。 [Windows 版 vCenter Server のインストーラのダウンロード](#)

手順

- 1 Windows 版 vCenter Server の ISO ファイルをダウンロードします。ISO ファイルをローカルで抽出するか、または ISO ファイルをドライブとしてマウントします。
- 2 ソフトウェア インストーラで、**autorun.exe** ファイルをダブルクリックし、インストーラを起動します。
- 3 Windows 版 vCenter Server を選択し、インストール をクリックします。

インストーラは、バックグラウンドでチェックを実行して既存の vCenter Single Sign-On 設定を検索し、アップグレード プロセスに影響する可能性がある問題がある場合には通知します。

vCenter Server のインストーラが起動し、ようこそページが開きます。

- 4 検出された情報およびアップグレード パスがインストーラで表示されたら、それが正しいことを確認します。
ようこそ画面ではなく、要件が満たされていないことを指摘するダイアログ ボックスが表示される場合は、ダイアログ ボックス内の指示に従ってください。
- 5 インストール ウィザードの手順を完了し、使用許諾契約に同意します。

インストーラは、バックグラウンドでアップグレード前チェックを行い、アップグレードの失敗の原因になる可能性がある問題を検出します。古い証明書が現在の VMware のセキュリティ基準を満たさない場合には、警告が表示されます。

- 6 Platform Services Controller インスタンスを構成します。
 - vCenter Server と vCenter Single Sign-On が同じマシンにインストールされている場合、Platform Services Controller を構成して 次へ をクリックします。
 - vCenter Server と vCenter Single Sign-On が同じマシンに置かれていない場合は、外部 Platform Services Controller について求められた情報を入力し、次へ をクリックします。

組み込みの Platform Services Controller の場合、インストーラは vCenter Single Sign-On ドメインの *System-Domain* を Platform Services Controller に対して選択されている新しいドメインに移行させます。外部 Platform Services Controller の場合、インストーラは入力された認証情報を使用して Platform Services Controller インスタンスに接続することによって、入力された情報を検証します。

- 7 ポートを構成し、次へ をクリックします。
インストーラは、選択されたポートが使用できるかどうかをチェックし、それらのポートが使用できない場合はエラー メッセージを表示します。
- 8 インストール、データ、およびエクスポート データの各ディレクトリを構成し、次へ をクリックします。
インストーラは、選択されたディレクトリでディスク領域とアクセス許可のチェックを実行し、選択されたディレクトリが要件を満たさない場合にはエラー メッセージを表示します。

- 9 [サマリ] ページを確認して、設定が正しいことを確認します。vCenter Server マシンと vCenter Server データベースのバックアップを作成したことを確認し、アップグレード をクリックします。

インストーラによってアップグレード プロセスが開始されると、進捗状況インジケータが表示されます。プロセスが完了すると、インストーラがアップグレードの状態を検証します。

- 10 終了 をクリックする前に、アップグレード後の手順を書き留めます。

- 11 終了 をクリックし、アップグレードを完了します。

結果

Windows 版 vCenter Server のアップグレードが完了します。アップグレード後のタスクの詳細については、[6 章 vCenter Server のアップグレード後](#)を参照してください。

Windows 版 vCenter Server 5.5 のアップグレード

Windows 版 vCenter Server のインストーラを使用して、既存の vCenter Server 5.5 デプロイをアップグレードできます。

vCenter Server 5.5 サービスの構成により、アップグレード後のコンポーネントとサービスのデプロイ方法は異なります。

- vCenter Server と同じ仮想マシンまたは物理サーバに vCenter Single Sign-On 5.5 が置かれている場合、インストーラは、組み込みの Platform Services Controller デプロイを使用する vCenter Server に構成をアップグレードします。
- vCenter Server とは異なる仮想マシンまたは物理サーバに vCenter Single Sign-On 5.5 が置かれている場合、インストーラは構成を外部の Platform Services Controller デプロイを使用する vCenter Server にアップグレードします。
- vCenter Server と vCenter Single Sign-On によって使用されている vCenter Server 5.5 ポートは保持されます。アップグレード中、ポートを変更することはできません。必要なポートの詳細については、[vCenter Server および Platform Services Controller に必要なポート](#)を参照してください。
- vCenter Server サービスは、vCenter Server と別個にデプロイされなくなりました。個別にデプロイされた 5.5 サービスは、アップグレード プロセス中にアップグレードされ、vCenter Server 仮想マシンまたは物理サーバに移行されます。サービス移行の詳細については、[vCenter Server 6.0 へのアップグレード中の Windows サービス用の分散 vCenter Server の移行](#)および [vCenter Server のアップグレード パスの例](#)を参照してください。

- インストーラは、Microsoft SQL Server Express のデータベースを vCenter Server に含まれる PostgreSQL データベースに自動的に移行します。VC 6.0 へアップグレードする前に Microsoft SQL Server Express から Microsoft SQL Server へ移行する方法については、VMware のナレッジベースの記事 <http://kb.vmware.com/kb/1028601> および Microsoft のドキュメントを参照してください。PostgreSQL データベースへ移行せずにアップグレードする方法については、VMware のナレッジベースのこちらの記事 <http://kb.vmware.com/kb/2109321> を参照してください。

注： 外部の vCenter Single Sign-On を使用している場合は、これを Platform Services Controller 6.0 にアップグレードしてから vCenter Server 5.5 インスタンスを 6.0 にアップグレードする必要があります。外部デプロイの vCenter Single Sign-On 5.5 のアップグレードを参照してください。

- デプロイ オプションについては、[vCenter Server のデプロイ モデル](#)および [Windows 版 vCenter Server 6.0 のアップグレード プロセス](#)についてを参照してください。
- バージョンが混在した環境での vCenter Server の動作の詳細については、[vCenter Server のアップグレード時のバージョン混在の移行環境](#)を参照してください。
- vCenter Single Sign-On 5.5 のアップグレードの詳細については、[外部デプロイの vCenter Single Sign-On 5.5 のアップグレード](#)を参照してください。
- アップグレード後の手順の詳細については、[6 章 vCenter Server のアップグレード後](#)を参照してください。

前提条件

- 構成がこのアップグレード要件を満たしていることを確認します。[Windows 版 vCenter Server の要件](#)を参照してください。
- アップグレード タスクの準備を完了します。[3 章 vCenter Server をアップグレードする前に行う作業](#)を参照してください。
- vCenter Server 構成とデータベースのバックアップが作成済みであることを確認します。
- VMware ディレクトリ サービスが安定した状態にあり、停止できることを確認するには、このサービスを手動で再起動します。vCenter Server アップグレード ソフトウェアでアップグレード プロセス中に vCenter Single Sign-On をアンインストールするには、VMware ディレクトリ サービスを停止する必要があります。
- vCenter Server のインストーラをダウンロードします。[Windows 版 vCenter Server のインストーラのダウンロード](#)を参照してください。
- vCenter Single Sign-On 5.5 が vCenter Server と異なる仮想マシンまたは物理サーバに置かれている場合、vCenter Single Sign-On 5.5 をアップグレードしてから vCenter Server 5.5 のアップグレードを開始してください。[外部デプロイの vCenter Single Sign-On 5.5 のアップグレード](#)を参照してください。

手順

- 1 Windows 版 vCenter Server の ISO ファイルをダウンロードします。ISO ファイルをローカルで抽出するか、または ISO ファイルをドライブとしてマウントします。
- 2 ソフトウェア インストーラで、**autorun.exe** ファイルをダブルクリックし、インストーラを起動します。

3 Windows 版 vCenter Server を選択し、インストール をクリックします。

インストーラは、バックグラウンドで既存の vCenter Single Sign-On 設定を検索し、アップグレード プロセスに影響する問題があれば通知します。

vCenter Server のインストーラが起動し、画面が開きます。

4 [次へ] をクリックして、使用許諾契約書に同意します。

5 vCenter Server および vCenter Single Sign-On の認証情報を入力します。

オプション	操作
vCenter Single Sign-On が同じ仮想マシンまたは物理サーバにインストールされている場合	<ol style="list-style-type: none"> 1 vCenter Single Sign-On の認証情報を入力します。 2 (オプション) 異なる認証情報を vCenter Server ユーザーに使用するには、[vCenter Server の認証情報と同じ認証情報を使用する] チェック ボックスを選択解除し、使用する認証情報を入力します。 3 [次へ] をクリックします。 <p>インストーラは、バックグラウンドでチェックを行い、アップグレードの失敗の原因になる可能性がある問題を検出します。古い証明書が現在の VMware のセキュリティ基準を満たさない場合には、警告が表示されます。</p>
vCenter Single Sign-On が異なる仮想マシンまたは物理サーバにインストールされている場合	<ol style="list-style-type: none"> 1 vCenter Server の認証情報を入力し、[次へ] をクリックします。 インストーラは、バックグラウンドでチェックを行い、アップグレードの失敗の原因になる可能性がある問題を検出します。 2 vCenter Server を既存の Platform Services Controller 6.0 の vCenter Single Sign-On インスタンスに登録します。 <ol style="list-style-type: none"> a (オプション) デフォルトの vCenter Single Sign-On HTTPS ポートを変更します。 b vCenter Single Sign-On 管理者パスワードを入力して、[次へ] をクリックします。 3 リモート サーバによって送信された証明書を確認します。

6 ポートを構成し、次へ をクリックします。

vCenter Single Sign-On がポート 80 と 443 を使用できるようにするため、これらのポートが利用されておらず、占有できることを確認します。そうでない場合、インストール時にはカスタム ポートが使用されます。

インストーラは、選択されたポートが使用できるかどうかをチェックし、それらのポートが使用できない場合はエラー メッセージを表示します。

7 インストール、データ、およびエクスポート データの各ディレクトリを構成し、次へ をクリックします。

インストーラは、選択されたディレクトリのディスク容量と権限のチェックを実行し、選択されたディレクトリが要件を満たさない場合にはエラー メッセージを表示します。

8 [VMware カスタマ エクスペリエンス改善プログラム (CEIP)] ページを参照し、プログラムへの参加を希望するかどうかを選択します。

CEIP の詳細については、『vCenter Server およびホスト管理』の「カスタマ エクスペリエンス改善プログラムの構成」セクションを参照してください。

- 9 [サマリ] ページを確認して、設定が正しいことを確認します。チェックボックスを選択して vCenter Server マシンと vCenter Server データベースのバックアップを作成したことを確認し、アップグレード をクリックします。

インストーラによってアップグレード プロセスが開始され、進捗状況インジケータが表示されます。プロセスが完了すると、インストーラがアップグレードの状態を検証します。

- 10 終了 をクリックする前に、アップグレード後の手順を書き留めます。
- 11 終了 をクリックし、アップグレードを完了します。

結果

Windows 版 vCenter Server のアップグレードが完了します。アップグレード後のタスクの詳細については、[6 章 vCenter Server のアップグレード後](#)を参照してください。

VIMPatch での Java コンポーネントと vCenter Server tc Server の更新

VIMPatch ISO ファイルを使用すると、JRE サーバに依存している vCenter Server コンポーネントの Java バージョンを個別に更新できます。

vCenter Server コンポーネントを再インストールせずにパッチを適用できます。このパッチにより、JRE の更新が実施されます。

前提条件

- VMware ダウンロード ページ (<https://my.vmware.com/group/vmware/patch>) から Java Components パッチをダウンロードします。名前の形式は、VMware-VIMPatch-6.0.0-build_number-YYYYMMDD.iso です。
- パッチを適用するとすべてのサービスが停止するため、vCenter Server コンポーネント操作を停止します。

手順

- 1 vCenter Server コンポーネントがインストールされているシステムに、VMware-VIMPatch-6.0.0-build_number-YYYYMMDD.iso をマウントします。
- 2 `ISO_mount_directory/autorun.exe` をダブルクリックします。
vCenter Server Java コンポーネントの更新ウィザードを開きます。
- 3 [すべてをパッチ] をクリックします。

このパッチは、Java コンポーネントが最新かどうかをチェックし、必要に応じてサイレントで更新します。

vCenter Server Appliance および Platform Services Controller アプライアンスのアップグレードとパッチ適用

5

vCenter Server Appliance をアップグレードするには、クライアント統合プラグインを使用します。パッチで vCenter Server Appliance および Platform Services Controller アプライアンスを更新するには、アプライアンス管理インターフェイスを使用するか、アプライアンス シェルで使用可能な `software-packages` ユーティリティを使用します。

重要： vCenter Server Appliance 5.1 Update 3 以降から vCenter Server Appliance 6.0 へのアップグレードがサポートされています。vCenter Server Appliance 5.0 をアップグレードするには、まず vCenter Server Appliance をバージョン 5.1 Update 3 または 5.5 Update 2 にアップグレードしてから、それを vCenter Server Appliance 6.0 にアップグレードします。vCenter Server Appliance 5.0 からバージョン 5.1 Update 3 へのアップグレードの詳細については、VMware vSphere 5.1 のドキュメントを参照してください。vCenter Server Appliance 5.0 からバージョン 5.5 Update 2 へのアップグレードの詳細については、VMware vSphere 5.5 のドキュメントを参照してください。

vCenter Server Appliance のバージョン 6.0 では、最大 1,000 台のホストと最大 10,000 台の仮想マシンを含む環境に適した、組み込みの PostgreSQL データベースが使用されます。

vCenter Server Appliance のバージョン 6.0 は、ESXi の 1 台の仮想マシンごとに 32 個の仮想 CPU をサポートする、仮想ハードウェア バージョン 8 でデプロイされます。vCenter Server Appliance で管理するホストによっては、ESXi ホストをアップグレードし、vCenter Server Appliance のハードウェア バージョンを更新して、より多くの仮想 CPU をサポートできます。

- ESXi 5.5.x は、仮想ハードウェアのバージョンは 10 まで、仮想マシンあたりの仮想 CPU は 64 個までサポートします。
- ESXi 6.0.x は、仮想ハードウェアのバージョンは 11 まで、仮想マシンあたりの仮想 CPU は 128 個までサポートします。

vCenter Server Appliance のデプロイの詳細については、vSphere のインストールとセットアップを参照してください。

vCenter Server Appliance のインベントリとその他の構成制限については、『構成の上限』ドキュメントを参照してください。

vCenter Server Appliance の構成の詳細については、vCenter Server Appliance の構成を参照してください。この章には、次のトピックが含まれています。

- [vCenter Server Appliance のアップグレード](#)
- [vCenter Server Appliance および Platform Services Controller アプライアンスのパッチ適用](#)

vCenter Server Appliance のアップグレード

vCenter Server Appliance の最新のバージョンにアップグレードするには、クライアント統合プラグインを使用する必要があります。vCenter Server Appliance のアップグレードに必要なインストール ファイルはすべて、VMware の Web サイトからダウンロードできる ISO ファイルに含まれています。

vCenter Server Appliance をアップグレードする前に、ISO ファイルをダウンロードして、このファイルのアップグレードを実行する Windows ホスト マシンにマウントします。クライアント統合プラグインをインストールし、アップグレード ウィザードを開始します。

vCenter Server Appliance のアップグレード要件の詳細については、[vCenter Server Appliance の要件](#)を参照してください。

vCenter Server Appliance のアップグレード中に要求される入力の詳細については、[vCenter Server Appliance のアップグレードに必要な情報](#)を参照してください。

vCenter Server Appliance のアップグレードは古いバージョンから最新のバージョンへの移行で、ESXi ホスト 5.0 以降に新しい vCenter Server Appliance 6.0 をデプロイすることになります。アップグレードする vCenter Server Appliance の構成設定は、新しくデプロイされた vCenter Server Appliance に移行および適用されます。古いアプライアンスからのアップグレードを容易に行うために、新しいアプライアンスには一時的な IP アドレスが割り当てられます。アップグレードする vCenter Server Appliance の IP アドレスおよびホスト名は、アップグレード プロセスの一環として vCenter Server Appliance 6.0 に適用されます。アップグレードの最後に、アップグレードした vCenter Server Appliance がパワー オフされます。

重要： アップグレードしている vCenter Server Appliance が IPv4 と IPv6 が混在する環境で構成された場合、IPv4 の設定のみが保持されます。

アップグレードしている vCenter Server Appliance で非短期の分散仮想ポート グループが使用される場合、ポート グループは保持されません。アップグレード後に、新しいアプライアンスを古いアプライアンスの元の非短期の分散仮想ポート グループに手動で接続できます。

DHCP 環境では、アップグレードを試行している vCenter Server Appliance および vCenter Server Appliance 6.0 が異なるネットワークにあるホストで実行される場合、vCenter Server Appliance のアップグレードは失敗します。

vCenter Server Appliance のアップグレード プロセスについて

vCenter Server Appliance 5.1 Update 3 および 5.5.x から 6.0 にアップグレードできます。

アップグレードには、次のプロセスが含まれます。

- 1 vCenter Server Appliance 5.1 Update 3 または 5.5.x 構成のエクスポート。
- 2 vCenter Server Appliance 6.0 のデプロイ。
- 3 vCenter Server Appliance 5.1 Update 3 または 5.5.x サービスおよび構成データの新しい vCenter Server Appliance 6.0 デプロイへの移行。

非短期の分散仮想ポート グループは移行されません。アップグレード後に、新しいアプライアンスを非短期の分散仮想ポート グループに手動で接続できます。

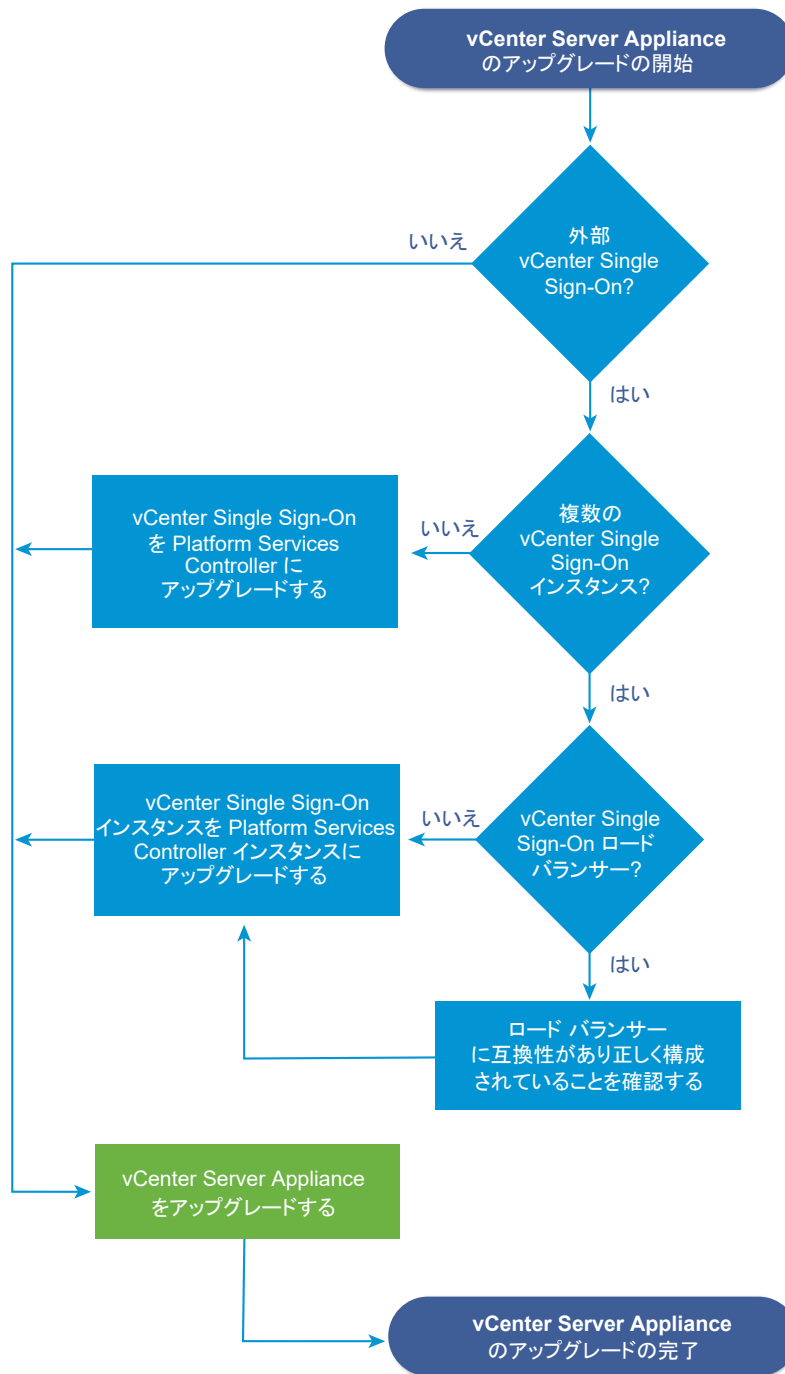
4 アップグレードを行う vCenter Server Appliance 5.1 Update 3 または 5.5.x マシンのパワーオフ。

注： 外部の vCenter Single Sign-On サーバに登録されている vCenter Server Appliance のアップグレードは、vCenter Server Appliance 5.5.x でのみサポートされています。

現在使用している vCenter Server Appliance が 5.1 Update 3 よりも前のバージョンの場合、vCenter Server Appliance 6.0 にアップグレードする前に 5.1 Update 3 以降にアップグレードする必要があります。

vCenter Server Appliance インスタンスが複数ある場合、同時アップグレードはサポートされていません。一度に 1 つのインスタンスをアップグレードする必要があります。

図 5-1. vCenter Server Appliance のアップグレード ワークフロー



- 適切なロード バランサーを使用するための vCenter Single Sign-On と Platform Services Controller の互換性情報および要件については、[vCenter Single Sign-On and Platform Services Controller High Availability Compatibility Matrix](#) を参照してください。
- vCenter Server Appliance の要件については、[vCenter Server Appliance の要件](#)を参照してください。
- vCenter Server Appliance のアップグレード準備については、[3 章 vCenter Server をアップグレードする前に行う作業](#)を参照してください。

- vCenter Server Appliance のアップグレード手順については、5 章 [vCenter Server Appliance および Platform Services Controller アプライアンスのアップグレードとパッチ適用](#)を参照してください。
- vCenter Server Appliance のアップグレード後の手順については、6 章 [vCenter Server のアップグレード後](#)を参照してください。

vCenter Server Appliance のインストーラのダウンロード

vCenter Server Appliance の .iso インストーラとクライアント統合プラグインをダウンロードします。

前提条件

<https://my.vmware.com/web/vmware/> で Customer Connect アカウントを作成します。

手順

- 1 VMware の Web サイト (<https://my.vmware.com/web/vmware/downloads>) から vCenter Server Appliance のインストーラをダウンロードします。
- 2 md5sum が正しいことを確認します。

MD5 チェックサムをの使用については、VMware Web サイトのトピックをご覧ください (<http://www.vmware.com/download/md5.html>)。
- 3 クライアント統合プラグインをインストールする Windows 仮想マシンまたは物理サーバに ISO イメージをマウントし、vCenter Server Appliance をデプロイまたはアップグレードします。

Windows 仮想マシンを使用している場合、vSphere Web Client を使用し、仮想マシンの CD/DVD ドライブ用のデータストア ISO ファイルとして ISO イメージを構成できます。vSphere 仮想マシン管理を参照してください。

クライアント統合プラグインのインストール

vCenter Server Appliance をデプロイまたはアップグレードする前に、クライアント統合プラグインをインストールする必要があります。

前提条件

[vCenter Server Appliance のインストーラのダウンロード](#)。

手順

- 1 vCenter Server Appliance インストーラで、vcsa ディレクトリに移動し、VMware-ClientIntegrationPlugin-6.0.0.exe をダブルクリックします。

[クライアント統合プラグインのインストール] ウィザードが表示されます。
- 2 [ようこそ] ページで [次へ] をクリックします。
- 3 エンド ユーザー使用許諾契約書の条項を読んで同意し、[次へ] をクリックします。
- 4 (オプション) クライアント統合プラグインのインストール フォルダのデフォルト パスを変更し、[次へ] をクリックします。

- 5 ウィザードの [プラグインをインストールする準備ができました] ページで、情報を確認してから [インストール] をクリックします。
- 6 インストールが完了したら、[終了] をクリックします。

vCenter Single Sign-On が組み込まれた vCenter Server Appliance のアップグレード

クライアント統合プラグインを使用し、組み込みの vCenter Single Sign-On インスタンスを使用する vCenter Server Appliance 5.1 Update 3 および 5.5.x を、Platform Services Controller が組み込まれた vCenter Server Appliance 6.0 にアップグレードできます。

vCenter Server Appliance のバージョン 6.0 をデプロイできるのは、ESXi 5.0 以降を実行しているホスト上のみです。このため、アップグレードする vCenter Server Appliance が ESXi 5.0 よりも前のバージョンが存在するホストで実行されている場合には、まず ESXi 5.0 以降をインストールする必要があります。これにより、アップグレード ウィザードは 6.0 バージョンの vCenter Server Appliance をそのホストに移行することができるようになります。

vCenter Server Appliance インスタンスに、正しい完全修飾ドメイン名 (FQDN) が指定された証明書を設定するには、次に示すいずれかの方法でそのインスタンスをデプロイする必要があります。

- DHCP を使用して vCenter Server Appliance を起動して、DHCP によって完全修飾ホスト名を割り当てる。
- 既存の vCenter Server に vCenter Server Appliance をデプロイして、デプロイ時にホスト名の OVF プロパティを設定する。

正しい FQDN を使用して vCenter Server Appliance をデプロイしない場合は、証明書を再生成する必要があります。 [vCenter Server Appliance のアップグレード後の起動中の VMware Component Manager のエラー](#) を参照してください。

前提条件

- vSphere ネットワーク上のすべてのマシンの時刻が同期していることを確認します。 [vSphere ネットワーク上の時計の同期](#) を参照してください。
- ターゲットの vCenter Server Appliance をデプロイする ESXi ホストが、ロックダウンまたはメンテナンスモードになっていないことを確認します。
- アップグレードする vCenter Server Appliance で、アップグレードに必要なデータを格納するための十分な空きディスク容量があることを確認します。
- アップグレードする vCenter Server Appliance でポート 22 が開放されていることを確認します。アップグレードプロセスによりインバウンド SSH 接続を確立し、既存のアプライアンスからエクスポートしたデータをダウンロードします。
- アップグレードする vCenter Server Appliance が存在する、ソースの ESXi ホストでポート 443 が開放されていることを確認します。アップグレードプロセスによりソースの ESXi ホストへの HTTPS 接続を確立して、vCenter Server Appliance がアップグレードできる状態であることを確認し、新規アプライアンスおよび既存アプライアンス間の SSH 接続を設定します。

- 既存の vCenter Server Appliance 用の vCenter Server SSL 証明書が適切に構成されていることを確認します。当社のナレッジベースの記事 [KB2057223](#) を参照してください。
- 外部データベースを使用する場合は、vCenter Server Appliance データベースをバックアップします。
- アップグレードする vCenter Server Appliance のスナップショットを作成します。
- 新しいバージョンのクライアント統合プラグインをインストールします。[クライアント統合プラグインのインストール](#)を参照してください。

手順

- 1 ソフトウェア インストーラのディレクトリで、[vcsa-setup.html] をダブルクリックします。
- 2 ブラウザがクライアント統合プラグインを検出するまで 3 秒ほど待機し、プロンプトが表示されたらブラウザ上でプラグインを実行できるようにします。
- 3 ホーム ページで、[アップグレード] をクリックします。
- 4 「サポートされるアップグレード」警告メッセージで、[OK] をクリックして vCenter Server Appliance アップグレード ウィザードを起動します。
- 5 使用許諾契約書を読んで同意し、[次へ] をクリックします。
- 6 vCenter Server Appliance をデプロイするターゲット サーバに接続し、[次へ] をクリックします。
 - a ESXi ホストの FQDN アドレスまたは IP アドレスを入力します。
 - b ESXi ホストの管理者権限を持つユーザー（たとえば、root ユーザー）のユーザー名とパスワードを入力します。
- 7 （オプション） 証明書の警告が表示された場合は、[はい] をクリックしてそれに同意します。
- 8 vCenter Server Appliance 6.0 の名前を入力します。
- 9 （オプション） [SSH の有効化] チェック ボックスを選択して、vCenter Server Appliance への SSH 接続を有効にします。
- 10 [ソース アプライアンスへの接続] ページで、アップグレードするアプライアンスの詳細を入力します。
 - a [既存のアプライアンスのバージョン] ドロップダウン メニューから、vCenter Server Appliance 6.0 にアップグレードする vCenter Server Appliance のバージョンを選択します。

オプション	説明
vCSA 5.1 U3	vCenter Server Appliance バージョン 5.1 Update 3 をアップグレードできるようにします。
vCSA 5.5	vCenter Server Appliance バージョン 5.5.x をアップグレードできるようにします。

- b [既存のアプライアンス タイプ] ドロップダウン メニューから、[組み込み Platform Services Controller] を選択します。

- c [vCenter Server Appliance] で、アップグレードする vCenter Server Appliance の必須データを入力します。

オプション	操作
vCenter Server の IP アドレス/FQDN	アップグレードする vCenter Server Appliance の IP アドレスまたは FQDN を入力します。
vCenter 管理者ユーザー名	vCenter Single Sign-On 管理者ユーザー名を入力します。 vCenter Server Appliance 5.5.x をアップグレードする場合、これは administrator@vsphere.local です。
vCenter 管理者パスワード	vCenter Single Sign-On 管理者のパスワードを入力します。
vCenter HTTPS ポート	必要に応じて、デフォルトの vCenter HTTPS ポート番号を変更します。 デフォルト値は 443 です。
アプライアンス (OS) の root パスワード	root ユーザーのパスワードを入力します。
一時的なアップグレード ファイル パス	必要に応じて、デフォルト パスを、構成データを保存するフォルダに変更します。 デフォルトでは、アップグレードする vCenter Server Appliance の設定についてのデータと情報はすべて /tmp/vmware/cis-export-folder にエクスポートされます。データは、後で vCenter Server Appliance 6.0 に移行されます。
パフォーマンスなどの履歴データの移行	必要に応じて、データベースに保存されているオプションのパフォーマンス データと履歴データの移行を有効にするかどうかを選択します。 これには、アラーム、イベント、統計情報などについての情報が含まれます。これらの情報サイズが大きい場合、移行によってアップグレードが遅くなる可能性があります。

- d [ソース ESXi ホスト] で、アップグレードする vCenter Server Appliance が存在するホストについての情報を入力します。

オプション	説明
ESXi ホストの IP アドレス/FQDN	アップグレードする vCenter Server Appliance が存在する ESXi ホストの IP アドレスまたは FQDN。
ESXi ホストのユーザー名	プライマリ ホストにおける管理権限を持つユーザーのユーザー名。
ESXi ホストのパスワード	管理者ユーザーのパスワード。

- 11 (オプション) 警告メッセージが表示される場合は、[はい] をクリックして受け入れます。
- 12 新たにデプロイされたアプライアンスの vCenter Single Sign-On を設定し、[次へ] をクリックします。

重要： この手順は、vCenter Server Appliance 5.1 Update 3 をアップグレードする場合にのみ行う必要があります。vCenter Server Appliance 5.5.x からアップグレードする場合、vCenter Single Sign-On データは自動的に vCenter Server Appliance 6.0 に移行されます。

オプション	説明
vCenter SSO のパスワード	vCenter Single Sign-On のパスワードを入力します。 パスワードは 8 ～ 20 文字で、1 つ以上の大文字、1 つ以上の小文字、1 つ以上の数字、1 つ以上の特殊文字（ドル記号 (\$)、感嘆符 (!)、丸括弧 (())、アット記号 (@) など）が含まれている必要があります。
パスワードの確認	vCenter Single Sign-On のパスワードを確認します。

オプション	説明
SSO ドメイン名	vCenter Single Sign-On のドメイン名を入力します。 このドメイン名は RFC 1035 標準に準拠する必要があります。
SSO サイト名	vCenter Single Sign-On のサイト名を入力します。

- 13 ウィザードの [アプライアンスのサイズの選択] ページで、vSphere インベントリ サイズに適した vCenter Server Appliance サイズを選択し、[次へ] をクリックします。

オプション	説明
極小 (最大でホスト 10 台、仮想マシン 100 台)	2 個の CPU と 8 GB のメモリが搭載されたアプライアンスをデプロイします。
小 (最大でホスト 100 台、仮想マシン 1,000 台)	4 個の CPU と 16 GB のメモリが搭載されたアプライアンスをデプロイします。
中 (最大でホスト 400 台、仮想マシン 4,000 台)	8 個の CPU と 24 GB のメモリが搭載されたアプライアンスをデプロイします。
大 (最大でホスト 1,000 台、仮想マシン 10,000 台)	16 個の CPU と 32 GB のメモリが搭載されたアプライアンスをデプロイします。

- 14 利用可能なデータストアのリストから、仮想マシンのすべての構成ファイルと仮想ディスクが格納される場所を選択します。また必要に応じて、[シン ディスク モードの有効化] を選択して、シン プロビジョニングを有効にします。
- 15 アップグレードする vCenter Server Appliance と新たにデプロイされた vCenter Server Appliance 間の通信に使用する一時ネットワークを選択し、vCenter Server Appliance の IP 割り当て方法を選択し、[次へ] をクリックします。

[一時的なネットワークの選択] ドロップダウン メニューに表示されるネットワークは、ESXi ネットワーク設定によって異なります。非短期分散仮想ポート グループはサポートされていないため、このドロップダウン メニューには表示されません。

オプション	説明
DHCP	DHCP サーバを使用して IP アドレスが割り当てられます。
固定	IP アドレスとネットワーク設定の入力を求められます。 a 新しい vCenter Server Appliance の一時 IP アドレスを入力します。 b サブネット マスクを入力します。 c ネットワーク ゲートウェイを入力します。 d ネットワーク DNS サーバの FQDN または IP アドレスを入力します。 名前はコンマで区切る必要があります。

- 16 [VMware カスタマ エクスペリエンス改善プログラム (CEIP)] ページを参照し、プログラムへの参加を希望するかどうかなを選択します。

CEIP の詳細については、『vCenter Server およびホスト管理』の「カスタマ エクスペリエンス改善プログラムの構成」セクションを参照してください。

- 17 [設定の確認] ページで、vCenter Server Appliance アップグレードの設定を確認し、[終了] をクリックしてプロセスを完了します。
- 18 (オプション) デプロイの完了後に、[https://vcenter_server_appliance_IP_address/vsphere-client] リンクをクリックして vSphere Web Client を開始し、vCenter Server Appliance の vCenter Server インスタンスにログインします。
- 19 [閉じる] をクリックして、ウィザードを終了します。

結果

vCenter Server Appliance がアップグレードされます。古い vCenter Server Appliance はパワーオフされ、新しいアプライアンスが起動します。

次のステップ

古い vCenter Server Appliance が非短期分散仮想ポート グループを使用している場合は、ポート グループの設定を保存するために、新しいアプライアンスを元の非短期分散仮想ポート グループに手動で接続できます。vSphere Distributed Switch で仮想マシン ネットワークを構成する方法については、『vSphere ネットワーク』を参照してください。

外部 vCenter Single Sign-On 環境の vCenter Server Appliance のアップグレード

外部の vCenter Single Sign-On インスタンスに登録されている vCenter Server Appliance 5.5.x を外部 Platform Services Controller で vCenter Server Appliance 6.0 にアップグレードするには、クライアント統合プラグインを使用します。

vCenter Server Appliance のバージョン 6.0 をデプロイできるのは、ESXi 5.0 以降を実行しているホスト上のみです。このため、アップグレードする vCenter Server Appliance が ESXi 5.0 よりも前のバージョンが存在するホストで実行されている場合には、まず ESXi 5.0 以降をインストールする必要があります。これにより、アップグレード ウィザードは 6.0 バージョンの vCenter Server Appliance をそのホストに移行することができるようになります。

バージョン混在環境は本番環境ではサポートされておらず、環境の機能が制限される可能性があります。vCenter Server Appliance のバージョンを移行する時以外は、そのような環境はお勧めできません。すべての vCenter Server Appliance インスタンスをアップグレードして Platform Services Controller に結合すると、リンク モード機能が拡張リンク モード機能に置き換えられます。

vCenter Server Appliance インスタンスに、正しい完全修飾ドメイン名 (FQDN) が指定された証明書を設定するには、次に示すいずれかの方法でそのインスタンスをデプロイする必要があります。

- DHCP を使用して vCenter Server Appliance を起動して、DHCP によって完全修飾ホスト名を割り当てる。
- 既存の vCenter Server に vCenter Server Appliance をデプロイして、デプロイ時にホスト名の OVF プロパティを設定する。

正しい FQDN を使用して vCenter Server Appliance をデプロイしない場合は、証明書を再生成する必要があります。vCenter Server Appliance のアップグレード後の起動中の VMware Component Manager のエラーを参照してください。

前提条件

- vSphere ネットワーク上のすべてのマシンの時刻が同期していることを確認します。[vSphere ネットワーク上の時計の同期](#)を参照してください。
- ターゲットの vCenter Server Appliance をデプロイする ESXi ホストが、ロックダウンまたはメンテナンスモードになっていないことを確認します。
- アップグレードする vCenter Server Appliance で、アップグレードに必要なデータを格納するための十分な空きディスク容量があることを確認します。
- アップグレードする vCenter Server Appliance でポート 22 が開放されていることを確認します。アップグレード プロセスによりインバウンド SSH 接続を確立し、既存のアプライアンスからエクスポートしたデータをダウンロードします。
- アップグレードする vCenter Server Appliance が存在する、ソースの ESXi ホストでポート 443 が開放されていることを確認します。アップグレード プロセスによりソースの ESXi ホストへの HTTPS 接続を確立して、vCenter Server Appliance がアップグレードできる状態であることを確認し、新規アプライアンスおよび既存アプライアンス間の SSH 接続を設定します。
- 既存の vCenter Server Appliance 用の vCenter Server SSL 証明書が適切に構成されていることを確認します。当社のナレッジベースの記事 [KB2057223](#) を参照してください。
- 外部データベースを使用する場合は、vCenter Server Appliance データベースをバックアップします。
- 外部でデプロイされた vCenter Single Sign-On 5.5 を外部でデプロイされた Platform Services Controller にアップグレードします。vCenter Single Sign-On 5.5 のアップグレードの詳細については、[外部デプロイの vCenter Single Sign-On 5.5 のアップグレード](#)を参照してください。
- アップグレードする vCenter Server Appliance のスナップショットを作成します。
- 新しいバージョンのクライアント統合プラグインをインストールします。[クライアント統合プラグインのインストール](#)を参照してください。

手順

- 1 ソフトウェア インストーラのディレクトリで、[vcsa-setup.html] をダブルクリックします。
- 2 ブラウザがクライアント統合プラグインを検出するまで 3 秒ほど待機し、プロンプトが表示されたらブラウザ上でプラグインを実行できるようにします。
- 3 ホーム ページで、[アップグレード] をクリックします。
- 4 「サポートされるアップグレード」警告メッセージで、[OK] をクリックして vCenter Server Appliance アップグレード ウィザードを起動します。
- 5 使用許諾契約書を読んで同意し、[次へ] をクリックします。
- 6 vCenter Server Appliance をデプロイするターゲット サーバに接続し、[次へ] をクリックします。
 - a ESXi ホストの FQDN アドレスまたは IP アドレスを入力します。
 - b ESXi ホストの管理者権限を持つユーザー（たとえば、root ユーザー）のユーザー名とパスワードを入力します。
- 7 （オプション） 証明書の警告が表示された場合は、[はい] をクリックしてそれに同意します。

- 8 vCenter Server Appliance 6.0 の名前を入力します。
- 9 (オプション) [SSH の有効化] チェック ボックスを選択して、vCenter Server Appliance への SSH 接続を有効にします。
- 10 [ソース アプライアンスへの接続] ページで、アップグレードするアプライアンスの詳細を入力します。
 - a [既存のアプライアンスのバージョン] ドロップダウン メニューから、vCenter Server Appliance 6.0 にアップグレードする vCenter Server Appliance のバージョンを選択します。

オプション	説明
vCSA 5.1 U3	vCenter Server Appliance バージョン 5.1 Update 3 をアップグレードできるようにします。
vCSA 5.5	vCenter Server Appliance バージョン 5.5.x をアップグレードできるようにします。

- b [既存のアプライアンス タイプ] ドロップダウン メニューで、[vCenter Server] を選択します。

- c [vCenter Server Appliance] で、アップグレードする vCenter Server Appliance の必須データを入力します。

オプション	操作
vCenter Server の IP アドレス/FQDN	アップグレードする vCenter Server Appliance の IP アドレスまたは FQDN を入力します。
vCenter 管理者ユーザー名	vCenter Single Sign-On 管理者ユーザー名を入力します。 vCenter Server Appliance 5.5.x をアップグレードする場合、これは administrator@vsphere.local です。
vCenter 管理者パスワード	vCenter Single Sign-On 管理者のパスワードを入力します。
vCenter HTTPS ポート	必要に応じて、デフォルトの vCenter HTTPS ポート番号を変更します。 デフォルト値は 443 です。
アプライアンス (OS) の root パスワード	root ユーザーのパスワードを入力します。
一時的なアップグレード ファイル パス	必要に応じて、デフォルト パスを、構成データを保存するフォルダに変更します。 デフォルトでは、アップグレードする vCenter Server Appliance の設定についてのデータと情報はすべて /tmp/vmware/cis-export-folder にエクスポートされます。データは、後で vCenter Server Appliance 6.0 に移行されます。
パフォーマンスなどの履歴データの移行	必要に応じて、データベースに保存されているオプションのパフォーマンス データと履歴データの移行を有効にするかどうかを選択します。 これには、アラーム、イベント、統計情報などについての情報が含まれます。これらの情報サイズが大きい場合、移行によってアップグレードが遅くなる可能性があります。

- d [ソース ESXi ホスト] で、アップグレードする vCenter Server Appliance が存在するホストについての情報を入力します。

オプション	説明
ESXi ホストの IP アドレス/FQDN	アップグレードする vCenter Server Appliance が存在する ESXi ホストの IP アドレスまたは FQDN。
ESXi ホストのユーザー名	プライマリ ホストにおける管理権限を持つユーザーのユーザー名。
ESXi ホストのパスワード	管理者ユーザーのパスワード。

- 11 (オプション) 警告メッセージが表示される場合は、[はい] をクリックして受け入れます。
- 12 ウィザードの [アプライアンスのサイズの選択] ページで、vSphere インベントリ サイズに適した vCenter Server Appliance サイズを選択し、[次へ] をクリックします。

オプション	説明
極小 (最大でホスト 10 台、仮想マシン 100 台)	2 個の CPU と 8 GB のメモリが搭載されたアプライアンスをデプロイします。
小 (最大でホスト 100 台、仮想マシン 1,000 台)	4 個の CPU と 16 GB のメモリが搭載されたアプライアンスをデプロイします。

オプション	説明
中 (最大でホスト 400 台、仮想マシン 4,000 台)	8 個の CPU と 24 GB のメモリが搭載されたアプライアンスをデプロイします。
大 (最大でホスト 1,000 台、仮想マシン 10,000 台)	16 個の CPU と 32 GB のメモリが搭載されたアプライアンスをデプロイします。

- 13 利用可能なデータストアのリストから、仮想マシンのすべての構成ファイルと仮想ディスクが格納される場所を選択します。また必要に応じて、[シン ディスク モードの有効化] を選択して、シン プロビジョニングを有効にします。

- 14 アップグレードする vCenter Server Appliance と新たにデプロイされた vCenter Server Appliance 間の通信に使用する一時ネットワークを選択し、vCenter Server Appliance の IP 割り当て方法を選択し、[次へ] をクリックします。

[一時的なネットワークの選択] ドロップダウン メニューに表示されるネットワークは、ESXi ネットワーク設定によって異なります。非短期分散仮想ポート グループはサポートされていないため、このドロップダウン メニューには表示されません。

オプション	説明
DHCP	DHCP サーバを使用して IP アドレスが割り当てられます。
固定	IP アドレスとネットワーク設定の入力を求められます。 a 新しい vCenter Server Appliance の一時 IP アドレスを入力します。 b サブネット マスクを入力します。 c ネットワーク ゲートウェイを入力します。 d ネットワーク DNS サーバの FQDN または IP アドレスを入力します。 名前はコンマで区切る必要があります。

- 15 [設定の確認] ページで、vCenter Server Appliance アップグレードの設定を確認し、[終了] をクリックしてプロセスを完了します。

- 16 (オプション) デプロイの完了後に、[https://vcenter_server_appliance_ip_address/vsphere-client] リンクをクリックして vSphere Web Client を開始し、vCenter Server Appliance の vCenter Server インスタンスにログインします。

- 17 [閉じる] をクリックして、ウィザードを終了します。

結果

vCenter Server Appliance がアップグレードされます。古い vCenter Server Appliance はパワーオフされ、新しいアプライアンスが起動します。

次のステップ

古い vCenter Server Appliance が非短期分散仮想ポート グループを使用している場合は、ポート グループの設定を保存するために、新しいアプライアンスを元の非短期分散仮想ポート グループに手動で接続できます。

vSphere Distributed Switch で仮想マシン ネットワークを構成する方法については、『vSphere ネットワーク』を参照してください。

vCenter Server Appliance および Platform Services Controller アプライアンスのパッチ適用

VMware は、プラットフォーム内のサードパーティ製品、主要な製品機能、またはこの両方に関連する vCenter Server Appliance のパッチを定期的に提供しています。アプライアンス管理インターフェイスまたはアプライアンス シェルを使用して、組み込みの Platform Services Controller で vCenter Server を含む vCenter Server Appliance に、外部 Platform Services Controller または Platform Services Controller で vCenter Server に、パッチを適用できます。

VMware は、パッチを 2 種類の形式で配布しています。1 つは ISO ベース、もう 1 つは URL ベースのパッチ モデルです。

- ISO イメージのパッチは、<https://my.vmware.com/group/vmware/patch> からダウンロードできます。

VMware は、利用可能なパッチが含まれる 2 種類の ISO イメージを公開しています。

ダウンロード ファイル名	説明
VMware-vCenter-Server-Appliance-product_version-build_number-patch-TP.iso	vCenter Server Appliance および Platform Services Controller アプライアンス用のサードパーティ パッチ。セキュリティおよびサードパーティ製品（JRE、tcServer、SLES OS コンポーネントなど）に関連する修正のみが含まれています。
VMware-vCenter-Server-Appliance-product_version-build_number-patch-FP.iso	vCenter Server Appliance および Platform Services Controller アプライアンス用のフル製品パッチ。セキュリティおよびサードパーティ製品（JRE、tcServer、SLES OS コンポーネントなど）に関連する VMware ソフトウェア パッチおよび修正が含まれています。

- 利用可能なパッチの供給元としてリポジトリ URL を使用するように vCenter Server Appliance および Platform Services Controller アプライアンスを構成できます。アプライアンスにはデフォルトの VMware リポジトリ URL が事前に設定されます。

ZIP 形式のパッチを VMware の Web サイト (<https://my.vmware.com/web/vmware/downloads>) からダウンロードし、カスタム リポジトリをローカル Web サーバに構築できます。ダウンロード ファイル名は VMware-vCenter-Server-Appliance-product_version-build_number-updaterepo.zip です。

利用可能なパッチがある場合、セキュリティおよびサードパーティ製品（JRE、tcServer、SLES OS コンポーネントなど）に関連するサードパーティ パッチのみを適用したり、またはすべての VMware ソフトウェア のパッチをサードパーティ パッチとともに適用することもできます。

重要： サードパーティ製のパッチの多くは、セキュリティ関連のパッチです。セキュリティに関連するパッチは、常に適用する必要があります。

外部 Platform Services Controller で vCenter Server Appliance をアップデートする前に、Platform Services Controller およびそのレプリケート パートナー（vCenter Single Sign-On ドメインにある場合）にパッチを適用する必要があります。詳細については、[vSphere 6.0 および互換性のある VMware 製品のアップデート手順](#)を参照してください。

アプライアンス管理インターフェイスを使用した vCenter Server Appliance へのパッチ適用

組み込み Platform Services Controller を使用する vCenter Server、外部 Platform Services Controller を使用する vCenter Server、または Platform Services Controller のいずれかを含む vCenter Server Appliance の仮想アプライアンス管理インターフェイスにログインして、インストールされているパッチの表示、新しいパッチがあるかどうかの確認とインストール、使用可能なパッチの自動チェックの構成を行うことができます。

ISO ベースのパッチ適用を実行するには、ISO イメージをダウンロードして、ISO イメージをアプライアンスの CD/DVD ドライブに接続し、ISO イメージで使用可能なパッチがあるかどうか確認して、パッチをインストールします。

URL ベースのパッチ適用を実行するには、リポジトリ URL で使用可能なパッチを確認して、パッチをインストールします。アプライアンスのビルド プロファイルのデフォルトの VMware リポジトリ URL が vCenter Server Appliance に事前に設定されます。デフォルトの VMware リポジトリ URL またはカスタムのリポジトリ URL（データ センター内で実行されているローカル Web サーバ上に以前ビルドしたリポジトリ URL など）を使用するようにアプライアンスを構成できます。

vCenter Server Appliance 管理インターフェイスへのログイン

vCenter Server Appliance 管理インターフェイスにログインして、vCenter Server Appliance の構成設定にアクセスします。

注： ログイン セッションは、vCenter Server Appliance 管理インターフェイスを 10 分間アイドル状態で放置すると、期限切れになります。

前提条件

vCenter Server Appliance が正常にデプロイされ、実行されていることを確認します。

手順

- 1 Web ブラウザで、vCenter Server Appliance 管理インターフェイス (<https://appliance-IP-address-or-FQDN:5480>) に移動します。
- 2 root としてログインします。

デフォルトの root パスワードは、vCenter Server Appliance のデプロイ時に設定したパスワードです。

URL ベースのパッチ適用のためのリポジトリの構成

URL ベースでパッチを適用する場合、デフォルトでは、アプライアンスのビルド プロファイル用に vCenter Server Appliance に事前設定されている、デフォルトの VMware リポジトリ URL を使用します。実際の環境要件に適したパッチの供給元として、カスタムのリポジトリ URL を構成できます。

デフォルトでは、URL ベースのパッチ適用に使用されるリポジトリは、デフォルトの VMware リポジトリ URL です。

注： `proxy.set` コマンドを使用して、vCenter Server Appliance とリポジトリ URL 間の通信用のプロキシサーバを構成できます。アプライアンス シェルの API コマンドの詳細については、vCenter Server Appliance の構成を参照してください。

vCenter Server Appliance がインターネットに接続されていない場合、またはセキュリティ ポリシーで要求される場合は、データ センター内のローカル Web サーバ上で実行されるカスタム リポジトリをビルドおよび構成し、データをデフォルトの VMware リポジトリ URL からレプリケートできます。オプションで、カスタムのパッチ適用リポジトリをホストする Web サーバにアクセスするための認証ポリシーを設定できます。

前提条件

root として vCenter Server Appliance 管理インターフェイスにログインします。

手順

- 1 カスタム リポジトリ URL を構成する場合、リポジトリをローカル Web サーバに構築します。
 - a VMware の Web サイト (<https://my.vmware.com/web/vmware/downloads>) から vCenter Server Appliance のパッチ ZIP ファイルをダウンロードします。
 - b Web サーバ上でルートの下にリポジトリ ディレクトリを作成します。
たとえば、**vc_update_repo** ディレクトリを作成します。
 - c ZIP ファイルをそのリポジトリ ディレクトリに解凍します。
解凍されたファイルは manifest および package-pool サブディレクトリに配置されます。
- 2 vCenter Server Appliance 管理インターフェイスで、[更新] をクリックします。
- 3 [接続設定] をクリックします。
- 4 リポジトリの設定を選択します。

オプション	説明
デフォルト リポジトリの使用	アプライアンスのビルド プロファイルに事前設定されている、デフォルトの VMware リポジトリ URL を使用します。
指定されたリポジトリの使用	カスタム リポジトリを使用します。リポジトリ URL を入力する必要があります。たとえば、 <i>http://web_server_name.your_company.com/vc_update_repo</i> です。 リポジトリ ポリシーで認証が要求される場合はユーザー名とパスワードも入力します。

- 5 [OK] をクリックします。

次のステップ

vCenter Server Appliance のパッチの確認およびインストール

vCenter Server Appliance のパッチの確認およびインストール

パッチは ISO イメージからまたはリポジトリ URL から直接、確認およびインストールできます。

重要： パッチのインストール中、アプライアンス内で実行されているサービスは使用できなくなります。メンテナンス期間にこの手順を実行する必要があります。障害に備えた予防策として、vCenter Server Appliance をバックアップできます。vCenter Server のバックアップおよびリストアの詳細については、vSphere のインストールとセットアップを参照してください。

前提条件

- root として vCenter Server Appliance 管理インターフェイスにログインします。
- <https://my.vmware.com/group/vmware/patch> で以前にダウンロードした ISO イメージからアプライアンスにパッチを適用する場合は、その ISO イメージを vCenter Server Appliance の CD/DVD ドライブに接続する必要があります。vSphere Web Client を使用し、ISO イメージをアプライアンスの CD/DVD ドライブ用のデータストア ISO ファイルとして構成できます。vSphere 仮想マシン管理 を参照してください。
- リポジトリ URL からアプライアンスにパッチを適用する場合は、リポジトリ設定の構成が完了していることと、現在のリポジトリ URL がアクセス可能であることを確認します。[URL ベースのパッチ適用のためのリポジトリの構成](#) を参照してください。
- 外部の Platform Services Controller を使用する vCenter Server Appliance にパッチを適用する場合は、Platform Services Controller とそのレプリケーション パートナー（vCenter Single Sign-On ドメイン内に存在する場合）にパッチが適用されていることを確認します。

手順

- 1 vCenter Server Appliance 管理インターフェイスで、[更新] をクリックします。

[現在のバージョンの詳細] ペインで、vCenter Server Appliance のバージョンおよびビルド番号を確認できます。インストールされたパッチ（ある場合）の履歴を確認することもできます。

- 2 [更新のチェック] をクリックして、ソースを選択します。

オプション	説明
URL の確認	使用可能なパッチについて、構成済みのリポジトリ URL をスキャンします
CDROM の確認	アプライアンスの CD/DVD ドライブに接続した ISO イメージをスキャンして使用可能なパッチがないか確認します

[使用可能なアップデート] ペインで、選択したソースに使用可能なパッチについての詳細を表示できます。

重要： 更新によっては、システムの再起動が必要なものもあります。これらのアップデートに関する情報は、[使用可能なアップデート] ペインで確認できます。

- 3 [更新のインストール] をクリックし、適用するパッチの範囲を選択します。

オプション	説明
すべての更新のインストール	使用可能なすべての VMware およびサードパーティのパッチを適用します
サードパーティの更新のインストール	サードパーティのパッチのみを適用します

- 4 エンド ユーザー使用許諾契約書を読んで同意します。
- 5 インストールが完了したら、[OK] をクリックします。
- 6 パッチのインストールでアプライアンスの再起動を必要とする場合は、[サマリ] をクリックし、[再起動] をクリックしてアプライアンスをリセットします。

結果

[使用可能なアップデート] ペインで、アプライアンスの変更された更新ステータスを確認できます。

vCenter Server Appliance パッチの自動チェックの有効化

構成済みのリポジトリ URL に使用可能なパッチが存在するかどうかを定期的に自動チェックするように vCenter Server Appliance を構成できます。

前提条件

- root として vCenter Server Appliance 管理インターフェイスにログインします。
- リポジトリ設定の構成が完了していることと、現在のリポジトリ URL がアクセス可能であることを確認します。
[URL ベースのパッチ適用のためのリポジトリの構成](#) を参照してください。

手順

- 1 vCenter Server Appliance 管理インターフェイスで、[更新] をクリックします。
- 2 [接続設定] をクリックします。
- 3 [アップデートの自動チェック] を選択し、使用可能なパッチの自動チェックを行う日時を UTC 時間で選択します。
- 4 [OK] をクリックします。

結果

アプライアンスによって、構成済みのリポジトリ URL に使用可能なパッチがあるかどうかを確認する定期チェックが実行されます。[使用可能なアップデート] ペインで、使用可能なパッチについての情報を確認できます。使用可能なパッチについての通知は、vCenter Server Appliance の健全性ステータスでも確認できます。vCenter Server Appliance の構成 を参照してください。

アプライアンス シェルを使用した vCenter Server Appliance へのパッチ適用

組み込み Platform Services Controller を使用する vCenter Server、外部 Platform Services Controller を使用する vCenter Server、または Platform Services Controller を含む vCenter Server Appliance のアプライアンス シェルの `software-packages` ユーティリティを使用して、インストールされたパッチの確認、新しいパッチのステージング、および新しいパッチのインストールを行うことができます。

ISO ベースのパッチ適用を実行するには、ISO イメージをダウンロードして、ISO イメージをアプライアンスの CD/DVD ドライブに接続し、オプションで使用可能なパッチを ISO イメージからアプライアンスにステージングして、パッチをインストールします。

URL ベースのパッチ適用を実行するには、オプションで使用可能なパッチをリポジトリ URL からアプライアンスにステージングして、パッチをインストールします。アプライアンスのビルド プロファイルのデフォルトの VMware リポジトリ URL が vCenter Server Appliance に事前に設定されます。`update.set` コマンドを使用して、デフォルトの VMware リポジトリ URL またはカスタムのリポジトリ URL（データ センター内で実行されているローカル Web サーバ上に以前ビルドしたリポジトリ URL など）を使用するようにアプライアンスを構成できます。`proxy.set` コマンドを使用して、vCenter Server Appliance とリポジトリ URL 間の通信用のプロキシ サーバを構成することもできます。

vCenter Server Appliance にインストールされているすべてのパッチのリストの表示

`software-packages` ユーティリティを使用して、現在 vCenter Server Appliance に適用されているパッチのリストを表示できます。インストールされているパッチのリストを時系列で表示したり、特定のパッチの詳細情報を表示したりすることもできます。

手順

- 1 アプライアンス シェルにアクセスして、スーパー管理者ロールを持つユーザーとしてログインします。

スーパー管理者ロールが割り当てられているデフォルトのユーザーは `root` です。

- 2 vCenter Server Appliance にインストールされているパッチおよびソフトウェア パッケージの完全なリストを表示するには、次のコマンドを実行します。

```
software-packages list
```

- 3 vCenter Server Appliance に適用されているすべてのパッチを時系列で表示するには、次のコマンドを実行します。

```
software-packages list --history
```

リストが時系列に表示されます。このリスト内の単一のパッチには、異なる複数のパッケージの更新が含まれていることがあります。

- 4 特定のパッチの詳細情報を表示するには、次のコマンドを実行します。

```
software-packages list --patch patch_name
```

たとえば、VMware-vCenter-Server-Appliance-Patch1 パッチの詳細情報を表示するには、次のコマンドを実行します。

```
software-packages list --patch VMware-vCenter-Server-Appliance-Patch1
```

ベンダー、説明、インストール日など、パッチに関する詳細情報の完全なリストが表示されます。

URL ベースのパッチ適用の構成

URL ベースのパッチを適用する場合、アプライアンスのビルド プロファイル用に vCenter Server Appliance に事前設定されている、デフォルトの VMware リポジトリ URL を使用します。 `update.set` コマンドを使用し、パッチの供給元としてデフォルトまたはカスタムのリポジトリ URL を使用するようにアプライアンスを構成し、パッチの自動チェックを有効にすることができます。

デフォルトでは、URL ベースのパッチ適用に使用されるリポジトリは、デフォルトの VMware リポジトリ URL です。

注： `proxy.set` コマンドを使用して、vCenter Server Appliance とリポジトリ URL 間の通信用のプロキシサーバを構成できます。アプライアンス シェルの API コマンドの詳細については、vCenter Server Appliance の構成を参照してください。

vCenter Server Appliance がインターネットに接続されていない場合、またはセキュリティ ポリシーで要求される場合は、データ センター内のローカル Web サーバ上で実行されるカスタム リポジトリをビルドおよび構成し、データをデフォルトの VMware リポジトリ URL からレプリケートできます。オプションで、カスタムのパッチ適用リポジトリをホストする Web サーバにアクセスするための認証ポリシーを設定できます。

手順

- 1 カスタム リポジトリ URL を構成する場合、リポジトリをローカル Web サーバに構築します。
 - a VMware の Web サイト (<https://my.vmware.com/web/vmware/downloads>) から vCenter Server Appliance のパッチ ZIP ファイルをダウンロードします。
 - b Web サーバ上でルートの下にリポジトリ ディレクトリを作成します。
たとえば、**vc_update_repo** ディレクトリを作成します。
 - c ZIP ファイルをそのリポジトリ ディレクトリに解凍します。
解凍されたファイルは manifest および package-pool サブディレクトリに配置されます。
- 2 アプライアンス シェルにアクセスして、スーパー管理者ロールを持つユーザーとしてログインします。
スーパー管理者ロールが割り当てられているデフォルトのユーザーは root です。
- 3 URL ベースのパッチ適用の現在の設定情報を表示するには、`update.get` コマンドを実行します。
現在のリポジトリ URL、デフォルトのリポジトリ URL、アプライアンスがパッチを最後にチェックした時間、アプライアンスがパッチを最後にインストールした時間、およびパッチの自動チェックの現在の構成に関する情報を表示できます。
- 4 URL ベースのパッチ適用に使用するリポジトリを構成します。

- デフォルトの VMware リポジトリ URL を使用するようにアプライアンスを構成するには、次のコマンドを実行します。

```
update.set --currentURL default
```

- カスタムのリポジトリ URL を使用するようにアプライアンスを構成するには、次のコマンドを実行します。

```
update.set --currentURL http://web_server_name.your_company.com/vc_update_repo [--username username] [--password password]
```

角括弧 [] でコマンドのオプションを囲みます。

カスタム リポジトリに認証が必要な場合、`--username username` オプションおよび `--password password` オプションを使用します。

- 5 指定したリポジトリ URL 内の vCenter Server Appliance パッチの定期的な自動チェックを有効にするには、次のコマンドを実行します。

```
update.set --CheckUpdates enabled [--day day] [--time HH:MM:SS]
```

角括弧 [] でコマンドのオプションを囲みます。

パッチの定期チェックが行われるように曜日を設定するには、`--day day` オプションを使用します。Monday などの特定の曜日を設定することも、Everyday を設定することもできます。デフォルト値は Everyday です。

パッチの定期チェックを実行するために UTC で時間を設定するには、`--time HH:MM:SS` オプションを使用します。デフォルト値は 00:00:00 です。

アプライアンスは、指定したリポジトリ URL 内で、利用可能なパッチを定期的にチェックします。

6 vCenter Server Appliance パッチの自動チェックを無効にするには、次のコマンドを実行します。

```
update.set --CheckUpdates disabled
```

次のステップ

利用可能なパッチの自動チェックを実行するようにアプライアンスを構成した場合は、vCenter Server Appliance の健全性ステータスを表示して、利用可能なパッチに関する情報を定期的に確認できます。vCenter Server Appliance の構成 を参照してください。

vCenter Server Appliance へのパッチのステージング

使用可能パッチをインストールする前に、それらのパッチをアプライアンスにステージングできます。software-packages ユーティリティを使用し、ISO イメージをアプライアンスに接続してローカル リポジトリからパッチをステージングすることも、リポジトリ URL を使用してリモート リポジトリから直接ステージングすることもできます。

前提条件

- <https://my.vmware.com/group/vmware/patch> で以前にダウンロードした ISO イメージからパッチをステージングする場合は、その ISO イメージを vCenter Server Appliance の CD/DVD ドライブに接続する必要があります。vSphere Web Client を使用し、ISO イメージをアプライアンスの CD/DVD ドライブ用のデータストア ISO ファイルとして構成できます。vSphere 仮想マシン管理 を参照してください。
- リモート リポジトリからパッチをステージングする場合は、リポジトリ設定の構成が完了していることと、現在のリポジトリ URL がアクセス可能であることを確認します。[URL ベースのパッチ適用の構成](#) を参照してください。

手順

- 1 アプライアンス シェルにアクセスして、スーパー管理者ロールを持つユーザーとしてログインします。

スーパー管理者ロールが割り当てられているデフォルトのユーザーは root です。

- 2 パッチをステージングします。

- 接続される ISO イメージに含まれているパッチをステージングするには、次のコマンドを実行します。

```
software-packages stage --iso
```

- 現在のリポジトリ URL に含まれているパッチをステージングするには、次のコマンドを実行します。

```
software-packages stage --url
```

デフォルトでは、現在のリポジトリ URL はデフォルトの VMware リポジトリ URL です。

サードパーティ パッチだけをステージングする場合は、`--thirdParty` オプションを使用します。

- アプライアンスに現在構成されていないリポジトリ URL に含まれているパッチをステージングするには、次のコマンドを実行します。

```
software-packages stage --url URL_of_the_repository
```

サードパーティ パッチだけをステージングする場合は、`--thirdParty` オプションを使用します。

エンド ユーザー使用許諾契約書に直接同意する場合は、`--acceptEulas` オプションを使用します。

たとえば、エンド ユーザー使用許諾契約書に直接同意し、現在のリポジトリ URL からサードパーティ パッチだけをステージングするには、次のコマンドを実行します。

```
software-packages stage --url --thirdParty --acceptEulas
```

ステージングのプロセスでは、このコマンドにより、パッチが VMware パッチであり、ステージング領域に十分な空き領域があり、パッチが変更されていないことが検証されます。まったく新しいパッチか、アップグレード可能な既存のパッケージのパッチのみがステージングされます。

- 3 (オプション) ステージングされたパッチについての情報を表示するには、次のコマンドを実行します。

```
software-packages list --staged
```

各パッチにはメタデータ ファイルが含まれており、メタデータ ファイルにはパッチのバージョン、製品名、システムの再起動が必要かどうかなどの情報が書き込まれています。

- 4 (オプション) ステージングされたパッチのリストを表示するには、次のコマンドを実行します。

```
software-packages list --staged --verbose
```

- 5 (オプション) ステージングされたパッチのステージングを解除するには、次のコマンドを実行します。

```
software-packages unstage
```

ステージング プロセスによって生成されたディレクトリとファイルがすべて削除されます。

次のステップ

ステージングされたパッチをインストールします。 [vCenter Server Appliance パッチのインストール](#) を参照してください。

重要： ISO イメージからパッチをステージングした場合は、その ISO イメージをアプライアンスの CD/DVD ドライブに接続したままにします。ISO イメージは、ステージングおよびインストール プロセス全体を通じてアプライアンスの CD/DVD ドライブに接続されている必要があります。

vCenter Server Appliance パッチのインストール

software-packages ユーティリティを使用して、ステージングされたパッチをインストールできます。

software-packages ユーティリティを使用すると、パッチ ペイロードをステージングすることなく、ISO イメージまたはリポジトリ URL からパッチを直接インストールすることもできます。

重要： パッチのインストール中、アプライアンス内で実行されているサービスは使用できなくなります。この手順は、メンテナンス期間に実行する必要があります。障害対策として、事前に vCenter Server Appliance をバックアップできます。vCenter Server のバックアップとリストアの詳細については、vSphere のインストールとセットアップを参照してください。

前提条件

- ステージングされたパッチをインストールする場合は、正しいパッチ ペイロードがステージングされていることを確認してください。 [vCenter Server Appliance へのパッチのステージング](#)を参照してください。
- ISO イメージから以前にステージングしたパッチをインストールする場合は、その ISO イメージが vCenter Server Appliance の CD/DVD ドライブに接続していることを確認します。 [vCenter Server Appliance へのパッチのステージング](#)を参照してください。
- <https://my.vmware.com/group/vmware/patch> から以前にダウンロードした ISO イメージから直接パッチをインストールする場合は、その ISO イメージを vCenter Server Appliance の CD/DVD ドライブに接続する必要があります。vSphere Web Client を使用して、ISO イメージをアプライアンスの CD/DVD ドライブ用のデータストア ISO ファイルとして構成できます。vSphere 仮想マシン管理 を参照してください。
- リポジトリからパッチを直接インストールする場合は、リポジトリの設定が完了していることと、現在のリポジトリ URL がアクセス可能であることを確認します。 [URL ベースのパッチ適用の構成](#)を参照してください。
- 外部の Platform Services Controller を使用する vCenter Server Appliance にパッチを適用する場合は、Platform Services Controller とそのレプリケーション パートナー (vCenter Single Sign-On ドメイン内に存在する場合) にパッチが適用されていることを確認します。

手順

- 1 アプライアンス シェルにアクセスして、スーパー管理者ロールを持つユーザーとしてログインします。

スーパー管理者ロールが割り当てられているデフォルトのユーザーは root です。

- 2 パッチをインストールします。

- ステージングされたパッチをインストールするには、次のコマンドを実行します。

```
software-packages install --staged
```

- 接続された ISO イメージからパッチを直接インストールするには、次のコマンドを実行します。

```
software-packages install --iso
```

- リポジトリ URL からパッチを直接インストールするには、次のコマンドを実行します。

```
software-packages install --url
```

デフォルトの VMware リポジトリ URL が、デフォルトで設定されています。

サードパーティのパッチのみをインストールする場合は、`--thirdParty` オプションを使用します。

- 現在設定されていないリポジトリ URL からパッチを直接インストールする場合は、次のコマンドを実行します。

```
software-packages install --url URL_of_the_repository
```

サードパーティのパッチのみをインストールする場合は、`--thirdParty` オプションを使用します。

エンド ユーザー使用許諾契約書に直接同意する場合は、`--acceptEulas` オプションを使用します。

たとえば、エンド ユーザー使用許諾契約書に直接同意し、パッチをステージングしないで、設定したリポジトリ URL からサードパーティのパッチのみをインストールするには、次のコマンドを実行します。

```
software-packages install --url --thirdParty --acceptEulas
```

- 3 パッチのインストールがアプライアンスの再起動を必要とする場合は、次のコマンドを実行してアプライアンスをリセットします。

```
shutdown reboot -r "patch reboot"
```

vCenter Server のアップグレード後

6

vCenter Server へのアップグレード後は、アップグレード後のオプションと要件を検討してください。

- データベースのアップグレード ログを確認できます。[データベース アップグレード ログの収集](#) を参照してください。
- アップグレード中に変更が要求された可能性のある、すべてのコンポーネントの再構成を行います。
- 認証プロセスを理解しており、アイデンティティ ソースを特定していることを確認します。
- vSphere Update Manager など、vCenter Server のそのインスタンスにリンクされている追加モジュールをアップグレードします。
- 必要に応じて、vCenter Server インベントリの ESXi ホストを、vCenter Server インスタンスと同じバージョンにアップグレードまたは移行します。

この章には、次のトピックが含まれています。

- [vCenter Server アップグレード後のコンポーネントの構成](#)
- [アップグレード後の移行された vCenter Server サービスの再構成](#)
- [vSphere Authentication Proxy のインストールまたはアップグレード](#)
- [vSphere Client へのアップグレード](#)
- [vCenter Server での VMware vCenter Server - tc Server 設定の構成](#)
- [vCenter Server 管理者ユーザーの設定](#)
- [vCenter Server 環境への認証](#)
- [vCenter Single Sign-On による vCenter Server の ID ソース](#)
- [ESXi 証明書とキー ファイルのリストア](#)
- [別の外部 Platform Services Controller への vCenter Server の再ポイント](#)
- [組み込み Platform Services Controller を使用するスタンドアロン vCenter Server の、外部 Platform Services Controller を使用する vCenter Server への再構成](#)
- [組み込み Platform Services Controller を使用する vCenter Server の複数の参加済みインスタンスの、外部 Platform Services Controller を使用する vCenter Server への再構成](#)

vCenter Server アップグレード後のコンポーネントの構成

構成に適用するアップグレード後のオプションと要件を完了させます。

アップグレード前にローカル Auto Deploy サービスを vCenter Server に登録していた場合、そのサービスは自動的にアップグレードされ、場所の変更はありません。アップグレード前にリモート Auto Deploy サービスを vCenter Server に登録していた場合、そのサービスは、アップグレード時に vCenter Server がインストールされているマシンに移行されます。

アップグレード前に vSphere Web Client サービスを vCenter Server に登録していた場合、そのサービスは自動的にアップグレードされ、場所の変更はありません。アップグレード前にリモート vSphere Web Client を vCenter Server に登録していた場合、そのサービスは、アップグレード時に vCenter Server がインストールされているマシンに移行されます。

アップグレード中に vCenter Server の物理サーバまたは仮想マシンに移行される、以前に分散されたコンポーネント サービスの再ポイントについては、[アップグレード後の移行された vCenter Server サービスの再構成](#)を参照してください。

ホスト上の vSphere HA を構成するには、SSL 証明書のチェックが必要です。

手順

- 1 ライセンス ポータルにアクセスするには、当社の Web サイトでアカウント ページにログインします。ライセンス ポータルで、vCenter Server ライセンスをアップグレードします。vSphere Web Client を使用して、アップグレードしたライセンス キーを vCenter Server ホストに割り当てます。
- 2 Oracle データベースでは、Oracle JDBC Driver (ojdbc14.jar または ojdbc5.jar) を [VMware vCenter Server]\tomcat\lib フォルダにコピーします。
- 3 Microsoft SQL Server データベースでは、アップグレードのバルク ログが有効な場合はアップグレードの完了後に無効にします。
- 4 vSphere HA クラスタが存在する場合、SSL 証明書の確認を有効にする必要があります。

アップグレード時に証明書のチェックが有効になっていないと、vSphere HA はホストでの構成に失敗します。

- a インベントリ パネルで vCenter Server インスタンスを選択します。
- b [管理] タブ、[全般] サブタブの順に選択します。
- c [SSL 設定] フィールドが [vCenter には検証済みのホスト SSL 証明書が必要です] に設定されていることを確認します。

アップグレード後の移行された vCenter Server サービスの再構成

以前に vCenter Server とは別にデプロイされた vCenter Server 5.x サービスは、アップグレード プロセスで vCenter Server システムに移行された後、再構成が必要になることがあります。

vCenter Server コンポーネントは個別にデプロイできなくなりました。vCenter Server 5.x のコンポーネントが以前に vCenter Server システムとは異なるシステムにデプロイされていた場合、それらのコンポーネントはアップグレード ソフトウェアによって vCenter Server システムに移行されます。場合によっては、移行されたサービスで再ポイントなどのアクションが必要になることがあります。

LogInsight や Splunk などの外部レシーバにログのリモート リレーを行う vCenter Server Appliance 5.5 インスタンスの場合、アップグレード ソフトウェアは vCenter Server Appliance 6.0 に含まれている VMware Syslog サービスにリレー構成を移行します。

バージョンが混在した環境でアップグレードを行う場合、vCenter Single Sign-On インスタンスを使用していた vCenter Server 5.x インスタンスは影響を受けません。それらのインスタンスは、アップグレード前と同様に、アップグレードされた Platform Services Controller インスタンスと連携し続け、問題が発生したり、更新が必要になったりすることはありません。vCenter Server 5.5 インスタンスはバージョン 5.5 の vSphere Web Client からは引き続き認識されますが、バージョン 6.0 の vSphere Web Client インスタンスからは認識されません。[vCenter Server のアップグレード時のバージョン混在の移行環境](#) を参照してください。

手順

- 1 vSphere Auto Deploy サービスが以前 vCenter Server とは別のマシンにインストールされていて、アップグレード プロセスで再配置された場合は、再配置された vSphere Auto Deploy サービスを参照するように DHCP 設定と TFTP 設定を更新します。
 - a `deploy-tftp.zip` をダウンロードし、tftp ルート フォルダを置き換えます。
構成は TFTP クライアントに基づいて変えることができます。
 - b アップグレードされた vSphere Auto Deploy サービスとその `.tramp` ファイルを使用するように DHCP `.conf` ファイルを構成し直します。
構成は DHCP 設定に基づいて変えることができます。
- 2 vSphere Web Client が以前 vCenter Server とは別のマシンにインストールされていて、アップグレード プロセスで再配置された場合は、新しい場所を参照するように FQDN と IP アドレスを更新します。
- 3 VMware vSphere Syslog Collector が以前 vCenter Server とは別のマシンにインストールされていた場合、vSphere Syslog Collector サーバの新しい場所（新たにアップグレードされた Windows 版 vCenter Server 6.0）に ESXi ホストを再ポイントします。
- 4 vSphere ESXi Dump Collector サーバが以前 vCenter Server とは別のマシンにインストールされていた場合、vSphere ESXi Dump Collector サーバの新しい場所に ESXi ホストを再ポイントします。
- 5 アップグレードされた vCenter Server Appliance 内の vSphere Syslog サービスにログのリモート リレーの構成変更を適用するには、6.0 へのアップグレードが完了した直後にこのサービスを再起動します。
- 6 バージョン 5.5 と 6.0 が混在した暫定的な環境が続いている間にまだアップグレードされていない vCenter Server 5.5 インスタンスを表示するには、レガシー vSphere Web Client を再起動します。
- 7 vCenter Server 5.x サービスのいずれかが別の仮想マシンまたは物理サーバでまだ実行されている場合は、それらを停止して削除できます。
それらは vCenter Server 6.0 では使用されません。

vSphere Authentication Proxy のインストールまたはアップグレード

vSphere Authentication Proxy をインストールすると、Active Directory の認証情報を使用せずに ESXi ホストをドメインに参加させることができます。vSphere Authentication Proxy は、ホスト構成に Active

Directory の認証情報を保存する必要をなくすことにより、PXE 起動のホストや、Auto Deploy を使用してプロビジョニングされるホストのセキュリティを強化します。

お使いのシステムに vSphere Authentication Proxy の以前のバージョンがインストールされている場合、この手順を実行することで vSphere Authentication Proxy が最新のバージョンにアップグレードされます。

vSphere Authentication Proxy は、関連付けられた vCenter Server と同じマシンか、vCenter Server にネットワーク接続できる別のマシンにインストールできます。vSphere Authentication Proxy は、バージョン 5.0 以降の vCenter Server でサポートされています。

vSphere Authentication Proxy サービスは、vCenter Server との通信のために IPv4 アドレスに拘束され、IPv6 はサポートされません。vCenter Server インスタンスは、IPv4 のみ、IPv4/IPv6 混在モード、または IPv6 のみのネットワーク環境内のホスト マシンにインストールできますが、vSphere Web Client 経由で vCenter Server に接続するマシンで vSphere Authentication Proxy サービスを機能させるには、IPv4 アドレスを使用する必要があります。

前提条件

- vSphere Authentication Proxy をインストールするマシンに、Microsoft .NET Framework 3.5 をインストールします。
- 管理者権限があることを確認します。
- ホスト マシンに、サポートされているプロセッサおよびオペレーティング システムがあることを確認します。
- ホスト マシンに有効な IPv4 アドレスがあることを確認します。vSphere Authentication Proxy は、ネットワーク環境が IPv4 のみのマシンまたは IPv4/IPv6 混合モードのマシンにインストールできますが、IPv6 のみの環境内のマシンにはインストールできません。
- vSphere Authentication Proxy を Windows Server 2008 R2 ホスト マシンにインストールする場合は、support.microsoft.com Web サイトにある Windows のナレッジ ベースの記事 981506 で説明されている、Windows のホットフィックスをダウンロードしてインストールします。このホットフィックスがインストールされていないと、vSphere Authentication Proxy Adapter の初期化に失敗します。この問題が発生すると、「Failed to bind CAM website with CTL」および「Failed to initialize CAMAdapter」に類似したエラー メッセージが camadapter.log に表示されます。
- vCenter Server のインストーラをダウンロードします。

次の情報を収集してインストールまたはアップグレードを完了します。

- vSphere Authentication Proxy をインストールする場所（デフォルトの場所を使用しない場合）。
- vSphere Authentication Proxy が接続する vCenter Server のアドレスおよび認証情報：IP アドレスまたは名前、HTTP ポート、ユーザー名、およびパスワード。
- vSphere Authentication Proxy をネットワーク上で識別するためのホスト名または IP アドレス。

手順

- 1 認証プロキシ サービスをインストールするホスト マシンをドメインに追加します。
- 2 ドメイン管理者のアカウントを使用して、ホスト マシンにログインします。

- 3 ソフトウェアのインストール ディレクトリで `autorun.exe` ファイルをダブルクリックし、インストーラーを起動します。
- 4 [VMware vSphere Authentication Proxy] を選択し、[インストール] をクリックします。
- 5 ウィザードの指示に従って、インストールまたはアップグレードを完了します。

インストール中、認証サービスは、Auto Deploy が登録されている vCenter Server インスタンスに登録されます。

結果

vSphere Authentication Proxy サービスのインストール時、インストーラにより、認証プロキシ サービスを実行するために適切な権限のあるドメイン アカウントが作成されます。アカウント名は接頭辞 `CAM-` で始まり、32 文字で構成されます。また、ランダムに生成されたパスワードが関連付けられます。パスワードは、期限なしで設定されます。アカウントの設定は変更しないでください。

次のステップ

vSphere Authentication Proxy を使用してドメインに参加するように ESXi を構成します。『vSphere セキュリティ』ドキュメントを参照してください。

vSphere Client へのアップグレード

仮想マシンのユーザーと vCenter Server の管理者は、vSphere Client 6.0 を使用して vCenter Server 6.0 に接続するか、ESXi 6.0 のホストに直接接続する必要があります。

VI Client 2.5、vSphere Client 4.x、vSphere Client 5.x、および vSphere Client 6.0 を同じマシンにインストールすることができます。vCenter Server のアップグレード後には、vSphere Client の動作を妨げる可能性がある互換性の問題を避けるため、vSphere Client を同じバージョンにアップグレードしてください。

vSphere Client のアップグレード作業にダウンタイムは必要ありません。仮想マシンやクライアントをパワーオフする必要はありません。

前提条件

- vCenter Server インストーラまたは vSphere Client インストーラがあることを確認します。
- システムの管理者グループのメンバーであることを確認します。
- システムがインターネットに接続できることを確認します。

手順

- 1 (オプション) Windows のコントロール パネルの [プログラムの追加と削除] を使用して、以前の vCenter Server のクライアントを削除します。

以前のバージョンの vCenter Server クライアントを削除する必要はありません。これらのバージョンは、レガシー ホストに接続する必要がある場合に役立ちます。

2 vSphere Client インストーラを実行します。

- vCenter Server のインストーラを起動します。ソフトウェアのインストーラ ディレクトリで、`autorun.exe` ファイルをダブルクリックし、[vSphere Client][] を選択します。
- vSphere Client をダウンロードする場合は、`VMware-viclient-build number.exe` ファイルをダブルクリックします。

結果

vSphere Client 6.0 をインストールしたら、ESXi ホストのドメイン名または IP アドレスと、そのマシンのユーザーのユーザー名およびパスワードを使用して、ESXi ホストに接続できます。

次のステップ

vSphere Client を使用して、自分のユーザー名およびパスワードで ESXi ホストに直接接続します。

ログインするとき、またはいくつかの操作を行なったときに vSphere Client でセキュリティ警告や例外が表示される場合は、IE (Internet Explorer) のセキュリティ設定が「高」に設定されている可能性があります。たとえば、パフォーマンス チャートを開いたり、[サマリ] タブを表示したりする場合に、セキュリティ設定が「高」に設定されます。IE のセキュリティ設定が高に設定されている場合は、IE の [Internet Explorer WebBrowser コントロールのスクリプトの実行] 設定を有効にします。

vCenter Server での VMware vCenter Server - tc Server 設定の構成

vCenter Server 5.1 以降では、Windows ユーザー インターフェイスから VMware Tomcat Server 設定を構成できなくなりました。vCenter Server 5.1 以降では、Apache Tomcat 7 のエンタープライズバージョンである VMware vCenter Server - tc Server が使用されます。Tomcat バージョン 7 では、Windows ユーザー インターフェイスでコントロール パネルが表示されません。代わりに、構成ファイルを手動で編集して Tomcat を構成します。

Java オプションの設定は、次のファイルに保存されています。

- vCenter Server。インストール ディレクトリ\VMware\Infrastructure\tomcat\conf\wrapper.conf
- vCenter Inventory Service。インストール ディレクトリ\VMware\Infrastructure\Inventory Service\conf\wrapper.conf
- Profile-Driven Storage Service。インストール ディレクトリ\VMware\Infrastructure\Profile-Driven Storage\conf\wrapper.conf
- vSphere Web Client。インストール ディレクトリ\VMware\vSphereWebClient\server\bin\service\conf\wrapper.conf

表 6-1. wrapper.conf ファイルの Inventory Service および Profile-Driven Storage サービスの最大 JVM ヒープ サイズ設定

Java オプション	設定とデフォルト値
<p><code>maxmemorysize</code></p> <p>最大 JVM ヒープ サイズ (メガバイト)。この設定によって、Java ヒープの最大サイズが制御されます。このパラメータを調整すると、ガベージコレクションのオーバーヘッドを縮小して、サーバの応答時間とスループットを向上させることができます。一部のアプリケーションに対しては、このオプションのデフォルト設定は低すぎるため、マイナーなガベージコレクションの数が多くなります。</p>	<p>インベントリ サービス : <code>wrapper.java.maxmemory=2048</code></p> <p>Profile-Driven Storage サービス :</p> <p><code>wrapper.java.maxmemory=1024</code></p> <p>vSphere Web Client : 大規模なデプロイでは、このオプションを <code>wrapper.java.maxmemory=2048</code> に設定することが必要になる場合もあります。</p>
<p><code>ping.timeoutduration</code></p>	<p>vSphere Web Client : 大規模なデプロイでは、このオプションを <code>wrapper.ping.timeout=120</code> に設定することが必要になる場合もあります。</p>

vCenter Server セキュリティとポートの設定は、次のファイルに保存されています。

- インストール ディレクトリ\VMware\Infrastructure\tomcat\conf\server.xml
- インストール ディレクトリ\VMware\Infrastructure\tomcat\conf\catalina.properties

表 6-2. server.xml および catalina.properties ファイルの vCenter Server のポートとセキュリティの設定

vCenter Server のポートまたはセキュリティの設定	設定とデフォルト値
ベースのシャットダウン ポート	<code>base.shutdown.port=8003</code>
<p>ベースの JMX ポート</p> <p><code>com.springsource.tcserver.serviceability.rmi.JmxSocketListener</code> クラスによって実装されるリスナーは tc Server に対して固有です。このリスナーによって、tc Server の JMX 管理が有効になり、また、このリスナーは tc Server のインスタンスを管理するために AMS 管理コンソールが使用する JMX 構成です。このポート属性は、AMS などの管理製品が接続する JMX サーバのポートを指定します。デフォルトの <code>catalina.properties</code> ファイルでは、<code>\$ {jmx.port}</code> 変数が 6969 に設定されます。このバインド属性は JMX サーバのホストを指定します。デフォルトでは、この属性は <code>localhost (127.0.0.1)</code> に設定されています。</p> <p>デフォルト設定の -1 ではポートが無効になります。</p>	<code>base.jmx.port=-1</code>
Web サービス HTTPS	<code>bio-vmsl.http.port=8080</code>
Web サービス HTTPS	<code>bio-vmsl.https.port=8443</code>
SSL 証明書	<code>bio-vmsl.keyFile.name=C:\ProgramData\VMware\VMware VirtualCenter\SSL\rui.pfx</code>
SSL 証明書のパスワード	<code>bio-vmsl.SSL.password=testpassword</code>

『Getting Started with vFabric tc Server』 および 『vFabric tc Server Administration』 (<https://www.vmware.com/support/pubs/vfabric-tcserver.html>) を参照してください。

[サービス] の下の [管理ツール] コントロール パネルから vCenter Server の Windows サービスを 管理することができます。vCenter Server の Windows サービスは、VMware VirtualCenter Management Webservices として表示されます。

vCenter Server のアップグレード後の最大データベース接続数の設定

vCenter Server はデフォルトで最大 50 個のデータベース接続を同時に確立します。前のバージョンの vCenter Server でこの値を 50 未満に構成したあとで vCenter Server 5.x へのアップグレードを実行した場合、アップグレードではデフォルト設定の 50 がリストアされます。前のバージョンの vCenter Server でこの値を 50 より上に設定した場合は、システム上で vCenter Server 5.x へのアップグレード後もその値が維持されます。デフォルト以外の設定を再構成できます。

vCenter Server で多数の処理が実行されることが頻繁にあり、パフォーマンスを重視する場合は、データベース接続の数を増やすことができます。データベースが共有されていて、データベースへの接続にコストがかかる場合は、この数値の減少を検討してください。システムでこれらの問題がない場合は、この値を変更しません。

この作業は、データベースの認証を構成する前に行います。認証の構成については、データベースのドキュメントを参照してください。

手順

- 1 vSphere Web Client から vCenter Server に接続します。
- 2 インベントリで vCenter Server を選択します。
- 3 [管理] タブをクリックします。
- 4 [設定] を選択します。
- 5 [全般] を選択します。
- 6 [Edit] をクリックします。
- 7 [データベース] を選択します。
- 8 必要に応じて [最大接続数] の値を変更します。
- 9 [OK] をクリックします。
- 10 vCenter Server を再起動します。

結果

新しいデータベース設定が有効になります。

vCenter Server 管理者ユーザーの設定

vCenter Server 管理者ユーザーの設定方法は、vCenter Single Sign-On のデプロイ状況によって異なります。

vSphere 5.1 よりも前のバージョンの vSphere では、vCenter Server 管理者は、ローカルのオペレーティングシステムの管理者グループに属するユーザーになります。

vSphere 5.1.x、5.5、および 6.0 では、vCenter Server のインストール時に、デフォルト（初期） vCenter Server 管理者ユーザーまたはグループを設定する必要があります。vCenter Server および vCenter Single Sign-On が同じ仮想マシンまたは物理サーバにデプロイされる場合、ローカルのオペレーティング システムの「管理者」グループを vCenter Server 管理ユーザーとして指定できます。このオプションがデフォルトになります。この動作は vCenter Server 5.0 から変更されていません。

より大規模なインストールの場合で、vCenter Single Sign-On が異なる仮想マシンまたは物理サーバにデプロイされた Platform Services Controller および vCenter Server の一部となると、vCenter Server 5.0 と同様の動作を維持することはできません。代わりに、vCenter Server 管理者ロールを、Active Directory、OpenLDAP、またはシステム アイデンティティ ソースの vCenter Single Sign-On サーバに登録されているユーザーまたはグループに割り当てます。

vCenter Server 環境への認証

vCenter Server バージョン 5.1 以降では、vCenter Single Sign-On を通じてユーザー認証を行います。

vCenter Server 5.1 より前の vCenter Server バージョンでは、ユーザーが vCenter Server に接続する際に、vCenter Server は Active Directory ドメインまたはローカルのオペレーティング システム ユーザーのリストでユーザーを検証することで、ユーザーの認証を行います。

administrator@*your_domain_name* のユーザーには、デフォルトで vCenter Single Sign-On 管理者権限が付与されています。administrator@*your_domain_name* のユーザーが、vSphere Web Client から vCenter Single Sign-On サーバにログインすると、vCenter Single Sign-On 管理者権限を他のユーザーに割り当てることができます。これらのユーザーは、vCenter Server を管理するユーザーと異なる場合があります。

ユーザーは vSphere Web Client を使用して、vCenter Server にログインできます。ユーザーが vCenter Single Sign-On に認証されます。ユーザーは、権限を持つすべての vCenter Server インスタンスを表示できます。ユーザーが vCenter Server に接続した後は、追加の認証は必要ありません。オブジェクトに対してユーザーが実行できるアクションは、それらのオブジェクトに対するユーザーの vCenter Server 権限によって異なります。

vCenter Single Sign-On の詳細については、vSphere セキュリティ を参照してください。

vCenter Single Sign-On による vCenter Server の ID ソース

アイデンティティ ソースを使用して、vCenter Single Sign-On に 1 つ以上のドメインを添付できます。ドメインは vCenter Single Sign-On サーバがユーザー認証に使用できるユーザーまたはグループのリポジトリです。

ID ソースは、ユーザーおよびグループデータの集合体です。ユーザーおよびグループのデータは、Active Directory、OpenLDAP、またはローカルで vCenter Single Sign-On がインストールされたマシンのオペレーティング システムに格納されます。

インストールが完了すると、vCenter Single Sign-On のすべてのインスタンスに *your_domain_name* のアイデンティティ ソース (vsphere.local など) があります。このアイデンティティ ソースは vCenter Single Sign-On の内部のもので、vCenter Single Sign-On 管理者は、アイデンティティ ソースを追加したり、デフォルトのアイデンティティ ソースを設定したり、vsphere.local アイデンティティ ソースのユーザーおよびグループを作成したりできます。

ID ソースのタイプ

バージョン 5.1 より前の vCenter Server バージョンは、Active Directory およびローカル オペレーティング システムのユーザーをユーザー リポジトリとしてサポートしていました。このため、ローカル オペレーティング システムのユーザーは常に vCenter Server システムから認証可能でした。vCenter Server バージョン 5.1 およびバージョン 5.5 では、認証に vCenter Single Sign-On を使用します。vCenter Single Sign-On 5.1 がサポートしているアイデンティティソースのリストについては、vSphere 5.1 のドキュメントを参照してください。

vCenter Single Sign-On 5.5 は以下のタイプのユーザー リポジトリをアイデンティティ ソースとしてサポートしていますが、デフォルトでサポートするアイデンティティ ソースは 1 つだけです。

- Active Directory バージョン 2003 以降。vSphere Web Client では、[Active Directory (統合 Windows 認証)] として表示されます。vCenter Single Sign-On では単一の Active Directory ドメインをアイデンティティ ソースとして指定できます。ドメインは、子ドメインを持たせたり、フォレスト ルート ドメインにしたりできます。VMware のナレッジベースの記事 [2064250](#) に、vCenter Single Sign-On でサポートされている Microsoft Active Directory の信頼関係についての解説があります。
- LDAP を用いた Active Directory。vCenter Single Sign-On は LDAP を用いた Active Directory の複数のアイデンティティ ソースをサポートします。このアイデンティティ ソース タイプは、vSphere 5.1 とともに含まれる vCenter Single Sign-On サービスとの互換性のために含まれています。vSphere Web Client に [LDAP サーバとしての Active Directory] として表示されます。
- OpenLDAP バージョン 2.4 以降。vCenter Single Sign-On は複数の OpenLDAP アイデンティティ ソースをサポートします。vSphere Web Client では、[OpenLDAP] として表示されます。
- ローカル オペレーティング システム ユーザー。ローカル オペレーティング システム ユーザーは、vCenter Single Sign-On サーバが実行されているオペレーティング システムのローカル ユーザーです。ローカル オペレーティング システムのアイデンティティ ソースは、基本的な vCenter Single Sign-On サーバの展開にのみ使用でき、複数の vCenter Single Sign-On インスタンスを用いた展開では使用できません。1 つのローカル オペレーティング システム アイデンティティ ソースのみが許可されます。vSphere Web Client では、[localos] として表示されます。

注： Platform Services Controller が vCenter Server システムと異なるマシン上に存在する場合は、ローカル オペレーティング システムのユーザーを使用しないでください。組み込みデプロイでローカル オペレーティング システムのユーザーを使用するのは理にかなっていますが、お勧めしません。

- vCenter Single Sign-On のシステム ユーザー。vCenter Single Sign-On のインストール時に、vsphere.local という名前のただ 1 つのシステム アイデンティティ ソースが作成されます。vSphere Web Client では、[vsphere.local] として表示されます。

注： いかなる場合でも、デフォルトのドメインが 1 つだけ存在します。ユーザーがデフォルト以外のドメインからログインした場合、このユーザーが正常に認証されるためにはドメイン名 (*DOMAIN/user*) を追加する必要があります。

vCenter Single Sign-On のアイデンティティ ソースは vCenter Single Sign-On 管理者ユーザーが管理します。

アイデンティティ ソースは vCenter Single Sign-On サーバ インスタンスに追加できます。リモートのアイデンティティ ソースは、Active Directory および OpenLDAP のサーバ実装に限定されます。

vCenter Single Sign-On の詳細については、『vSphere セキュリティ』を参照してください。

ESXi 証明書とキー ファイルのリストア

vSphere Web Services SDK を使用して ESXi ホストの証明書を置き換えると、以前の証明書とキーが .bak ファイルに追加されます。.bak ファイルの情報を現在の証明書とキー ファイルに移動すれば、以前の証明書をリストアできます。

ホストの証明書とキーは /etc/vmware/ssl/rui.crt と /etc/vmware/ssl/rui.key にあります。vSphere Web Services SDK の vim.CertificateManager 管理対象オブジェクトを使用してホストの証明書とキーを置き換えると、以前のキーと証明書が /etc/vmware/ssl/rui.bak ファイルに追加されます。

注： HTTP PUT、vifs、または ESXi Shell を使用して証明書を置き換えると、既存の証明書は .bak ファイルに追加されません。

手順

- 1 ESXi ホストで、/etc/vmware/ssl/rui.bak ファイルを探します。

ファイルの形式は次のようになります。

```
## Host private key and certificate backup from 2014-06-20 08:02:49.961#-----BEGIN PRIVATE
KEY-----
previous key
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
previous cert
-----END CERTIFICATE-----
```

- 2 -----BEGIN PRIVATE KEY----- から -----END PRIVATE KEY----- までのテキストを /etc/vmware/ssl/rui.key ファイルにコピーします。

-----BEGIN PRIVATE KEY----- および -----END PRIVATE KEY----- も含めます。

- 3 -----BEGIN CERTIFICATE----- から -----END CERTIFICATE----- までのテキストを /etc/vmware/ssl/rui.crt ファイルにコピーします。

-----BEGIN CERTIFICATE----- および -----END CERTIFICATE----- も含めます。

- 4 ホストを再起動するか、キーを使用するすべてのサービスに ssl_reset イベントを送信します。

```
for s in /etc/init.d/*; do $s | grep ssl_reset > /dev/null; if [ $? == 0 ]; then $s
ssl_reset; fi; done
```

別の外部 Platform Services Controller への vCenter Server の再ポイント

同一の vCenter Single Sign-On ドメインに外部 Platform Services Controller インスタンスを追加することにより、システムの高可用性が確保されます。

外部 Platform Services Controller の応答が停止している場合、または外部 Platform Services Controller のロードを分散させる必要がある場合は、vCenter Server インスタンスを、同じドメインおよびサイト内の他の Platform Services Controller に再ポイントします。

- vCenter Server インスタンスを再ポイントできるのは、同じドメインおよびサイト内の空き容量があり正常に稼動している既存の Platform Services Controller インスタンスです。
- 同じドメインおよびサイトに新しい Platform Services Controller インスタンスをインストールまたはデプロイし、そのインスタンスに vCenter Server インスタンスを再ポイントすることもできます。

前提条件

- 古い Platform Services Controller インスタンスが応答しなくなった場合は、`cmsso-util unregister` コマンドでノードの削除と古い `vmdir` データのクリーンアップを実行します。Platform Services Controller インスタンスの廃止については、<https://kb.vmware.com/kb/2106736> を参照してください。
- `vdcrepadmin -f showservers` コマンドを実行して、すべての Platform Services Controller インスタンス（古いインスタンス、新しいインスタンスを含む）が、同じ vCenter Single Sign-On ドメインおよびサイトに含まれていることを確認します。このコマンドの使用方法については、<https://kb.vmware.com/kb/2127057> を参照してください。

手順

- 1 vCenter Server インスタンスにログインします。
 - vCenter Server Appliance の場合、`root` として vCenter Server Appliance シェルにログインします。
 - Windows 上の vCenter Server インスタンスの場合、管理者として vCenter Server 仮想マシンまたは物理サーバにログインします。
- 2 vCenter Server インスタンスが Windows で実行されている場合は、Windows コマンド プロンプトで、`C:\Program Files\VMware\VCServer\bin` に移動します。
- 3 `cmsso-util repoint` コマンドを実行します。

```
cmsso-util repoint --repoint-psc psc_fqdn_or_static_ip [--dc-port port_number]
```

角括弧 [] でコマンドのオプションを囲みます。

ここでの `psc_fqdn_or_static_ip` は、Platform Services Controller を特定するために使用するシステム名です。このシステム名は、FQDN または固定 IP アドレスにする必要があります。

注： FQDN 値は大文字と小文字を区別します。

Platform Services Controller がカスタム HTTPS ポートで実行される場合は、`--dc-port port_number` オプションを使用します。HTTPS ポートのデフォルト値は 443 です。

- 4 vSphere Web Client を使用して vCenter Server インスタンスにログインし、vCenter Server が実行中であり管理可能であることを確認します。

結果

vCenter Server インスタンスが新しい Platform Services Controller に登録されます。

組み込み Platform Services Controller を使用するスタンドアロン vCenter Server の、外部 Platform Services Controller を使用する vCenter Server への再構成

組み込み Platform Services Controller を使用するスタンドアロン vCenter Server を展開またはインストールしており、vCenter Single Sign-On ドメインに vCenter Server インスタンスを追加して拡張しようとしている場合、既存の vCenter Server インスタンスを再構成し、外部 Platform Services Controller に再ポイントできます。

図 6-1. 組み込み Platform Services Controller を使用するスタンドアロン vCenter Server インスタンスの再構成および外部 Platform Services Controller へのそのインスタンスの再ポイント

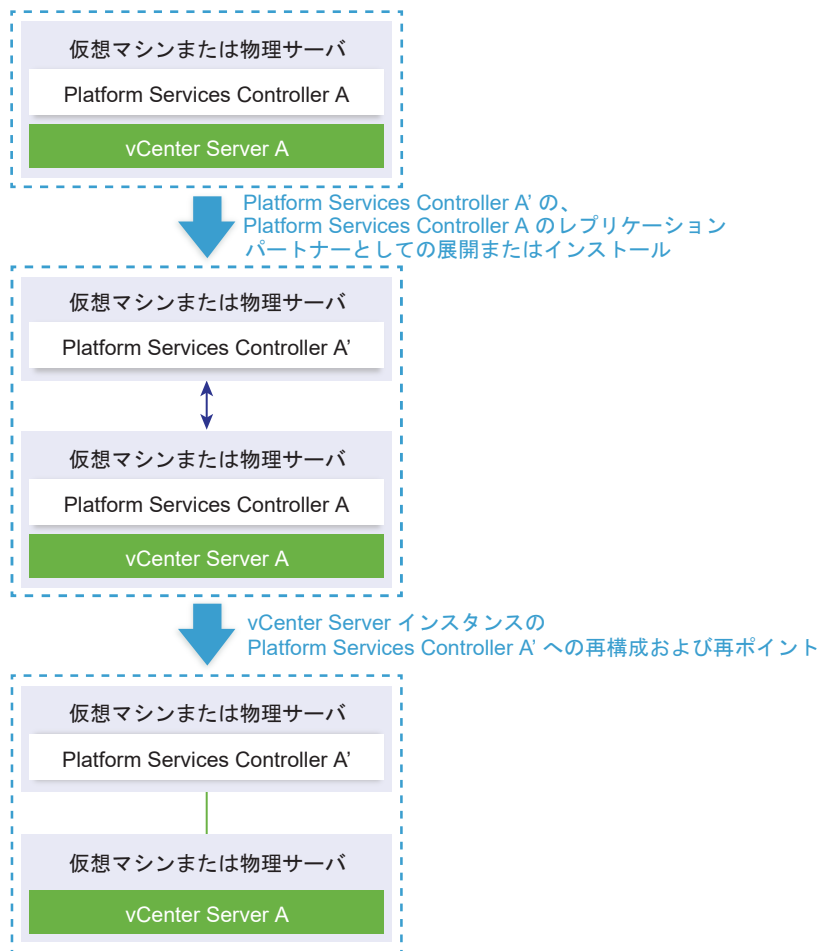


表 6-3. 凡例

矢印または直線	説明
	2 つの Platform Services Controller インスタンスの間のレプリケーション関係
	外部 Platform Services Controller を使用する vCenter Server の登録
	移行手順

注： 組み込み Platform Services Controller を使用する vCenter Server インスタンスを再構成し、このインスタンスを外部 Platform Services Controller インスタンスに再ポイントする処理は、実行後は組み込み Platform Services Controller を使用する vCenter Server に戻すことはできない、一方向の処理です。

前提条件

- 外部 Platform Services Controller インスタンスを、同じ vCenter Single Sign-On サイト内の既存の組み込み Platform Services Controller インスタンスのレプリケーション パートナーとして展開またはインストールします。

注： 現在の vCenter Single Sign-On サイトは、vmfad-cli コマンドを使用することで特定できます。

- 組み込み Platform Services Controller を使用する vCenter Server Appliance の場合、root として アプライアンス シェルにログインし、コマンドを実行します。

```
/usr/lib/vmware-vmafd/bin/vmafd-cli get-site-name --server-name localhost
```

- 組み込み Platform Services Controller を使用する vCenter Server インスタンスの Windows インストールの場合、管理者として Windows マシンにログインし、Windows コマンド プロンプトを開き、コマンドを実行します。

```
C:\Program Files\VMware\vCenter Server\vmafdd\vmafd-cli get-site-name --server-name localhost
```

- 組み込み Platform Services Controller を使用する vCenter Server と外部 Platform Services Controller インスタンスのスナップショットを作成しておくことで、再構成に失敗したときに、そのスナップショットに戻せるようにします。

手順

- 1 組み込み Platform Services Controller を使用する vCenter Server インスタンスにログインします。

オプション	手順
組み込み Platform Services Controller を使用する vCenter Server Appliance の場合	<p>アプライアンス シェルに root としてログインします。</p> <ul style="list-style-type: none"> ■ アプライアンス コンソールに直接アクセスできる場合は、Alt+F1 を押します。 ■ リモート接続する場合は、SSH などのリモート コンソール接続を使用して、アプライアンスへのセッションを開始します。
組み込み Platform Services Controller を使用する vCenter Server の Windows インストール環境の場合	Windows マシンに管理者としてログインします。

- 2 すべての Platform Services Controller サービスが実行されていることを確認します。

オプション	手順
組み込み Platform Services Controller を使用する vCenter Server Appliance の場合	<code>service-control --status --all</code> コマンドを実行します。
組み込み Platform Services Controller を使用する vCenter Server の Windows インストール環境の場合	[スタート] - [コントロール パネル] - [管理ツール] - [サービス] を選択します。

稼働していなければならない Platform Services Controller サービスとして、VMware License Service、VMware Identity Management Service、VMware Security Token Service、VMware Certificate Service、および VMware Directory Service があります。

- 3 組み込み Platform Services Controller インスタンスを使用する vCenter Server が Windows で実行されている場合、Windows コマンド プロンプトを開き、`C:\Program Files\VMware\vCenter Server\bin` に移動します。

- 4 `cmsso-util reconfigure` コマンドを実行します。

```
cmsso-util reconfigure --repoint-psc psc_fqdn_or_static_ip --username username --domain-name domain_name --passwd password [--dc-port port_number]
```

ここで、角括弧 [] で囲まれているのはオプションの項目です。

ここでの `psc_fqdn_or_static_ip` は、外部 Platform Services Controller インスタンスを特定するために使用するシステム名です。このシステム名は、FQDN または固定 IP アドレスにする必要があります。

注： FQDN 値は大文字と小文字を区別します。

`username` オプションと `password` オプションは、vCenter Single Sign-On `domain_name` の管理者ユーザー名とパスワードです。

カスタムの HTTPS ポートで外部 Platform Services Controller が稼働している場合は、`--dc-port` オプションを使用します。HTTPS ポートのデフォルト値は 443 です。

たとえば、外部 Platform Services Controller がカスタムの HTTPS ポート 449 番で稼働している場合は、次のオプションを指定して実行する必要があります。

```
cmsso-util reconfigure --repoint-psc psc.acme.local --username administrator --domain-name vsphere.local --passwd Password1! --dc-port 449
```

- 5 vSphere Web Client を使用して vCenter Server インスタンスにログインし、vCenter Server が実行中であり管理可能であることを確認します。

結果

組み込み Platform Services Controller を使用する vCenter Server が降格され、vCenter Server が外部 Platform Services Controller にリダイレクトされます。

次のステップ

追加の vCenter Server および Platform Services Controller インスタンスを vCenter Single Sign-On ドメインに展開またはインストールできます。

組み込み Platform Services Controller を使用する vCenter Server の複数の参加済みインスタンスの、外部 Platform Services Controller を使用する vCenter Server への再構成

組み込み Platform Services Controller を使用する vCenter Server の参加済みインスタンスが 2 つ以上展開またはインストールされている場合、参加済み外部 Platform Services Controller インスタンスを使用する複数の vCenter Server インスタンスとして、それらを再構成できます。

図 6-2. 2 つの vCenter Single Sign-On サイトにまたがる、組み込み Platform Services Controller を使用する 3 つの参加済み vCenter Server インスタンスの再構成例

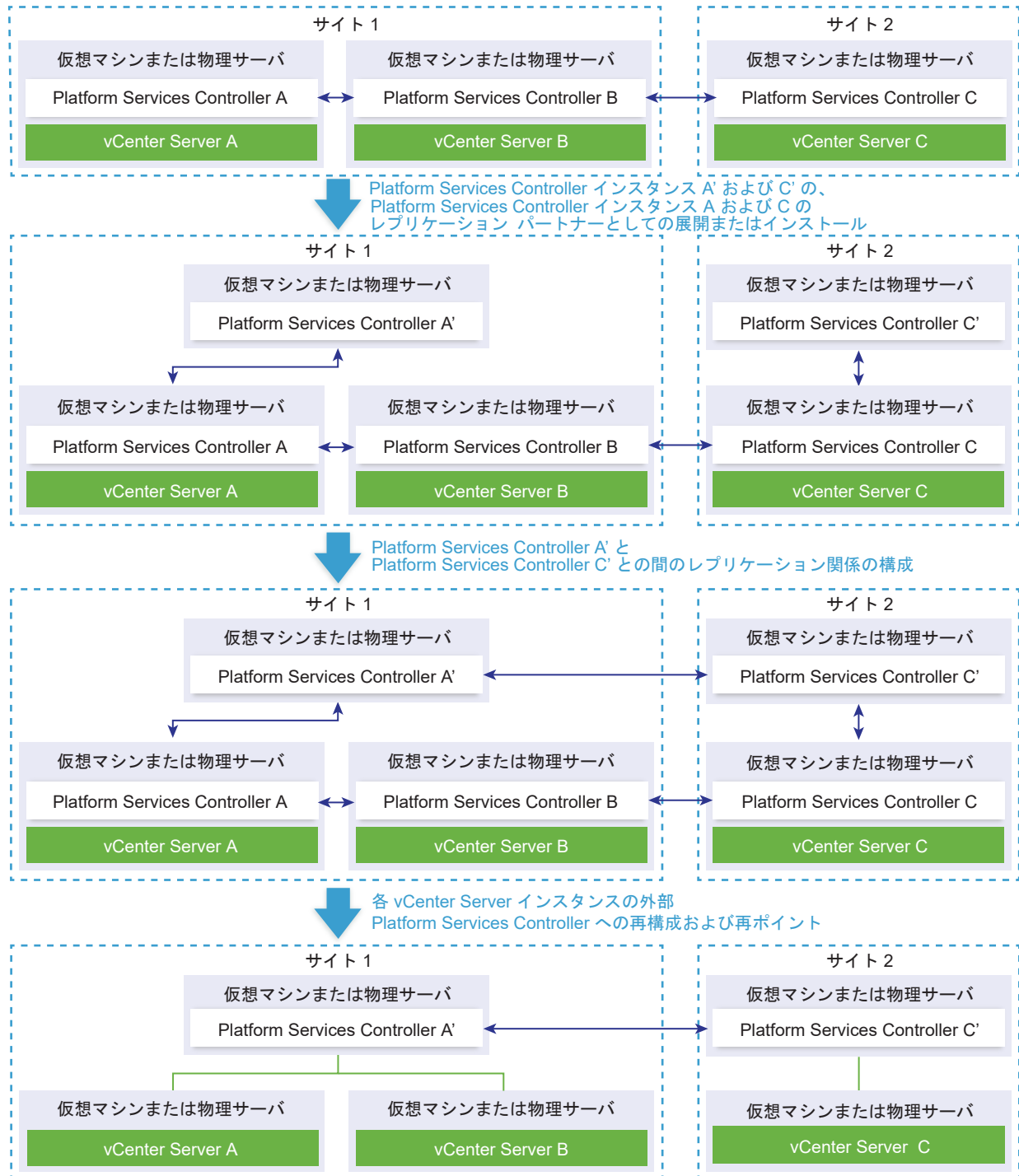


表 6-4. 凡例

矢印または直線	説明
	2 つの Platform Services Controller インスタンスの間のレプリケーション関係
	外部 Platform Services Controller を使用する vCenter Server の登録
	移行手順

注： 組み込み Platform Services Controller を使用する vCenter Server インスタンスを再構成し、このインスタンスを外部 Platform Services Controller インスタンスに再ポイントする処理は、実行後は組み込み Platform Services Controller を使用する vCenter Server に戻すことはできない、一方向の処理です。

前提条件

- 各 vCenter Single Sign-On サイトについて、このサイトからの既存の組み込み Platform Services Controller インスタンスのレプリケーション パートナーとして、外部 Platform Services Controller インスタンスを展開またはインストールします。

注： 現在の vCenter Single Sign-On サイトは、vmfad-cli コマンドを使用することで特定できます。

- 組み込み Platform Services Controller を使用する vCenter Server Appliance の場合、root として アプライアンス シェルにログインし、コマンドを実行します。

```
/usr/lib/vmware-vmafd/bin/vmafd-cli get-site-name --server-name localhost
```

- 組み込み Platform Services Controller を使用する vCenter Server インスタンスの Windows インストールの場合、管理者として Windows マシンにログインし、Windows コマンド プロンプトを開き、コマンドを実行します。

```
C:\Program Files\VMware\vCenter Server\vmafdd\vmafd-cli get-site-name --server-name localhost
```

- 組み込み Platform Services Controller を使用する vCenter Server インスタンスと外部 Platform Services Controller インスタンスのスナップショットを作成しておくことで、再構成に失敗したときに、そのスナップショットに戻せるようにします。

組み込み Platform Services Controller インスタンスのサービスが実行されていることの確認

組み込みから外部 Platform Services Controller に vCenter Server インスタンスが確実に再ポイントされるようにするには、既存の組み込み Platform Services Controller インスタンスのすべてのサービスが実行されている必要があります。

手順

- 1 組み込み Platform Services Controller を使用する vCenter Server インスタンスにログインします。

オプション	手順
組み込み Platform Services Controller を使用する vCenter Server Appliance の場合	<p>アプライアンス シェルに root としてログインします。</p> <ul style="list-style-type: none"> ■ アプライアンス コンソールに直接アクセスできる場合は、Alt+F1 を押します。 ■ リモート接続する場合は、SSH などのリモート コンソール接続を使用して、アプライアンスへのセッションを開始します。
組み込み Platform Services Controller を使用する vCenter Server の Windows インストール環境の場合	Windows マシンに管理者としてログインします。

- 2 すべての Platform Services Controller サービスが実行されていることを確認します。

オプション	手順
組み込み Platform Services Controller を使用する vCenter Server Appliance の場合	<code>service-control --status --all</code> コマンドを実行します。
組み込み Platform Services Controller を使用する vCenter Server の Windows インストール環境の場合	[スタート] - [コントロール パネル] - [管理ツール] - [サービス] を選択します。

稼働していなければならない Platform Services Controller サービスとして、VMware License Service、VMware Identity Management Service、VMware Security Token Service、VMware Certificate Service、および VMware Directory Service があります。

- 3 組み込み Platform Services Controller を使用する各 vCenter Server インスタンスについて、この手順を繰り返します。

すべての外部 Platform Services Controller インスタンスの間のレプリケーション関係の構成

各 vCenter Single Sign-On サイト内に外部レプリケーション Platform Services Controller インスタンスを展開またはインストール後、すべての外部 Platform Services Controller インスタンスをレプリケーション関係に参加させる必要があります。

図 6-3. 異なる vCenter Single Sign-On サイトでの 2 つの外部 Platform Services Controller インスタンス間のレプリケーション関係の構成例

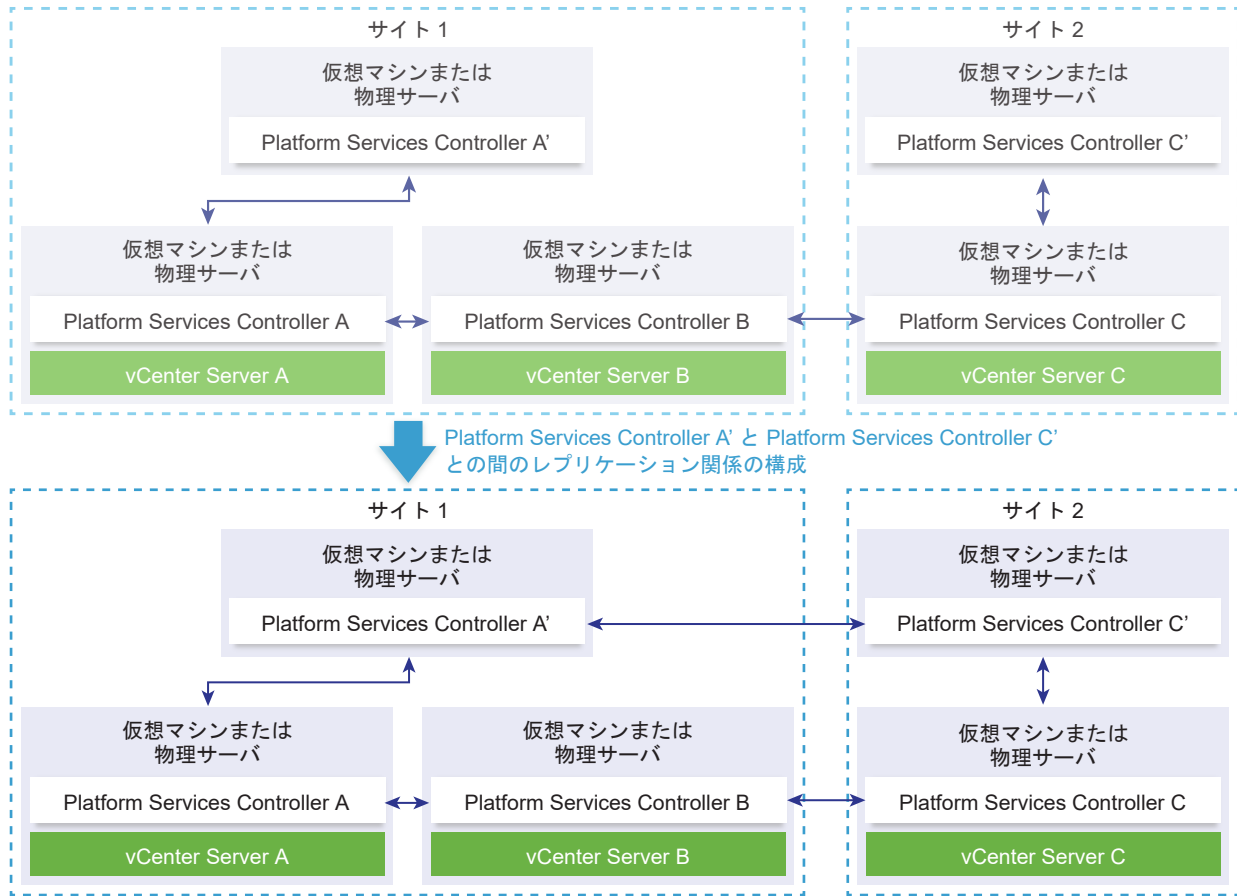


表 6-5. 凡例

矢印または直線	説明
	2 つの Platform Services Controller インスタンスの間のレプリケーション関係
	外部 Platform Services Controller を使用する vCenter Server の登録
	移行手順

2 つの Platform Services Controller インスタンス間のレプリケーション関係を構成するには、vCenter Server のいずれか、または vCenter Single Sign-On ドメインからの Platform Services Controller インスタンスのいずれかへの接続を使用できます。

手順

- 1 vCenter Server または vCenter Single Sign-On ドメインからの Platform Services Controller インスタンスに接続します。

オプション	手順
vCenter Server Appliance または Platform Services Controller アプライアンスに接続する場合	<p>アプライアンス Bash シェルに root としてログインします。</p> <ol style="list-style-type: none"> 1 アプライアンス シェルへのログイン <ul style="list-style-type: none"> ■ アプライアンス コンソールに直接アクセスできる場合は、Alt+F1 を押します。 ■ リモート接続する場合は、SSH などのリモート コンソール接続を使用して、アプライアンスへのセッションを開始します。 2 Bash シェルの有効化 <pre>shell.set --enabled true</pre> 3 shell コマンドを実行します。
vCenter Server の Windows インストールまたは Platform Services Controller に接続する場合	<p>管理者として Windows マシンにログインし、Windows コマンド プロンプトを開きます。</p>

- 2 showpartners パラメータを使用し、1 つの外部 Platform Services Controller インスタンスに対して vdcleanup コマンドを実行します。

vCenter Single Sign-On ドメイン内の Platform Services Controller インスタンスの他の Platform Services Controller インスタンスとの間の既存のパートナー関係を特定します。

- vCenter Server Appliance または Platform Services Controller アプライアンスへの接続を使用している場合、次のコマンドを実行します。

```
/usr/lib/vmware-vmware/bin/vdcleanup -f showpartners -h psc_fqdn_or_static_ip -u administrator
```

- vCenter Server の Windows インストールまたは Platform Services Controller への接続を使用している場合、次のコマンドを実行します。

```
C:\Program Files\VMware\VMware vCenter Server\vmware-vmware\bin\vdcleanup -f showpartners -h psc_fqdn_or_static_ip -u administrator
```

プロンプトが表示されたら、vCenter Single Sign-On 管理者パスワードを入力します。

- 3 各外部 Platform Services Controller インスタンスに対して、手順 2 を繰り返します。

vCenter Single Sign-On ドメイン内のすべての Platform Services Controller インスタンス間の既存のパートナー関係を特定します。

- 4 別の外部 Platform Services Controller インスタンスとのレプリケーション関係に参加していない外部 Platform Services Controller インスタンスがある場合、createagreement パラメータを使用してこの Platform Services Controller インスタンスに対して vdcleanup コマンドを実行し、このインスタンスを別の外部 Platform Services Controller インスタンスに参加させます。

- vCenter Server Appliance または Platform Services Controller アプライアンスへの接続を使用している場合、次のコマンドを実行します。

```
/usr/lib/vmware-vmware/bin/vdcrepadmin -f createagreement -2 -h
psc_fqdn_or_static_ip -H partner_psc_fqdn_or_static_ip -u administrator
```

- vCenter Server の Windows インストールまたは Platform Services Controller への接続を使用している場合、次のコマンドを実行します。

```
C:\Program Files\VMware\VMware vCenter Server\vmware-vmware\bin\vdcrepadmin -f
createagreement -2 -h psc_fqdn_or_static_ip -H partner_psc_fqdn_or_static_ip -u
administrator
```

プロンプトが表示されたら、vCenter Single Sign-On 管理者パスワードを入力します。

2 つの Platform Services Controller インスタンス間のパートナー関係が作成されます。

- 5 別の外部 Platform Services Controller インスタンスとのレプリケーション関係に参加していない各外部 Platform Services Controller インスタンスに対し、手順 4 を繰り返します。
- 6 外部 Platform Services Controller インスタンスのリング パートナーシップ トポロジが構成されたことを確認するため、手順 2 から手順 3 を繰り返します。

各 vCenter Server インスタンスの再構成と組み込みから外部 Platform Services Controller インスタンスへの再ポイント

再構成を利用すると、組み込まれた各 Platform Services Controller を降格し、vCenter Server インスタンスをリダイレクトして外部 Platform Services Controller インスタンスを使用することができます。

図 6-4. 組み込まれた Platform Services Controller による 3 つの結合された vCenter Server インスタンスの再構成と外部 Platform Services Controller インスタンスへの再ポイントの例

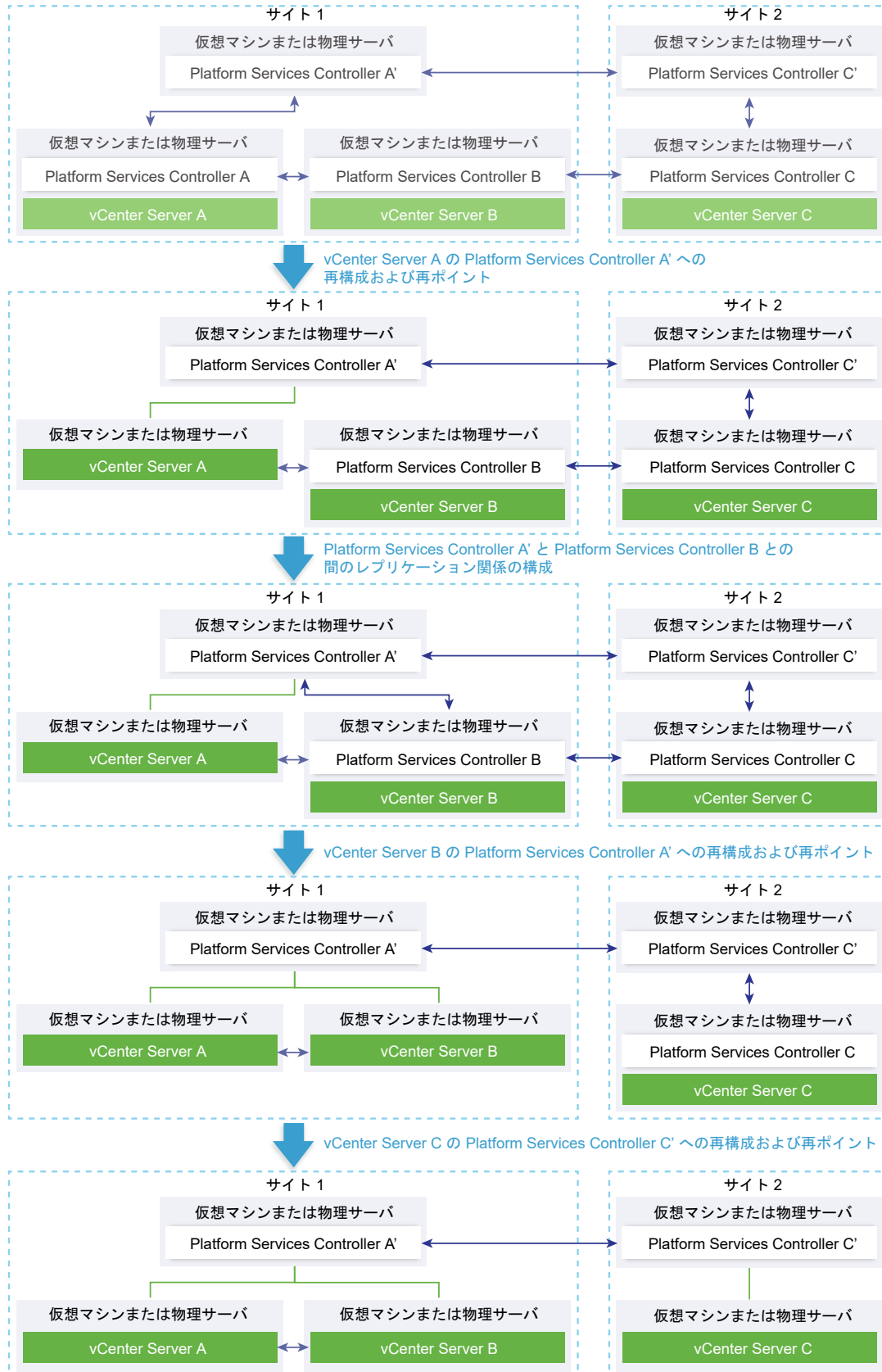


表 6-6. 凡例

矢印または直線	説明
	2 つの Platform Services Controller インスタンスの間のレプリケーション関係
	外部 Platform Services Controller を使用する vCenter Server の登録
	移行手順

手順

- 1 組み込み Platform Services Controller を使用する vCenter Server インスタンスにログインします。

オプション	手順
組み込み Platform Services Controller を使用する vCenter Server Appliance の場合	<p>アプライアンス シェルに root としてログインします。</p> <ul style="list-style-type: none"> ■ アプライアンス コンソールに直接アクセスできる場合は、Alt+F1 を押します。 ■ リモート接続の場合は、SSH などのリモート コンソール接続を使用して、アプライアンスへのセッションを開始します。
組み込み Platform Services Controller を使用する vCenter Server の Windows インストール環境の場合	Windows マシンに管理者としてログインします。

- 2 Platform Services Controller インスタンスが組み込まれ、外部 Platform Services Controller インスタンスが使用される vCenter Server が直接のレプリケーション パートナーでない場合、そのようなレプリケーション関係を作成します。

- Platform Services Controller が組み込まれた vCenter Server Appliance については、アプライアンスの Bash シェルから次のコマンドを実行します。

```
/usr/lib/vmware-vmware/bin/vdcrepadmin -f createagreement -h localhost -H
psc_fqdn_or_static_ip -u administrator
```

- Platform Services Controller が組み込まれた vCenter Server の Windows インストールについては、Windows のコマンド プロンプトから次のコマンドを実行します。

```
C:\Program Files\VMware\vCenter Server\vmware-vmware\bin\vdcrepadmin -f
createagreement -h localhost -H psc_fqdn_or_static_ip -u administrator
```

プロンプトが表示されたら、vCenter Single Sign-On 管理者パスワードを入力します。

- 3 Platform Services Controller インスタンスを組み込まれた vCenter Server が Windows で実行されている場合、Windows コマンド プロンプトで C:\Program Files\VMware\vCenter Server\bin に移動します。

- 4 cmsso-util reconfigure コマンドを実行します。

```
cmsso-util reconfigure --repoint-psc psc_fqdn_or_static_ip --username username --
domain-name domain_name --passwd password [--dc-port port_number]
```

ここで、角括弧 [] で囲まれているのはオプションの項目です。

ここでの *psc_fqdn_or_static_ip* は、外部 Platform Services Controller インスタンスを特定するために使用するシステム名です。このシステム名は、FQDN または固定 IP アドレスにする必要があります。

注： FQDN 値は大文字と小文字を区別します。

username オプションと *password* オプションは、vCenter Single Sign-On *domain_name* の管理者ユーザー名とパスワードです。

カスタムの HTTPS ポートで外部 Platform Services Controller が稼働している場合は、*--dc-port* オプションを使用します。HTTPS ポートのデフォルト値は 443 です。

たとえば、外部 Platform Services Controller がカスタムの HTTPS ポート 449 番で稼働している場合は、次のオプションを指定して実行する必要があります。

```
cmsso-util reconfigure --repoint-psc psc.acme.local --username administrator --
domain-name vsphere.local --passwd Password1! --dc-port 449
```

重要： 別の vCenter Single Sign-On サイト内にある外部 Platform Services Controller インスタンスを使用するように、vCenter Server インスタンスを再ポイントした場合、vCenter Server インスタンスをこの vCenter Single Sign-On サイトに移動する必要があります。異なる vCenter Single Sign-On サイト間で vCenter Server を移動する方法に関する詳細は、VMware ナレッジベースの記事 [Repointing the VMware vCenter Server 6.0 between sites in a vSphere Domain](#) を参照してください。

- 5 vSphere Web Client を使用して vCenter Server インスタンスにログインし、vCenter Server が実行中であり管理可能であることを確認します。
- 6 組み込み Platform Services Controller を使用する各 vCenter Server インスタンスについて、この手順を繰り返します。

結果

組み込み Platform Services Controller を使用する vCenter Server インスタンスが降格され、vCenter Server インスタンスが外部 Platform Services Controller インスタンスにリダイレクトされます。

Update Manager のアップグレード

7

64 ビット オペレーティング システムにインストールされている Update Manager バージョン 5.x からのみ Update Manager 6.0 にアップグレードできます。

バージョン 5.x より前の Update Manager または、32 ビット プラットフォームで動作する Update Manager を実行している場合は、Update Manager 6.0 へのインプレース アップグレードを実行できません。Update Manager 5.0 インストール メディアに同梱されているデータ移行ツールを使用して、Update Manager システムを、64 ビット オペレーティング システムで動作する Update Manager 5.0 にアップグレードしてから、バージョン 5.0 からバージョン 6.0 へのインプレース アップグレードを実行する必要があります。データ移行ツールの使用方法の詳細については、Update Manager 5.0 に関する『VMware vSphere Update Manager のインストールと管理』ドキュメントを参照してください。

Update Manager をアップグレードするときに、インストール パスとパッチのダウンロード場所を変更することはできません。これらのパラメータを変更するには、アップグレードではなく、新しいバージョンの Update Manager をインストールする必要があります。

以前のバージョンの Update Manager は 512 ビットのキーと自己署名証明書を使用しますが、これらはアップグレード時に置き換えられません。よりセキュリティの高い 2048 ビットのキーが必要な場合は、Update Manager 6.0 を新規インストールするか、Update Manager Utility を使用して既存の証明書を置き換えます。

仮想マシン パッチ スキャンや修正のスケジュール設定タスクは、アップグレード時に削除されません。アップグレードの終了後、以前のリリースのスケジュール設定スキャン タスクを編集して削除できます。既存のスケジュール設定修正タスクは削除できますが、編集はできません。

仮想マシンのパッチ ベースラインはアップグレード中に削除されます。これらのベースラインを含んだ既存のスケジュール設定タスクは正常に実行され、仮想マシンのパッチ ベースラインを使用するスキャンおよび修正操作のみ無視されます。

Update Manager データベースは、Update Manager のアップグレード時にアップグレードする必要があります。アップグレード時に、データベース内の既存のデータを残すか、置き換えるかを選択できます。

Update Manager をインストールまたはアップグレードすると、Update Manager で必要な Java コンポーネント（JRE）がシステムにサイレントでインストールまたはアップグレードされます。Update Manager 5.5 Update 1 以降、Update Manager のアップグレード手順とは別に、Java コンポーネントのバージョンを Update Manager のリリースとは非同期にリリースされるバージョンにアップグレードすることができます。

この章には、次のトピックが含まれています。

- [Update Manager サーバのアップグレード](#)

Update Manager サーバのアップグレード

64 ビットのマシンにインストールされている Update Manager のインスタンスをアップグレードするには、まず vCenter Server を互換性のあるバージョンにアップグレードする必要があります。

この Update Manager 6.0 リリースでは、Update Manager 5.x からのみアップグレードが可能です。

前提条件

- データベース ユーザーに必要な権限セットを必ず付与します。『VMware vSphere Update Manager インストールおよび管理』の「Update Manager データベースの準備」の章を参照してください。
- Update Manager サービスを停止し、Update Manager データベースをバックアップします。インストーラがデータベース スキーマをアップグレードするため、データベースは以前の Update Manager バージョンとの互換性を持たなくなります。これを元に戻すことはできません。

手順

- 1 vCenter Server を互換性のあるバージョンにアップグレードします。

注： vCenter Server のインストール ウィザードでは、vCenter Server をアップグレードすると Update Manager との互換性がなくなることが警告されます。

プロンプト メッセージが表示された場合は、vCenter Server を実行しているマシンを再起動する必要があります。再起動しないと、Update Manager をアップグレードできない可能性があります。

- 2 ソフトウェアのインストーラのディレクトリで、autorun.exe ファイルをダブルクリックして、[vSphere Update Manager] - [Server] を選択します。

autorun.exe を実行できない場合は、UpdateManager フォルダを参照して VMware-UpdateManager.exe を実行します。

- 3 インストーラの言語を選択して、[OK] をクリックします。
- 4 アップグレードに関する警告するメッセージが表示されたら、[OK] をクリックします。
- 5 ようこそページを確認して、[次へ] をクリックします。
- 6 使用許諾契約書を読んで同意し、[次へ] をクリックします。
- 7 サポート情報を確認し、古いアップグレード ファイルを削除するかどうかを選択し、インストール後すぐにデフォルトのダウンロード元からアップデートをダウンロードするかどうかを選択して、[次へ] をクリックします。

[リポジトリから古いホスト アップグレード ファイルを削除] の選択を解除した場合は、Update Manager 6.0 では使用できないファイルが保持されます。

[インストールの直後に、デフォルト ソースからアップデートをダウンロード] の選択を解除した場合は、デフォルトのダウンロード スケジュールに従って Update Manager が毎日 1 回アップデートをダウンロードするか、ダウンロード設定ページの [今すぐダウンロード] をクリックするとすぐにアップデートがダウンロードされます。デフォルトのダウンロード スケジュールは、インストール完了後に変更できます。

- 8 vCenter Server システムの認証情報を入力し、[次へ] をクリックします。

元の vCenter Server システムへの Update Manager の登録を有効にしておく場合は、元のインストールの vCenter Server システムの IP アドレスを保持し、認証情報を入力します。

- 9 Update Manager データベースのデータベース パスワードを入力し、[次へ] をクリックします。

データベース パスワードは、DSN で Windows NT 認証を使用していない場合にのみ必要です。

- 10 データベース アップグレード ページで、[はい、Update Manager データベースをアップグレードします] と [既存の Update Manager データベースをバックアップしました] を選択し、[次へ] をクリックします。

- 11 (オプション) 既存のリモート データベースが既に最新のスキーマにアップグレードされている場合は、データベースの再初期化警告ページで、そのデータベースを保持するように選択します。

既存のデータベースを空のデータベースで置き換えると、既存のデータはすべて失われます。

- 12 Update Manager のポート設定を指定し、プロキシ設定の構成を行うかどうかを選択して、[次へ] をクリックします。

Update Manager がインストールされているコンピュータがインターネットにアクセスできる場合は、プロキシ設定を構成します。

- 13 (オプション) プロキシ サーバとポートの情報、プロキシの認証を行うかどうかを指定して、[次へ] をクリックします。

- 14 [インストール] をクリックして、アップグレードを開始します。

- 15 [終了] をクリックします。

結果

Update Manager サーバがアップグレードされました。

次のステップ

Update Manager Client プラグインをアップグレードします。

ホストをアップグレードする前に行う作業

8

ホストを正しくアップグレードするために、変更点を理解し、それに備えてください。

この章には、次のトピックが含まれています。

- ESXi アップグレードのベスト プラクティス
- ESXi 6.0 のアップグレード オプション
- サードパーティ製のカスタム VIB があるホストのアップグレード
- vSphere Update Manager で実行されるアップグレードには、手動で割り当てられた IP アドレスを使用する
- ESXi インストーラを起動するためのメディア オプション
- リモート管理アプリケーションの使用
- ESXi インストーラのダウンロード

ESXi アップグレードのベスト プラクティス

ホストをアップグレードする際は、この操作を正常に実行するため、ベスト プラクティスのプロセスを理解し、それに従う必要があります。

ESXi のアップグレードを正常に実行するには、次のベスト プラクティスに従います。

- 1 ESXi のアップグレード プロセス、そのプロセスが既存のデプロイ環境に与える影響、およびアップグレードに必要な準備事項を理解していることを確認します。
 - vSphere システムに VMware のソリューションまたはプラグインが含まれている場合は、それらのソリューションまたはプラグインに、アップグレード後の vCenter Server のバージョンとの互換性があることを確認します。VMware 製品の相互運用性マトリックス (http://www.vmware.com/resources/compatibility/sim/interop_matrix.php) を参照してください。
 - **ESXi 6.0 のアップグレード オプション**を読み、サポートされているアップグレード シナリオ、およびアップグレードの実行時に使用できるオプションやツールについて理解します。
 - インストール上の既知の問題については、VMware vSphere リリース ノートを参照してください。
- 2 アップグレードのためにシステムを準備します。
 - 現在の ESXi バージョンでアップグレードがサポートされていることを確認します。 **ESXi 6.0 のアップグレード オプション** を参照してください。

- 使用中のシステム ハードウェアが、ESXi の要件に準拠していることを確認します。2 章 アップグレード要件および『VMware 互換性ガイド』（英語版）(<http://www.vmware.com/resources/compatibility/search.php>) を参照してください。システムの互換性、ネットワークおよびホスト バス アダプタ (HBA) カードとの I/O の互換性、ストレージの互換性、およびバックアップ ソフトウェアの互換性を確認します。
 - アップグレード用に、使用可能なディスク容量がホスト上に十分あることを確認します。
 - ホストに SAN が接続されている場合は、アップグレードを続行する前にファイバ チャネル システムを外してください。BIOS では HBA カードを無効にしないでください。
- 3 アップグレードを実行する前に、ホストをバックアップしてください。アップグレードに失敗した場合は、ホストをリストアできます。
 - 4 選択したアップグレード オプションによっては、ホスト上のすべての仮想マシンを移行またはパワーオフする必要があります。アップグレード方法の説明を参照してください。
 - 5 アップグレードが終わったら、システムをテストしてアップグレードが正常に完了したことを確認します。
 - 6 ホストのライセンスを適用します。ESXi 6.0 へのアップグレード後の、ライセンスの適用 を参照してください。
 - 7 ログ ファイルに十分なディスク ストレージを確保するため、リモート ログ機能用の syslog サーバの設定を検討します。リモート ホスト上のログ機能を設定することは、ローカル ストレージが不十分なホストで特に重要です。vSphere Syslog Collector は vCenter Server 6.0 にサービスとして含まれ、すべてのホストからのログの収集に使用できます。システム ログに必要な空き容量 を参照してください。syslog および syslog サーバの設定と構成、ホスト プロファイル インターフェイスからの syslog の設定、および vSphere Syslog Collector のインストールについては、『vSphere のインストールとセットアップ』ドキュメントを参照してください。
 - 8 アップグレードに失敗しても、ホストをバックアップしてある場合はホストをリストアできます。

ESXi 6.0 のアップグレード オプション

VMware では、ESXi 5.x ホストを ESXi 6.0 ホストにアップグレードする方法をいくつか提供しています。

ESXi 6.0 へのアップグレードの詳細とサポート レベルは、アップグレードするホストと使用するアップグレード方法によって異なります。ESXi の最新バージョンからアップグレード予定バージョンへのアップグレード パスのサポートを確認します。VMware 製品の相互運用性マトリックス (http://www.vmware.com/resources/compatibility/sim/interop_matrix.php) を参照してください。

ESXi 5.x ホストのほか、別途リリースされたドライバまたはその他のサードパーティのカスタム機能のアップグレード、CD または DVD を使用した対話型アップグレード、スクリプトを使用したアップグレード、または vSphere Update Manager によるアップグレードが可能です。カスタム VIB を持つ ESXi 5.x ホストをバージョン 6.0 にアップグレードすると、カスタム VIB が移行されます。サードパーティ製のカスタム VIB があるホストのアップグレードを参照してください。

ESXi 6.0 への直接のアップグレードでサポートされる方法は、以下のとおりです。

- vSphere Update Manager。
- CD、DVD、または USB ドライブからの対話的なアップグレード。

- スクリプトを使用したアップグレード。
- vSphere Auto Deploy。ESXi 5.x ホストが vSphere Auto Deploy を使用してデプロイされた場合は、vSphere Auto Deploy を使用して、ESXi 6.0 イメージでホストを再プロビジョニングすることができます。
- `esxcli` コマンド。

vSphere Update Manager

vSphere Update Manager は、クラスタ化されたホスト、仮想マシン、およびゲスト OS にアップグレード、移行、更新、およびパッチ適用を実行するソフトウェアです。vSphere Update Manager は、ホストと仮想マシンのアップグレードを組織的に調整します。サイトで vCenter Server を使用している場合、VMware では vSphere Update Manager を使用することをお勧めします。ホストの組織的なアップグレードの実施方法については、[vSphere Update Manager を使用した、ホストの組織的なアップグレード](#)を参照してください。仮想マシンの組織的なアップグレードの実行方法については、『VMware vSphere Update Manager のインストールと管理』ドキュメントを参照してください。

CD/DVD または USB フラッシュ ドライブにある ESXi インストーラの ISO イメージを使用した、対話型アップグレード

ESXi 6.0 インストーラを CD/DVD または USB フラッシュ ドライブから実行して、アップグレードを対話的に行うことができます。ホストの数が少ない導入の場合はこの方法が適しています。インストーラはフレッシュインストールと同じ動作をしますが、ESXi 5.0.x、ESXi 5.1.x、または ESXi 5.5.x のインストールにすでに含まれているターゲット ディスクを選択すると、ホストが 6.0 にアップグレードされます。また、既存のホスト設定および構成ファイルの一部を移行して、既存の VMFS データストアを保持することもできます。[ホストの対話型アップグレード](#)を参照してください。

スクリプトによるアップグレードの実行

ESXi 5.0.x、ESXi 5.1.x、または ESXi 5.5.x から ESXi 6.0 にホストをアップグレードする場合、更新スクリプトを実行することで効率的な無人アップグレードを実行できます。スクリプトによるアップグレードは、複数のホストをデプロイするのに効率的な方法です。スクリプトを使用して、ESXi を CD、DVD、USB フラッシュ ドライブからアップグレードしたり、インストーラの PXE (Preboot Execution Environment) を指定してアップグレードできます。対話的なインストールからスクリプトを呼び出すこともできます。[スクリプトを使用した、ホストのインストールまたはアップグレード](#)を参照してください。

vSphere Auto Deploy

ESXi 5.x ホストが vSphere Auto Deploy を使用してデプロイされている場合は、vSphere Auto Deploy を使用して、ホストを再プロビジョニングし、新しいイメージ プロファイルで再起動します。このプロファイルには、ESXi アップグレードまたはパッチ、ホスト構成プロファイルが含まれ、さらに VMware のパートナーが提供するサードパーティ製ドライバまたは管理エージェントが任意で含まれます。vSphere ESXi Image Builder CLI を使用すると、カスタム イメージを作成できます。[vSphere Auto Deploy を使用した、ホストの再プロビジョニング](#)を参照してください。

esxcli

ESXi の `esxcli` コマンドライン ユーティリティを使用して、ESXi 5.0.x ホスト、ESXi 5.1.x ホスト、または ESXi 5.5.x ホストを ESXi 6.0 ホストにアップグレードできます。

esxupdate ユーティリティおよび vihostupdate ユーティリティは、ESXi 6.0 へのアップグレードではサポートされません。 [esxcli コマンドを使用した、ホストのアップグレード](#) を参照してください。

サードパーティ製のカスタム VIB があるホストのアップグレード

ホストには、サードパーティ製のドライバや管理エージェントなど向けのカスタム vSphere インストーラバンドル (VIB) をインストールできます。ESXi 5.x ホストを ESXi 6.0 にアップグレードする場合、VIB がインストーラ ISO に含まれているかどうかにかかわらず、サポートされるカスタム VIB はすべて移行されます。

ホストまたはインストーラ ISO イメージに、競合をもたらし、アップグレードを妨げる VIB が含まれる場合、エラーメッセージに競合している VIB が示されます。ホストをアップグレードするには、次のいずれかの操作を実行します。

- 競合する VIB をホストから削除して、アップグレードをもう一度試します。vSphere Update Manager を使用している場合は、修正処理中にサードパーティ製のソフトウェアモジュールを削除するオプションを選択します。詳細については、『VMware vSphere Update Manager のインストールと管理』ドキュメントを参照してください。esxcli コマンドを使用しても、競合する VIB を削除できます。詳細については、[ホストからの VIB の削除](#) を参照してください。
- vSphere ESXi Image Builder CLI を使用して、競合を解決するカスタム ISO イメージを作成します。vSphere ESXi Image Builder CLI のインストールと使用法の詳細については、『vSphere のインストールとセットアップ』ドキュメントを参照してください。

vSphere Update Manager で実行されるアップグレードには、手動で割り当てられた IP アドレスを使用する

vSphere Update Manager を使用して、ホストを ESXi 5.x から ESXi 6.0 にアップグレードする場合、そのホストには手動で割り当てた IP アドレスを使用する必要があります。手動で割り当てた IP アドレスは、固定 IP アドレスとも呼ばれます。

Dynamic Host Configuration Protocol (DHCP) を使用して要求された IP アドレスは、vSphere Update Manager で実行されるホストのアップグレード中に問題を引き起こすことがあります。DHCP サーバ上で構成されたリース期間が失効したために、アップグレードまたは移行操作中にホストがその DHCP IP アドレスを失った場合、vSphere Update Manager はそのホストに接続できなくなります。その場合、ホストのアップグレードまたは移行が成功しても、vSphere Update Manager ではアップグレードまたは移行が失敗したと報告されます。これは、vSphere Update Manager がホストに接続できないためです。この問題を回避するため、ホストに手動で割り当てられた IP アドレスを使用します。

ESXi インストーラを起動するためのメディア オプション

ESXi インストーラが、ESXi をインストールするシステムにアクセスできる必要があります。

次の起動メディアが ESXi インストーラ用にサポートされています。

- CD/DVD からの起動。 [ESXi インストーラ ISO イメージのダウンロードおよび CD または DVD への書き込み](#) を参照してください。

- USB フラッシュ ドライブからの起動。USB フラッシュ ドライブのフォーマットによる ESXi インストールまたはアップグレードの起動 を参照してください。
- ネットワークからの PXE 起動。ESXi インストーラの PXE 起動
- リモート管理アプリケーションを使用した、リモートの場所からの起動。リモート管理アプリケーションの使用 を参照してください。

ESXi インストーラ ISO イメージのダウンロードおよび CD または DVD への書き込み

ESXi のインストール CD/DVD がない場合は作成できます。

カスタム インストール スクリプトが含まれているインストーラ ISO イメージを作成することもできます。カスタムのインストールまたはアップグレード スクリプトを含む、インストーラ ISO イメージの作成 を参照してください。

手順

- 1 VMware の Web サイト <https://my.vmware.com/web/vmware/downloads> から ESXi インストーラをダウンロードします。

ESXi はデータセンターおよびクラウド インフラストラクチャの下に表示されます。

- 2 md5sum が正しいことを確認します。

MD5 チェックサムを使用して、VMware Web サイトのトピックを確認します (<http://www.vmware.com/download/md5.html>)。

- 3 ISO イメージを CD または DVD に書き込みます。

USB フラッシュ ドライブのフォーマットによる ESXi インストールまたはアップグレードの起動

USB フラッシュ ドライブをフォーマットして、ESXi インストールまたはアップグレードを起動できます。

この手順の説明では、USB フラッシュ ドライブが /dev/sdb として検出されることを前提としています。

注： インストール スクリプトが含まれている `ks.cfg` ファイルを、インストールまたはアップグレードの起動に使用している同じ USB フラッシュ ドライブ上に置くことはできません。

前提条件

- Linux マシンとこれに対するスーパーユーザー アクセス
- Linux マシンが検出することのできる USB フラッシュ ドライブ
- `isolinux.cfg` ファイルを含む ESXi ISO イメージの「VMware-VMvisor-Installer-バージョン番号-build_number.x86_64.iso」
- Syslinux パッケージ

手順

- 1 USB フラッシュ ドライブが `/dev/sdb` として検出されない場合、または USB フラッシュ ドライブの検出方法が不明な場合は、検出方法を指定してください。

- a コマンド ラインで、現在のログ メッセージを表示するコマンドを実行します。

```
tail -f /var/log/messages
```

- b USB フラッシュ ドライブを接続します。

次のメッセージに似た形式で、USB フラッシュ ドライブを特定するいくつかのメッセージが表示されます。

```
Oct 25 13:25:23 ubuntu kernel: [ 712.447080] sd 3:0:0:0: [sdb] Attached SCSI removable disk
```

この例では、`sdb` によって USB ドライブが識別されます。デバイスが異なるものとして識別された場合は、`sdb` の代わりにその識別を使用します。

- 2 USB フラッシュ デバイスにパーティション テーブルを作成します。

```
/sbin/fdisk /dev/sdb
```

- a `d` と入力して、すべてのパーティションが削除されるまで、パーティションを削除します。
- b `n` と入力して、ディスク全体を占めるプライマリ パーティション 1 を作成します。
- c `t` と入力して、FAT32 ファイル システムに適した設定にタイプを設定します (`c` など)。
- d `a` と入力して、パーティション 1 にアクティブ フラグを設定します。
- e `p` と入力して、パーティション テーブルを出力します。

結果は次のようになります。

```
Disk /dev/sdb: 2004 MB, 2004877312 bytes 255 heads, 63 sectors/track, 243 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes Device Boot Start End Blocks Id
System /dev/sdb1 1 243 1951866 c W95 FAT32 (LBA)
```

- f `w` と入力して、パーティション テーブルを書き込み、プログラムを終了します。

- 3 USB フラッシュ ドライブを Fat32 ファイル システムを指定してフォーマットします。

```
/sbin/mkfs.vfat -F 32 -n USB /dev/sdb1
```

- 4 USB フラッシュ ドライブに Syslinux ブートローダーをインストールします。

Syslinux 実行ファイルと `mbr.bin` ファイルの場所は、Syslinux バージョンによって異なる可能性があります。例えば、Syslinux 6.02 をダウンロードした場合、次のコマンドを実行します。

```
/usr/bin/syslinux /dev/sdb1
cat /usr/lib/syslinux/mbr/mbr.bin > /dev/sdb
```

- 5 ターゲット ディレクトリを作成し、USB フラッシュ ドライブをこれにマウントします。

```
mkdir /usbdisk
mount /dev/sdb1 /usbdisk
```

- 6 ターゲット ディレクトリを作成し、ESXi インストーラ ISO イメージをこれにマウントします。

```
mkdir /esxi_cdrom
mount -o loop VMware-VMvisor-Installer-6.x.x-XXXXXX.x86_64.iso /esxi_cdrom
```

- 7 ISO イメージの内容を USB フラッシュ ドライブにコピーします。

```
cp -r /esxi_cdrom/* /usbdisk
```

- 8 ファイル名 isolinux.cfg を syslinux.cfg に変更します。

```
mv /usbdisk/isolinux.cfg /usbdisk/syslinux.cfg
```

- 9 /usbdisk/syslinux.cfg ファイルで、APPEND -c boot.cfg の行を APPEND -c boot.cfg -p 1 に編集します。

- 10 USB フラッシュ ドライブをアンマウントします。

```
umount /usbdisk
```

- 11 インストーラ ISO イメージをアンマウントします。

```
umount /esxi_cdrom
```

結果

これで、USB フラッシュ ドライブにより ESXi インストーラを起動することができます。

USB フラッシュ ドライブを作成して、ESXi インストール スクリプトまたはアップグレード スクリプトを保存する

ESXi のスクリプトによるインストールまたはアップグレードに使用する ESXi のインストール スクリプトまたはアップグレード スクリプトを、USB フラッシュ ドライブに格納することができます。

インストール マシンに複数の USB フラッシュ ドライブがある場合、インストール ソフトウェアは、接続されたすべての USB フラッシュ ドライブでインストールまたはアップグレード スクリプトを検索します。

この手順の説明では、USB フラッシュ ドライブが /dev/sdb として検出されることを前提としています。

注： インストールまたはアップグレード スクリプトを含む ks ファイルは、インストールまたはアップグレードの起動に使用している同じ USB フラッシュ ドライブ上に置くことはできません。

前提条件

- Linux マシン
- ESXi のインストールまたはアップグレード スクリプト、ks.cfg キックスタート ファイル

■ USB フラッシュ ドライブ

手順

- 1 インストール スクリプトまたはアップグレード スクリプトにアクセスできる Linux マシンに、USB フラッシュ ドライブを接続します。

- 2 パーティション テーブルを作成します。

```
/sbin/fdisk /dev/sdb
```

- a d を入力して、すべてのパーティションが削除されるまで、パーティションを削除します。
- b n を入力して、ディスク全体を占めるプライマリ パーティション 1 を作成します。
- c t を入力して、FAT32 ファイル システムに適した設定にタイプを設定します (c など)。
- d p と入力して、パーティション テーブルを出力します。

結果は次のようになります。

```
Disk /dev/sdb: 2004 MB, 2004877312 bytes
255 heads, 63 sectors/track, 243 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Device Boot      Start         End      Blocks   Id  System
/dev/sdb1            1         243        1951866    c   W95 FAT32 (LBA)
```

- e w と入力してパーティション テーブルを書き込み、終了します。

- 3 USB フラッシュ ドライブを Fat32 ファイル システムを指定してフォーマットします。

```
/sbin/mkfs.vfat -F 32 -n USB /dev/sdb1
```

- 4 USB フラッシュ ドライブをマウントします。

```
mount /dev/sdb1 /usbdisk
```

- 5 ESXi のインストール スクリプトを USB フラッシュ ドライブにコピーします。

```
cp ks.cfg /usbdisk
```

- 6 USB フラッシュ ドライブをアンマウントします。

結果

USB フラッシュ ドライブには、ESXi のインストール スクリプトまたはアップグレード スクリプトが格納されています。

次のステップ

ESXi インストーラの起動時に、インストール スクリプトまたはアップグレード スクリプトの場所としてこの USB フラッシュ ドライブの場所を参照します。 [インストール スクリプトまたはアップグレード スクリプトを開始するための起動オプションの入力](#) および [PXE 構成ファイルについて](#) を参照してください。

カスタムのインストールまたはアップグレード スクリプトを含む、インストーラ ISO イメージの作成

独自のインストールまたはアップグレード スクリプトを使用して、標準の ESXi インストーラ ISO イメージをカスタマイズできます。このカスタマイズを行うと、カスタマイズしたインストーラ ISO イメージを起動するときに、スクリプトを使用して無人インストールまたは無人アップグレードを実行できるようになります。

[インストール スクリプトおよびアップグレード スクリプトについて](#) および [boot.cfg ファイルについて](#) も参照してください。

前提条件

- Linux マシン
- ESXi ISO イメージ VMware-VMvisor-Installer-6.x.x-XXXXXXX.x86_64.iso。ここで、6.x.x はインストールする ESXi のバージョンであり、XXXXXXX はインストーラ ISO イメージのビルド番号です。
- カスタムのインストールまたはアップグレード スクリプト、ks_cust.cfg キックスタート ファイル

手順

- 1 VMware Web サイトから ESXi ISO イメージをダウンロードします。
- 2 ISO イメージをフォルダにマウントします。

```
mount -o loop VMware-VMvisor-Installer-6.x.x-XXXXXXX.x86_64.iso /
esxi_cdrom_mount
```

XXXXXXX には、インストールまたはアップグレード後のバージョンの ESXi ビルド番号を指定します。

- 3 cdrom の中身を別のフォルダにコピーします。

```
cp -r /esxi_cdrom_mount /esxi_cdrom
```

- 4 キックスタート ファイルを /esxi_cdrom にコピーします。

```
cp ks_cust.cfg /esxi_cdrom
```

- 5 (オプション) kernelopt オプションを使用してインストールまたはアップグレード スクリプトの場所を指定するように、boot.cfg ファイルを変更します。

スクリプトのパスを入力するには、大文字を使用する必要があります。例：

```
kernelopt=runweasel ks=cdrom:/KS_CUST.CFG
```

インストールまたはアップグレードは、インストール中またはアップグレード中にキックスタート ファイルを指定する必要なく、完全に自動化されています。

- 6 ISO イメージを再作成します。

```
mkisofs -relaxed-filenames -J -R -o custom_esxi.iso -b isolinux.bin -c
boot.cat -no-emul-boot -boot-load-size 4 -boot-info-table /esxi_cdrom
```

結果

ISO イメージにカスタムのインストールまたはアップグレード スクリプトが含まれます。

次のステップ

この ISO イメージを使用して ESXi をインストールします。

ESXi インストーラの PXE 起動

PXE (Preboot Execution Environment) を使用してホストを起動し、ネットワーク インターフェイスから ESXi インストーラを起動することができます。

ESXi 6.0 は、フラッシュ メモリまたはローカル ハード ドライブにインストールするように設計された ISO 形式で配布されます。これらのファイルを展開し、PXE を使用して起動することができます。

PXE では、DHCP (Dynamic Host Configuration Protocol) と TFTP (File Transfer Protocol) を使用して、ネットワーク経由でオペレーティング システムを起動します。

PXE 起動を行うには、いくつかのネットワーク インフラストラクチャと、PXE 対応のネットワーク アダプタを搭載したマシンが必要です。ESXi を実行できるほとんどのマシンには、PXE 起動が可能なネットワーク アダプタがあります。

注： vSphere Auto Deploy サーバに IPv4 アドレスがあることを確認します。PXE 起動は、IPv4 でのみサポートされています。

TFTP サーバ、PXELINUX、および gPXE について

TFTP (Trivial File Transfer Protocol) は FTP サービスに似ており、通常は、システムのネットワーク起動や、ルータなどのネットワーク デバイスへのファームウェアの読み込みにのみ使用します。

ほとんどの Linux ディストリビューションには、tftp-hpa サーバのコピーが含まれています。サポートされているソリューションが必要な場合は、希望するベンダーからサポートされている TFTP サーバを購入してください。

TFTP サーバを Microsoft Windows ホストで実行する場合は、tftpd32 バージョン 2.11 以降を使用してください。<http://tftpd32.jounin.net/> を参照してください。以前のバージョンの tftpd32 は、PXELINUX および gPXE との互換性がありませんでした。

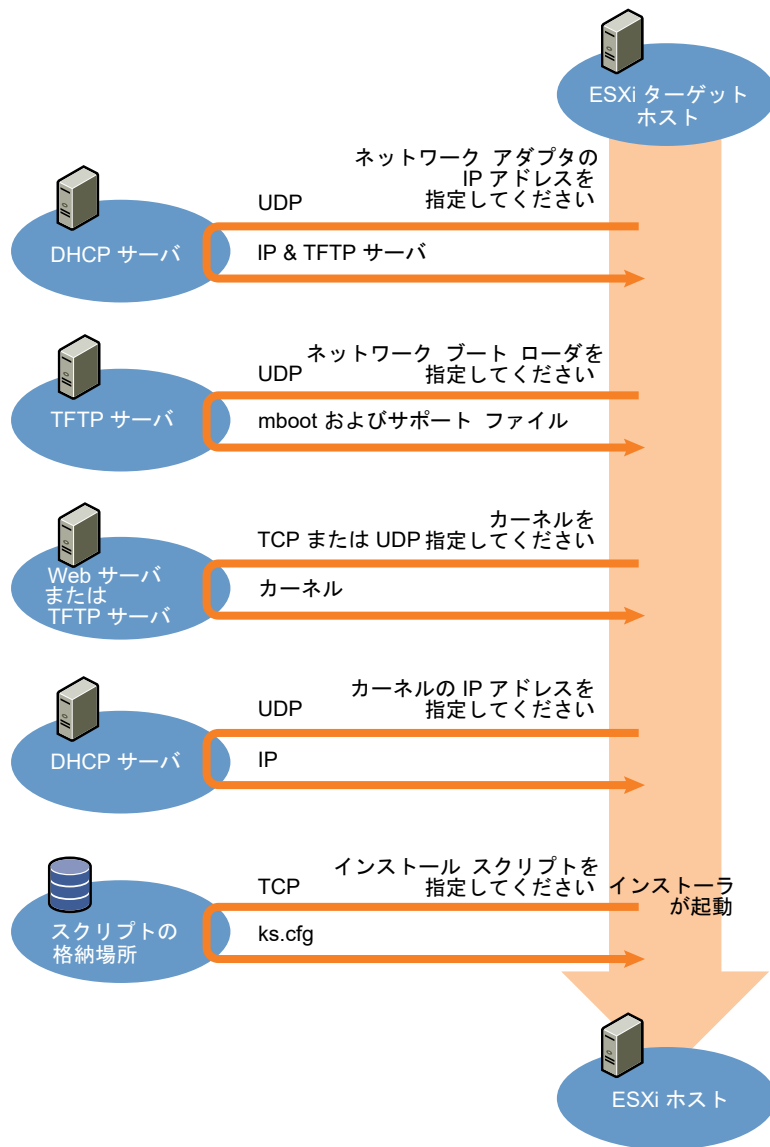
TFTP サーバは、VMware Marketplace にあるアプライアンス パッケージのいずれかで取得することもできます。

PXELINUX と gPXE の環境では、ターゲット マシンで ESXi インストーラを起動できます。PXELINUX は、<http://www.kernel.org/pub/linux/utils/boot/syslinux/> から入手できる SYSLINUX パッケージに含まれますが、多くの Linux ディストリビューションにも付属します。PXELINUX の多くのバージョンには gPXE も含まれます。Red Hat Enterprise Linux バージョン 5.3 などの一部のディストリビューションには、gPXE が含まれていない PXELINUX の旧バージョンが含まれます。

gPXE を使用しない場合、負荷の高いネットワーク上で ESXi のインストーラを起動する際に問題が発生することがあります。TFTP は、大量のデータを転送する際に確実性が低下する場合があります。gPXE なしで PXELINUX を使用する場合、pxelinux.0 バイナリ ファイル、構成ファイル、カーネル、およびその他のファイルは TFTP で転送されます。gPXE を使用する場合は、gpxelinux.0 バイナリ ファイルと構成ファイルだけが TFTP で転送されます。gPXE を使用すると、ESXi のインストーラの起動に必要なカーネルおよびその他のファイルを Web サーバを介して転送できます。

注： VMware は PXELINUX バージョン 3.86 での PXE 起動をテストしています。これはサポートの制限を示すものではありません。PXE 起動のインフラストラクチャを設定する際に使用する、サードパーティ製エージェントのサポートについては、ベンダーにお問い合わせください。

図 8-1. PXE 起動のインストール プロセスの概要



DHCP の構成例

ESXi インストーラを PXE 起動するには、DHCP サーバが TFTP サーバのアドレスと、pxelinux.0 または gpxelinux.0 ディレクトリへのポインタを送信する必要があります。

ターゲット マシンは、DHCP サーバを使用して IP アドレスを取得します。DHCP サーバは、ターゲット マシンの起動が許可されているかどうかと、PXELINUX バイナリの場所（通常は TFTP サーバ上）を判断する必要があります。ターゲット マシンははじめて起動するときに、ネットワーク全体にパケットをブロードキャストして、起動に必要な情報を要求します。DHCP サーバがこれに応答します。

注意： ネットワークにすでに DHCP サーバがある場合は、新規に設定しないでください。複数の DHCP サーバが DHCP 要求に応答すると、マシンが不正な、または競合する IP アドレスを取得するか、正しい起動情報を受け取れない可能性があります。DHCP サーバを設定する前に、ネットワーク管理者に確認してください。DHCP の構成についてサポートが必要な場合は、DHCP サーバのベンダーに問い合わせてください。

多くの DHCP サーバは、ホストを PXE 起動できます。Microsoft Windows 用の DHCP バージョンを使用している場合は、DHCP サーバのドキュメントを参照して、next-server 引数と filename 引数をターゲット マシンに渡す方法を確認してください。

gPXE の例

この例は、gPXE を有効にするように ISC DHCP バージョン 3.0 サーバを構成する方法を示しています。

```
allow booting;
allow bootp;
# gPXE options
option space gppe;
option gppe-encap-opts code 175 = encapsulate gppe;
option gppe.bus-id code 177 = string;
class "pxeclients" {
  match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
  next-server TFTP server address;
  if not exists gppe.bus-id {
    filename "/gpxelinux.0";
  }
}
subnet Network address netmask Subnet Mask {
  range Starting IP AddressEnding IP Address;
}
```

マシンが PXE 起動を行うときには、DHCP サーバが IP アドレスと TFTP サーバの gpxelinux.0 バイナリ ファイルの場所を示します。割り当てられた IP アドレスは、構成ファイルのサブセット セクションで定義されている範囲内になります。

PXELINUX（gPXE なし）の例

この例は、PXELINUX を有効にするように ISC DHCP バージョン 3.0 サーバを構成する方法を示しています。

```
#
# DHCP Server Configuration file.
# see /usr/share/doc/dhcp*/dhcpd.conf.sample
```

```
#
ddns-update-style ad-hoc;
allow booting;
allow bootp;
class "pxeclients" {
match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
next-server xxx.xxx.xx.xx;
filename = "pxelinux.0";
}
subnet 192.168.48.0 netmask 255.255.255.0 {
range 192.168.48.100 192.168.48.250;
}
```

マシンが PXE 起動を行うときには、DHCP サーバが IP アドレスと TFTP サーバの `pxelinux.0` バイナリ ファイルの場所を示します。割り当てられた IP アドレスは、構成ファイルのサブセット セクションで定義されている範囲内になります。

PXE 構成ファイルについて

PXE 構成ファイルでは、ターゲットの ESXi ホストが起動して TFTP サーバに接続するときにそのホストに表示するメニューを定義します。ESXi インストーラを PXE 起動するには、PXE 構成ファイルが必要です。

TFTP サーバは、ネットワーク上で常に PXE クライアントをリッスンしています。PXE クライアントが PXE サービスを要求していることを検出すると、起動メニューが含まれているネットワーク パッケージをそのクライアントに送信します。

必要なファイル

PXE の構成ファイルには、次のファイルへのパスを含める必要があります。

- `mboot.c32` はブート ロードです。
- `boot.cfg` はブート ロード構成ファイルです。

[boot.cfg ファイルについて](#) を参照してください。

PXE 構成ファイルのファイル名

PXE 構成ファイルのファイル名には、次のいずれかのオプションを選択します。

- `01-mac_address_of_target_ESXi_host`。例： `01-23-45-67-89-0a-bc`
- ターゲット ESXi ホストの IP アドレスの 16 進表記。
- デフォルト

初期起動ファイル `pxelinux.0` または `gpxelinux.0` が、PXE 構成ファイルのロードを試行します。ARP タイプコード（イーサネットは 01）をプリフィックスとする、ターゲット ESXi ホストの MAC アドレスが試されます。これに失敗した場合は、ターゲット ESXi システムの IP アドレスの 16 進表記が試されます。最後に、`default` というファイルのロードが試されます。

PXE の構成ファイルの場所

ファイルを TFTP サーバの `var/lib/tftpboot/pxelinux.cfg/` に保存します。

たとえば、このファイルは TFTP サーバの `/tftpboot/pxelinux.cfg/01-00-21-5a-ce-40-f6` に保存できます。ターゲット ESXi ホストのネットワーク アダプタの MAC アドレスは `00-21-5a-ce-40-f6` です。

[] PXELINUX および PXE 構成ファイルを使用した、ESXi インストーラの PXE 起動

TFTP サーバで、PXELINUX および PXE 構成ファイルを使用して、ESXi インストーラを PXE 起動することができます。

[インストール スクリプトおよびアップグレード スクリプトについて](#) および [boot.cfg ファイルについて](#) も参照してください。

前提条件

次のコンポーネントが使用する環境内にあることを確認します。

- VMware Web サイトからダウンロードした ESXi インストーラ ISO イメージ。
- gPXE での PXE 起動をサポートする TFTP サーバ。 [TFTP サーバ、PXELINUX、および gPXE について](#) を参照してください。
- PXE 起動用に構成された DHCP サーバ。 [DHCP の構成例](#) を参照してください。
- PXELINUX。
- お使いのバージョンの ESXi でサポートされるハードウェア構成のサーバ。 <http://www.vmware.com/resources/compatibility/search.php> の『VMware 互換性ガイド』を参照してください。
- TFTP トラフィックを許可するネットワーク セキュリティ ポリシー (UDP ポート 69)。
- (任意) インストール スクリプト (キックスタート ファイル)。 [インストール スクリプトおよびアップグレード スクリプトについて](#) を参照してください。
- ターゲット ESXi ホストに、PXE をサポートするネットワーク アダプタ。
- IPv4 ネットワーク。IPv6 は PXE 起動には使用できません。

ほとんどの場合、ネイティブ VLAN を使用します。PXE 起動で使用する VLAN ID を指定する場合は、使用している NIC で VLAN ID の仕様がサポートされていることを確認します。

手順

- 1 TFTP サーバに `/tftpboot/pxelinux.cfg` ディレクトリを作成します。
- 2 Linux マシンに PXELINUX をインストールします。
PXELINUX は Syslinux パッケージに含まれます。ファイルを展開し、`pxelinux.0` ファイルを見つけて、TFTP サーバ上の `/tftpboot` ディレクトリにコピーします。
- 3 次の情報を各クライアント ホストに送信するように、DHCP サーバを構成します。
 - TFTP サーバの名前または IP アドレス
 - 初期起動ファイルの名前 (`pxelinux.0`)
- 4 ESXi インストーラ イメージの内容を、TFTP サーバ上の `/var/lib/tftpboot` ディレクトリにコピーします。

- 5 (オプション) スクリプトを使用したインストールの場合は、`boot.cfg` ファイルの `kernel` コマンドの後の行に `kernelopt` オプションを追加して、インストール スクリプトの場所を指定します。

次のコードをモデルとして使用します。XXX.XXX.XXX.XXX には、インストール スクリプトが置かれたサーバの IP アドレスを指定します。esxi_ksFiles は、ks.cfg ファイルが格納されているディレクトリです。

```
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
```

- 6 PXE の構成ファイルを作成します。

このファイルでは、オペレーティング システムがない場合にホストを起動する方法を定義します。PXE 構成ファイルは、起動ファイルを参照します。次のコードをモデルとして使用します。XXXXXX には、ESXi インストーラ イメージのビルド番号を指定します。

```
DEFAULT menu.c32
MENU TITLE ESXi-6.x.x-XXXXXX-full Boot Menu
NOHALT 1
PROMPT 0
TIMEOUT 80
LABEL install
KERNEL mboot.c32
APPEND -c location of boot.cfg
MENU LABEL ESXi-6.x.x-XXXXXX-full ^Installer
LABEL hddboot
LOCALBOOT 0x80
MENU LABEL ^Boot from local disk
```

- 7 ターゲット ホスト マシンのメディア アクセス コントロール (MAC) アドレスを使用して、ファイルの名前を指定します。01-mac_address_of_target_ESXi_host。

たとえば、01-23-45-67-89-0a-bc と指定します。

- 8 PXE の構成ファイルを TFTP サーバの `/tftpboot/pxelinux.cfg` に保存します。
- 9 ネットワーク アダプタを使用してマシンを起動します。

PXELINUX および isolinux.cfg PXE 構成ファイルを使用した ESXi インストーラの PXE 起動

PXELINUX を使用して ESXi インストーラを PXE 起動し、isolinux.cfg ファイルを PXE 構成ファイルとして使用することができます。

[インストール スクリプトおよびアップグレード スクリプトについて](#) および [boot.cfg ファイルについて](#) も参照してください。

前提条件

次のコンポーネントが使用する環境内にあることを確認します。

- VMware Web サイトからダウンロードした ESXi インストーラ ISO イメージ。
- PXELINUX での PXE 起動をサポートする TFTP サーバ。 [TFTP サーバ、PXELINUX、および gPXE について](#) を参照してください。

- PXE 起動用に構成された DHCP サーバ。DHCP の構成例 を参照してください。
- PXELINUX。
- お使いのバージョンの ESXi でサポートされるハードウェア構成のサーバ。 <http://www.vmware.com/resources/compatibility/search.php> の『VMware 互換性ガイド』を参照してください。
- TFTP トラフィックを許可するネットワーク セキュリティ ポリシー (UDP ポート 69)。
- (任意) インストール スクリプト (キックスタート ファイル)。インストール スクリプトおよびアップグレード スクリプトについて を参照してください。
- ターゲット ESXi ホストに、PXE をサポートするネットワーク アダプタ。
- IPv4 ネットワーク。IPv6 は PXE 起動には使用できません。

ほとんどの場合、ネイティブ VLAN を使用します。PXE 起動で使用する VLAN ID を指定する場合は、使用している NIC で VLAN ID の仕様がサポートされていることを確認します。

手順

- 1 TFTP サーバに /tftpboot/pxelinux.cfg ディレクトリを作成します。

- 2 Linux マシンに PXELINUX をインストールします。

PXELINUX は Syslinux パッケージに含まれます。ファイルを展開し、pxelinux.0 ファイルを見つけて、TFTP サーバ上の /tftpboot ディレクトリにコピーします。

- 3 DHCP サーバを構成します。

DHCP サーバは、次の情報をクライアント ホストに送信します。

- TFTP サーバの名前または IP アドレス
- 初期起動ファイルの名前 (pxelinux.0)

- 4 ESXi インストーラ イメージの内容を、TFTP サーバ上の /var/lib/tftpboot ディレクトリにコピーします。

- 5 (オプション) スクリプトを使用したインストールの場合は、boot.cfg ファイルの kernel コマンドの後の行に kernelopt オプションを追加して、インストール スクリプトの場所を指定します。

次の例の XXX.XXX.XXX.XXX は、インストール スクリプトが置かれたサーバの IP アドレスです。

```
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
```

- 6 ESXi インストーラ ISO イメージから、isolinux.cfg ファイルを /tftpboot/pxelinux.cfg ディレクトリにコピーします。

isolinux.cfg ファイルには次のコードが含まれています。XXXXXX は、ESXi インストーラ イメージのビルド番号です。

```
DEFAULT menu.c32
MENU TITLE ESXi-6.x.x-XXXXXX-full Boot Menu
NOHALT 1
PROMPT 0
```

```

TIMEOUT 80
LABEL install
KERNEL mboot.c32
APPEND -c location of boot.cfg
MENU LABEL ESXi-6.x.x-XXXXXX-full ^Installer
LABEL hddboot
LOCALBOOT 0x80
MENU LABEL ^Boot from local disk

```

- 7 ファイル名 `isolinux.cfg` を、ターゲット ホスト マシンの MAC アドレスに変更します： `01-mac_address_of_target_ESXi_host`。例： `01-23-45-67-89-0a-bc`
- 8 ネットワーク アダプタを使用してマシンを起動します。

gPXE を使用した ESXi インストーラの PXE 起動

gPXE を使用して、ESXi インストーラを PXE 起動できます。

[インストール スクリプトおよびアップグレード スクリプトについて](#) および [boot.cfg ファイルについて](#) も参照してください。

前提条件

次のコンポーネントが使用する環境内にあることを確認します。

- VMware Web サイトからダウンロードした ESXi インストーラ ISO イメージ
- ターゲット ESXi ホストからアクセス可能な HTTP Web サーバ
- PXE 起動用に構成された DHCP サーバ。 `/etc/dhcpd.conf` は、TFTP サーバを使用するクライアント ホスト用に構成され、初期起動ファイルは `gpxelinux.0/undionly.kpxe` に設定されています。[DHCP の構成例](#) を参照してください。
- お使いのバージョンの ESXi でサポートされるハードウェア構成のサーバ。<http://www.vmware.com/resources/compatibility/search.php> の『ハードウェア互換性ガイド』を参照してください。
- gPXELINUX
- (任意) ESXi のインストール スクリプト。[インストール スクリプトおよびアップグレード スクリプトについて](#) を参照してください。

ほとんどの場合、ネイティブ VLAN を使用します。PXE 起動で使用する VLAN ID を指定する必要がある場合は、使用している NIC で VLAN ID の仕様がサポートされていることを確認します。

手順

- 1 ESXi インストーラ ISO イメージの内容を、HTTP サーバ上の `/var/www/html` ディレクトリにコピーします。

2 HTTP サーバの情報を使用して boot.cfg ファイルを変更します。

次のコードをモデルとして使用します。XXX.XXX.XXX.XXXには、HTTP サーバの IP アドレスを指定します。kernelopt 行を含めるかどうかは任意です。スクリプトを使用したインストールのためにインストールスクリプトの場所を指定するには、このオプションを含めます。

```
title=Loading ESX installer
kernel=http://XXX.XXX.XXX.XXX/tboot.b00
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
modules=http://XXX.XXX.XXX.XXX/b.b00 --- http://XXX.XXX.XXX.XXX/useropts.gz --- http://
XXX.XXX.XXX.XXX/k.b00 --- http://XXX.XXX.XXX.XXX/a.b00 --- http://XXX.XXX.XXX.XXX/s.v00
--- http://XXX.XXX.XXX.XXX/weaselin.t00 --- http://XXX.XXX.XXX.XXX/tools.t00 --- http://
XXX.XXX.XXX.XXX/imgdb.tgz --- http://XXX.XXX.XXX.XXX/imgpayld.tgz
```

3 ホストを gPXE 起動し、Ctrl + B を押して GPT メニューにアクセスします。

4 次のコマンドを入力して、ESXi インストーラで起動します。XXX.XXX.XXX.XXXには HTTP サーバの IP アドレスを指定します。

```
dhcp net0 ( if dhcp is not set)
kernel -n mboot.c32 http://XXX.XXX.XXX.XXX/mboot.c32
imgargs mboot.c32 -c http://XXX.XXX.XXX.XXX/boot.cfg
boot mboot.c32
```

ソフトウェア FCoE による ESXi のインストールおよび起動

FCoE オフロード機能が装備された VMware ソフトウェア FCoE アダプタおよびネットワーク アダプタを使用して、FCoE LUN から ESXi をインストールおよび起動できます。ホストには専用 FCoE HBA は必要ありません。

ソフトウェア FCoE による ESXi のインストールおよび起動の詳細については、『vSphere ストレージ』ドキュメントを参照してください。

リモート管理アプリケーションの使用

リモート管理アプリケーションによって、リモートの場所にあるサーバに ESXi をインストールできます。

インストールがサポートされているリモート管理アプリケーションには、HP iLO (Integrated Lights-Out)、DRAC (Dell Remote Access Card)、IBM 管理モジュール (MM)、RSA II (Remote Supervisor Adapter II) があります。現在、サポートされているサーバモデルとリモート管理ファームウェアバージョンのリストについては、[サポートされているリモート管理のサーバモデルとファームウェアバージョン](#)を参照してください。リモート管理アプリケーションのサポートについては、ベンダーに問い合わせてください。

リモート管理アプリケーションを使用して、リモートからの ESXi のインストールを、対話的に行ったり、スクリプトを使用して行うことができます。

リモート管理アプリケーションを使用して ESXi をインストールする場合、ピーク容量で稼働しているシステムまたはネットワークでは、仮想 CD が破壊されるという問題に直面することがあります。ISO イメージからのリモートインストールが失敗した場合は、物理 DVD メディアからインストールを実行します。

ESXi インストーラのダウンロード

ESXi のインストーラをダウンロードします。

前提条件

<https://my.vmware.com/web/vmware/> で Customer Connect アカウントを作成します。

手順

- 1 VMware の Web サイト (<https://my.vmware.com/web/vmware/downloads>) から ESXi インストーラをダウンロードします。

ESXi はデータセンターおよびクラウド インフラストラクチャの下に表示されます。

- 2 md5sum が正しいことを確認します。

MD5 チェックサムを使用については、VMware Web サイトのトピックをご覧ください (<http://www.vmware.com/download/md5.html>)。

ホストのアップグレード

9

vCenter Server および vSphere Update Manager をアップグレードした後、ESXi 5.x ホストを ESXi 6.0 にアップグレードします。ESXi 5.0.x、ESXi 5.1.x、および ESXi 5.5.x ホストは ESXi 6.0 に直接アップグレードできます。

ホストのアップグレードには、[ESXi 6.0 のアップグレード オプション](#)に記載されているツールと方法を使用できます。

注意： vCenter Server によって管理されているホストをアップグレードする場合、ESXi をアップグレードする前に、vCenter Server にアップグレードする必要があります。正しい順序でアップグレードしなかった場合は、データが消失したり、サーバにアクセスできなくなる可能性があります。

この章には、次のトピックが含まれています。

- vSphere Update Manager を使用した、ホストの組織的なアップグレード
- スクリプトを使用した、ホストのインストールまたはアップグレード
- vSphere Auto Deploy を使用した、ホストの再プロビジョニング
- esxcli コマンドを使用した、ホストのアップグレード
- ホストの対話型アップグレード

vSphere Update Manager を使用した、ホストの組織的なアップグレード

組織的なアップグレードによって、vSphere インベントリのオブジェクトを 2 つのプロセスでアップグレードできます。1 つめのプロセスはホストのアップグレード、2 つめのプロセスが仮想マシンのアップグレードです。このプロセスは、より多くのプロセスを自動化するためにクラスタ レベルで構成することも、細かく制御するために個別のホストまたは仮想マシン レベルで構成することもできます。

たとえば、ESXi 5.x ホストを ESXi 6.0 にアップグレードするホスト アップグレード ベースラインを定義したり、VMware Tools や仮想マシン ハードウェアを最新バージョンにアップグレードする仮想マシン アップグレード ベースラインを定義したりできます。ウィザードを使用したワークフローで、まずクラスタ全体のホストのアップグレードをスケジュール設定してから、すべての仮想マシンのアップグレードをスケジュール設定します。

重要： ホストを ESXi 6.0 にアップグレードすると、バージョン 5.x ESXi ソフトウェアにロールバックできません。アップグレードを実行する前に、ホストをバックアップします。そうすることで、アップグレードや移行に失敗した場合に、5.x ホストをリストアできます。

ウィザードを使用したワークフローでは、間違った手順でアップグレードすることを防ぐことができます。たとえば、ウィザードでは、クラスタ内のホストをアップグレードする前に仮想マシンのハードウェアをアップグレードできないようになっています。

DRS (Distributed Resource Scheduler) を使用すると、アップグレード プロセス中の仮想マシンのダウンタイムを防ぐことができます。

Update Manager では、定義したアップグレード ベースラインに対するホストと仮想マシンのコンプライアンスが監視されます。コンプライアンス違反があった場合は詳細レポートとダッシュボード ビューに表示されます。

Update Manager では一括修正がサポートされています。

Update Manager によって、次の vSphere コンポーネントがアップグレードされます。

- ESXi カーネル (vmkernel)
- 仮想マシンのハードウェア
- VMware Tools
- 仮想アプライアンス

ここにリストされていないコンポーネントについては、ほかの方法でアップグレードできます。また、サードパーティ製コンポーネントについては、適切なサードパーティ製ツールを使用します。

次の各トピックでは、Update Manager を使用して ESXi ホストの組織的なアップグレードを実行する方法を説明しています。

- [ホストおよびクラスタの設定の構成](#)
- [vSphere Update Manager を使用した、ホストの組織的アップグレードの実行](#)

Update Manager を使用してホスト上の仮想マシンの組織的なアップグレードを実行する方法については、『VMware vSphere Update Manager のインストールと管理』ドキュメントを参照してください。

[]ホストおよびクラスタの設定の構成

vSphere DRS (Distributed Resource Scheduler)、vSphere HA (High Availability)、および vSphere FT (フォールト トレランス) が有効になっているクラスタの vSphere オブジェクトをアップデートするとき、そのクラスタ全体で vSphere DPM (Distributed Power Management)、HA アドミッション コントロール、および FT を一時的に無効にすることができます。アップデートが完了したあと、Update Manager がこれらの機能をリストアします。

アップデートを適用するには、修正中にホストがメンテナンス モードに切り替わる必要がある場合があります。ホストがメンテナンス モードのとき、仮想マシンは実行できません。可用性を確保するため、vCenter Server は、ホストがメンテナンス モードになる前にクラスタ内のほかの ESXi ホストに仮想マシンを移行できます。vCenter Server が仮想マシンを移行することができるのは、クラスタが vSphere vMotion 用に構成されていて、かつ DRS が有効になっている場合です。

ホストに実行中の仮想マシンがない場合、DPM がホストをスタンバイ モードに切り替えて Update Manager の操作を妨げる可能性があります。スキャンおよびステージングの正常な完了を確実にするため、Update Manager は、これらの操作中に DPM を無効にします。修正を正常に実行するには、修正処理前に DPM および HA のアドミッション コントロールを無効にすることを、Update Manager に許可する必要があります。処理が完了すると、Update Manager は DPM と HA のアドミッション コントロールをリストアします。Update Manager は、ステージングおよび修正前には HA のアドミッション コントロールを無効にしますが、スキャン前には無効化しません。

DPM がすでにホストをスタンバイ モードに切り替えている場合は、Update Manager はホストをパワーオンしてからスキャン、ステージング、および修正を実行します。スキャン、ステージング、または修正が完了したあと、Update Manager は DPM と HA のアドミッション コントロールをオンにし、必要に応じて VMware DPM がホストをスタンバイ モードに切り替えます。Update Manager は、パワーオフ状態のホストを修正しません。

ホストがスタンバイ モードで、かつ、何らかの理由で DPM が手動で無効になっている場合、Update Manager はこれらのホストを修正またはパワーオンしません。

クラスタ内で、HA アドミッション コントロールを一時的に無効にして vSphere vMotion を続行することができます。このアクションによって、修正するホストのマシンのダウンタイムを防ぐことができます。クラスタ全体を修正したあと、Update Manager は HA のアドミッション コントロールの設定をリストアします。

クラスタ内のホスト上にあるいずれかの仮想マシンに対して FT がオンになっている場合、FT を一時的にオフにしてから、クラスタで Update Manager の操作を実行します。ホスト上のいずれかの仮想マシンで FT がオンになっている場合、Update Manager はそのホストを修正しません。同じアップデートを使用してクラスタ内のすべてのホストを修正し、修正後にフォールトトレランスを再度有効にできるようにします。プライマリ仮想マシンとセカンダリ仮想マシンを、ESXi バージョンとパッチレベルの異なるホストに常駐させることはできません。

Virtual SAN クラスタの一部であるホストを修正する場合は、次の動作に注意してください。

- ホストの修正プロセスは完了するまでに長い時間がかかることがあります。
- 設計上、Virtual SAN クラスタの 1 台のホストのみをいつでもメンテナンス モードにすることができます。
- Update Manager は、Virtual SAN クラスタの一部であるホストを並行して修正するオプションを設定した場合にも、これらのホストを順次修正します。
- ホストが Virtual SAN クラスタのメンバーであり、さらにそのホスト上の任意の仮想マシンが「許容する障害の数 = 0」の設定の仮想マシンストレージポリシーを使用している場合、そのホストがメンテナンス モードに入るときに異常な遅延が発生する可能性があります。この遅延は、Virtual SAN データストア クラスタにおいて、Virtual SAN が仮想マシン データを 1 つのディスクから別のディスクへ移行する必要があるために発生します。遅延は数時間かかる場合があります。これは、仮想マシンストレージポリシーを「許容する障害の数 = 1」に設定することで回避できます。この設定では、Virtual SAN データストアに仮想マシン ファイルのコピーを 2 つ作成することになります。

vSphere Update Manager を使用した、ホストの組織的アップグレードの実行

vSphere Update Manager では、1 つのアップグレード ベースラインまたはベースライン グループを使用することにより、vSphere インベントリ内の ESXi ホストを組織的にアップグレードできます。

このワークフローは、vSphere インベントリ内のホストを組織的にアップグレードするプロセスの概要を示しています。vSphere Update Manager 6.0 では、ESXi 5.x が実行されているホストの ESXi 6.0 へのアップグレードがサポートされています。

組織的なアップグレードは、フォルダ レベル、クラスター レベル、またはデータセンター レベルで実行できます。

注： 最後の 2 つの手順は、相互に代替となる手順ですので、両方を実行する必要はありません。どちらかの手順を選択してください。

前提条件

- システムが vCenter Server 6.0、ESXi 6.0、および vSphere Update Manager 6.0 の要件を満たしていることを確認してください。 [Update Manager サーバのアップグレード](#)を参照してください。
- vCenter Server バージョン 6.0 をインストールするか、バージョン 6.0 にアップグレードします。 [4 章 Windows 版 vCenter Server のアップグレードおよび更新](#)を参照してください。
- vSphere Update Manager バージョン 6.0 をインストールするか、バージョン 6.0 にアップグレードします。 [7 章 Update Manager のアップグレード](#)を参照してください。

手順

1 ホストのメンテナンス モードの設定の構成

ESXi ホストのアップデートは、それらを適用する前にホストをメンテナンス モードに切り替える必要がある場合があります。Update Manager は、これらのアップデートを適用する前に ESXi ホストをメンテナンス モードにします。ホストをメンテナンス モードにできなかった場合の Update Manager の対応方法を設定できます。

2 クラスター設定の構成

1 つのクラスターにある複数の ESXi ホストの場合、修正処理は連続または並行して実行できます。一部の機能が原因で修正が失敗する場合があります。VMware DPM、HA のアドミSSION コントロール、または Fault Tolerance が有効な場合は、修正が正常に行われるように、それらの機能を一時的に無効にする必要があります。

3 PXE 起動の ESXi ホストの修正の有効化

PXE 起動の ESXi ホストの修正を他のソフトウェアが開始できるように、Update Manager を構成できます。この修正によって、ホストにパッチとソフトウェア モジュールがインストールされますが、通常、再起動するとホストの更新は失われます。

4 ホスト アップグレード イメージのインポートとホスト アップグレード ベースラインの作成

Update Manager リポジトリにインポートした ESXi 6.0 イメージを使用して、ESXi ホスト アップグレード ベースラインを作成できます。

5 ホスト ベースライン グループの作成

ベースライン グループには、1 つのホスト アップグレード ベースラインと複数のパッチ ベースラインまたはエクステンション ベースラインを組み合わせるか、複数のパッチ ベースラインおよびエクステンション ベースラインを組み合わせることができます。

6 オブジェクトへのベースラインおよびベースライン グループの添付

特定のベースラインおよびベースライン グループを基準に、コンプライアンス情報を確認してインベントリ内のオブジェクトを修正するには、最初に既存のベースラインおよびベースライン グループをそれらオブジェクトに添付する必要があります。

7 手動による ESXi ホストのスキンの開始

修正の前に、添付されたベースラインおよびベースライン グループを基準に vSphere オブジェクトをスキャンする必要があります。vSphere インベントリ内のホストのスキンをすぐに実行するには、手動でスキンを開始します。

8 vSphere オブジェクトのコンプライアンス情報の表示

添付したベースラインおよびベースライン グループを基準にした仮想マシン、仮想アプライアンス、およびホストのコンプライアンス情報を確認できます。

9 アップグレード ベースラインを基準にしたホストの修正

一度につき 1 つの添付されたアップグレード ベースラインを基準に、ESXi ホストを修正できます。ESXi 6.0 イメージを含んだ単一のアップグレード ベースラインを使用して、vSphere インベントリ内のすべてのホストをアップグレードできます。

10 ベースライン グループを基準にしたホストの修正

添付されたアップグレード、パッチ、およびエクステンションのベースライン グループを基準にホストを修正できます。ベースライン グループには、複数のパッチ ベースラインおよびエクステンション ベースラインが含まれるか、複数のパッチ ベースラインおよびエクステンション ベースラインと組み合わせられた 1 つのアップグレード ベースラインが含まれます。

ホストのメンテナンス モードの設定の構成

ESXi ホストのアップデートは、それらを適用する前にホストをメンテナンス モードに切り替える必要がある場合があります。Update Manager は、これらのアップデートを適用する前に ESXi ホストをメンテナンス モードにします。ホストをメンテナンス モードにできなかった場合の Update Manager の対応方法を設定できます。

クラスタとは異なるコンテナ内のホスト、または個別のホストの場合、vMotion での仮想マシンの移行は実行できません。vCenter Server で仮想マシンを別のホストに移行できない場合、Update Manager の対応方法を構成できます。

Virtual SAN クラスタの一部であるホストは、一度に 1 台のみメンテナンス モードにできます。これは、Virtual SAN クラスタの特異性です。

ホストが Virtual SAN クラスタのメンバーであり、さらにそのホスト上の任意の仮想マシンが「許容する障害の数 = 0」の設定の仮想マシン ストレージ ポリシーを使用している場合、そのホストがメンテナンス モードに入るときに異常な遅延が発生する可能性があります。この遅延は、Virtual SAN データストア クラスタにおいて、Virtual SAN が仮想マシン データを 1 つのディスクから別のディスクへ移行する必要があるために発生します。遅延は数時間かかる場合があります。これは、仮想マシン ストレージ ポリシーを「許容する障害の数 = 1」に設定することで回避できます。この設定では、Virtual SAN データストアに仮想マシン ファイルのコピーを 2 つ作成することになります。

前提条件

必要な権限 : VMware vSphere Update Manager.Configure

手順

- 1 vSphere Client または vSphere Web Client を使用して、Update Manager が登録されている vCenter Server システムに接続します。
- 2 vCenter Server への接続に使用しているクライアントによっては、以下の手順を実行します。

クライアント	手順
vSphere Web Client	1 [設定] タブで、[管理] の下の [ホスト/クラスタ設定] をクリックします。 [[編集]] をクリックします。
vSphere Client	1 [構成] タブで、[設定] の下の [ESXi ホスト/クラスタ設定] をクリックします。

- 3 [メンテナンス モードの設定] で、[仮想マシンのパワー状態] ドロップダウン メニューからオプションを選択して、修正対象のホスト上で実行中の仮想マシンおよびアプライアンスのパワー状態の変更を指定します。

オプション	説明
仮想マシンのパワーオフ	修正前にすべての仮想マシンおよび仮想アプライアンスのパワーオフ
仮想マシンのサスペンド	修正前にすべての実行中の仮想マシンおよび仮想アプライアンスのサスペンド
仮想マシンのパワー状態を変更しない	仮想マシンおよび仮想アプライアンスを現在のパワー状態のままにします。これはデフォルトの設定です。

- 4 (オプション) [障害発生時にメンテナンス モードへの切り替えを再試行] を選択し、再試行遅延と再試行回数を指定します。

修正前にホストがメンテナンス モードに切り替わることに失敗した場合、Update Manager は、再試行遅延時間の経過後、[再試行回数] フィールドで指定した回数までホストをメンテナンス モードにしようと試みます。

- 5 (オプション) [ホストがメンテナンス モードに入るのを妨げる可能性があるリムーバブル メディア デバイスを一時的に無効にします] を選択します。

Update Manager は、CD/DVD ドライブまたはフロッピー ドライブが接続されている仮想マシンが配置されたホストを修正しません。ホストの仮想マシンに取り外し可能なメディア ドライブが接続されていると、ホストがメンテナンス モードに切り替わることができず、修正が中断する場合があります。

修正後に、取り外し可能なメディア デバイスがまだ利用できる場合は、Update Manager はそれらのデバイスを再接続します。

- 6 [適用] をクリックします。

結果

これらの設定がデフォルトの障害時対応の設定になります。個々の修正タスクを構成する際は、異なる設定を指定することができます。

クラスタ設定の構成

1 つのクラスタにある複数の ESXi ホストの場合、修正処理は連続または並行して実行できます。一部の機能が原因で修正が失敗する場合があります。VMware DPM、HA のアドミッション コントロール、または Fault Tolerance が有効な場合は、修正が正常に行われるように、それらの機能を一時的に無効にする必要があります。

注： ホストを並行して修正すると、クラスタの修正に必要な時間を短くしてパフォーマンスを大幅に向上することができます。Update Manager は、DRS によって設定されたクラスタ リソースの制約に影響を与えずに、ホストを並行して修正します。ホストが Virtual SAN クラスタの一部である場合には、ホストを並行して修正しないでください。Virtual SAN クラスタの特性のため、クラスタ内にメンテナンス モードのホストが他にあるとき、ホストはメンテナンス モードに入ることはできません。

前提条件

必要な権限：VMware vSphere Update Manager.Configure

手順

- 1 vSphere Client または vSphere Web Client を使用して、Update Manager が登録されている vCenter Server システムに接続します。
- 2 vCenter Server への接続に使用しているクライアントによっては、以下の手順を実行します。

クライアント	手順
vSphere Web Client	<ol style="list-style-type: none"> 1 [管理] タブで、[設定] の下の [ホスト/クラスタ設定] をクリックします。 2 [[編集]] をクリックします。
vSphere Client	<ol style="list-style-type: none"> 1 [構成] タブで、設定の下にある [ESX ホスト/クラスタ設定] をクリックします。

3 無効または有効にする機能のチェック ボックスを選択します。

オプション	説明
分散電力管理 (DPM)	<p>VMware DPM は、クラスタ内で実行している仮想マシンのリソース使用状況を監視します。十分に余分な容量がある場合は、VMware DPM はクラスタ内のほかのホストへ仮想マシンを移動し、元のホストをスタンバイ モードにして節電することを推奨します。容量が不足している場合は、スタンバイ ホストをパワーオンの状態に戻すように、VMware DPM が推奨する場合があります。</p> <p>DPM を無効にすることを選択しなかった場合、Update Manager は、VMware DPM が有効になっているクラスタをスキップします。VMware DPM を一時的に無効にすることを選択した場合、Update Manager はクラスタで DPM を無効にし、そのクラスタのホストを修正して、修正が完了したあと VMware DPM を再度有効にします。</p>
HA (High Availability) のアドミッション コントロール	<p>アドミッション コントロールは VMware HA が使用するポリシーです。これにより、クラスタ内のフェイルオーバーのキャパシティが確保されます。修正時に HA のアドミッション コントロールが有効になっている場合、クラスタ内の仮想マシンが vMotion で移行されない場合があります。</p> <p>HA のアドミッション コントロールを無効にすることを選択しなかった場合、Update Manager は HA のアドミッション コントロールが有効になっているクラスタをスキップします。HA のアドミッション コントロールを一時的に無効にすることを選択した場合、Update Manager は HA のアドミッション コントロールを無効にして、クラスタを修正します。そして、修正が完了したあと HA のアドミッション コントロールを再度有効にします。</p>
Fault Tolerance (FT)	<p>FT は、プライマリ仮想マシンと同一のセカンダリ仮想マシンを自動的に作成して保守することで、仮想マシンを継続的に使用できるようにします。ホスト上の仮想マシンで FT をオフにすることを選択しなかった場合、Update Manager はそのホストを修正しません。</p>
クラスタ内のホストの並行修正を有効にします	<p>Update Manager は、クラスタ内の各ホストを並行修正できます。Update Manager は、DRS 設定に影響を与えずに並行修正できるホストの最大数を継続的に評価します。このオプションを選択しなかった場合、Update Manager はクラスタ内の各ホストを順次修正します。</p> <p>設計上、Virtual SAN クラスタの 1 台のホストのみをいつでもメンテナンス モードにすることができます。Update Manager は、Virtual SAN クラスタの一部であるホストを並行して修正するオプションを選択した場合にも、これらのホストを順次修正します。</p>
ホストをメンテナンスモードに切り替える必要がある場合に、パワーオフ状態およびサスペンド状態の仮想マシンをクラスタの他のホストに移行する	<p>Update Manager は、サスペンド状態およびパワーオフ状態の仮想マシンを、メンテナンスモードに切り替える必要があるホストから、クラスタ内のほかのホストに移行します。[メンテナンス モードの設定] ペインで、修正前に仮想マシンをパワーオフまたはサスペンドするように選択できます。</p>

4 [適用] をクリックします。

結果

これらの設定がデフォルトの障害時対応の設定になります。個々の修正タスクを構成する際は、異なる設定を指定することができます。

PXE 起動の ESXi ホストの修正の有効化

PXE 起動の ESXi ホストの修正を他のソフトウェアが開始できるように、Update Manager を構成できます。この修正によって、ホストにパッチとソフトウェア モジュールがインストールされますが、通常、再起動するとホストの更新は失われます。

Update Manager の [構成] タブにあるグローバル設定では、ESX Agent Manager または Cisco Nexus 1000V などのソリューションが PXE 起動の ESXi ホストの修正を開始できるように設定できます。逆に、[修正] ウィザードの [パワーオン状態の PXE 起動の ESXi ホストのパッチ修正を有効] 設定では、Update Manager が PXE 起動のホストにパッチを適用できるように設定できます。

再起動後に ステートレスのホストで更新を保持するには、更新を含む PXE 起動イメージを使用します。Update Manager では、更新を適用する前に PXE 起動イメージを更新できるため、再起動によって更新が失われることはありません。Update Manager そのものは、PXE 起動の ESXi ホストでの再起動が必要な更新をインストールすることはないため、ホストを再起動することはありません。

前提条件

必要な権限：VMware vSphere Update Manager.Configure

手順

- 1 vSphere Client または vSphere Web Client を使用して、Update Manager が登録されている vCenter Server システムに接続します。
- 2 vCenter Server への接続に使用しているクライアントによっては、以下の手順を実行します。

クライアント	手順
vSphere Web Client	<ol style="list-style-type: none"> 1 [管理] タブで、[設定] の下の [ホスト/クラスタ設定] をクリックします。 2 [[編集]] をクリックします。
vSphere Client	<ol style="list-style-type: none"> 1 [構成] タブで、設定の下にある [ESX ホスト/クラスタ設定] をクリックします。

- 3 PXE 起動の ESXi ホストでソリューション用のソフトウェアのインストールを有効化するには、[PXE 起動の ESXi ホストへの追加ソフトウェアのインストールを許可] を選択します。
- 4 [適用] をクリックします。

ホスト アップグレード イメージのインポートとホスト アップグレード ベースラインの作成

Update Manager リポジトリにインポートした ESXi 6.0 イメージを使用して、ESXi ホスト アップグレード ベースラインを作成できます。

ESXi .iso イメージを使用して、ESXi 5.x ホストを ESXi 6.0 にアップグレードできます。

ホストをアップグレードするには、VMware から VMware-VMvisor-Installer-6.0.0-build_number.x86_64.iso 形式の名前で配布されている ESXi インストーラ イメージ、または vSphere ESXi Image Builder を使用して作成されたカスタム イメージを使用します。

前提条件

ファイルのアップロード権限があることを確認してください。ユーザー、グループ、ロール、および権限の管理に関する詳細については、『vCenter Server およびホスト管理』を参照してください。

Update Manager が登録されている vCenter Server システムに vSphere Client を接続し、ホーム ページのソリューションおよびアプリケーション アイコンの [Update Manager] をクリックします。

手順

- 1 [ESXi イメージ] タブで、右上にある [ESXi イメージのインポート] をクリックします。
- 2 [ESXi イメージのインポート] ウィザードの ESXi イメージの選択ページで、アップロードする ESXi イメージを検索して選択します。
- 3 [次へ] をクリックします。

注意： インポート ウィザードは閉じないでください。インポート ウィザードを閉じると、アップロード処理が停止します。

- 4 (オプション) [セキュリティ警告] ウィンドウで、証明書の警告を処理するためのオプションを選択します。

インストール時に vCenter Server および ESXi ホスト用に生成される証明書は、信頼性のある認証局によって署名されていません。そのため、これらのいずれかのシステムへの SSL 接続が確立するたびに、クライアントで警告が表示されます。

オプション	操作
無視	[無視] をクリックすると、現在の SSL 証明書を引き続き使用して、アップロード プロセスを開始します。
キャンセル	[キャンセル] をクリックすると、ウィンドウが閉じ、アップロード プロセスが停止されます。
この証明書をインストールし、セキュリティ警告をすべて表示しない	証明書をインストールし、セキュリティ警告が表示されないようにするには、このチェック ボックスを選択し、[無視] をクリックします。

- 5 ファイルがアップロードされたら、[次へ] をクリックします。
- 6 (オプション) ホスト アップグレード ベースラインの作成
 - a [ESXi イメージを使用してベースラインを作成] を選択したままにします。
 - b ホスト アップグレード ベースラインの名前を入力し、必要に応じて説明を入力します。
- 7 [終了] をクリックします。

結果

アップロードした ESXi イメージが、インポートされた ESXi イメージ ペインに表示されます。ESXi イメージに含まれているソフトウェア パッケージに関するその他の情報は、ソフトウェア パッケージ ペインで確認できます。

ホスト アップグレード ベースラインも作成した場合、新しいベースラインは、[ベースラインおよびグループ] タブの ベースライン ペインに表示されます。

次のステップ

環境内のホストをアップグレードするには、ホスト アップグレード ベースラインを作成する必要があります (まだ作成していない場合)。

ホスト ベースライン グループの作成

ベースライン グループには、1つのホスト アップグレード ベースラインと複数のパッチ ベースラインまたはエクステンション ベースラインを組み合わせるか、複数のパッチ ベースラインおよびエクステンション ベースラインを組み合わせることができます。

注： いつでも[新規ベースライン グループ] ウィザードにある[終了]をクリックしてベースライン グループを保存し、あとの段階でそこにベースラインを追加できます。

手順

- 1 vSphere Client または vSphere Web Client を使用して、Update Manager が登録されている vCenter Server システムに接続します。
- 2 [ベースラインおよびグループ] タブで、ベースライン グループ ペインの上にある[作成]をクリックします。
- 3 vCenter Server への接続に使用しているクライアントによっては、以下の手順を実行します。

クライアント	手順
vSphere Web Client	<ol style="list-style-type: none"> 1 [ホスト ベースライン] タブの [管理] で、[ベースライン グループ] ペインの上部にある [作成] をクリックします。 2 ベースライン グループの一意の名前を入力し、[次へ] をクリックします。
vSphere Client	<ol style="list-style-type: none"> 1 [ベースラインおよびグループ] タブで、ベースライン グループ ペインの上部にある [作成] をクリックします。 2 ベースライン グループの一意の名前を入力します。 3 ベースライン グループのタイプから [ホスト ベースライン グループ] を選択して、[次へ] をクリックします。

- 4 ベースライン グループに含めるホスト アップグレード ベースラインを 1 つ選択します。
- 5 (オプション) vSphere Client を使用している場合、アップグレード ページの一番下にある [新規ホスト アップグレード ベースラインの作成] をクリックして新しいホスト アップグレード ベースラインを作成し、[新規ベースライン] ウィザードを完了します。
- 6 [次へ] をクリックします。
- 7 ベースライン グループに含めるパッチ ベースラインを選択します。
- 8 (オプション) vSphere Client を使用している場合、[パッチ] ページの一番下にある [新規ホスト パッチ ベースラインの作成] をクリックして新しいパッチ ベースラインを作成し、[新規ベースライン] ウィザードを完了します。
- 9 [次へ] をクリックします。
- 10 ベースライン グループに含めるエクステンション ベースラインを選択します。
- 11 (オプション) vSphere Client を使用している場合、[パッチ] ページの一番下にある [新規エクステンション ベースラインの作成] をクリックして新しいエクステンション ベースラインを作成し、[新規ベースライン] ウィザードを完了します。
- 12 終了準備の完了ページで [終了] をクリックします。

結果

ホスト ベースライン グループがベースライン グループ ペインに表示されます。

オブジェクトへのベースラインおよびベースライン グループの添付

特定のベースラインおよびベースライン グループを基準に、コンプライアンス情報を確認してインベントリ内のオブジェクトを修正するには、最初に既存のベースラインおよびベースライン グループをそれらオブジェクトに添付する必要があります。

Update Manager Client のコンプライアンス ビューで、ベースラインおよびベースライン グループをオブジェクトに添付できます。

ベースラインおよびベースライン グループは個々のオブジェクトに添付することもできますが、フォルダ、vApp、クラスタ、データ センターなどのコンテナ オブジェクトに添付する方がより効率的な方法です。各 vSphere オブジェクトは、その親コンテナ オブジェクトに添付されたベースラインを継承します。あるオブジェクトをコンテナから削除すると、そのオブジェクトから継承したベースラインは削除されます。

使用している vCenter Server システムが共通の vCenter Single Sign-On ドメインで他の vCenter Server システムに接続している場合、Update Manager が登録されている vCenter Server システムによって管理されているオブジェクトにベースラインまたはベースライン グループを添付できます。添付するベースラインおよびベースライン グループは、vCenter Server システムに登録された Update Manager インスタンス専用のものです。

前提条件

ベースラインの添付権限を保有していることを確認します。

手順

- 1 Update Manager が登録されている vCenter Server システムに vSphere Client を接続し、[ホーム] - [インベントリ] を選択します。
- 2 ベースラインを添付するオブジェクトのタイプを選択します。
たとえば、[ホストおよびクラスタ] または [仮想マシンおよびテンプレート] を選択します。
- 3 インベントリ内のオブジェクトを選択して、[Update Manager] タブをクリックします。
使用している vCenter Server システムが共通の vCenter Single Sign-On ドメインで他の vCenter Server システムに接続している場合、[Update Manager] タブは、Update Manager インスタンスが登録されている vCenter Server システムでのみ利用できます。
- 4 上部右隅にある [添付] をクリックします。
- 5 [ベースラインまたはグループの添付] ウィンドウで、オブジェクトに添付する 1 つ以上のベースラインまたはベースライン グループを選択します。
1 つ以上のベースライン グループを選択すると、グループ内のすべてのベースラインが選択されます。グループ内のベースラインを個別に選択解除することはできません。
- 6 (オプション) [ベースライン グループの作成] または [ベースラインの作成] リンクをクリックして、ベースライン グループまたはベースラインを作成し、各ウィザードの残りの手順を完了します。
- 7 [添付] をクリックします。

結果

添付対象として選択したベースラインおよびベースライン グループは、[Update Manager] タブの添付されたベースライン グループ ペインおよび添付されたベースライン ペインに表示されます。

手動による ESXi ホストのスキンの開始

修正の前に、添付されたベースラインおよびベースライン グループを基準に vSphere オブジェクトをスキャンする必要があります。vSphere インベントリ内のホストのスキャンをすぐに実行するには、手動でスキャンを開始します。

手順

- 1 Update Manager が登録されている vCenter Server システムに vSphere Client を接続し、ナビゲーション バーで [ホーム] - [インベントリ] - [ホストおよびクラスタ] を選択します。
- 2 ホスト、データ センター、またはコンテナ オブジェクトのいずれかを選択して、[アップデートの有無のスキャン] を選択します。
- 3 スキャンするアップデートのタイプを選択します。
[パッチおよびエクステンション] または [アップグレード] をスキャンできます。
- 4 [スキャン] をクリックします。

結果

選択したインベントリ オブジェクトとすべての子オブジェクトは、添付されているベースラインのすべてのパッチ、エクステンション、およびアップグレードを基準にスキャンされます。仮想インフラストラクチャの規模が大きく、かつスキャンを開始したオブジェクトがオブジェクト階層の上位にあるほど、スキャンにかかる時間は長くなります。

vSphere オブジェクトのコンプライアンス情報の表示

添付したベースラインおよびベースライン グループを基準にした仮想マシン、仮想アプライアンス、およびホストのコンプライアンス情報を確認できます。

コンテナ オブジェクトを選択すると、添付されているベースラインの全体的なコンプライアンス状態と、個々のコンプライアンス状態をすべて確認できます。コンテナ オブジェクトに添付されているベースラインをそれぞれ選択すると、ベースラインのコンプライアンス状態が表示されます。

仮想マシン、アプライアンス、またはホストをそれぞれ選択すると、添付されているすべてのベースラインを基準に、選択したオブジェクト全体のコンプライアンス状態とアップデートの数が表示されます。さらに、そのオブジェクトに添付されている各ベースラインを選択すると、そのベースラインのコンプライアンス状態ごとにグループ化されたアップデートの数が表示されます。

手順

- 1 vSphere Client または vSphere Web Client を使用して、Update Manager が登録されている vCenter Server システムに接続します。

2 コンプライアンス情報を表示するオブジェクトのタイプを選択します。

クライアント	手順
vSphere Web Client	<ol style="list-style-type: none"> 表示するコンプライアンス情報によって、次の手順を実行します。 <ol style="list-style-type: none"> ホストのコンプライアンス情報を表示するには、[ホーム] - [ホストおよびクラスタ] を選択し、ホスト、クラスタ、データセンターまたは vCenter Server インスタンスを選択します。 仮想マシンのコンプライアンス情報を表示するには、[ホーム] - [仮想マシンおよびテンプレート] を選択し、仮想マシン、フォルダ、仮想アプライアンスを選択します。 [管理] タブを選択し、[Update Manager] タブを選択します。
vSphere Client	<ol style="list-style-type: none"> 表示するコンプライアンス情報によって、次の手順を実行します。 <ol style="list-style-type: none"> ホストのコンプライアンス情報を表示するには、[ホーム] - [インベントリ] - [ホストおよびクラスタ] を選択し、ホスト、クラスタ、データセンターまたは vCenter Server インスタンスを選択します。 仮想マシンのコンプライアンス情報を表示するには、[ホーム] - [インベントリ] - [仮想マシンおよびテンプレート] を選択し、仮想マシン、フォルダ、仮想アプライアンスを選択します。 [Update Manager] タブを選択します。

3 添付されたベースラインの 1 つを選択し、そのベースラインに対するオブジェクトのコンプライアンス情報を表示します。

アップグレード ベースラインを基準にしたホストの修正

一度につき 1 つの添付されたアップグレード ベースラインを基準に、ESXi ホストを修正できます。ESXi 6.0 イメージを含んだ単一のアップグレード ベースラインを使用して、vSphere インベントリ内のすべてのホストをアップグレードできます。

注： または、ベースライン グループを使用してホストをアップグレードすることもできます。[ベースライン グループを基準にしたホストの修正](#)を参照してください。

Update Manager 6.0 は、ESXi 5.x から ESXi 6.0 へのアップグレードをサポートします。ESXi 5.0、ESXi 5.1 または ESXi 5.5 へのホストのアップグレードは、サポートされていません。

ホストをアップグレードするには、VMware から VMware-VMvisor-Installer-6.0.0-build_number.x86_64.iso 形式の名前で配布されている ESXi インストーラ イメージ、または vSphere ESXi Image Builder を使用して作成されたカスタム イメージを使用します。

ESXi 5.x ホスト上のサードパーティ製ソフトウェア モジュールは、ESXi 6.0 にアップグレードした後も影響を受けません。

注： ESXi 5.x から ESXi 6.0 へのアップグレードに失敗した場合は、以前の ESXi 5.x インスタンスにロールバックすることはできません。

前提条件

アップグレード ベースラインを基準にホストを修正するには、ホストにそのベースラインを添付します。

[アップグレードの詳細] ウィンドウでスキャン メッセージを確認し、ESXi 6.0 へのアップグレードを妨げる可能性のある、ハードウェア、サードパーティ製ソフトウェア、および構成の潜在的な問題がないか確認します。

手順

- 1 vSphere Client または vSphere Web Client を使用して、Update Manager が登録されている vCenter Server システムに接続します。

クライアント	手順
vSphere Web Client	<ol style="list-style-type: none"> 1 [ホーム] - [ホストおよびクラスタ] を選択します。 2 インベントリ オブジェクト ナビゲータで、データセンター、クラスタまたはホストを右クリックし、[Update Manager] - [修正] の順に選択します。 <p>コンテナ オブジェクトを選択する場合、選択したオブジェクトのすべてのホストが修正されます。</p>
vSphere Client	<ol style="list-style-type: none"> 1 ナビゲーション バーで [ホーム] - [インベントリ] - [ホストおよびクラスタ] の順に選択します。 2 オブジェクト ナビゲータで、データセンター、クラスタまたはホストを右クリックし、[修正] を選択します。 <p>コンテナ オブジェクトを選択する場合、選択したオブジェクトのすべてのホストが修正されます。</p>

[修正] ウィザードが開きます。

- 2 [アップグレード ベースライン] を選択します。
 - 3 修正ウィザードの修正の選択ページで、適用するアップグレード ベースラインを選択します。
 - 4 (オプション) 修正するホストを選択し、[次へ] をクリックします。
- 1 台のホストを修正し、コンテナ オブジェクトは修正しない場合、そのホストはデフォルトで選択されます。
- 5 エンド ユーザー使用許諾契約書ページで条項に同意して、[次へ] をクリックします。
 - 6 (オプション) ESXi 6.0 のアップグレード ページで、ホスト上のサポートされていないデバイス、または現在サポートされていない VMFS データストアについての警告を無視するオプションを選択して修正を続行します。
 - 7 [次へ] をクリックします。
 - 8 スケジュール設定ページで、タスクの一意の名前と説明（説明は任意）を入力します。
- スケジュール設定済みのタスクに対して設定した時刻は、Update Manager が接続される vCenter Server インスタンスの時刻です。
- 9 [ただちに] を選択してウィザードを完了した直後に処理を開始するか、修正処理を開始するタイミングを指定して、[次へ] をクリックします。

- 10 ホストの修正オプション ページの [パワー状態] ドロップダウン メニューで、修正するホストで実行されている仮想マシンおよび仮想アプライアンスのパワー状態の変更を選択できます。

オプション	説明
仮想マシンのパワーオフ	修正を行う前に、すべての仮想マシンと仮想アプライアンスをパワーオフします。
仮想マシンのサスペンド	修正を行う前に、すべての実行中の仮想マシンと仮想アプライアンスをサスペンドします。
仮想マシンのパワー状態を変更しない	仮想マシンおよび仮想アプライアンスを現在のパワー状態のままにします。 ホスト上の仮想マシンがパワーオフまたはサスペンドの状態になるか、DRS クラスタ内のほかのホストに vMotion で移行されない限り、ホストはメンテナンス モードを開始できません。

アップデートの一部では、修正の前にホストをメンテナンス モードにすることが求められます。ホストがメンテナンス モードのとき、仮想マシンおよび仮想アプライアンスは実行できません。

仮想マシンの可用性を犠牲にしてホスト修正時のダウンタイムを短縮するには、修正の前に仮想マシンおよび仮想アプライアンスをシャットダウンまたはサスペンドするように選択できます。DRS クラスタで仮想マシンをパワーオフしない場合は修正に時間がかかりますが、仮想マシンが vMotion によってほかのホストに移行されるため、修正プロセス全体にわたって仮想マシンが使用可能になります。

- 11 (オプション) [失敗した場合はメンテナンス モードの開始を再試行] を選択し、再試行の回数を指定して、次の再試行までの待機時間を指定します。

再試行遅延時間の経過後、Update Manager が再度ホストをメンテナンス モードにしようと試みます。これは、[再試行回数] フィールドで指定された回数によって実行されます。

- 12 (オプション) [ホスト上の仮想マシンに接続されているすべてのリムーバブル メディア デバイスを無効にします] を選択します。

Update Manager は、CD ドライブ、DVD ドライブまたはフロッピー ドライブが接続されている仮想マシンが配置されたホストを修正しません。クラスタ化された環境では、接続されているメディア デバイスと同じデバイスまたはマウントされた ISO イメージがターゲット ホストにない場合に、それらのメディア デバイスによって vMotion が使用できなくなる場合があります、その場合、ソース ホストがメンテナンス モードを開始することもできません。

修正後に、取り外し可能なメディア デバイスがまだ利用できる場合は、Update Manager はそれらのデバイスを再接続します。

- 13 [次へ] をクリックします。

14 クラスタ修正オプションを編集します。

クラスタ修正オプション ページを使用できるのは、クラスタのホストを修正する場合のみです。

オプション	詳細
選択したクラスタのいずれかで DPM (Distributed Power Management) が有効になっている場合は無効にする	Update Manager は、DPM がアクティブになっているクラスタを修正しません。 DPM は、クラスタ内で実行中の仮想マシンのリソース使用状況を監視します。十分に余分な容量がある場合、DPM は、クラスタ内のほかのホストへ仮想マシンを移動して、元のホストをスタンバイ モードにして節電することを推奨します。ホストをスタンバイ モードに切り替えると、修正が中断する場合があります。
選択したクラスタのいずれかで High Availability のアドミッション コントロールが有効になっている場合は無効にする	Update Manager は、HA のアドミッション コントロールがアクティブになっているクラスタを修正しません。 アドミッション コントロールは vSphere HA が使用するポリシーです。これにより、クラスタ内のフェイルオーバーのキャパシティが確保されます。修正時に HA のアドミッション コントロールが有効になっている場合、クラスタ内の仮想マシンが vMotion で移行されない場合があります。
選択したホストの仮想マシンで Fault Tolerance (FT) が有効になっている場合は無効にする	ホスト上のいずれかの仮想マシンで FT がオンになっている場合、Update Manager はそのホストを修正しません。 FT を有効にするには、プライマリ仮想マシンとセカンダリ仮想マシンが実行されているホストが同じバージョンで、それらのホストに同じパッチがインストールされている必要があります。それらのホストに異なるパッチを適用すると、FT を再度有効にすることができません。
選択したクラスタ内にあるホストの並行修正を有効にする	クラスタ内の各ホストを並行修正します。この設定が選択されていない場合は、Update Manager はクラスタ内の各ホストを順次修正します。 設計上、Virtual SAN クラスタの 1 台のホストのみをいつでもメンテナンス モードにすることができます。Update Manager は、Virtual SAN クラスタの一部であるホストを並行して修正するオプションを選択した場合にも、これらのホストを順次修正します。 デフォルトでは、Update Manager は、DRS 設定に影響を与えずに同時に修正できるホストの最大数を継続的に確認します。同時に修正されるホスト数は、特定の数に指定できます。 注： Update Manager は、仮想マシンがパワーオフ状態またはサスペンド状態のホストのみを同時に修正します。ホストの修正オプション ページのメンテナンス モードの設定ペインにある [電源状態] メニューから、仮想マシンをパワーオフまたはサスペンドするように選択できます。
ホストをメンテナンス モードにする必要がある場合は、パワーオフおよびサスペンド状態の仮想マシンをクラスタ内のほかのホストに移行する	Update Manager は、サスペンド状態およびパワーオフ状態の仮想マシンを、メンテナンス モードに切り替える必要があるホストから、クラスタ内のほかのホストに移行します。修正を行う前に、メンテナンス モードの設定ペインで仮想マシンをパワーオフまたはサスペンドするように選択できます。

15 (オプション) クラスタ修正オプション ページで [レポートの生成] をクリックしてクラスタ修正オプションのレポートを生成し、[次へ] をクリックします。

16 終了準備の完了ページで [終了] をクリックします。

例

注： [最近のタスク] ペインに、修正タスクが表示され、多くの場合プロセスは 約 22 % で維持されます。プロセスの完了までにおよそ 15 分かかります。

ベースライン グループを基準にしたホストの修正

添付されたアップグレード、パッチ、およびエクステンションのベースライン グループを基準にホストを修正できます。ベースライン グループには、複数のパッチ ベースラインおよびエクステンション ベースラインが含まれるか、複数のパッチ ベースラインおよびエクステンション ベースラインと組み合わせられた 1 つのアップグレード ベースラインが含まれます。

ホスト ベースライン グループを使用して、組織的なアップグレードを実行できます。ベースライン グループのアップグレード ベースラインが最初に実行され、続いてパッチ ベースラインおよびエクステンション ベースラインが実行されます。

注： または、単一のアップグレード ベースラインを使用してホストをアップグレードすることもできます。[アップグレード ベースラインを基準にしたホストの修正](#)を参照してください。

前提条件

少なくとも 1 つのベースライン グループがホストに添付されていることを確認します。

[アップグレードの詳細] ウィンドウでスキャン メッセージを確認し、ESXi 6.0 へのアップグレードを妨げる可能性のある、ハードウェア、サードパーティ製ソフトウェア、および構成の潜在的な問題がないか確認します。

手順

- 1 vSphere Client または vSphere Web Client を使用して、Update Manager が登録されている vCenter Server システムに接続します。

クライアント	手順
vSphere Web Client	<ol style="list-style-type: none"> 1 [ホーム] - [ホストおよびクラスタ] を選択します。 2 インベントリ オブジェクト ナビゲータで、データセンター、クラスタまたはホストを右クリックし、[Update Manager] - [修正] を選択します。 <p>コンテナ オブジェクトを選択する場合、選択したオブジェクトのすべてのホストが修正されます。</p>
vSphere Client	<ol style="list-style-type: none"> 1 ナビゲーション バーで [ホーム] - [インベントリ] - [ホストおよびクラスタ] を選択します。 2 オブジェクト ナビゲータで、データセンター、クラスタまたはホストを右クリックし、[修正] を選択します。コンテナ オブジェクトを選択する場合、選択したオブジェクトのすべてのホストが修正されます。 <p>コンテナ オブジェクトを選択する場合、選択したオブジェクトのすべてのホストが修正されます。</p>

[修正] ウィザードが開きます。

- 2 [修正] ウィザードの修正の選択ページで、適用するベースライン グループまたはベースラインを選択します。
- 3 (オプション) 修正するホストを選択し、[次へ] をクリックします。
1 台のホストを修正し、コンテナ オブジェクトは修正しない場合、そのホストはデフォルトで選択されます。
- 4 エンド ユーザー使用許諾契約書ページで条項に同意して、[次へ] をクリックします。
- 5 (オプション) ESXi 6.0 のアップグレード ページで、ホスト上のサポートされていないデバイス、または現在サポートされていない VMFS データストアについての警告を無視するオプションを選択して修正を続行します。
- 6 [次へ] をクリックします。

- 7 (オプション) パッチとエクステンション ページで、修正対象から除外する特定のパッチまたはエクステンションを選択解除して、[次へ] をクリックします。
- 8 (オプション) 除外する動的パッチおよびエクステンション ページで、除外するパッチまたはエクステンションの一覧を確認し、[次へ] をクリックします。
- 9 スケジュール設定ページで、タスクの一意の名前と説明（説明は任意）を入力します。
スケジュール設定済みのタスクに対して設定した時刻は、Update Manager が接続される vCenter Server インスタンスの時刻です。
- 10 [ただちに] を選択してウィザードを完了した直後に処理を開始するか、修正処理を開始するタイミングを指定して、[次へ] をクリックします。
- 11 ホストの修正オプション ページの [パワー状態] ドロップダウン メニューで、修正するホストで実行されている仮想マシンおよび仮想アプライアンスのパワー状態の変更を選択できます。

オプション	説明
仮想マシンのパワーオフ	修正を行う前に、すべての仮想マシンと仮想アプライアンスをパワーオフします。
仮想マシンのサスペンド	修正を行う前に、すべての実行中の仮想マシンと仮想アプライアンスをサスペンドします。
仮想マシンのパワー状態を変更しない	仮想マシンおよび仮想アプライアンスを現在のパワー状態のままにします。 ホスト上の仮想マシンがパワーオフまたはサスペンドの状態になるか、DRS クラスタ内のほかのホストに vMotion で移行されない限り、ホストはメンテナンス モードを開始できません。

アップデートの一部では、修正の前にホストをメンテナンス モードにすることが求められます。ホストがメンテナンス モードのとき、仮想マシンおよび仮想アプライアンスは実行できません。

仮想マシンの可用性を犠牲にしてホスト修正時のダウンタイムを短縮するには、修正の前に仮想マシンおよび仮想アプライアンスをシャットダウンまたはサスペンドするように選択できます。DRS クラスタで仮想マシンをパワーオフしない場合は修正に時間がかかりますが、仮想マシンが vMotion によってほかのホストに移行されるため、修正プロセス全体にわたって仮想マシンが使用可能になります。

- 12 (オプション) [失敗した場合はメンテナンス モードの開始を再試行] を選択し、再試行の回数を指定して、次の再試行までの待機時間を指定します。

再試行遅延時間の経過後、Update Manager が再度ホストをメンテナンス モードにしようと試みます。これは、[再試行回数] フィールドで指定された回数によって実行されます。

- 13 (オプション) [ホスト上の仮想マシンに接続されているすべてのリムーバブル メディア デバイスを無効にします] を選択します。

Update Manager は、CD ドライブ、DVD ドライブまたはフロッピー ドライブが接続されている仮想マシンが配置されたホストを修正しません。クラスタ化された環境では、接続されているメディア デバイスと同じデバイスまたはマウントされた ISO イメージがターゲット ホストにない場合に、それらのメディア デバイスによって vMotion が使用できなくなる場合があります。その場合、ソース ホストがメンテナンス モードを開始することもできません。

修正後に、取り外し可能なメディア デバイスがまだ利用できる場合は、Update Manager はそれらのデバイスを再接続します。

- 14 (オプション) ESXi のパッチ設定のチェック ボックスを選択して、Update Manager がパワーオン状態の PXE 起動の ESXi ホストをパッチできるようにします。

このオプションは、パッチ ベースラインまたはエクステンション ベースラインを基準にホストを修正する場合にのみ表示されます。

- 15 [次へ] をクリックします。

- 16 クラスタ修正オプションを編集します。

クラスタ修正オプション ページを使用できるのは、クラスタのホストを修正する場合のみです。

オプション	詳細
選択したクラスタのいずれかで DPM (Distributed Power Management) が有効になっている場合は無効にする	Update Manager は、DPM がアクティブになっているクラスタを修正しません。 DPM は、クラスタ内で実行中の仮想マシンのリソース使用状況を監視します。十分に余分な容量がある場合、DPM は、クラスタ内のほかのホストへ仮想マシンを移動して、元のホストをスタンバイ モードにして節電することを推奨します。ホストをスタンバイ モードに切り替えると、修正が中断する場合があります。
選択したクラスタのいずれかで High Availability のアドミッション コントロールが有効になっている場合は無効にする	Update Manager は、HA のアドミッション コントロールがアクティブになっているクラスタを修正しません。 アドミッション コントロールは vSphere HA が使用するポリシーです。これにより、クラスタ内のフェイルオーバーのキャパシティが確保されます。修正時に HA のアドミッション コントロールが有効になっている場合、クラスタ内の仮想マシンが vMotion で移行されない場合があります。
選択したホストの仮想マシンで Fault Tolerance (FT) が有効になっている場合は無効にする	ホスト上のいずれかの仮想マシンで FT がオンになっている場合、Update Manager はそのホストを修正しません。 FT を有効にするには、プライマリ仮想マシンとセカンダリ仮想マシンが実行されているホストが同じバージョンで、それらのホストに同じパッチがインストールされている必要があります。それらのホストに異なるパッチを適用すると、FT を再度有効にすることができません。
選択したクラスタ内にあるホストの並行修正を有効にする	クラスタ内の各ホストを並行修正します。この設定が選択されていない場合は、Update Manager はクラスタ内の各ホストを順次修正します。 設計上、Virtual SAN クラスタの 1 台のホストのみをいつでもメンテナンス モードにすることができます。Update Manager は、Virtual SAN クラスタの一部であるホストを並行して修正するオプションを選択した場合にも、これらのホストを順次修正します。 デフォルトでは、Update Manager は、DRS 設定に影響を与えずに同時に修正できるホストの最大数を継続的に確認します。同時に修正されるホスト数は、特定の数に指定できます。 注： Update Manager は、仮想マシンがパワーオフ状態またはサスペンド状態のホストのみを同時に修正します。ホストの修正オプション ページのメンテナンス モードの設定ペインにある [電源状態] メニューから、仮想マシンをパワーオフまたはサスペンドするように選択できます。
ホストをメンテナンス モードにする必要がある場合は、パワーオフおよびサスペンド状態の仮想マシンをクラスタ内のほかのホストに移行する	Update Manager は、サスペンド状態およびパワーオフ状態の仮想マシンを、メンテナンス モードに切り替える必要があるホストから、クラスタ内のほかのホストに移行します。修正を行う前に、メンテナンス モードの設定ペインで仮想マシンをパワーオフまたはサスペンドするように選択できます。

- 17 (オプション) クラスタ修正オプション ページで [レポートの生成] をクリックしてクラスタ修正オプションのレポートを生成し、[次へ] をクリックします。

- 18 終了準備の完了ページで [終了] をクリックします。

例

注： [最近のタスク] ペインに、修正タスクが表示され、プロセスは多くの場合、約 22 % で維持されます。プロセスはまだ実行中で、完了までにおよそ 15 分かかります。

スクリプトを使用した、ホストのインストールまたはアップグレード

スクリプトを使用した無人インストールまたはアップグレードを行って、ESXi ホストを簡単にデプロイできます。スクリプトを使用したインストールまたはアップグレードでは、複数のホストを効率的にデプロイできます。

インストールまたはアップグレード スクリプトには、ESXi のインストール設定が含まれます。スクリプトは、同様の構成にするホストすべてに適用できます。

スクリプトでインストールまたはアップグレードする場合、サポートされているコマンドを使用してスクリプトを作成する必要があります。スクリプトを編集し、各ホストに固有の設定を変更できます。

インストールまたはアップグレード スクリプトは、次のいずれかの場所に配置できます。

- FTP サーバ
- HTTP/HTTPS サーバ
- NFS サーバ
- USB フラッシュ ドライブ
- CD-ROM ドライブ

インストール スクリプトまたはアップグレード スクリプトを開始するための起動オプションの入力

インストール スクリプトまたはアップグレード スクリプトを起動するには、ESXi インストーラの起動コマンド ラインで起動オプションを入力します。

起動時に、キックスタート ファイルへのアクセス オプションの指定が必要な場合があります。起動オプションは、ブート ロードで Shift + O を押すことで入力できます。PXE 起動のインストールの場合は、boot.cfg ファイルの kernelopts 行を使用してオプションを渡すことができます。 [boot.cfg ファイルについて](#) および [ESXi インストーラの PXE 起動](#) を参照してください。

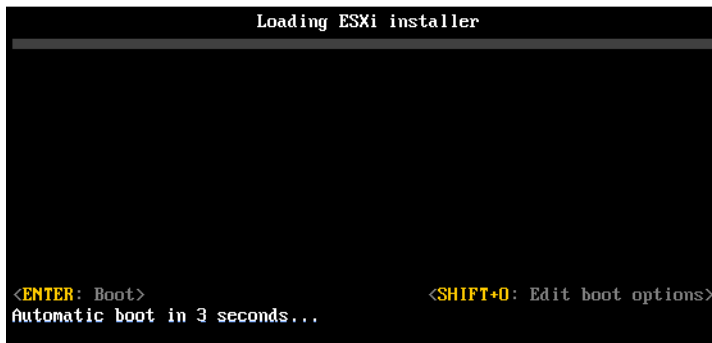
インストール スクリプトの場所を指定するには、ks=filepath オプションを設定します。ここで、filepath は、キックスタート ファイルの場所を示します。このオプションを設定しないと、スクリプトを使用したインストールまたはアップグレードを開始できません。ks=filepath を省略すると、テキスト インストーラが実行されます。

サポートされている起動オプションは [起動オプション](#) に記載されています。

手順

- 1 ホストを起動します。

- 2 ESXi インストーラのウィンドウが表示されたら、Shift + O を押して起動オプションを編集します。



- 3 `runweasel` コマンド プロンプトで、
`ks=location of installation script plus boot command-line options` と入力します。

例： 起動オプション

次の起動オプションを入力します。

```
ks=http://00.00.00.00/kickstart/ks-osdc-pdp101.cfg nameserver=00.00.0.0 ip=00.00.00.000
netmask=255.255.255.0 gateway=00.00.00.000
```

起動オプション

スクリプトを使用したインストールを実行する際には、起動時にキックスタート ファイルへのアクセス オプションを指定することが必要な場合があります。

サポートされる起動オプション

表 9-1. ESXi インストール用の起動オプション

起動オプション	説明
<code>BOOTIF=hwtype-MAC address</code>	<code>netdevice</code> オプションに似ていますが、 syslinux.zytor.com サイトで SYSLINUX の IPAPPEND オプションで説明されている、PXELINUX 形式に関する点が異なります。
<code>gateway=ip address</code>	このネットワーク ゲートウェイを、インストール スクリプトおよびインストール メディアをダウンロードするために使用する、デフォルトのゲートウェイとして設定します。
<code>ip=ip address</code>	インストール スクリプトおよびインストール メディアのダウンロードに使用する固定 IP アドレスを設定します。注：このオプションでは PXELINUX 形式もサポートされています。 syslinux.zytor.com のサイトで、SYSLINUX の中の IPAPPEND オプションを参照してください。

表 9-1. ESXi インストール用の起動オプション（続き）

起動オプション	説明
<code>ks=cdrom:/path</code>	<p><i>path</i>にあるスクリプトによるインストールを実行します。このスクリプトは CD-ROM ドライブの CD にあります。各 CDROM は、このパスと一致するファイルが見つかるまでマウントされ、チェックされます。</p> <p>重要： カスタム インストールまたはアップグレード スクリプトを使用してインストーラ ISO イメージを作成した場合は、大文字を使用してスクリプトのパスを入力する必要があります。例：<code>ks=cdrom:/KS_CUST.CFG</code>。</p>
<code>ks=file://path</code>	<i>path</i> にあるスクリプトを使用してインストールを実行します。
<code>ks=protocol://serverpath</code>	ネットワーク上の指定された URL に置かれたスクリプトを使用してインストールを実行します。 <i>protocol</i> は、http、https、ftp、または nfs になります。nfs プロトコルを使用している例は、 <code>ks=nfs://host/porturl-path</code> です。NFS URL の形式は、RFC 2224 で指定されています。
<code>ks=usb</code>	接続された USB ドライブにあるスクリプトにアクセスして、インストールを実行します。 <code>ks.cfg</code> という名前のファイルが検索されます。このファイルは、ドライブのルート ディレクトリに置かれている必要があります。複数の USB フラッシュ ドライブが接続されている場合は、 <code>ks.cfg</code> ファイルが見つかるまでそれらのドライブが検索されます。サポートされているのは FAT16 および FAT32 のファイル システムだけです。
<code>ks=usb:/path</code>	USB 上にある、指定されたパスにあるスクリプト ファイルを使用して、スクリプトによるインストールを実行します。
<code>ksdevice=device</code>	インストール スクリプトとインストール メディアの検索時にネットワーク アダプタ <i>device</i> の使用を試みます。MAC アドレス (00:50:56:C0:00:01 など) で指定します。この場所は vmnicNN 名にもできます。このサブコマンドを指定せず、ネットワーク経由でファイルを取得する必要がある場合は、最初に検出された接続済みネットワーク アダプタがデフォルトで使用されます。
<code>nameserver=ip address</code>	インストール スクリプトとインストール メディアのダウンロードに使用するドメイン名サーバを指定します。
<code>netdevice=device</code>	インストール スクリプトとインストール メディアの検索時にネットワーク アダプタ <i>device</i> の使用を試みます。MAC アドレス (00:50:56:C0:00:01 など) で指定します。この場所は vmnicNN 名にもできます。このサブコマンドを指定せず、ネットワーク経由でファイルを取得する必要がある場合は、最初に検出された接続済みネットワーク アダプタがデフォルトで使用されます。
<code>netmask=subnet mask</code>	インストール スクリプトおよびインストール メディアをダウンロードするネットワーク インターフェイスのサブネット マスクを指定します。
<code>vlanid=vlanid</code>	指定した VLAN 上に置くネットワーク カードを構成します。

インストール スクリプトおよびアップグレード スクリプトについて

インストール/アップグレード スクリプトはサポートされているコマンドを含むテキストファイルで、たとえば `ks.cfg` などがあります。

スクリプトのコマンド セクションには、ESXi のインストール オプションが含まれます。このセクションは必須で、スクリプトの先頭にある必要があります。

サポートされている、インストールまたはアップグレード スクリプトの保存場所

スクリプトを使用したインストールおよびアップグレードで ESXi インストーラがインストールまたはアップグレード スクリプト（キックスタート ファイル）にアクセスできる場所は、いくつかあります。

インストールまたはアップグレード スクリプトの保存場所として、次のメディアおよび場所を使用できます。

- CD/DVD。カスタムのインストールまたはアップグレード スクリプトを含む、インストーラ ISO イメージの作成を参照してください。
- USB フラッシュ ドライブ。USB フラッシュ ドライブを作成して、ESXi インストール スクリプトまたはアップグレード スクリプトを保存するを参照してください。
- 次のプロトコルでアクセス可能なネットワークの場所。NFS、HTTP、HTTPS、FTP

インストールまたはアップグレード スクリプトのパス

インストールまたはアップグレード スクリプトのパスを指定できます。

`ks=http://XXX.XXX.XXX.XXX/kickstart/KS.CFG` は、ESXi のインストール スクリプトのパスです。`XXX.XXX.XXX.XXX` には、スクリプトが置かれたマシンの IP アドレスを指定します。インストール スクリプトおよびアップグレード スクリプトについてを参照してください。

対話型インストールの場合にインストール スクリプトを起動するには、`ks=` オプションを手動で入力します。インストール スクリプトまたはアップグレード スクリプトを開始するための起動オプションの入力を参照してください。

インストール スクリプトおよびアップグレード スクリプトのコマンド

デフォルトのインストールまたはアップグレード スクリプトを変更する場合や、独自のスクリプトを作成する場合には、サポートされているコマンドを使用します。インストーラの起動時に起動コマンドで指定するインストール スクリプトでは、サポートされているコマンドを使用します。

ESXi をインストールまたはアップグレードするディスクを判断するには、インストール スクリプトに `install` または `upgrade` または `installorupgrade` のいずれかのコマンドが必要です。`install` コマンドでは、ほかのパーティションが作成されたあとに使用可能なすべての領域を占有する VMFS データストアを含む、デフォルトのパーティションが作成されます。

accepteula または vmaccepteula（必須）

ESXi の使用許諾契約書に同意します。

clearpart (任意)

ディスク上の既存のパーティションをすべてクリアします。install コマンドを指定する必要があります。既存のスクリプトの clearpart コマンドを編集するときには注意してください。

<code>--drives=</code>	指定したドライブ上のパーティションを削除します。
<code>--alldrives</code>	<code>--drives=</code> の要件を無視し、すべてのドライブのパーティションの削除を可能にします。
<code>--ignoredrives=</code>	指定するドライブ以外のすべてのドライブのパーティションを削除します。 <code>--drives=</code> フラグまたは <code>--alldrives</code> フラグを指定していない場合に必要です。
<code>--overwritevmfs</code>	指定したドライブ上の VMFS パーティションの上書きを可能にします。デフォルトでは、VMFS パーティションの上書きは許可されません。
<code>--firstdisk=</code> <code>disk-type1</code> <code>[disk-type2,...]</code>	最初に検出された、対象となるディスクをパーティショニングします。デフォルトでは、対象となるディスクは次の順序で設定されます。 <ol style="list-style-type: none"> ローカルに接続されたストレージ (local) ネットワーク ストレージ (remote) USB ディスク (usb) <p>引数に添付されたコンマ区切りのリストを使用して、ディスクの順序を変更できます。フィルタ リストを指定すると、デフォルト設定が上書きされます。フィルタ (ESXi がインストールされる最初のディスクの esx、モデルおよびベンダー情報、VMkernel デバイス ドライバの名前など) を組み合わせて、特定のディスクを指定できます。たとえば、モデル名が ST3120814A のディスク、および通常のローカル ディスクではなく mptsas ドライバを使用するディスクを指定する場合、引数は <code>--firstdisk=ST3120814A,mptsas,local</code> になります。</p>

dryrun (任意)

インストール スクリプトを解析し、確認します。インストールは実行されません。

install

これが新規インストールであることを指定します。スクリプトを使用した ESXi 4.1 のインストールに使用された、廃止になった autopart コマンドの代わりに使用します。ESXi をインストールまたはアップグレードするディスクを判断するには、install、upgrade、または installorupgrade コマンドが必要です。

<code>--disk=</code> or <code>--drive=</code>	パーティショニングするディスクを指定します。コマンド <code>--disk=diskname</code> では、 <i>diskname</i> が以下のような形式で表示されます。 <ul style="list-style-type: none"> パス : <code>--disk=/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0</code> MPX 名 : <code>--disk=mpx.vmhba1:C0:T0:L0</code> VML 名 : <code>--disk=vml.000000034211234</code>
---	---

■ vmkLUN UID : `--disk=vmkLUN_UID`

使用できるディスク名形式については、[ディスク デバイス名](#) を参照してください。

`--firstdisk=`
`disk-type1,`
`[disk-type2,...]`

最初に検出された、対象となるディスクをパーティショニングします。デフォルトでは、対象となるディスクは次の順序で設定されます。

- 1 ローカルに接続されたストレージ (local)
- 2 ネットワーク ストレージ (remote)
- 3 USB ディスク (usb)

引数に添付されたコンマ区切りのリストを使用して、ディスクの順序を変更できます。フィルタ リストを指定すると、デフォルト設定が上書きされます。ESX がインストールされた最初のディスクを指定する `esx`、モデルおよびベンダー情報、`vmkernel` デバイス ドライバの名前など、フィルタを組み合わせて特定のディスクを指定することができます。たとえば、モデル名が ST3120814A のディスク、および通常のローカル ディスクではなく `mptsas` ドライバを使用するディスクを指定する場合、引数は `--firstdisk=ST3120814A,mptsas,local` になります。

`--ignoressd`

パーティショニングの対象からソリッド ステート ディスクを除外します。このオプションは、`install` コマンドおよび `--firstdisk` オプションとともに使用できます。このオプションは `--firstdisk` オプションよりも優先されます。また、`upgrade` コマンドおよび `installorupgrade` コマンドと、`--drive` オプションまたは `--disk` オプションと同時に使用しても無効になります。自動パーティション化の際に SSD のフォーマットを避けるための詳細については、『vSphere ストレージ』ドキュメントを参照してください。

`--overwritevsan`

Virtual SAN ディスク グループ内のディスク (SSD または HDD (磁気)) に ESXi をインストールする場合は、`--overwritevsan` オプションを使用する必要があります。選択したディスクに Virtual SAN パーティションがない状態でこのオプションを使用した場合、インストールは失敗します。Virtual SAN ディスク グループ内のディスクに ESXi をインストールする場合、結果は選択したディスクによって異なります。

- SSD を選択した場合は、同じディスク グループ内の SSD および基盤となるすべての HDD がワイプされます。
- HDD を選択した場合は、ディスク グループのサイズが 2 より大きくなり、選択した HDD のみワイプされます。
- HDD ディスクを選択した場合は、ディスク グループのサイズが 2 以下になり、SSD および選択した HDD がワイプされます。

Virtual SAN ディスク グループの管理の詳細については、『vSphere ストレージ』ドキュメントを参照してください。

`--overwritevmfs`

インストール前に、ディスク上の既存の VMFS データストアを上書きするために必要です。

<code>--preservevmfs</code>	インストール時に、ディスク上の既存の VMFS データストアを保持します。
<code>--novmfsdisk</code>	このディスク上に VMFS パーティションが作成されないようにします。ディスク上に VMFS パーティションが既に存在する場合は、 <code>--overwritevmfs</code> と共に使用する必要があります。

installorupgrade

ESXi をインストールまたはアップグレードするディスクを判断するには、`install`、`upgrade`、または `installorupgrade` コマンドが必要です。

<code>--disk=</code> or <code>--drive=</code>	パーティショニングするディスクを指定します。コマンド <code>--disk=diskname</code> では、 <i>diskname</i> が以下のような形式で表示されます。 <ul style="list-style-type: none"> ■ パス：<code>--disk=/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0</code> ■ MPX 名：<code>--disk=mpx.vmhba1:C0:T0:L0</code> ■ VML 名：<code>--disk=vml.000000034211234</code> ■ vmkLUN UID：<code>--disk=vmkLUN_UID</code>
---	---

使用できるディスク名形式については、[ディスク デバイス名](#) を参照してください。

<code>--firstdisk=</code> <i>disk-type1</i> , [<i>disk-type2</i> ,...]	最初に検出された、対象となるディスクをパーティショニングします。デフォルトでは、対象となるディスクは次の順序で設定されます。 <ol style="list-style-type: none"> 1 ローカルに接続されたストレージ (local) 2 ネットワーク ストレージ (remote) 3 USB ディスク (usb)
---	---

引数に添付されたコンマ区切りのリストを使用して、ディスクの順序を変更できます。フィルタ リストを指定すると、デフォルト設定が上書きされます。ESX がインストールされた最初のディスクを指定する `esx`、モデルおよびベンダー情報、`vmkernel` デバイス ドライバの名前など、フィルタを組み合わせると特定のディスクを指定することができます。たとえば、モデル名が ST3120814A のディスク、および通常のローカル ディスクではなく `mptsas` ドライバを使用するディスクを指定する場合、引数は `--firstdisk=ST3120814A,mptsas,local` になります。

<code>--overwritevsan</code>	Virtual SAN ディスク グループ内のディスク (SSD または HDD (磁気)) に ESXi をインストールする場合は、 <code>--overwritevsan</code> オプションを使用する必要があります。選択したディスクに Virtual SAN パーティションがない状態でこのオプションを使用した場合、インストールは失敗します。Virtual SAN ディスク グループ内のディスクに ESXi をインストールする場合、結果は選択したディスクによって異なります。 <ul style="list-style-type: none"> ■ SSD を選択した場合は、同じディスク グループ内の SSD および基盤となるすべての HDD がワイプされます。
------------------------------	---

- HDD を選択した場合は、ディスク グループのサイズが 2 より大きくなり、選択した HDD のみワイプされます。
- HDD ディスクを選択した場合は、ディスク グループのサイズが 2 以下になり、SSD および選択した HDD がワイプされます。

Virtual SAN ディスク グループの管理の詳細については、『vSphere ストレージ』ドキュメントを参照してください。

`--overwritevmfs`

ディスク上に VMFS パーティションが存在するが、ESX または ESXi のインストールは存在しない場合に、ESXi をインストールします。このオプションを指定しないと、ディスク上に VMFS パーティションが存在するが ESX または ESXi が存在しない場合、インストーラの実行に失敗します。

keyboard (任意)

システムのキーボード タイプを設定します。

keyboardType

選択したキーボード タイプのキーボード マップを指定します。 *keyboardType* には、次のいずれかを指定する必要があります。

- ベルギー語
- ポルトガル語 (ブラジル)
- クロアチア語
- チェコスロバキア語
- デンマーク語
- デフォルト
- エストニア語
- フィンランド語
- フランス語
- ドイツ語
- ギリシャ語
- アイスランド語
- イタリア語
- 日本語
- ラテン アメリカ言語
- ノルウェー語
- ポーランド語
- ポルトガル語

- Russian
- スロベニア語
- スペイン語
- スウェーデン語
- フランス語 (スイス)
- ドイツ語 (スイス)
- トルコ語
- 米国 Dvorak
- ウクライナ語
- 英語 (英国)

serialnum または vmserialnum (任意)

ESXi 5.0.x では廃止されました。ESXi 5.1 以降でサポートされています。ライセンスを構成します。指定しなかった場合、ESXi は評価モードでインストールされます。

`--esx=<license-key>` 使用する vSphere のライセンス キーを指定します。形式は 5 文字のグループを連結したものです (XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX)。

network (任意)

システムのネットワーク アドレスを指定します。

`--bootproto=[dhcp|static]` ネットワーク設定を DHCP から取得するか手動で設定するかを指定します。

`--device=` ネットワーク カードの MAC アドレスを指定するか、vmnicNN 形式で vmnic0 のようにデバイス名を指定します。このオプションは、仮想スイッチのアップリンク デバイスを参照します。

`--ip=` インストールするマシンの IP アドレスを xxx.xxx.xxx.xxx 形式で設定します。--bootproto=static オプションを指定する場合に必要です。それ以外の場合は無視されます。

`--gateway=` デフォルトのゲートウェイを IP アドレスで、xxx.xxx.xxx.xxx 形式で指定します。--bootproto=static オプションと同時に使用します。

`--nameserver=` プライマリ ネーム サーバを IP アドレスとして指定します。 --bootproto=static オプションと同時に使用します。DNS を使用しない場合はこのオプションは省略します。

--nameserver オプションでは、2 つの IP アドレスを指定することもできます。
例: `--nameserver="10.126.87.104[,10.126.87.120]"`

<code>--netmask=</code>	インストールしたシステムのサブネット マスクを 255.xxx.xxx.xxx 形式で指定します。--bootproto=static オプションと同時に使用します。
<code>--hostname=</code>	インストールしたシステムのホスト名を指定します。
<code>--vlanid= <i>vlanid</i></code>	システムの VLAN を指定します。--bootproto=dhcp オプションまたは --bootproto=static オプションと同時に使用します。1 ~ 4096 の整数を指定します。
<code>--addvmportgroup=(0 1)</code>	仮想マシンで使用される仮想マシン ネットワークのポート グループを追加するかどうかを指定します。デフォルト値は 1 です。

paranoid (任意)

警告メッセージでインストールが中断されます。このコマンドを省略した場合、警告メッセージが記録されます。

part または partition (任意)

追加の VMFS データストアをシステムに作成します。作成できるデータストアは、各ディスクにつき 1 つだけです。install コマンドと同じディスクでは使用できません。ディスクごとに 1 つのパーティションしか指定できず、指定するのは VMFS パーティションでなければなりません。

<code>datastore name</code>	パーティションのマウント先を指定します。
<code>--ondisk= or --ondrive=</code>	パーティションを作成するディスクまたはドライブを指定します。
<code>--firstdisk=</code> <code>disk-type1,</code> <code>[disk-type2,...]</code>	最初に検出された、対象となるディスクをパーティショニングします。デフォルトでは、対象となるディスクは次の順序で設定されます。 1 ローカルに接続されたストレージ (local) 2 ネットワーク ストレージ (remote) 3 USB ディスク (usb) 引数に添付されたコンマ区切りのリストを使用して、ディスクの順序を変更できます。フィルタ リストを指定すると、デフォルト設定が上書きされます。ESX がインストールされた最初のディスクを指定する esx、モデルおよびベンダー情報、vmkernel デバイス ドライバの名前など、フィルタを組み合わせて特定のディスクを指定することができます。たとえば、モデル名が ST3120814A のディスク、および通常のローカル ディスクではなく mptsas ドライバを使用するディスクを指定する場合、引数は --firstdisk=ST3120814A,mptsas,local になります。

reboot (任意)

スクリプトを使用したインストールが完了したあと、マシンを再起動します。

<code><--noeject></code>	CD は、インストール後に取り外されません。
--------------------------------	------------------------

rootpw (必須)

システムの root パスワードを設定します。

--iscrypted パスワードが暗号化されていることを示します。

password パスワード値を指定します。

アップグレード

ESXi をインストールまたはアップグレードするディスクを判断するには、install、upgrade、または installorupgrade コマンドが必要です。

--disk= or --drive= パーティショニングするディスクを指定します。コマンド **--disk=diskname** では、*diskname* が以下のような形式で表示されます。

- パス : **--disk=/vmfs/devices/disks/mpx.vmhbal:C0:T0:L0**
- MPX 名 : **--disk=mpx.vmhbal:C0:T0:L0**
- VML 名 : **--disk=vm1.000000034211234**
- vmkLUN UID : **--disk=vmkLUN_UID**

使用できるディスク名形式については、[ディスク デバイス名](#) を参照してください。

--firstdisk= 最初に検出された、対象となるディスクをパーティショニングします。デフォルトでは、対象となるディスクは次の順序で設定されます。

disk-type1,

[disk-type2,...]

- 1 ローカルに接続されたストレージ (local)
- 2 ネットワーク ストレージ (remote)
- 3 USB ディスク (usb)

引数に添付されたコンマ区切りのリストを使用して、ディスクの順序を変更できます。フィルタ リストを指定すると、デフォルト設定が上書きされます。ESX がインストールされた最初のディスクを指定する **esx**、モデルおよびベンダー情報、**vmkernel** デバイス ドライバの名前など、フィルタを組み合わせて特定のディスクを指定することができます。たとえば、モデル名が ST3120814A のディスク、および通常のローカル ディスクではなく **mptsas** ドライバを使用するディスクを指定する場合、引数は **--firstdisk=ST3120814A,mptsas,local** になります。

%include または include (任意)

解析する別のインストール スクリプトを指定します。このコマンドはマルチライン コマンドと同様に処理されますが、1 つの引数だけを使用します。

filename 例 : **%include part.cfg**

%pre (任意)

キックスタート構成が評価される前に実行するスクリプトを指定します。たとえば、含めるキックスタート ファイル用にファイルを生成する際に使用できます。

```
--interpreter          使用するインタプリタを指定します。デフォルトは busybox です。
=[python|busybox]
```

%post (任意)

パッケージのインストールが完了したあとに、指定したスクリプトを実行します。複数の %post セクションを指定した場合は、インストール スクリプト内に出現する順序で実行されます。

```
--interpreter          使用するインタプリタを指定します。デフォルトは busybox です。
=[python|busybox]

--timeout=secs         スクリプト実行時のタイムアウトを指定します。タイムアウトになったときにスクリプトが終了していなかった場合、スクリプトは強制的に終了されます。

--ignorefailure        true を指定した場合、%post スクリプトがエラーで終了しても、インストールは正常に終了したと見なされます。
=[true|false]
```

%firstboot

最初の起動中のみ実行する init スクリプトを作成します。このスクリプトは、次回以降の起動では無効になります。複数の %firstboot セクションを指定した場合は、キックスタート ファイル内に出現する順序で実行されます。

注： %firstboot スクリプトのセマンティックの確認は、システムが最初に起動するまで実行できません。

%firstboot スクリプトに、インストールが完了したあとでなければ分からない、深刻なエラーが含まれている場合があります。

```
--interpreter          使用するインタプリタを指定します。デフォルトは busybox です。
=[python|busybox]
```

注： %firstboot スクリプトのセマンティックの確認は、システムが最初に起動するまで実行できません。スクリプトにエラーが含まれていても、インストールが完了するまで検出されません。

ディスク デバイス名

インストール スクリプトのコマンド install、upgrade、および installorupgrade では、ディスク デバイス名を指定する必要があります。

表 9-2. ディスク デバイス名

フォーマット	例	説明
VML	vml.00025261	VMkernel が報告するデバイス名
MPX	mpx.vmhba0:C0:T0:L0	デバイス名

boot.cfg ファイルについて

ブート ロードー構成ファイル `boot.cfg` は、`mboot.c32` ブート ロードーが ESXi のインストールで使用するカーネル、カーネル オプション、およびブート モジュールを指定します。

`boot.cfg` ファイルは ESXi のインストーラで提供されます。`boot.cfg` ファイルの `kernelopt` 行を変更して、インストール スクリプトの場所を指定したり、ほかのブート オプションを渡したりすることができます。

`boot.cfg` ファイルの構文は次のとおりです。

```
# boot.cfg -- mboot configuration file
#
# Any line preceded with '#' is a comment.

title=STRING
kernel=FILEPATH
kernelopt=STRING
modules=FILEPATH1 --- FILEPATH2... --- FILEPATHn

# Any other line must remain unchanged.
```

`boot.cfg` に記述されるコマンドがブート ロードーを構成します。

表 9-3. `boot.cfg` に記述されるコマンド

コマンド	説明
<code>title=STRING</code>	ブート ロードーのタイトルを <code>STRING</code> に設定します。
<code>kernel=FILEPATH</code>	カーネル パスを <code>FILEPATH</code> に設定します。
<code>kernelopt=STRING</code>	カーネル ブート オプションに <code>STRING</code> を追加します。
<code>modules=FILEPATH1 --- FILEPATH2... --- FILEPATHn</code>	読み込むモジュールを 3 つのハイフン (---) で区切ってリストします。

たとえば、HTTP サーバの情報を使用して `boot.cfg` ファイルを変更する場合は、[gPXE を使用した ESXi インストーラの PXE 起動](#)を参照してください。

カスタムのインストールまたはアップグレード スクリプトを含む、インストーラ ISO イメージの作成、[PXELINUX および PXE 構成ファイルを使用した、ESXi インストーラの PXE 起動](#)、[PXELINUX および isolinux.cfg PXE 構成ファイルを使用した ESXi インストーラの PXE 起動](#)、および [ESXi インストーラの PXE 起動](#)も参照してください。

スクリプトを使用した、CD または DVD からの ESXi のインストールまたはアップグレード

インストールまたはアップグレードのオプションを指定するスクリプトを使用して、CD-ROM または DVD-ROM ドライブから ESXi をインストールまたはアップグレードすることができます。

ホスト起動時に起動オプションを入力して、インストール スクリプトまたはアップグレード スクリプトを起動できます。インストール スクリプトが含まれているインストーラ ISO イメージを作成することもできます。インストーラ ISO イメージを使用すると、インストーラ ISO イメージを起動するときに、スクリプトを使用した無人インストールを実行できます。[カスタムのインストールまたはアップグレード スクリプトを含む、インストーラ ISO イメージの作成](#) を参照してください。

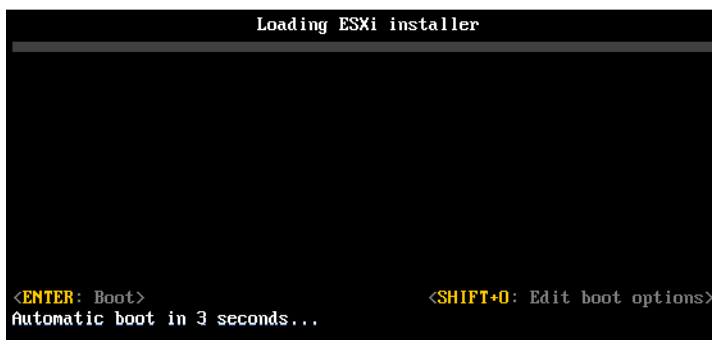
前提条件

スクリプトを使用したインストールまたはアップグレードを実行する前に、次の前提条件を満たしているかどうかを確認します。

- インストールまたはアップグレードを実行するシステムがハードウェア要件を満たしていること。[ESXi のハードウェア要件](#) を参照してください。
- インストール CD または DVD に ESXi インストーラ ISO があること。[ESXi インストーラ ISO イメージのダウンロードおよび CD または DVD への書き込み](#) を参照してください。
- デフォルトのインストール/アップグレード スクリプト (`ks.cfg`) またはカスタムのインストール/アップグレード スクリプトがシステムにアクセスできること。[インストール スクリプトおよびアップグレード スクリプトについて](#) を参照してください。
- スクリプトを使用したインストールまたはアップグレードを実行するための起動コマンドを選択済みであること。[インストール スクリプトまたはアップグレード スクリプトを開始するための起動オプションの入力](#) を参照してください。起動コマンドの完全なリストについては、[起動オプション](#) を参照してください。

手順

- 1 ローカルの CD-ROM または DVD-ROM ドライブから ESXi のインストーラを起動します。
- 2 ESXi インストーラのウィンドウが表示されたら、Shift + O を押して起動オプションを編集します。



- 3 デフォルトのインストール/アップグレード スクリプト、または作成したインストール/アップグレード スクリプト ファイルを呼び出す起動オプションを入力します。

起動オプションの形式は `ks=` です。

4 [Enter] を押します。

結果

指定したオプションを使用して、インストール、アップグレード、または移行が実行されます。

スクリプトを使用した、USB フラッシュ ドライブからの ESXi のインストールまたはアップグレード

インストールまたはアップグレードのオプションを指定するスクリプトを使用して、USB フラッシュ ドライブから ESXi をインストールまたはアップグレードすることができます。

サポートされている起動オプションは [起動オプション](#) に記載されています。

前提条件

スクリプトを使用したインストールまたはアップグレードを実行する前に、次の前提条件を満たしているかどうかを確認します。

- ESXi のインストールまたはアップグレードを実行するシステムが、インストールまたはアップグレード用のハードウェア要件を満たしていること。 [ESXi のハードウェア要件](#) を参照してください。
- 起動可能な USB フラッシュ ドライブに ESXi インストーラ ISO があること。 [USB フラッシュ ドライブのフォーマットによる ESXi インストールまたはアップグレードの起動](#) を参照してください。
- デフォルトのインストール/アップグレード スクリプト (ks.cfg) またはカスタムのインストール/アップグレード スクリプトがシステムにアクセスできること。 [インストール スクリプトおよびアップグレード スクリプトについて](#) を参照してください。
- スクリプトを使用したインストール、アップグレード、または移行を実行するための起動オプションを選択済みであること。 [インストール スクリプトまたはアップグレード スクリプトを開始するための起動オプションの入力](#) を参照してください。

手順

- 1 USB フラッシュ ドライブから ESXi のインストーラを起動します。
- 2 ESXi インストーラのウィンドウが表示されたら、Shift + O を押して起動オプションを編集します。



- 3 デフォルトのインストール/アップグレード スクリプト、または作成したインストール/アップグレード スクリプト ファイルを呼び出す起動オプションを入力します。

起動オプションの形式は `ks=` です。

- 4 [Enter] を押します。

結果

指定したオプションを使用して、インストール、アップグレード、または移行が実行されます。

インストーラの PXE 起動による、スクリプトを使用した ESXi のインストールまたはアップグレードの実行

ESXi 6.0 には、インストーラを PXE 起動し、インストール スクリプトまたはアップグレード スクリプトを使用する、多くのオプションがあります。

- PXE インフラストラクチャの設定については、[ESXi インストーラの PXE 起動](#) を参照してください。
- インストール スクリプトの作成および配置については、[インストール スクリプトおよびアップグレード スクリプトについて](#) を参照してください。
- ESXi のインストーラを PXE 起動しインストール スクリプトを使用する具体的な手順については、次のトピックを参照してください。
 - [PXELINUX および isolinux.cfg PXE 構成ファイルを使用した ESXi インストーラの PXE 起動](#)
 - [PXELINUX および PXE 構成ファイルを使用した、ESXi インストーラの PXE 起動](#)
 - [gPXE を使用した ESXi インストーラの PXE 起動](#)
- vSphere Auto Deploy を使用して PXE 起動によるスクリプトを使用したアップグレードを実行する方法については、[vSphere Auto Deploy を使用した、ホストの再プロビジョニング](#) を参照してください。

vSphere Auto Deploy を使用した、ホストの再プロビジョニング

ホストが vSphere Auto Deploy を使用してデプロイされた場合は、Auto Deploy を使用して、異なるバージョンの ESXi を含む新しいイメージ プロファイルでホストを再プロビジョニングすることができます。イメージ プロファイルは、ESXi Image Builder PowerCLI を使用して作成および管理できます。

注： ESXi 6.0 以降のイメージを使用するようにホストをアップグレードする場合、Auto Deploy サーバは、VMCA による署名付きの証明書を使用して ESXi ホストをプロビジョニングします。現在カスタム証明書を使用している場合は、アップグレード後にカスタム証明書を使用するようにホストを設定できます。

対応する vCenter Server システムをバージョン 6 にアップグレードすると、Auto Deploy サーバは自動的にアップグレードされます。バージョン 6 以降、Auto Deploy サーバは必ず vCenter Server システムと同じ管理ノードに配置されます。

ホストの再プロビジョニング

vSphere Auto Deploy では、複数の再プロビジョニング オプションがサポートされます。単純な再起動や、異なるイメージ プロファイルまたは異なるホスト プロファイルを使用した再プロビジョニングを実行できます。

Auto Deploy を使用して最初に起動するときには、環境を設定し、ルール セットにルールを追加する必要があります。『vSphere のインストールとセットアップ』の「vSphere Auto Deploy の準備」のトピックを参照してください。

次の再プロビジョニング操作が可能です。

- 単純な再起動。
- 起動操作中にユーザーが質問に対して行った回答の対象となるホストの再起動。
- 異なるイメージ プロファイルを使用した再プロビジョニング。
- 異なるホスト プロファイルを使用した再プロビジョニング。

シンプルな再起動操作によるホストの再プロビジョニング

Auto Deploy でプロビジョニングされているホストの単純な再起動では、すべての前提条件が満たされていることのみが必要です。このプロセスでは、以前に割り当てられたイメージ プロファイル、ホスト プロファイル、および vCenter Server の場所が使用されます。

設定には、DHCP サーバの設定、ルールの書き込み、Auto Deploy インフラストラクチャでのイメージ プロファイルの有効化が含まれます。

前提条件

最初の起動操作中に実行した設定が適切であることを確認します。

手順

- 1 ホスト用のイメージ プロファイルおよびホスト プロファイルが使用可能であることと、ホストに以前の起動操作で指定された識別情報（アセット タグ、IP アドレス）があることを確認します。
- 2 ホストをメンテナンス モードにします。

ホスト タイプ	操作
DRS クラスタの一部であるホスト	VMware DRS では、ホストがメンテナンス モードになると、仮想マシンが適切なホストに移行されます。
DRS クラスタの一部ではないホスト	すべての仮想マシンを別のホストに移行し、各ホストをメンテナンス モードにする必要があります。

- 3 ホストを再起動します。

結果

ホストがシャットダウンします。ホストが再起動するときに、そのホストは Auto Deploy サーバが提供するイメージ プロファイルを使用します。Auto Deploy サーバでは、vCenter Server システムに保存されているホスト プロファイルも適用します。

新しいイメージ プロファイルを使用したホストの再プロビジョニング

ホスト用のルールを変更し、コンプライアンスのテストおよび修復処理を実行することで、新しいイメージ プロファイル、ホスト プロファイル、または vCenter Server の場所を使用してホストを再プロビジョニングすることができます。

ホストの再プロビジョニングにはいくつかのオプションがあります。

- 使用する VIB でライブ アップデートがサポートされる場合は、`esxcli software vib` コマンドを使用できます。その場合は、新しい VIB を含むイメージ プロファイルを使用するように、ルール セットを更新する必要があります。
- テスト時に、`Apply-EsxImageProfile cmdlet` を使用して個々のホストにイメージ プロファイルを適用し、ホストを再起動して変更を有効にすることができます。`Apply-EsxImageProfile` コマンドレットは、ホストとイメージ プロファイルの関連付けを更新しますが、ホストに VIB をインストールすることはありません。
- その他すべての場合は、この手順を実行します。

前提条件

- ホスト上で起動するイメージ プロファイルを作成します。Image Builder PowerCLI を使用します。『vSphere のインストールとセットアップ』の「vSphere ESXi Image Builder CLI の使用」のトピックを参照してください。
- 最初の起動操作中に実行した設定が適切であることを確認します。

手順

- 1 PowerShell プロンプトで、`Connect-VIServer PowerCLI cmdlet` を実行して、Auto Deploy が登録されている vCenter Server システムに接続します。

Connect-VIServer myVCServer

この cmdlet はサーバ証明書の警告を返す場合があります。本番環境では、サーバ証明書の警告が表示されないことを確認します。開発環境では、この警告は無視できます。

- 2 使用するイメージ プロファイルが格納されているソフトウェア デポを特定するか、Image Builder PowerCLI を使用してカスタム イメージ プロファイルを定義します。
- 3 `Add-EsxSoftwareDepot` を実行して、イメージ プロファイルが含まれるソフトウェア デポを PowerCLI セッションに追加します。

デポのタイプ	Cmdlet
リモート デポ	<code>Add-EsxSoftwareDepot depot_url</code> を実行します。
ZIP ファイル	<ol style="list-style-type: none"> a ZIP ファイルをローカル ファイル パスにダウンロードするか、PowerCLI マシンにローカルなマウント ポイントを作成します。 b <code>Add-EsxSoftwareDepot C:\file_path\my_offline_depot.zip</code> を実行します。

- 4 `Get-EsxImageProfile` を実行してイメージ プロファイルのリストを表示し、使用するプロファイルを決定します。

- 5 `Copy-DeployRule` を実行し、`ReplaceItem` パラメータを指定して、イメージ プロファイルをホストに割り当てるルールを変更します。

次のコマンドレットは、*my_new_imageprofile* プロファイルを使用して、ルールがホストに割り当てる現在のイメージ プロファイルを置き換えます。コマンドレットが完了すると、`myrule` で新しいプロファイルがホストに割り当てられます。古いバージョンの `myrule` は、名前が変更され、非表示になります。

```
Copy-DeployRule myrule -ReplaceItem my_new_imageprofile
```

- 6 イメージをデプロイする各ホストのルール コンプライアンスをテストし、修復します。

[ルールのコンプライアンスのテストおよび修復](#) を参照してください。

結果

コンプライアンス修復後にホストを再起動すると、Auto Deploy によって、ホストが新しいイメージ プロファイルでプロビジョニングされます。

ルールの記述とホストへのホスト プロファイルの割り当て

Auto Deploy は、1 つ以上のホストにホスト プロファイルを割り当てることができます。ホスト プロファイルには、ストレージ構成、ネットワーク構成、またはホストのその他の特性に関する情報が含まれる場合があります。クラスタにホストを追加する場合は、そのクラスタのホスト プロファイルが使用されます。

多くの場合、ホスト プロファイルを明示的に指定する代わりに、ホストをクラスタに割り当てます。ホストは、割り当てられたクラスタのホスト プロファイルを使用します。

前提条件

- vSphere PowerCLI およびすべての前提となるソフトウェアをインストールします。詳細については、『vSphere のインストールとセットアップ』を参照してください。
- 使用するホスト プロファイルをエクスポートします。

手順

- 1 `Connect-VIServer` vSphere PowerCLI cmdlet を実行して、Auto Deploy が登録されている vCenter Server システムに接続します。

```
Connect-VIServer 192.XXX.X.XX
```

この cmdlet はサーバ証明書の警告を返す場合があります。本番環境では、サーバ証明書の警告が表示されないことを確認します。開発環境では、この警告は無視できます。

- 2 vSphere Web Client を使用して、使用する設定内容をホストに設定し、そのホストでホスト プロファイルを作成します。
- 3 `Get-VMhostProfile` vSphere PowerCLI cmdlet を実行して、ホスト プロファイルの作成元となる ESXi ホストを渡すことで、ホスト プロファイルの名前を探します。

- 4 vSphere PowerCLI プロンプトで、特定の属性（IP アドレスの範囲など）を備えたホストをホスト プロファイルに割り当てるルールを定義します。

```
New-DeployRule -Name "testrule2" -Item my_host_profile -Pattern "vendor=Acme,Zven",
"ipv4=192.XXX.1.10-192.XXX.1.20"
```

指定された属性を持つすべてのホストに、指定された項目が割り当てられます。この例は、testrule2 という名前のルールを指定します。このルールは、指定された範囲内の IP アドレスを持ち、メーカーが Acme または Zven のすべてのホストに、指定されたホスト プロファイル *my_host_profile* を割り当てます。

- 5 ルール セットにルールを追加します。

```
Add-DeployRule testrule2
```

デフォルトでは、作業ルール セットがアクティブなルール セットになります。また、ルール セットへのすべての変更は、ルールを追加した時にアクティブになります。NoActivate パラメータを使用すると、作業ルール セットはアクティブなルール セットになりません。

次のステップ

- Auto Deploy によってプロビジョニング済みのホストを新しいホスト プロファイルに割り当てるには、それらのホスト上でコンプライアンス テストおよび修復処理を実行します。詳細については、[ルールのコンプライアンスのテストおよび修復](#) を参照してください。
- プロビジョニングされていないホストをパワーオンし、ホスト プロファイルを使用してそれらのホストをプロビジョニングします。

ルールのコンプライアンスのテストおよび修復

Auto Deploy のルール セットにルールを追加したり、1 つ以上のルールに変更を加える場合、ホストが自動的にアップデートされません。ユーザーがルールのコンプライアンスをテストし修復を行った場合にのみ、Auto Deploy は新しいルールを適用します。

前提条件

- vSphere PowerCLI およびすべての前提となるソフトウェアをインストールします。
- インフラストラクチャに Auto Deploy を使用してプロビジョニングされた ESXi ホストが 1 つ以上含まれており、vSphere PowerCLI をインストールしたホストがそれらの ESXi ホストにアクセスできることを確認します。

手順

- 1 vSphere PowerCLI を使用して、現在使用可能な Auto Deploy ルールを確認します。

```
Get-DeployRule
```

システムは、該当するルールと、それに関連する項目およびパターンを返します。

- 2 使用可能なルール の 1 つに変更を加えます。

たとえば、イメージ プロファイルおよびルール の名前を変更することができます。

```
Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
```

すでにルール セットに追加されているルールは編集できません。代わりに、ルールをコピーして、変更する項目またはパターンを置き換えます。

- 3 ルール セットのコンプライアンスをテストするホストにアクセスできることを確認します。

```
Get-VMHost -Name MyEsxi42
```

- 4 そのホストのルール セットのコンプライアンスをテストし、後で使用するために、戻り値を変数にバインドする cmdlet を実行します。

```
$str = Test-DeployRuleSetCompliance MyEsxi42
```

- 5 ルール セットの内容と、ホストの構成の間の差異を確認します。

```
$str.itemlist
```

システムは、現在の項目と予想される項目の表を返します。

```
CurrentItem
ExpectedItem-----My Profile
25MyProfileUpdate
```

- 6 ホストの次の起動時に、変更されたルール セットを使用するように、ホストを修復します。

```
Repair-DeployRuleSetCompliance $str
```

次のステップ

変更したルールでインベントリの場所が指定されている場合、コンプライアンスの修復時に変更内容が即座に反映されます。それ以外のすべての変更内容は、ホストを起動することで、Auto Deploy によって新しいルールが適用され、ルール セットとホスト間のコンプライアンスが達成されます。

esxcli コマンドを使用した、ホストのアップグレード

vSphere CLI を使用すると、ESXi 5.x ホストをバージョン 6.0 にアップグレードして、ESXi 5.x および 6.0 ホストを更新またはパッチ適用できます。

vCLI の esxcli コマンドを使用するには、vSphere CLI (vCLI) をインストールする必要があります。vCLI のインストールおよび使用については、次のドキュメントを参照してください。

- vSphere Command-Line Interface スタート ガイド
- vSphere Command-Line Interface の例

- 『vSphere Command-Line Interface のリファレンス』は、vicfg- および関連 vCLI コマンドのリファレンスです。

注： esxcli コマンド実行中に Ctrl+C を押下すると、コマンドライン インターフェイスは、メッセージを表示せずに新しいプロンプトになります。ただし、コマンドは完了するまで実行を続けます。

vSphere Auto Deploy で導入した ESXi ホストでは、tools VIB は、最初の Auto Deploy インストールで使用するベース ブート イメージの一部である必要があります。tools VIB は後で別に追加できません。

VIB、イメージ プロファイル、およびソフトウェア デポ

esxcli コマンドを使用して ESXi をアップグレードするには、VIB、イメージ プロファイル、およびソフトウェア デポについて理解している必要があります。

vSphere ドキュメント セット全体のインストール作業およびアップグレード作業の説明で、次の技術用語が使用されます。

VIB

VIB は、ESXi のソフトウェア パッケージです。VMware およびパートナーは、ESXi プラットフォームを拡張するためのソリューション、ドライバ、CIM プロバイダ、およびアプリケーションをパッケージ化します。VIB は、ソフトウェア デポで使用できます。VIB を使用すると、ISO イメージを作成およびカスタマイズしたり、VIB を非同期的にホストにインストールすることで ESXi ホストをアップグレードしたりできます。

イメージ プロファイル

イメージ プロファイルは VIB で構成され、ESXi イメージを定義します。イメージ プロファイルには常に基本 VIB が含まれ、ほかの VIB が含まれる場合もあります。イメージ プロファイルは、vSphere ESXi Image Builder を使用して調査および定義します。

ソフトウェア デポ

ソフトウェア デポは、VIB とイメージ プロファイルの集合体です。ソフトウェア デポはファイルとフォルダの階層であり、HTTP URL（オンラインのデポの場合）または ZIP ファイル（オフラインのデポの場合）を介して使用できます。VMware および VMware のパートナーがデポを提供します。大規模な VMware インストールを導入している企業では、内部にデポを作成して、ESXi ホストを vSphere Auto Deploy でプロビジョニングしたり、ESXi インストール用に ISO をエクスポートしたりする場合があります。

VIB およびホストの許容レベルについて

各 VIB は、許容レベルとともにリリースされます。この許容レベルは変更することができません。ホストの許容レベルで、どの VIB をホストにインストールできるかが決まります。

許容レベルは、esxcli software vib install コマンドと esxcli software vib update コマンドを使用してインストールされた個々の VIB、vSphere Update Manager を使用してインストールされた VIB、およびイメージ プロファイル内の VIB に適用されます。

ホスト上のすべての VIB の許容レベルが、ホストの許容レベル以上である必要があります。たとえば、ホストの許容レベルが VMwareAccepted である場合は、許容レベルが VMwareCertified および VMwareAccepted の VIB をインストールできますが、許容レベルが PartnerSupported または CommunitySupported の VIB はインストールできません。許容レベルがホストの許容レベルよりも厳密ではない VIB をインストールする場合は、vSphere Web Client を使用するか、`esxcli software acceptance` コマンドを実行して、ホストの許容レベルを変更できます。

ホストにインストールしてイメージ プロファイルと共に使用できる VIB を指定したり、VIB に対して利用できるサポートのレベルを指定したりできるように、ホストの許容レベルを設定するのがベスト プラクティスです。たとえば、テスト環境のホストより限定的な許容レベルを本番環境のホストに設定できます。

VMware は、次の許容レベルをサポートしています。

VMwareCertified

VMwareCertified 許容レベルは、最も厳しい要件です。このレベルの VIB では、同じテクノロジーに対して VMware 内部で行われる品質保証テストと完全に同等な、詳細なテストが行われます。現在は、I/O Vendor Program (IOVP) プログラム ドライバのみがこのレベルで公開されています。この許容レベルの場合は、VMware が VIB に対するサポート コールを受けます。

VMwareAccepted

この許容レベルの VIB では検証テストが行われますが、このテストはソフトウェアのすべての機能を完全にテストするものではありません。テストはパートナーが実行し、VMware がテスト結果を確認します。現在このレベルで公開されている VIB には、CIM プロバイダや PSA プラグインがあります。VMware は、この許容レベルの VIB に対するサポート コールを、パートナーのサポート組織に送ります。

PartnerSupported

PartnerSupported 許容レベルの VIB は、VMware が信頼するパートナーによって公開されます。そのパートナーがすべてのテストを実行します。VMware はテスト結果を確認しません。このレベルは、パートナーが VMware システム用に採用する、新しいテクノロジー、または主要ではないテクノロジーに使用されます。現在は、標準以外のハードウェア ドライバを使用する、Infiniband、ATAoE、SSD などのドライバ VIB テクノロジーがこのレベルにあります。VMware は、この許容レベルの VIB に対するサポート コールを、パートナーのサポート組織に送ります。

CommunitySupported

CommunitySupported 許容レベルは、VMware パートナー プログラムに参加していない個人または企業が作成した VIB に使用されます。このレベルの VIB に対しては VMware が承認したテスト プログラムが実行されておらず、VMware のテクニカル サポートや VMware パートナーによるサポートを受けられません。

表 9-4. ホストへのインストールの要件となる VIB 許容レベル

ホストの許容レベル	VMwareCertified VIB	VMwareAccepted VIB	PartnerSupported VIB	CommunitySupported VIB
VMwareCertified	x			
VMwareAccepted	x	x		

表 9-4. ホストへのインストールの要件となる VIB 許容レベル（続き）

ホストの許容レベル	VMwareCertified VIB	VMwareAccepted VIB	PartnerSupported VIB	CommunitySupported VIB
PartnerSupported	x	x	x	
CommunitySupported	x	x	x	x

ホストの許容レベルとアップデートの許容レベルのマッチング

ホストの許容レベルを、インストールする VIB またはイメージ プロファイルの許容レベルと一致するように変更することができます。ホスト上のすべての VIB の許容レベルが、ホストの許容レベル以上である必要があります。

ここに記載されている手順を使用して、ホストの許容レベル、およびインストールする VIB またはイメージ プロファイルの許容レベルを確認し、必要に応じてホストの許容レベルを変更します。

`--server=server_name` を使用して接続先サーバを指定すると、サーバはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照するか、vCLI コマンド プロンプトで `esxcli --help` を実行します。

前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

手順

- 1 VIB またはイメージ プロファイルの許容レベルを取得します。

オプション	説明
すべての VIB に関する情報をリストします。	<code>esxcli --server=server_name software sources vib list --depot=depot_URL</code>
指定した VIB に関する情報をリストします。	<code>esxcli --server=server_name software sources vib list --viburl=vib_URL</code>
すべてのイメージ プロファイルに関する情報をリストします。	<code>esxcli --server=server_name software sources profile list --depot=depot_URL</code>
指定したイメージ プロファイルに関する情報をリストします。	<code>esxcli --server=server_name software sources profile get --depot=depot_URL --profile=profile_name</code>

- 2 ホストの許容レベルを取得します。

```
esxcli --server=server_name software acceptance get
```

- 3 （オプション） VIB の許容レベルがホストの許容レベルよりも厳格な場合は、ホストの許容レベルを変更します。

```
esxcli --server=server_name software acceptance set --level=acceptance_level
```


acceptance_level には、VMwareCertified、VMwareAccepted、PartnerSupported、または CommunitySupported を指定できます。*acceptance_level* の値では、大文字と小文字が区別されます。

注： `esxcli software vib` または `esxcli software profile` コマンドの `--force` オプションを使用すると、許容レベルがホストより低い VIB またはイメージ プロファイルを追加することができます。その場合、警告が表示されます。設定の整合性がなくなったため、ホスト上で VIB のインストール、VIB の削除、およびその他の特定の操作を実行すると、警告が繰り返し表示されます。

更新するためにホストをメンテナンス モードにする必要があるか、再起動する必要があるかの確認

ライブ インストールでインストール可能な VIB の場合、ホストの再起動は不要ですが、ホストをメンテナンス モードにすることが必要な場合があります。その他の VIB およびプロファイルの場合は、インストールまたは更新後にホストの再起動が必要な場合があります。

`--server=server_name` を使用して接続先サーバを指定すると、サーバはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照するか、vCLI コマンド プロンプトで `esxcli --help` を実行します。

前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

手順

- 1 VIB またはイメージ プロファイルをインストールする場合に、ホストをメンテナンス モードにする必要があるか、またインストールまたは更新後にホストを再起動する必要があるかを確認します。

次のいずれかのコマンドを実行します。

オプション	説明
VIB の確認	<code>esxcli --server=server_name software sources vib get -v absolute_path_to_vib</code>
デポ内の VIB の確認	<code>esxcli --server=server_name software sources vib get --depot=depot_name</code>
デポ内のイメージ プロファイルの確認	<code>esxcli --server=server_name software sources profile get --depot=depot_name</code>

2 戻り値を確認します。

VIB メタデータから読み取られる戻り値は、VIB またはイメージ プロファイルをインストールする前にホストがメンテナンス モードになっている必要があるかどうか、および VIB またはプロファイルのインストールでホストを再起動する必要があるかどうかを示します。

注： vSphere Update Manager は、esxupdate/esxcli スキャン結果に基づいて、メンテナンス モードが必要かどうかを判断します。VIB のライブ システムへのインストール後、Live-Install-Allowed の値が false に設定されている場合、Update Manager は、そのインストール結果に従ってホストを再起動します。VIB のライブ システムからの削除後、Live-Remove-Allowed の値が false に設定されている場合、Update Manager は、その削除結果に従ってホストを再起動します。いずれの場合でも、再起動時、Update Manager はホストを自動的にメンテナンス モードにします。

次のステップ

必要に応じ、ホストをメンテナンス モードにします。[ホストをメンテナンス モードに切り替える](#) を参照してください。ホストの再起動が必要で、そのホストが VMware HA クラスタに属している場合は、インストールまたは更新の前にホストをクラスタから削除するか、クラスタで HA を無効にします。

ホストをメンテナンス モードに切り替える

ライブ インストールを使用するインストールおよびアップデート操作の一部では、ホストをメンテナンス モードにする必要があります。

アップグレード操作でホストをメンテナンス モードにする必要があるかどうかを判断するには、[更新するためにホストをメンテナンス モードにする必要があるか、再起動する必要があるかの確認](#) を参照してください。

注： ホストが Virtual SAN クラスタのメンバーである場合、またそのホスト上の任意の仮想マシン オブジェクトがストレージ ポリシーの「許容する障害の数 =0」設定を使用している場合、そのホストがメンテナンス モードに入るときに異常な遅延が発生する可能性があります。この遅延は、Virtual SAN がメンテナンス操作を正常に完了するためにこのオブジェクトを退避させる必要があるため発生します。

`--server=server_name` を使用して接続先サーバを指定すると、サーバはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照するか、vCLI コマンド プロンプトで `esxcli --help` を実行します。

前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

手順

- 1 ホストがメンテナンス モードであるかどうかを確認します。

```
vicfg-hostops --server=server_name --operation info
```

- 2 ESXi ホストで実行されている各仮想マシンをパワーオフします。

オプション	コマンド
ゲスト OS をシャットダウンしてから、仮想マシンをパワーオフします	<code>vmware-cmd --server=server_namepath_to_vm stop soft</code>
強制的にパワーオフ操作を実行します	<code>vmware-cmd --server=server_namepath_to_vm stop hard</code>

または、仮想マシンのパワーオフを避けるために他のホストに移行できます。『vCenter Server およびホスト管理』ドキュメントのトピック「Migrating Virtual Machines」を参照してください。

- 3 ホストをメンテナンス モードにします。

```
vicfg-hostops --server=server_name --operation enter
```

- 4 ホストがメンテナンス モードであることを確認します。

```
vicfg-hostops --server=server_name --operation info
```

個々の VIB によるホストの更新

URL を指定してアクセスできるソフトウェア デポかオフラインの ZIP デポに格納されている VIB を使用して、ホストを更新できます。

重要： VMware 提供のデポで zip バンドルから ESXi を更新する場合、VMware Web サイトからオンラインまたはローカルでダウンロードするかのどちらかで、VMware は、トピックで VMware 提供デポに対して指定されたアップデート方法のみをサポートします。 [イメージ プロファイルによるホストのアップグレードまたは更新](#)。

`esxcli software vib update` コマンドおよび `esxcli software vib install` コマンドでは、アップグレード操作はサポートされません。 [vSphere のアップグレードとアップデートの違い](#) および [イメージ プロファイルによるホストのアップグレードまたは更新](#) を参照してください。

`--server=server_name` を使用して接続先サーバを指定すると、サーバはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照するか、vCLI コマンド プロンプトで `esxcli --help` を実行します。

前提条件

- vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。
- 更新するためにホストをメンテナンス モードにする必要があるか、それとも再起動する必要があるかを確認します。必要に応じ、ホストをメンテナンス モードにします。
[更新するためにホストをメンテナンス モードにする必要があるか、再起動する必要があるかの確認](#) を参照してください。
[ホストをメンテナンス モードに切り替える](#) を参照してください。
- 更新時に再起動が必要な場合、ホストが VMware HA クラスタに属しているときは、クラスタからホストを削除するか、クラスタで HA を無効にします。

手順

- 1 ホストにどの VIB がインストールされているか確認します。

```
esxcli --server=server_name software vib list
```

- 2 デポで利用可能な VIB を見つけます。

オプション	説明
URL を指定してアクセスできるデポから	<code>esxcli --server=server_name software sources vib list --depot=http://web_server/depot_name</code>
ローカルにある ZIP ファイルから	<code>esxcli --server=server_name software sources vib list --depot=absolute_path_to_depot_zip_file</code>

--proxy 引数を使用して、プロキシ サーバを指定することができます。

- 3 デポにある VIB を含めるか、新しい VIB をインストールするように、既存の VIB を更新します。

オプション	説明
URL を指定してアクセスできるデポから VIB を更新	<code>esxcli --server=server_name software vib update --depot=http://web_server/depot_name</code>
ローカルにある ZIP ファイルから VIB を更新	<code>esxcli --server=server_name software vib update --depot=absolute_path_to_depot_ZIP_file</code>
指定したオフラインのデポにある ZIP ファイルから、すべての VIB をインストール (VMware の VIB とパートナー提供の VIB の両方を含む)	<code>esxcli --server=server_name software vib install --depot path_to_VMware_vib_ZIP_file\VMware_vib_ZIP_file --depot path_to_partner_vib_ZIP_file\partner_vib_ZIP_file</code>

update コマンドおよび install コマンドのオプションを使用して、ドライ ラン、特定の VIB の指定、許可レベル検証のバイパスなどを行うことができます。本番稼働システムでは検証をバイパスしないでください。『esxcli Reference』(<http://www.vmware.com/support/developer/vcli/>) を参照してください。

- 4 VIB が ESXi ホストにインストールされていることを確認します。

```
esxcli --server=server_name software vib list
```

イメージ プロファイルによるホストのアップグレードまたは更新

URL を指定してアクセスできるソフトウェア デポかオフラインの ZIP デポに格納されているイメージ プロファイルを使用して、ホストをアップグレードまたは更新できます。

コマンド `esxcli software profile update` または `esxcli software profile install` を使用して、ESXi ホストをアップグレードまたは更新できます。アップグレードと更新の違いを理解するには、[vSphere のアップグレードとアップデートの違い](#) を参照してください。

ホストをアップグレードまたは更新する場合は、コマンド `esxcli software profile update` または `esxcli software profile install` により、最新バージョン (メジャーまたはマイナー) のすべてのイメージ プロファイルをホストに適用します。この操作と再起動の後、ホストは同じ最新バージョンの vCenter Server 環境に参加できます。

コマンド **esxcli software profile update** により、ISO インストーラを使用して、ESXi ホスト イメージの内容全体を、対応するアップグレード方法と同じレベルに引き上げます。潜在的な問題を検出するために、ISO インストーラでアップグレード前チェックが実行されますが、**esxcli** アップグレード方法では実行されません。ISO インストーラはホストをチェックして、ホストにアップグレードのための十分なメモリがあるか、サポート対象外のデバイスが接続されていないかどうかを確認します。ISO インストーラおよびその他の ESXi アップグレード方法の詳細については、[ESXi 6.0 のアップグレード オプション](#) を参照してください。

重要： VMware 提供のデポで、zip バンドルから ESXi をアップグレードまたは更新する場合、VMware Web サイトからオンライン、またはローカルにダウンロードされ、VMware は更新コマンド **esxcli software profile update --depot=depot_location --profile=profile_name** のみをサポートします。

--server=server_name を使用して接続先サーバを指定すると、サーバはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照するか、vCLI コマンド プロンプトで **esxcli --help** を実行します。

注： update コマンドおよび install コマンドのオプションを使用して、ドライ ラン、特定の VIB の指定、許容レベル検証のバイパスなどを行うことができます。本番稼働システムでは検証をバイパスしないでください。『vSphere Command-Line Interface のリファレンス』を参照してください。

前提条件

- vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で **esxcli** コマンドを実行します。
- 更新するためにホストをメンテナンス モードにする必要があるか、それとも再起動する必要があるかを確認します。必要に応じ、ホストをメンテナンス モードにします。

更新するためにホストをメンテナンス モードにする必要があるか、再起動する必要があるかの確認 を参照してください。ホストをメンテナンス モードに切り替える を参照してください。
- 更新時に再起動が必要な場合、ホストが VMware HA クラスタに属しているときは、クラスタからホストを削除するか、クラスタで HA を無効にします。

手順

- 1 ホストにどの VIB がインストールされているか確認します。

```
esxcli --server=server_name software vib list
```

- 2 デポで利用できるイメージ プロファイルを判断します。

```
esxcli --server=server_name software sources profile list --
depot=http://webserver/depot_name

--proxy 引数を使用して、プロキシ サーバを指定することができます。
```

3 既存のイメージ プロファイルを更新して、VIB を含めるか、新しい VIB をインストールします。

重要： `software profile update` コマンドでは、指定したプロファイルの対応する VIB を使用して既存の VIB を更新しますが、ターゲット サーバ上にインストールされているほかの VIB には影響を与えません。`software profile install` コマンドでは、デポのイメージ プロファイル内にある VIB をインストールし、ターゲット サーバ上にインストールされているその他すべての VIB を削除します。

オプション	説明
VMware Web サイトからオンラインでアクセス可能か、ローカル デポヘダウンロードできる、デポの VMware 提供の zip バンドルからのイメージ プロファイルをアップデートします。	<pre>esxcli software profile update --depot=depot_location --profile=profile_name</pre> <p>重要： VMware が提供する zip バンドルに対して、VMware がサポートする唯一のアップデート方法です。</p> <p>VMware 提供の zip バンドル名は、次の形式になります。 VMware-ESXi-6.0.0-build_number-depot.zip</p> <p>VMware 提供の zip バンドルのプロファイル名は、次のうちの 1 つの形式をとります。</p> <ul style="list-style-type: none"> ■ ESXi-6.0.0-build_number-standard ■ ESXi-6.0.0-build_number-notools (VMware ツールは含みません)
URL を指定してアクセスできるデポから、イメージ プロファイルを更新	<pre>esxcli --server=server_name software profile update --depot=http://webserver/depot_name --profile=profile_name</pre>
ターゲット サーバ上にローカルに格納されている ZIP ファイルから、イメージ プロファイルを更新	<pre>esxcli --server=server_name software profile update --depot=file:///path_to_profile_ZIP_file/profile_ZIP_file --profile=profile_name</pre>
ターゲット サーバ上の、データストアにコピーされた ZIP ファイルから、イメージ プロファイルを更新	<pre>esxcli --server=server_name software profile update --depot="[datastore_name]profile_ZIP_file" --profile=profile_name</pre>
ローカルにコピーされ、ターゲット サーバに適用された ZIP ファイルから、イメージ プロファイルを更新	<pre>esxcli --server=server_name software profile update --depot=/root_dir/path_to_profile_ZIP_file/profile_ZIP_file --profile=profile_name</pre>
URL を指定してアクセスできる指定されたプロファイル内に、すべての新しい VIB をインストール	<pre>esxcli --server=server_name software profile install --depot=http://webserver/depot_name --profile=profile_name</pre>
ターゲット上にローカルに格納されている ZIP ファイルから、指定したプロファイル内にすべての新しい VIB をインストール	<pre>esxcli --server=server_name software profile install --depot=file:///path_to_profile_ZIP_file/profile_ZIP_file --profile=profile_name</pre>
ターゲット サーバ上の、データストアにコピーされた ZIP ファイルから、すべての新しい VIB をインストール	<pre>esxcli --server=server_name software profile install --depot="[datastore_name]profile_ZIP_file" --profile=profile_name</pre>
ローカルにコピーされ、ターゲット サーバに適用された ZIP ファイルから、すべての新しい VIB をインストール	<pre>esxcli --server=server_name software profile install --depot=/root_dir/path_to_profile_ZIP_file/profile_ZIP_file --profile=profile_name</pre>

注： `update` コマンドおよび `install` コマンドのオプションを使用して、ドライ ラン、特定の VIB の指定、許容レベル検証のバイパスなどを行うことができます。本番稼働システムでは検証をバイパスしないでください。『vSphere Command-Line Interface のリファレンス』を参照してください。

- 4 VIB が ESXi ホストにインストールされていることを確認します。

```
esxcli --server=server_name software vib list
```

Zip ファイルを使用した ESXi ホストのアップデート

デポの Zip ファイルをダウンロードして、VIB またはイメージ プロファイルのホストをアップデートできます。

VMware パートナーは、管理エージェントまたは別途リリースされたドライバを提供するために、サードパーティ製 VIB を用意しています。

重要： VMware 提供のデポで zip バンドルから ESXi を更新する場合、VMware Web サイトからオンラインまたはローカルでダウンロードするかのどちらかで、VMware は、トピックで VMware 提供デポに対して指定されたアップデート方法のみをサポートします。 [イメージ プロファイルによるホストのアップグレードまたは更新](#)。

esxcli software vib update コマンドおよび **esxcli software vib install** コマンドでは、アップグレード操作はサポートされません。 [vSphere のアップグレードとアップデートの違い](#) および [イメージ プロファイルによるホストのアップグレードまたは更新](#) を参照してください。

--server=server_name を使用して接続先サーバを指定すると、サーバはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照するか、vCLI コマンド プロンプトで **esxcli --help** を実行します。

前提条件

- vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で **esxcli** コマンドを実行します。
- サードパーティ VMware パートナーから、デポ バンドルの ZIP ファイルをダウンロードします。
- 更新するためにホストをメンテナンス モードにする必要があるか、それとも再起動する必要があるかを確認します。必要に応じ、ホストをメンテナンス モードにします。

[更新するためにホストをメンテナンス モードにする必要があるか、再起動する必要があるかの確認](#) を参照してください。 [ホストをメンテナンス モードに切り替える](#) を参照してください。

- 更新時に再起動が必要な場合、ホストが VMware HA クラスタに属しているときは、クラスタからホストを削除するか、クラスタで HA を無効にします。

手順

- ◆ ZIP ファイルをインストールします。

```
esxcli --server=server_name software vib update --depot=/path_to_vib_ZIP/  
ZIP_file_name.zip
```

ホストからの VIB の削除

サードパーティ製の VIB や VMware VIB を ESXi ホストからアンインストールすることができます。

VMware パートナーは、管理エージェントまたは別途リリースされたドライバを提供するために、サードパーティ製 VIB を用意しています。

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

前提条件

- 削除後に再起動が必要で、ホストが VMware HA クラスタに属する場合は、そのホストに対して HA を無効にします。
- 更新するためにホストをメンテナンス モードにする必要があるか、それとも再起動する必要があるかを確認します。必要に応じ、ホストをメンテナンス モードにします。

[更新するためにホストをメンテナンス モードにする必要があるか、再起動する必要があるかの確認](#) を参照してください。[ホストをメンテナンス モードに切り替える](#) を参照してください。

- vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

手順

- 1 ESXi ホストで実行されている各仮想マシンをパワーオフします。

オプション	コマンド
ゲスト OS をシャットダウンしてから、仮想マシンをパワーオフします	<code>vmware-cmd --server=server_namepath_to_vm stop soft</code>
強制的にパワーオフ操作を実行します	<code>vmware-cmd --server=server_namepath_to_vm stop hard</code>

または、仮想マシンのパワーオフを避けるために他のホストに移行できます。『vCenter Server およびホスト管理』ドキュメントのトピック「Migrating Virtual Machines」を参照してください。

- 2 ホストをメンテナンス モードにします。

```
vicfg-hostops --server=server_name --operation enter
```

- 3 必要に応じ、仮想マシンをシャットダウンするか移行するかします。

- 4 ホストにどの VIB がインストールされているか確認します。

```
esxcli --server=server_name software vib list
```

- 5 VIB を削除します。

```
esxcli --server=server_name software vib remove --vibname=name
```

次のいずれかの形式で、1 つ以上の VIB を指定します。

- `name`
- `name:version`
- `vendor:name`

■ `vendor:name:version`

たとえば、ベンダーが指定した VIB を削除するコマンドでは、名前とバージョンを次の形式で指定します。

```
esxcli --server myEsxiHost software vib remove --vibName=PatchVendor:patch42:version3
```

注： remove コマンドでは、ほかにもいくつかのオプションがサポートされます。『vSphere Command-Line Interface のリファレンス』を参照してください。

esxcli コマンドを使用した、ホストへのサードパーティ製拡張機能の追加

esxcli software vib コマンドを使用して、VIB パッケージとしてリリースされるサードパーティ製拡張機能をシステムに追加できます。このコマンドを使用すると、VIB システムによりファイアウォール ルール セットが更新され、システムの再起動後にホスト デモンが更新されます。

ファイアウォール構成ファイルを使用して、その拡張機能用に有効にするホスト サービスのポート ルールを指定することもできます。『vSphere セキュリティ』には、ファイアウォール ルール セットを追加、適用、および更新する方法と、esxcli network firewall コマンドのリストが記載されています。

esxcli インストールまたはアップグレードのドライ ランの実行

--dry-run オプションを使用して、インストールまたはアップグレード操作の結果を事前に確認することができます。インストールまたはアップグレード手順のドライ ランでは、変更は一切行われませんが、--dry-run オプションなしでコマンドを実行した場合、実行される VIB レベルでの操作についてレポートされます。

--server=server_name を使用して接続先サーバを指定すると、サーバはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照するか、vCLI コマンド プロンプトで esxcli --help を実行します。

前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で esxcli コマンドを実行します。

手順

- 1 インストールまたはアップグレードのコマンドを、[--dry-run] オプションを追加して入力します。

- `esxcli --server=server_name software vib install --dry-run`
- `esxcli --server=server_name software vib update --dry-run`
- `esxcli --server=server_name software profile install --dry-run`
- `esxcli --server=server_name software profile update --dry-run`

2 返される出力内容を確認します。

出力では、どの VIB がインストールまたは削除されるか、およびインストールまたはアップグレードで再起動が必要かどうかを示されます。

次回ホストを再起動したあとでアクティブになるインストール済み VIB およびプロファイルの表示

`--rebooting-image` オプションを指定すると、ホストにインストールされ、次回ホストを再起動したあとでアクティブになる、VIB およびプロファイルがリストされます。

`--server=server_name` を使用して接続先サーバを指定すると、サーバはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照するか、vCLI コマンド プロンプトで `esxcli --help` を実行します。

前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

手順

1 次のいずれかのコマンドを入力します。

オプション	説明
VIB の場合	<code>esxcli --server=server_name software vib list --rebooting-image</code>
プロファイルの場合	<code>esxcli --server=server_name software profile get --rebooting-image</code>

2 返される出力内容を確認します。

出力には、次回再起動したあとにアクティブになる ESXi イメージの情報が示されます。再起動が保留中のイメージが作成されていない場合は、出力に何も表示されません。

ホストのイメージ プロファイルと許容レベルの表示

`software profile get` コマンドを使用すると、指定したホストに現在インストールされているイメージ プロファイルおよび許容レベルを表示できます。

このコマンドは、プロファイルの変更内容を含め、インストールされたイメージ プロファイル履歴の詳細も表示します。

`--server=server_name` を使用して接続先サーバを指定すると、サーバはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照するか、vCLI コマンド プロンプトで `esxcli --help` を実行します。

前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

手順

- 1 次のコマンドを入力します。

```
esxcli --server=server_name software profile get
```

- 2 出力内容を確認します。

ホストの対話型アップグレード

ESXi 5.x ホストを ESXi 6.0 にアップグレードするために、CD、DVD、または USB フラッシュ ドライブから ESXi インストーラを起動できます。

アップグレードを行う前に、ネットワーク ストレージの切断を検討してください。ネットワーク ストレージを切断することにより、使用可能なディスク ドライブをインストーラが検索する時間が短くなります。ネットワーク ストレージを切断すると、切断されたディスク上のファイルはすべて、インストール時に使用できなくなります。ESXi の既存のインストールが含まれている LUN は切断しないでください。

前提条件

- ESXi インストーラ ISO が次のいずれかの場所に存在することを確認します。
 - CD または DVD。インストール CD または DVD がない場合、作成できます。を参照してください。[ESXi インストーラ ISO イメージのダウンロードおよび CD または DVD への書き込み](#)
 - USB フラッシュ ドライブ。を参照してください。[USB フラッシュ ドライブのフォーマットによる ESXi インストールまたはアップグレードの起動](#)

注： PXE を使用して ESXi インストーラを起動し、対話型インストール、またはスクリプトによるインストールを実行します。[ESXi インストーラの PXE 起動](#) を参照してください。

- サーバ ハードウェアのクロックが UTC に設定されていることを確認すること。この設定はシステム BIOS にあります。
- ESXi Embedded がホスト上に配置されている必要があります。ESXi Installable および ESXi は、同じホスト上に共存できません。
- 5.0.x または 5.1.x ホストのアップグレードを行う場合、ESXi インストーラ ISO に含まれていない、サポートされているカスタム VIB が移行されます。を参照してください。[サードパーティ製のカスタム VIB があるホストのアップグレード](#)
- 起動順序の変更に関する情報については、ハードウェア ベンダーのドキュメントを参照してください。

手順

- 1 ESXi のインストーラ CD または DVD を CD-ROM または DVD-ROM ドライブに挿入するか、インストーラ USB フラッシュ ドライブを接続して、マシンを再起動します。

- 2 CD-ROM デバイスまたは USB フラッシュ ドライブから起動するように BIOS を設定します。
- 3 [ディスクの選択] パネルで、ESXi のインストールまたはアップグレードに使用するドライブを選択し、Enter を押します。

選択したディスクの情報を確認するには、[F1] を押します。

注： ディスクを選択するときは、リスト上のディスクの順序に注意してください。ディスクの順序は、BIOS によって決まります。ドライブが継続的に追加および削除されるシステムでは、順序が違っている場合があります。

- 4 インストーラが既存の ESXi インストールおよび VMFS データストアを検出した場合、ESXi をアップグレードまたはインストールします。

既存の VMFS データストアを保持できない場合は、ESXi のインストールのみを選択して既存の VMFS データストアを上書きするか、インストールをキャンセルします。既存の VMFS データストアを上書きする場合は、まずそのデータストアをバックアップしてください。

- 5 F11 キーを押して操作を確定し、アップグレードを開始します。
- 6 アップグレードが完了したら、インストール CD または DVD または USB フラッシュ ドライブを取り出します。
- 7 Enter を押してホストを再起動します。
- 8 ESXi をアップグレードするときに選択したドライブを最初の起動デバイスとして設定します。

ESXi ホストをアップグレードした後 に行う作業

10

ホストのアップグレードを完了するには、管理を行う vCenter Server システムにホストが再接続され、必要に応じてホストが再構成されていることを確認します。また、ホストが適切にライセンス供与されていることも確認します。

ESXi ホストをアップグレードした後は、次の操作を実行します。

- アップグレード ログを確認します。ログ ファイルは、vSphere Web Client を使用してエクスポートできます。
- vCenter Server システムがそのホストを管理している場合、vCenter Server のインベントリでホストを右クリックして [接続] を選択することで、ホストを vCenter Server に再接続する必要があります。
- アップグレードが完了すると、ESXi ホストは評価モードになります。評価期間は 60 日間です。評価期間が終了する前に、vSphere 6.0 ライセンスを割り当てる必要があります。既存のライセンスをアップグレードするか、Customer Connect から新規ライセンスを取得できます。vSphere Web Client を使用して、環境内のホストのライセンスを構成します。vSphere のライセンス管理の詳細については、『vCenter Server およびホスト管理』ドキュメントを参照してください。
- ホストの sdX デバイスはアップグレード後に番号が変わる可能性があります。必要に応じて、sdX デバイスを参照するスクリプトをアップデートします。
- ホスト上の仮想マシンをアップグレードします。11 章 [仮想マシンと VMware Tools のアップグレード](#)を参照してください。

この章には、次のトピックが含まれています。

- [ESXi の評価モードとライセンス モードについて](#)
- [ESXi 6.0 へのアップグレード後の、ライセンスの適用](#)
- [システム ログに必要な空き容量](#)
- [ESXi ホストでの syslog の構成](#)

ESXi の評価モードとライセンス モードについて

評価モードを使用すると、ESXi ホストの機能セット全体を評価検討できます。評価モードでは、vSphere Enterprise Plus のライセンスと同等の機能セットが提供されます。評価モードの有効期限が切れる前に、使用中のすべての機能をサポートするライセンスをホストに割り当てる必要があります。

たとえば、評価モードでは、vSphere vMotion テクノロジー、vSphere HA 機能、vSphere DRS 機能などを使用できます。これらの機能を継続して使用する場合は、それらをサポートするライセンスを割り当てる必要があります。

ESXi ホストのインストール可能なバージョンは、必ず評価モードでインストールされます。ESXi Embedded は、ハードウェア ベンダーによって内部ストレージ デバイスにあらかじめインストールされています。これは、評価モードになっているか、あらかじめライセンス付与されています。

評価期間は 60 日間で、ESXi ホストをオンにしたときに始まります。この 60 日の評価期間中はいつでも、ライセンス モードから評価モードに変更できます。評価期間のうち残りの期間は、すでに使用した時間だけ減少します。

たとえば、ESXi ホストを 20 日間評価モードで使用し、その後 vSphere Standard Edition のライセンス キーをそのホストに割り当てたとします。ホストを評価モードに再設定した場合、そのホストの機能セット全体は、残りの評価期間である 40 日間評価検討できます。

ESXi ホストのライセンス管理については、『vCenter Server およびホスト管理』のドキュメントを参照してください。

ESXi 6.0 へのアップグレード後の、ライセンスの適用

ESXi 6.0 にアップグレードした後で、vSphere 6.0 ライセンスを適用する必要があります。

ESXi 5.x ホストを ESXi 6.0 ホストにアップグレードすると、正しい vSphere 6.0 ライセンスを適用するまで、ホストは 60 日間の評価モード期間に入ります。 [ESXi の評価モードとライセンス モードについて](#)を参照してください。

既存の vSphere 5.x ライセンスをアップグレードするか、Customer Connect から vSphere 6.0 ライセンスを取得できます。vSphere 6.0 ライセンスを取得したら、vSphere Web Client のライセンス管理機能を使用して、アップグレードされた ESXi 6.0 のすべてのホストにライセンスを割り当てる必要があります。詳細については、ドキュメント『vCenter Server およびホスト管理』を参照してください。スクリプト化された方法を使用して ESXi 6.0 へのアップグレードを行う場合、キックスタート (ks) ファイルにライセンス キーを設定できます。

システム ログに必要な空き容量

Auto Deploy を使用して ESXi 6.0 ホストをインストールする場合、または VMFS ボリューム上のスクラッチ ディレクトリ内のデフォルトの場所とは別にログ ディレクトリを設定する場合、システム ログ用の十分な空き領域を用意するため、現在のログ サイズとローテーション設定の変更が必要になることがあります。

vSphere のすべてのコンポーネントではこのインフラストラクチャを使用しています。このインフラストラクチャでのログ容量のデフォルト値は、使用可能なストレージの量、およびシステム ログの構成内容に応じて変わります。Auto Deploy を使用してデプロイしたホストでは、ログが RAM ディスクに保存されます。つまり、ログに使用できる領域はわずかです。

ホストが Auto Deploy を使用してデプロイされている場合は、次のいずれかの方法でログ ストレージを再構成してください。

- ネットワーク経由でリモート コレクタにログをリダイレクトする。
- NAS ストアまたは NFS ストアにログをリダイレクトする。

NAS ストアや NFS ストアなどの非デフォルト ストレージにログをリダイレクトする場合は、ディスクにインストールされたホストのログ サイズとローテーションも再構成できます。

デフォルト構成を使用する ESXi ホストのログ ストレージを再構成する必要はありません。このストレージは、VMFS ボリュームのスクラッチ ディレクトリにログを格納します。これらのホストについては、ESXi 6.0 によって、インストールに最も適した方法でログが構成され、ログ メッセージの保存に十分な空き領域が用意されます。

表 10-1. `hostd`、`vpaxa`、`fdm` の各ログに対して推奨される最小サイズとローテーションの構成

ログ	ログ ファイルの最大サイズ	維持するローテーション数	必要な最小ディスク領域
管理エージェント (<code>hostd</code>)	10 MB	10	100 MB
VirtualCenter エージェント (<code>vpaxa</code>)	5 MB	10	50 MB
vSphere HA エージェント (フォールト ドメイン マネージャ (<code>fdm</code>))	5 MB	10	50 MB

`syslog` および `syslog` サーバの設定と構成、および vSphere Syslog Collector のインストールについては、『vSphere Installation and SetupvSphere のインストールとセットアップ』ドキュメントを参照してください。

ESXi ホストでの `syslog` の構成

すべての ESXi ホストは、VMkernel およびその他のシステム コンポーネントからのメッセージをログ ファイルに記録する `syslog` サービス (`vm syslogd`) を実行しています。

vSphere Web Client または `esxcli system syslog vCLI` コマンドを使用して `syslog` サービスを構成できます。

vCLI コマンドの使い方の詳細については、vSphere Command-Line Interface スタート ガイドを参照してください。

手順

- 1 vSphere Web Client のインベントリでホストを選択します。
- 2 [管理] タブをクリックします。
- 3 システム パネルで、[システムの詳細設定] をクリックします。
- 4 [システムの詳細設定] リストで、[Syslog] セクションに移動します。
- 5 ロギングをグローバルに設定するには、変更する設定を選択し、[編集] アイコンをクリックします。

オプション	説明
<code>Syslog.global.defaultRotate</code>	保持するアーカイブの最大数を設定します。この数字はグローバルに、また個別のサブローガーについて設定できます。
<code>Syslog.global.defaultSize</code>	システムのログ ローテーションを行う際のログのデフォルト サイズを KB で設定します。この数字はグローバルに、また個別のサブローガーについて設定できます。

オプション	説明
Syslog.global.LogDir	ログが保管されるディレクトリです。ディレクトリは、マウントされた NFS または VMFS ボリュームに置くことができます。リブートしても継続するのは、ローカル ファイル システムの /scratch ディレクトリのみです。ディレクトリは、[datastorename] path_to_file と指定します。ここでパスはデータストアをバックアップするボリュームのルートからの相対パスです。例えば、パスの [storage1] /systemlogs はパスの /vmfs/volumes/storage1/systemlogs にマップします。
Syslog.global.logDirUnique	このオプションを選択すると、ESXi ホストの名前を持つサブディレクトリを [Syslog.global.LogDir] で指定されるディレクトリの下に作成します。同一の NFS ディレクトリが複数の ESXi ホストで使用される場合、独自のディレクトリは役に立ちます。
Syslog.global.LogHost	syslog メッセージの転送先のリモート ホストと、そのリモート ホストが syslog メッセージを受信するポート。ssl://hostname:1514 のようにしてプロトコルとポートを含められます。UDP (デフォルト)、TCP、および SSL がサポートされています。リモート ホストには syslog がインストールされ、転送された syslog メッセージを受信するように正しく構成されている必要があります。構成の情報については、リモート ホストにインストールされた syslog サービスのドキュメントを参照してください。

6 (オプション) 任意のログに対して、デフォルトのログ サイズとログ ローテーションを上書きします。

- a カスタマイズするログの名前をクリックします。
- b [編集] アイコンをクリックし、ローテーション数とログ サイズを入力します。

7 [OK] をクリックします。

結果

syslog オプションの変更がすぐに有効になります。

仮想マシンと VMware Tools のアップグレード

11

ESXi ホストをアップグレードしたら、新機能を利用するためにホスト上の仮想マシンをアップグレードできます。

VMware は仮想マシンのアップグレード用に、次のツールを提供しています。

vSphere Web Client

仮想マシンのアップグレードを一度に 1 つの手順で実行する必要がありますが、vSphere Update Manager は必要ありません。仮想マシンのアップグレードの詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。

vSphere Update Manager

仮想マシンのアップグレードおよびパッチ適用の手順を自動化します。そのため、正しい順序でステップが実行されます。Update Manager を使用して、仮想マシン ハードウェア バージョンと VMware Tools を直接アップグレードできます。『VMware vSphere Update Manager のインストールと管理』ドキュメントを参照してください。

vSphere のアップグレードのトラブルシューティング

12

インストールおよびアップグレード ソフトウェアにより、インストール、アップグレード、または移行が失敗する原因となるホスト マシンの問題を特定することができます。

対話型のインストール、アップグレード、および移行では、エラーまたは警告がインストーラの最後のパネルに表示され、インストールまたはアップグレードを続けるか取り消すかを尋ねるメッセージが表示されます。スクリプトを使用したインストール、アップグレード、または移行の場合は、エラーや警告がインストール ログ ファイルに書き込まれます。既知の問題については、製品のリリース ノートも参照してください。

vSphere Update Manager には、これらのエラーや警告用のカスタム メッセージが用意されています。Update Manager によるホストのアップグレード スキャン中に事前チェック スクリプトで返された元のエラーおよび警告を表示するには、Update Manager のログ ファイル (`vmware-vum-server-log4cpp.log`) を参照してください。

『vSphere アップグレード ガイド』には、VMware 製品とその機能を使用する方法について記載されています。このガイドに記載されていない問題またはエラーの状況が発生した場合、VMware のナレッジベースで解決策が見つかることがあります。また、VMware のコミュニティ フォーラムで、同じ問題が発生した他のユーザーを見つけたり、アドバイスを求めたりすることも、サポート リクエストを提出して VMware のサービス プロフェッショナルのサポートを受けることもできます。

この章には、次のトピックが含まれています。

- [vCenter Server のインストールまたはアップグレードのトラブルシューティングのためのログの収集](#)
- [ESXi ホストをトラブルシューティングするためのログの収集](#)
- [インストールおよびアップグレードの事前チェック スクリプトで返されるエラーおよび警告](#)
- [アップグレードが失敗した場合の vCenter Server サービスのリストア](#)
- [vCenter Server Appliance のアップグレード後の起動中の VMware Component Manager のエラー](#)
- [サポートされていない互換モードに設定されている Microsoft SQL データベースを原因とする vCenter Server のインストールまたはアップグレードの失敗](#)

vCenter Server のインストールまたはアップグレードのトラブルシューティングのためのログの収集

vCenter Server のインストールまたはアップグレード ログ ファイルを収集できます。インストールまたはアップグレードが失敗した場合、ログ ファイルを確認することで、失敗の原因を特定できる可能性があります。

Windows 版 vCenter Server のインストールの失敗に関するログ ファイルの保存およびリカバリをインストール ウィザードで行うのか、手動で行うのかを選択できます。

vCenter Server Appliance のデブロイ ログ ファイルを収集することもできます。

インストール ウィザードを使用したインストール ログの収集

インストール ウィザードの [セットアップの中断] ページを使用して、Windows 版 vCenter Server のインストール ログ ファイルの生成された .zip ファイルを参照できます。

インストールに失敗すると、[セットアップの中断] ページが表示されます。ログ収集のチェック ボックスはデフォルトで選択されています。

手順

- 1 チェック ボックスを選択したままにし、[終了] をクリックします。

インストール ファイルがデスクトップの .zip ファイル (VMware-VCS-logs-time-of-installation-attempt.zip など) に収集されます。time-of-installation-attempt には、インストールが試行された年、月、日、時、分、秒が表示されます。

- 2 デスクトップの .zip ファイルからログ ファイルを取得します。

次のステップ

ログ ファイルを調査して、障害の原因を特定します。

インストール ログの手動による収集

インストール ログ ファイルを手動で取得して調査できます。

手順

- 1 インストール ログ ファイルの場所に移動します。

- %PROGRAMDATA%\VMware\vCenterServer\logs ディレクトリ、通常は C:\ProgramData\VMware\vCenterServer\logs
- %TEMP% ディレクトリ (通常は C:\Users\username\AppData\Local\Temp)
%TEMP% ディレクトリには、vminst.log、pkgmgr.log、pkgmgr-comp-msi.log、および vim-vcs-msi.log などのファイルがあります。

- 2 テキスト エディタでインストール ログ ファイルを開いて調査します。

vCenter Server Appliance のインストール ログの収集

最初の起動時に vCenter Server Appliance が応答を停止した場合は、インストール ログ ファイルを収集、確認して、エラーの原因を特定できます。

手順

- 1 アプライアンス シェルにアクセスします。

オプション	説明
アプライアンスに直接アクセスできる場合	Alt+F1 を押します。
リモート接続する場合	SSH などのリモート コンソール接続を使用して、アプライアンスへのセッションを開始します。

- 2 アプライアンスで認識されるユーザー名とパスワードを入力します。
- 3 アプライアンス シェルで、`pi shell` コマンドを実行して、Bash シェルにアクセスします。
- 4 Bash シェルで、`vc-support.sh` スクリプトを実行して、サポート バンドルを生成します。
このコマンドにより、`/var/tmp` に `.tgz` ファイルが生成されます。
- 5 生成されたサポート バンドルを `user@x.x.x.x:/tmp` フォルダにエクスポートします。

```
scp /var/tmp/vc-etco-vm-vlan11-dhcp-63-151.eng.vmware.com-2014-02-28--21.11.tgz
user@x.x.x.x:/tmp
```

- 6 どの `firstboot` スクリプトが失敗したかを判別します。

```
cat /var/log/firstboot/firstbootStatus.json
```

次のステップ

問題を発生させる可能性のある原因を特定するには、失敗した `firstboot` スクリプトのログ ファイルを調べます。

データベース アップグレード ログの収集

データベース アップグレード ログ ファイルを手動で取得して調査できます。

vCenter Server アップグレード プロセスが完了したら、データベース アップグレード ログを取得できます。

前提条件

手順

- 1 データベース アップグレード ログの場所に移動します。
- 2 テキスト エディタでデータベース アップグレード ログを開いて調査します。

結果

ログ ファイルを調査して、データベース アップグレード プロセスの詳細を確認できます。

例：データベース アップグレードの場所

- アップグレード前チェックについては、`%TEMP%\..\vcsUpgrade\vcdb_req.out` ファイルを確認します。

vcdb_req.err ファイルでは、アップグレード前の段階で識別されたエラーを追跡します。

- エクスポートの詳細については、`%TEMP%\..\vcsUpgrade\vcdb_export.out` ファイルを確認します。

`vcdb_export.err` ファイルには、アップグレードのエクスポートの段階で識別されたエラーが含まれています。

- インポートの詳細については、`ProgramData\Vmware\CIS\logs\vmware\vpv\vcdb_import.out` ファイルを確認します。

`vcdb_import.err` ファイルには、アップグレード プロセスのインポートの段階で識別されたエラーが含まれています。

- インプレース アップグレード ログの詳細については、`ProgramData\Vmware\CIS\logs\vmware\vpv\vcdb_inplace.out` ファイルを確認します。

`vcdb_inplace.err` ファイルには、インプレース アップグレード エラーが含まれています。

次のステップ

`vcdb_inplace.*` ログ ファイルを調査します。

ESXi ホストをトラブルシューティングするためのログの収集

ESXi のインストール ログ ファイルまたはアップグレード ログ ファイルを収集できます。インストールまたはアップグレードが失敗した場合、ログ ファイルを確認することで、失敗の原因を特定できる可能性があります。

解決方法

- 1 ESXi Shell で、または SSH を介して、`vm-support` コマンドを入力します。
- 2 `/var/tmp/` ディレクトリに移動します。
- 3 `.tgz` ファイルからログ ファイルを取得します。

インストールおよびアップグレードの事前チェック スクリプトで返されるエラーおよび警告

インストールおよびアップグレードの事前チェック スクリプトでは、インストール、アップグレード、または移行の失敗につながる可能性のあるホスト マシン上の問題を特定するためのテストが実行されます。

対話型のインストール、アップグレード、および移行では、エラーまたは警告がインストーラの最後のパネルに表示され、インストールまたはアップグレードを続けるか取り消すかを尋ねるメッセージが表示されます。スクリプトを使用したインストール、アップグレード、または移行の場合は、エラーや警告がインストール ログ ファイルに書き込まれます。

vSphere Update Manager には、これらのエラーや警告用のカスタム メッセージが用意されています。Update Manager によるホストのアップグレード スキャン中に事前チェック スクリプトによって返された元のエラーおよび警告を確認するには、Update Manager のログ ファイル (`vmware-vum-server-log4cpp.log`) を参照してください。

表 12-1. インストールおよびアップグレードの事前チェック スクリプトで返されるエラーコードおよび警告コード

エラーまたは警告	説明
64BIT_LONGMODESTATUS	ホスト プロセッサは 64 ビットである必要があります。
COS_NETWORKING	警告。有効なサービス コンソールの仮想 NIC で IPv4 アドレスが見つかりましたが、vmkernel の同じサブネット内に対応するアドレスがありません。警告は、そのような問題が検出されるたびに表示されます。
CPU_CORES	ホストには少なくとも 2 つのコアが必要です。
DISTRIBUTED_VIRTUAL_SWITCH	ホストで Cisco Virtual Ethernet Module (VEM) が検出された場合は、このテストにより、アップグレードに VEM ソフトウェアも含まれているかどうかチェックされます。またこのテストにより、そのアップグレードで、ホスト上の既存のバージョンと同じバージョンの Cisco Virtual Supervisor Module (VSM) がサポートされるかどうかも判別されます。ソフトウェアが欠落しているか、別のバージョンの VSM と互換性がある場合は、テストにより警告が返されます。結果には、アップグレード ISO で必要な VEM ソフトウェアのバージョンと、検出されたバージョン（検出された場合）が示されます。適切なバージョンの VEM ソフトウェアを含むカスタム インストール ISO を作成するには、ESXi Image Builder CLI を使用できます。
HARDWARE_VIRTUALIZATION	警告。ホストのプロセッサにハードウェア仮想化機能がないか、ハードウェア仮想化がホストの BIOS でオンになっていないと、ホストのパフォーマンスに影響します。ホスト マシンの起動オプションで、ハードウェアの仮想化を有効にします。ハードウェア ベンダーのマニュアルを参照してください。
MD5_ROOT_PASSWORD	このテストでは、root パスワードが MD5 形式でエンコードされているかどうかチェックされます。パスワードが MD5 形式でエンコードされていない場合、重要と見なされるのは 8 文字までです。その場合、アップグレード後に最初の 8 文字以外は認証されず、セキュリティの問題が発生する可能性があります。この問題を回避するには、当社のナレッジ ベースの記事 1024500 を参照してください。
MEMORY_SIZE	ホストをアップグレードするには、指定された量のメモリが必要です。
PACKAGE_COMPLIANCE	vSphere Update Manager のみです。このテストでは、ホストが正常にアップグレードされたことを確認するため、ホスト上の既存のソフトウェアが、アップグレード ISO に含まれるソフトウェアと同じかどうかチェックされます。不足しているパッケージがあったり、アップグレード ISO のパッケージより古いバージョンのパッケージであったりすると、テストでエラーが返され、ホストで見つかったソフトウェアとアップグレード ISO で見つかったソフトウェアが示されます。
PARTITION_LAYOUT	ソフトウェアをアップグレードまたは移行することができるのは、アップグレード対象のディスク上に最大で 1 つの VMFS パーティションが存在し、その VMFS パーティションがセクタ 1843200 以降から開始する場合のみです。

表 12-1. インストールおよびアップグレードの事前チェック スクリプトで返されるエラーコードおよび警告コード (続き)

エラーまたは警告	説明
POWERPATH	このテストでは、CIM モジュールとカーネル モジュールで構成される EMC PowerPath ソフトウェアがインストールされているかどうかチェックされます。ホストでこれらのコンポーネントのどちらかが検出された場合、テストでは、CIM、vmkernel、およびモジュールなどの対応するコンポーネントがアップグレードにも存在するかどうかチェックされます。存在しない場合には、テストによって警告が返され、どの PowerPath コンポーネントがアップグレード ISO 上に必要であり、どのコンポーネントが見つかったか (見つかった場合) が示されます。
PRECHECK_INITIALIZE	このテストでは、事前チェック スクリプトを実行できるかどうかチェックされます。
SANE_ESX_CONF	/etc/vmware/esx.conf ファイルがホスト上に存在する必要があります。
SPACE_AVAIL_ISO	vSphere Update Manager のみです。ホスト ディスクには、インストーラ CD または DVD の内容を格納するのに十分な空き容量が必要です。
SPACE_AVAIL_CONFIG	vSphere Update Manager のみです。ホスト ディスクには、再起動の間 5.x の構成を格納するのに十分な空き容量が必要です。
SUPPORTED_ESX_VERSION	ESXi 6.0 には、バージョン 5.x の ESXi ホストからのみアップグレードまたは移行できます。
TBOOT_REQUIRED	このメッセージは、vSphere Update Manager のアップグレードにのみ適用されます。ホスト システムがトラステッド ブート モード (tboot) で実行されていても、ESXi アップグレード ISO に tboot VIB が含まれていない場合は、このエラーでアップグレードに失敗します。このテストは、ホストのセキュリティ レベルの低下を招くアップグレードを阻止します。
UNSUPPORTED_DEVICES	警告。このテストでは、サポートされていないデバイスがチェックされます。一部の PCI デバイスは、ESXi 6.0 ではサポートされません。
UPDATE_PENDING	<p>このテストでは、再起動を必要とする VIB がホストにインストールされているかどうかチェックされます。そのような VIB が 1 つ以上インストールされているとテストは失敗しますが、ホストの再起動はまだ実行されません。このような場合、事前チェック スクリプトでは、ホストにどのパッケージがインストールされているかを確実に判定できないため、残りの事前チェック テストを信頼してアップグレードが安全かどうかを判断するのは危険である可能性があります。</p> <p>このエラーが表示された場合は、ホストを再起動してアップグレードを再試行してください。</p>

アップグレードが失敗した場合の vCenter Server サービスのリストア

外部 Platform Services Controller を使用する vCenter Server へのアップグレードが失敗する場合は、手動でリストアするか、vCenter Inventory Service や vCenter Server などのサービスを再ポイントする必要があります。

問題

アンインストール フェーズの後で vCenter Server のアップグレードの失敗が発生し、設定が前の状態（vCenter Server 5.1 または 5.5）に戻る場合は、Platform Services Controller 6.0 に含まれる vCenter Single Sign-On に vCenter Inventory Service や vCenter Server などのサービスが再登録されないことがあります。

原因

vCenter Inventory Service や vCenter Server などのサービスは、vCenter Server 6.0 へのアップグレード中に vCenter Single-Sign-On 5.1 または 5.5 から登録解除されます。サービスが登録解除された後でアップグレードの失敗が発生する場合には、登録情報が失われます。vCenter Server 6.0 へのアップグレードが再開されるたびに、インストーラは登録解除されたサービスを確認し、それらを登録解除されたままにします。vCenter Inventory Service や vCenter Server などのサービスは、新たにアップグレードされた Platform Services Controller 6.0 インスタンスに手動で再ポイントまたは登録する必要があります。ナレッジ ベースの記事 [2033620](#) を参照してください。

解決方法

- ◆ vCenter Single Sign-On にこれらのサービスを再ポイントまたは再登録するには、このナレッジ ベースの記事で手順を見つけてそれに従ってください。

vCenter Server Appliance のアップグレード後の起動中の VMware Component Manager のエラー

アップグレード後に vCenter Server Appliance の Component Manager を最初にデプロイすると、エラーで失敗します。

問題

vCenter Server Appliance インスタンスをデプロイすると、次のようなエラーが受信されます。

「firstboot スクリプト実行エラー。」

「vCenter Single Sign-On への接続時の SSL 証明書が一致しません。証明書内のホスト名が一致しませんでした。<vcenter-b.domain.com> != <localhost.localdom> または <localhost.localdom> または <localhost>」

原因

vCenter Server Appliance インスタンス名が、SSL 証明書内の名前と一致していません。証明書を再生成して、正しい完全修飾ドメイン名を取得する必要があります。

解決方法

- 1 vCenter Server Appliance 5.5 インスタンスをパワーオンします。
- 2 VAMI <https://IP:5480> にログインします。
- 3 ネットワーク設定に正しい IP アドレスとホスト名が設定されていることを確認します。
- 4 証明書の再生成 チェック ボックスをオンにします。
- 5 vCenter Server Appliance 5.5 インスタンスを再起動します。

vCenter Server、vSphere Web Client、vami、slapd、vCenter Inventory Service、および vCenter Single Sign-On の証明書が CN=vcenter-a.domain.com を含む証明書および DNS=vcenter-a.domain.com DNS=vcenter-a IP=192.168.2.100 を含む SubjectAltName を使用して再生成されます。証明書には *vcenter-b.domain.com* が含まれなくなります。

- 6 vCenter Server Appliance 6.0 のアップグレードを再実行します。

解決方法

[vCenter Single Sign-On が組み込まれた vCenter Server Appliance のアップグレード](#) を参照してください。

サポートされていない互換モードに設定されている Microsoft SQL データベースを原因とする vCenter Server のインストールまたはアップグレードの失敗

Microsoft SQL データベースを使用する vCenter Server のインストールの場合、データベースがサポート対象外のバージョンの互換モードに設定されていると、インストールが失敗します。

問題

次のエラー メッセージが表示されます。 入力された DB ユーザーには、選択された DB に vCenter Server をインストールしたり構成したりするのに必要な権限がありません。 次のエラーを修正してください: %s

原因

データベースのバージョンは、vCenter Server 用にサポートされるバージョンである必要があります。SQL の場合、データベースがサポート対象のバージョンであっても、サポート対象外のバージョンの互換モードで実行するように設定されていると、このエラーが発生します。たとえば、SQL 2008 が SQL 2000 互換モードで実行するように設定されていると、このエラーが発生します。

解決方法

- ◆ vCenter Server のデータベースがサポート対象のバージョンであり、サポート対象外のバージョンの互換モードに設定されていないことを確認してください。VMware 製品の相互運用性マトリックス (http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?) を参照してください。