

View アップグレード

変更日：2018 年 1 月 4 日
VMware Horizon 7 7.4



vmware®

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>) でご確認ください。このドキュメントに関するご意見およびご感想は、docfeedback@vmware.com までお送りください。

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

ヴァイエムウェア株式会社
105-0013 東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

Copyright © 2009-2018 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

目次

View のアップグレード 5

1 View のアップグレードの概要 6

2 アップグレードのシステム要件 9

Horizon 7 コンポーネントのバージョンの互換性マトリックス 9

View Composer の要件 10

View Composer でサポートされるオペレーティング システム 10

スタンドアロン View Composer のハードウェア要件 11

View Composer およびイベント データベースのデータベース要件 11

View Composer のアップグレード要件 12

Horizon 接続サーバの要件 13

Horizon 接続サーバのハードウェア要件 13

Horizon 接続サーバでサポートされるオペレーティング システム 13

View 接続サーバのアップグレード要件 14

Horizon Agent でサポートされるオペレーティング システム 16

3 View Server コンポーネントのアップグレード 17

View Composer のアップグレード 17

アップグレードのための vCenter Server および View Composer の準備 18

View Composer のアップグレード 20

View Composer から vCenter および ESXi 接続で TLSv1.0 を有効にする 21

View Composer のダイジェスト アクセス認証の有効化 22

View Composer データベースの手動アップグレード 22

別のマシンへの View Composer の移行 26

Horizon 接続サーバのアップグレード 32

アップグレードのための接続サーバの準備 32

レプリカ グループ内の接続サーバのアップグレード 33

接続サーバから vCenter 接続で TLSv1.0 を有効にする 36

別のマシンでの最新バージョンの接続サーバへのアップグレード 37

接続サーバをスナップショットに戻した後のレプリカ グループの作成 39

セキュリティ サーバのアップグレード 39

アップグレードのための View セキュリティ サーバの準備 40

View セキュリティ サーバとペアになっている View 接続サーバのアップグレード 40

Cloud Pod アーキテクチャ 環境のアップグレード 43

View Server のアップグレードによる HTML Access の許可 44

vCenter Server のアップグレード 44

デフォルトの SSL 証明書のサムプリントを受け入れる 45

Horizon 7 グループ ポリシー管理用テンプレート ファイルの使用 47

4 ESXi ホストおよび仮想マシンのアップグレード 48

5 リモート デスクトップおよび Horizon Client のアップグレード 51

リモート デスクトップのアップグレードのためのセキュリティ関連の要件 51

セッション ベースのデスクトップを提供する RDS ホストのアップグレード 51

View Agent または Horizon Agent のアップグレード 53

View Composer デスクトップ プールのアップグレード 55

クライアント アプリケーションのアップグレード 57

6 View セットアップで新機能を有効にするためのアップグレード後タスク 59

JMS メッセージ セキュリティ モードを拡張済みに変更する 59

領域を再利用するためにデスクトップ プールをアップグレードする作業 60

VMware Virtual SAN データストアを使用する場合のアップグレード作業 62

Non-Virtual SAN データストアから Virtual SAN データストアへのアップグレード 62

Virtual SAN Disk Format バージョン 1 からのアップグレード 63

Virtual SAN データストア上の Horizon View 5.3.x からのアップグレード 65

エンド ユーザー用の VMware Horizon Web ポータル ページの構成 66

7 View パッチの適用 71

View Composer へのパッチの適用 71

View 接続サーバへのパッチの適用 72

View Agent または Horizon Agent へのパッチの適用 73

Horizon Client のパッチの適用 74

8 View 環境における vSphere コンポーネントの個別アップグレード 76

View のアップグレード

『View のアップグレード』では、最新メンテナンス リリースの Horizon View 5.3、VMware Horizon™ 6 (with View)、VMware Horizon 6 バージョン 6.1 または 6.2 から VMware Horizon 7 にアップグレードする手順について説明します。View メンテナンスおよびパッチ リリースにアップグレードする場合も、このガイドを使用できます。

VMware vSphere® のバージョンもアップグレードしている場合、View のアップグレードの各段階で実行するアップグレードの手順をこのガイドで確認できます。

View のパッチ リリースについては、[7 章 View パッチの適用](#) を参照してください。

対象読者

このガイドは、この製品の最新バージョンへ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としています。このガイドに記載されている情報は、仮想マシンのテクノロジーとデータセンターの操作に精通した、経験豊富な Microsoft Windows または Linux システム管理者向けに書かれています。

View のアップグレードの概要

View のエンタープライズ展開のアップグレードには、高度な作業がいくつか含まれます。アップグレードは複数のステージからなるプロセスであり、特定の順序で手順を実行する必要があります。View 接続サーバおよび他の View サーバをアップグレードする前に View Composer をアップグレードします。

重要: Horizon 6 バージョン 6.2 以降では、View コンポーネントをインストールして FIPS モードで実行できます。View では非 FIPS インストールを FIPS インストールにアップグレードすることはできません。View では、FIPS モードでの Horizon 6 バージョン 6.2 から FIPS モードでの Horizon 7 へのアップグレードがサポートされています。新規インストールの実行が必要な場合は、『View のインストール』ドキュメントで「FIPS モードでの View のインストール」を参照してください。

アップグレード中、View は View Composer のプロビジョニング操作とメンテナンス操作をサポートしません。View Server が以前のバージョンを実行している移行期間中、リンク クローン デスクトップのプロビジョニングや再構成などの操作はサポートされません。View 接続サーバと View Composer のインスタンスをすべてアップグレードした場合のみ、これらの操作を正常に実行できます。

アップグレード処理は特定の順序で行う必要があります。各アップグレード ステージの中での順序も重要です。

注: ここでは、メジャー、マイナー、およびメンテナンス リリースの概要について説明します。パッチの情報については、[7 章 View パッチの適用](#)を参照してください。

以下のうち実行する必要があるタスクは、展開で使用する View のコンポーネントによって異なります。

- 1 View Composer および VMware vCenter Server[®] をホストする物理マシンまたは仮想マシンで、バックアップを行い、スケジュールを設定されている一部のタスクを一時的に停止します。[アップグレードのための vCenter Server および View Composer の準備](#)を参照してください。

vCenter Server とは別のマシンにインストールされているスタンドアロンの View Composer を使用している場合は、View Composer データベースと View Composer TLS/SSL 証明書のバックアップを作成する必要があるだけです。vCenter Server もアップグレードしたい場合は、vCenter Server のアップグレードを個別にスケジュールできます。

vCenter Server および ESXi のバージョンと互換性があるバージョンについての詳細は、http://www.vmware.com/resources/compatibility/sim/interop_matrix.php の VMware 製品の互換性一覧を参照してください。

- 2 View Composer を既存のホストでアップグレードするか、新しいマシンに移行します。[View Composer のアップグレード](#)を参照してください。
- 3 View 接続サーバ インスタンスをホストする物理マシンまたは仮想マシンで、バックアップを行い、さまざまな構成とシステム設定を記録します。[アップグレードのための接続サーバの準備](#)を参照してください。

レプリカ グループ内に複数の View 接続サーバ インスタンスがある場合は、グループ内の 1 つのインスタンスのみについてバックアップを作成して構成設定を記録します。その他の準備タスクについては、一度に 1 つのインスタンスについてタスクを実行し、続いてそのサーバ インスタンスのアップグレードを実行できます。

- 4 セキュリティ サーバとペアになっていない View 接続サーバ インスタンスをアップグレードします。[レプリカ グループ内の接続サーバのアップグレード](#)を参照してください。

ロード バランサを使用する複数の View 接続サーバ インスタンスから成る典型的な本番環境で、ダウンタイムを最小限に抑える必要がある場合は、View 接続サーバ インスタンスのアップグレード時に負荷分散クラスタからインスタンスを一度に 1 つずつ削除できます。

重要: 接続サーバ インスタンスを最新バージョンにアップグレード後は、以前のバージョンにインスタンスをダウングレードできません。複製したグループですべての接続サーバのインスタンスのアップグレード後は、以前のバージョンを実行する他のインスタンスを追加できません。

- 5 セキュリティ サーバを選択する場合は、バックアップを作成して、さまざまな構成とシステム設定を記録します。[アップグレードのための View セキュリティ サーバの準備](#)を参照してください。

ダウンタイムを最小限に抑える必要がある場合は、一度に 1 つのセキュリティ サーバについてタスクを実行し、続いてそのサーバのアップグレードを実行できます。

- 6 セキュリティ サーバを使用している場合は、各セキュリティ サーバとそのペアの View 接続サーバ インスタンスをアップグレードしてください。これらのペアを 1 つずつアップグレードする場合は、負荷分散グループから各セキュリティ サーバを削除して、ペアをアップグレードし、その後にセキュリティ サーバをグループに戻すことによって、ゼロ ダウンタイムを達成できます。[View セキュリティ サーバとペアになっている View 接続サーバのアップグレード](#)を参照してください。

- 7 Active Directory で使用するグループ ポリシーをアップグレードします。[Horizon 7 グループ ポリシー管理用 テンプレート ファイルの使用](#)を参照してください。

- 8 VMware vSphere コンポーネントもアップグレードしている場合は、vCenter Server をアップグレードします。[vCenter Server のアップグレード](#)を参照してください。

vCenter Server のアップグレード中に、既存のリモート デスクトップとアプリケーションのセッションは切断されません。プロビジョニング状態のリモート デスクトップは vCenter Server のアップグレード中にパワーオンされません。また、vCenter Server のアップグレード中に新しいデスクトップは起動されず、View Composer の操作は許可されません。

- 9 vSphere もアップグレードしている場合は、VMware[®] ESXi[™] ホストおよび仮想マシンをアップグレードします。[4 章 ESXi ホストおよび仮想マシンのアップグレード](#)を参照してください。

ホストがクラスタ環境で構成されている場合は、vMotion を使用して仮想マシンをクラスタ内の別のホストに移行することにより、ESXi ホストをゼロ ダウンタイムでアップグレードできます。

- 10 Windows ターミナル サービスサーバを現在デスクトップ ソースとして使用している場合は、Windows Server 2008 R2 以降にアップグレードし、RDS ホスト ロールがインストールされていることを確認します。[セッション ベースのデスクトップを提供する RDS ホストのアップグレード](#)を参照してください。

- 11 デスクトップ ソースとして、プール内の完全クローン デスクトップとして、および手動プール内の個別のデスクトップとして、それぞれ使用されている物理マシンまたは仮想マシン上で実行する Horizon™ Agent または View Agent™ ソフトウェアをアップグレードします。 [View Agent または Horizon Agent のアップグレード](#) を参照してください。
- 12 新しくアップグレードした仮想マシン デスクトップ ソースを使用して、デスクトップのアップグレードされたプールを作成します。 [View Composer デスクトップ プールのアップグレード](#) を参照してください。
- 13 エンド ユーザーのクライアント デバイスで実行する Horizon Client ソフトウェアをアップグレードします。 [クライアント アプリケーションのアップグレード](#) を参照してください。
- 14 Cloud Pod アーキテクチャの機能を使用する場合は、 [Cloud Pod アーキテクチャ 環境のアップグレード](#) を参照してください。

一部のコマンドは複数のステージを同時にアップグレードできるので、各ステージでの元に戻すことができない変更についてよく理解してから、本稼動環境をアップグレードすることをお勧めします。

重要: VMware View® Client with Local Mode 機能は、オフライン デスクトップを使用するためのもので、削除されました。そのため、この概要には View 転送サービンスタンスと View Client with Local Mode をアップグレードする手順は含まれていません。ローカル モード機能の代わりに、VMware Horizon 6.0 以降のリリースに含まれる VMware® Mirage™ を使用することを VMware はお勧めします。詳細については、https://www.vmware.com/support/pubs/view_pubs.html で入手可能な View リリース ノートを参照してください。

アップグレードのシステム要件

Horizon 7 の展開に含めるホストおよび仮想マシンは、特定のハードウェア要件およびオペレーティング システム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。

- [Horizon 7 コンポーネントのバージョンの互換性マトリックス](#)
- [View Composer の要件](#)
- [Horizon 接続サーバの要件](#)
- [Horizon Agent でサポートされるオペレーティング システム](#)

Horizon 7 コンポーネントのバージョンの互換性マトリックス

大企業ではアップグレードを段階的に実行する必要がある場合が多いため、コンポーネントは、少なくともアップグレード中において、ある程度の上位互換性と下位互換性が維持されるように設計されています。

以下のバージョンは、Horizon 7 へのアップグレードでサポートされています。

- Horizon View 5.3 の最新メンテナンス リリース
- VMware Horizon 6.0 (with View) の最新メンテナンス リリース
- VMware Horizon 6 バージョン 6.1 の最新メンテナンス リリース
- VMware Horizon 6 バージョン 6.2 の最新メンテナンス リリース

特定コンポーネントの最新メンテナンス リリースを確認するには、<https://docs.vmware.com/en/VMware-Horizon-7/index.html> で入手できる、そのリリースのリリース ノートを参照してください。

Horizon 接続サーバと Horizon Agent との互換性は、接続サーバのアップグレード時における相互運用に限られています。View Agent または Horizon Agent を管理する接続サーバのバージョンに合わせて、できるだけ早く View Agent または Horizon Agent をアップグレードする必要があります。

次の表に、コンポーネントの一覧と、バージョンの異なるその他のコンポーネントに対するそれぞれの互換性を示します。

表 2-1. VMware Horizon 7 と旧バージョンの View コンポーネントの互換性マトリックス

| | 接続サーバ : 旧バージョン | セキュリティ サーバ : 旧バージョン | View Composer : 旧バージョン | View Agent : 旧バージョン | Horizon Client (Windows) : 旧バージョン |
|--------------------------------|--------------------------------|-----------------------|------------------------|---------------------|-----------------------------------|
| 接続サーバ 7.0 | アップグレード時のみ | アップグレード前にベアになっていた場合のみ | いいえ | アップグレード時のみ | はい |
| セキュリティ サーバ 7.0 (PCoIP および RDP) | いいえ | 該当なし | いいえ | アップグレード時のみ | はい |
| View Composer 7.0 | アップグレード時のみ | アップグレード時のみ | 該当なし | アップグレード時のみ | 該当なし |
| Horizon Agent 7.0 | アップグレード時のみ (この表の後の注に記載した例外を参照) | いいえ | いいえ | 該当なし | アップグレード時のみ |
| Horizon Client 4.0 | はい | はい | はい | はい | 該当なし |

注意: アップグレード中、View Composer のプロビジョニング操作とメンテナンス操作はサポートされません。View Server が以前のバージョンを実行している移行期間中、リンク クローン デスクトップのプロビジョニングや再構成などの操作はサポートされません。接続サーバと View Composer のインスタンスをすべて最新バージョンにアップグレードした場合のみ、これらの操作を正常に実行できます。

vCenter Server および ESXi のバージョンと互換性があるバージョンについての詳細は、http://www.vmware.com/resources/compatibility/sim/interop_matrix.php の VMware 製品の互換性一覧を参照してください。

View Composer の要件

View Composer では、中央で管理される 1 つの基本イメージから複数のリンク クローン デスクトップを展開することができます。View Composer には特定のインストール要件およびストレージ要件があります。

View Composer でサポートされるオペレーティング システム

View Composer は 64 ビットのオペレーティング システムをサポートしますが、固有の要件と制限があります。View Composer は、vCenter Server と同じ物理マシンまたは仮想マシンにも、別のサーバにもインストールできます。

表 2-2. View Composer がサポートするオペレーティング システム

| オペレーティング システム | バージョン | エディション |
|----------------------------|--------|--------------------------------------|
| Windows Server 2008 R2 SP1 | 64 ビット | Standard Enterprise Datacenter |
| Windows Server 2012 R2 | 64 ビット | Standard Datacenter |
| Windows Server 2016 | 64 ビット | Standard Datacenter |

注: サービス パックなしの Windows Server 2008 R2 はサポートされません。

View Composer を vCenter Server とは異なる物理マシンまたは仮想マシンにインストールする場合は、[スタンドアロン View Composer のハードウェア要件](#) を参照してください。

スタンドアロン View Composer のハードウェア要件

View Composer を vCenter Server に使用するものとは別の物理または仮想マシンにインストールする場合、特定のハードウェア要件を満たす専用のマシンを使用する必要があります。

スタンドアロン View Composer インストールは、別の Windows Server マシンにインストールされた vCenter Server、または Linux ベースの vCenter Server Appliance と連携します。VMware では、それぞれの View Composer サービスと vCenter Server インスタンスを 1 対 1 で対応させることを推奨しています。

表 2-3. View Composer のハードウェア要件

| ハードウェア コンポーネント | 必須 | 推奨 |
|----------------|---|--|
| プロセッサ | 1.4 GHz 以上の Intel 64 または AMD 64 プロセッサで 2 つの CPU | 2 GHz 以上で 4 つの CPU |
| ネットワーク | 1 つ以上の 10/100Mbps ネットワーク インターフェイス カード (NIC) | 1Gbps NIC |
| メモリ | 4GB 以上の RAM | 50 以上のリモート デスクトップを展開する場合は 8 GB 以上の RAM |
| ディスク領域 | 40GB | 60 GB |

重要: View Composer をホストする物理マシンまたは仮想マシンは、変更されない IP アドレスを持っている必要があります。IPv4 環境では、固定 IP アドレスを構成します。IPv6 環境では、変更されない IP アドレスがマシンによって自動的に取得されます。

View Composer およびイベント データベースのデータベース要件

View Composer には、データを格納するための SQL データベースが必要です。View Composer データベースは、View Composer Server ホスト上に存在するか、View Composer Server ホストから利用できる必要があります。View イベントに関する View 接続サーバからの情報を記録するように、任意にイベント データベースをセットアップできます。

vCenter Server 用のデータベース サーバがすでに存在する場合、既存のインスタンスが http://www.vmware.com/resources/compatibility/sim/interop_matrix.php の「VMware 製品の互換運用性マトリックス」にあるバージョンであれば、View Composer でそれを使用できます。データベース サーバ インスタンスがまだ存在しない場合は、インストールする必要があります。

View Composer は、vCenter Server でサポートされるデータベース サーバのサブセットをサポートします。View Composer ではサポートされないデータベース サーバを vCenter Server ですでに使用している場合は、引き続き vCenter Server でそのデータベース サーバを使用し、View Composer で使用するための別のデータベース サーバをインストールします。

重要: vCenter Server と同じ SQL Server インスタンスに View Composer データベースを作成する場合は、vCenter Server データベースを上書きしないでください。

サポートされるデータベースの最新情報については、http://www.vmware.com/resources/compatibility/sim/interop_matrix.php で VMware 製品の互換運用性マトリックスを参照してください。[ソリューション/データベースの互換運用性] について、製品とバージョンを選択した後にデータベースを追加する手順でサポートされるデータベースをすべて表示するには、[すべて] を選択して [追加] をクリックします。

View Composer のアップグレード要件

View Composer のアップグレード処理には、特定の要件および制限事項があります。

View Composer インストーラを実行するには、そのシステムでの管理者権限を持つドメイン ユーザーである必要があります。

セキュリティ関連の要件

- View Composer では、CA（証明機関）が署名した SSL 証明書が必要です。View Composer をインストールした後で既存の証明書またはデフォルトの自己署名証明書を新しい証明書に置き換える予定にしている場合、新しい証明書をインポートして SviConfig ReplaceCertificate ユーティリティを実行し、新しい証明書を View Composer によって使用されるポートにバインドする必要があります。

vCenter Server と View Composer を同じ Windows Server コンピュータにインストールしている場合、これらは同じ SSL 証明書を使用できますが、証明書はそれぞれのコンポーネントについて個別に構成する必要があります。

セキュリティ証明書の要件に関する完全な情報については、『View のインストール』ドキュメントの「View Server の SSL 証明書の構成」を参照してください。

- vCenter Server、View Composer、および View Server の証明書には、証明書失効リスト (CRL) が含まれている必要があります。詳細については、『View のインストール』ガイドの「サーバ証明書の証明書失効チェックの構成」を参照してください。
- View Composer コンピュータで実行されているアプリケーションが、Microsoft Secure Channel (Schannel) セキュリティ パッケージで実装される SSLv2 を要求する Windows SSL ライブラリを使用していないことを確認します。View Composer インストーラにより、Microsoft Schannel 上の SSLv2 が無効になります。Java SSL を使用する Tomcat や OpenSSL を使用する Apache などのアプリケーションは、この制限による影響を受けません。SSLv3、TLSv1.0、および RC4 もデフォルトで無効になります。詳細については、『View セキュリティ』ドキュメントの「View で無効化された古いプロトコルと暗号化方式」を参照してください。

- View Composer のセキュリティを強化するために、View Composer サービスがインストールされている Windows Server コンピュータで強度の低い暗号化スイートを無効にします。『View のインストール』ドキュメントの「SSL/TLS で強度の低い暗号を無効にする」を参照してください。
- vSphere との互換性を引き続き維持するには、セキュリティ プロトコル構成を変更しなければならない場合があります。可能な場合は、View Composer にアップグレードする前に、ESXi および vCenter Server にパッチを適用して、TLSv1.1 と TLSv1.2 をサポートするようにします。パッチを適用できない場合は、アップグレードの前に View Composer で TLSv1.0 を再び有効にします。詳細については、[View Composer から vCenter および ESXi 接続で TLSv1.0 を有効にする](#)を参照してください。
- Horizon 7 バージョン 7.0.3 以降から、View Composer でダイジェスト アクセス認証を有効にしてセキュリティを強化できます。詳細については、[View Composer のダイジェスト アクセス認証の有効化](#)を参照してください。

Horizon 接続サーバの要件

Horizon 接続サーバはクライアント接続のブローカーとして機能し、受信したユーザーの要求を認証した後、適切なリモート デスクトップとアプリケーションに送信します。Horizon 接続サーバには、特定のハードウェア要件、オペレーティング システム要件、インストール要件、およびサポート ソフトウェア要件があります。

Horizon 接続サーバのハードウェア要件

Horizon 接続サーバのインストールタイプ（標準、レプリカ、セキュリティ サーバ、および登録サーバのインストール）はすべて、特定のハードウェア要件を満たす専用の物理マシンまたは仮想マシンにインストールする必要があります。

表 2-4. Horizon 接続サーバのハードウェア要件

| ハードウェア コンポーネント | Required | 推奨 |
|--------------------------------------|----------------------------|--|
| プロセッサ | Pentium IV 2.0GHz 以上のプロセッサ | 4 つの CPU |
| ネットワーク アダプタ | 100Mbps NIC | 1Gbps NIC |
| メモリ Windows Server 2008 R2 64 ビット | 4GB 以上の RAM | 50 以上のリモート デスクトップを展開する場合は 10GB 以上の RAM |
| メモリ Windows Server 2012 R2 64 ビット | 4GB 以上の RAM | 50 以上のリモート デスクトップを展開する場合は 10GB 以上の RAM |

上記の要件は、高可用性または外部アクセスのためにインストールする Horizon 接続サーバ（レプリカおよびセキュリティ サーバ） インスタンスにも適用されます。

重要: Horizon 接続サーバをホストする物理マシンまたは仮想マシンは、変更されない IP アドレスを持っている必要があります。IPv4 環境では、固定 IP アドレスを構成します。IPv6 環境では、変更されない IP アドレスがマシンによって自動的に取得されます。

Horizon 接続サーバでサポートされるオペレーティング システム

Horizon 接続サーバは、サポート対象の Windows Server オペレーティング システムにインストールする必要があります。

次のオペレーティング システムは、Horizon 接続サーバのすべてのインストールタイプ（標準、レプリカ、セキュリティ サーバ）をサポートします。

表 2-5. Horizon 接続サーバのオペレーティング システム サポート

| オペレーティング システム | バージョン | エディション |
|----------------------------|--------|--------------------------------------|
| Windows Server 2008 R2 SP1 | 64 ビット | Standard Enterprise Datacenter |
| Windows Server 2012 R2 | 64 ビット | Standard Datacenter |
| Windows Server 2016 | 64 ビット | Standard Datacenter |

注: サービス パックなしの Windows Server 2008 R2 はサポートされません。

View 接続サーバのアップグレード要件

View 接続サーバのアップグレード処理には、特定の要件および制限事項があります。

- View 接続サーバには最新リリース用の有効なライセンス キーが必要です。
- View 接続サーバの新しいバージョンのインストールに使用するドメイン ユーザー アカウントは、View 接続サーバ ホスト上での管理者権限を持っている必要があります。View 接続サーバの管理者は、vCenter Server の管理者認証情報を持っている必要があります。
- インストーラを実行する場合は、View Administrator アカウントを許可します。ローカル Administrators グループ、またはドメイン ユーザー/グループのアカウントを指定できます。View ではこのアカウントのみに、複製された View 接続サーバ インスタンスをインストールする権限を含む View の全管理権限を割り当てます。ドメインのユーザーまたはグループを指定する場合は、インストーラを実行する前に、Active Directory でアカウントを作成する必要があります。
- View 接続サーバをバックアップすると、View LDAP 構成が暗号化された LDIF データとしてエクスポートされます。暗号化されたバックアップ View 構成を復元するには、データ リカバリ パスワードを入力する必要があります。パスワードは 1 文字から 128 文字の間にする必要があります。

セキュリティ関連の要件

- View 接続サーバでは、CA（認証機関）によって署名され、クライアントが検証可能な SSL 証明書が必要です。View 接続サーバをインストールすると、CA 署名付き証明書がない場合にはデフォルトの自己署名証明書が生成されますが、デフォルトの自己署名証明書はできるだけ早く置き換える必要があります。自己署名証明書は、View Administrator で無効として表示されます。

また、更新したクライアントでは、クライアントとサーバ間の SSL ハンドシェイクの一部としてサーバの証明書に関する情報をやりとりすることが予想されます。多くの場合、更新されたクライアントは、自己署名証明書を信頼しません。

セキュリティ証明書の要件に関する完全な情報については、『View のインストール』ガイドの「View Server の SSL 証明書の構成」を参照してください。SSL 接続の負荷分散やオフロードなどのタスクを実行する中間サーバの設定方法を説明している『View への SSL 接続の設定シナリオ』ドキュメントも参照してください。

注: 元のサーバに CA によって署名された SSL 証明書がすでにある場合は、アップグレード中に、既存の CA 署名付き証明書を View が Windows Server の証明書ストアにインポートします。

- vCenter Server、View Composer、および View Server の証明書には、証明書失効リスト (CRL) が含まれている必要があります。詳細については、『View のインストール』ガイドの「サーバ証明書の証明書失効チェックの構成」を参照してください。

重要: 社内でインターネット アクセスのためにプロキシ設定を使用している場合、プロキシを使用するように View 接続サーバ ホストを構成する必要があります。この手順によって、サーバがインターネットの証明書失効チェック サイトにアクセスできることを保証します。Microsoft Netshell コマンドを使用して、View 接続サーバにプロキシ設定をインポートできます。詳細については、『View 管理』ガイドの「View Server 証明書失効チェックのトラブルシューティング」を参照してください。

- セキュリティ サーバをこの View 接続サーバ インスタンスとペアにする予定にしている場合、[セキュリティが強化された Windows ファイアウォール] がアクティブなプロファイルで [オン] に設定されていることを確認します。この設定はすべてのプロファイルで [オン] にすることを推奨します。デフォルトでは、IPsec ルールはセキュリティ サーバと View 接続サーバ間の接続を制御し、[セキュリティが強化された Windows ファイアウォール] を有効にする必要があります。
- お使いのネットワーク トポロジにおいて、セキュリティ サーバと View 接続サーバ インスタンスとの間にファイアウォールがある場合には、IPsec をサポートするようにファイアウォールを構成する必要があります。『View インストール ガイド』を参照してください。
- vSphere との互換性を引き続き維持するには、セキュリティ プロトコル構成を変更しなければならない場合があります。可能な場合は、View 接続サーバにアップグレードする前に、ESXi および vCenter Server にパッチを適用して、TLSv1.1 と TLSv1.2 をサポートするようにします。パッチを適用できない場合は、アップグレードの前に View 接続サーバで TLSv1.0 を再び有効にします。詳細については、[接続サーバから vCenter 接続で TLSv1.0 を有効にする](#)を参照してください。
- 6.2 より前のバージョンの View Agent を使用する Horizon 7 サーバを使用する場合は、PCoIP 接続向けに TLSv1.0 を有効にする必要があります。バージョン 6.2 よりも古い View Agent では、PCoIP 向けのセキュリティ プロトコル TLSv1.0 のみがサポートされます。接続サーバおよびセキュリティ サーバを含め、Horizon 7 サーバではデフォルトで TLSv1.0 が無効になっています。これらのサーバで PCoIP 接続向けに TLSv1.0 を有効にするには、<http://kb.vmware.com/kb/2130798> の VMware ナレッジベース (KB) に記載の手順に従って操作します。

追加の物理マシンまたは仮想マシン上で View 接続サーバ インスタンスの新規インストールを予定している場合は、『View のインストール』ドキュメントでインストール要件の完全なリストを参照してください。

Horizon Agent でサポートされるオペレーティング システム

Horizon Agent コンポーネント（以前のリリースでは View Agent と呼ばれていた）は、セッション管理、シングル サインオン、デバイスのリダイレクトなどの機能で使用されます。すべての仮想マシン、物理システム、および RDS ホストに、Horizon Agent をインストールする必要があります。

サポートされるゲスト OS のタイプとエディションは、Windows バージョンによって異なります。サポート対象の Windows 10 オペレーティング システムの最新情報については、VMware のナレッジベースの記事 KB<http://kb.vmware.com/kb/2149393> を参照してください。Windows 10 以外の Windows オペレーティング システムの場合には、VMware のナレッジベース (KB) の記事 <http://kb.vmware.com/kb/2150295> を参照してください。

Horizon Agent がインストールされている Windows オペレーティング システムでサポートされる特定の Remote Experience 機能の一覧については、VMware のナレッジベース (KB) の記事 <http://kb.vmware.com/kb/2150305> を参照してください。

セキュリティを強化するため、既知の脆弱性を除去するよう暗号化スイートを構成することをお勧めします。View Composer または Horizon Agent を実行する Windows マシン向けに暗号化スイートのドメイン ポリシーを設定アップする手順については、『View のインストール』ドキュメントにある View Composer または Horizon Agent の強度の弱い暗号化方式の無効化に関するトピックを参照してください。

View Server コンポーネントのアップグレード

3

アップグレードする必要があるサーバ コンポーネントとしては、View 接続サーバ、複製されたサーバ、およびセキュリティ サーバがあります。使用しているオプション コンポーネントによっては、View Composer のアップグレードも必要になる場合があります。

アップグレード作業を複数のメンテナンス期間に分散すると、処理の各段階で成功を確認したり、問題を発見したりすることができます。VMware では、最初のメンテナンス期間中にすべてのサーバ コンポーネントのアップグレードを推奨しています。

注: Horizon Client のローカル モード機能は削除されたため、View 転送サーバ インスタンスは不要になりました。ローカル モード機能の代わりに、VMware Horizon 6.0 以降のリリースに含まれる Mirage を使用することをお勧めします。詳細については、https://www.vmware.com/support/pubs/view_pubs.html で入手可能な View リリース ノートを参照してください。

View のパッチ リリースについては、[7 章 View パッチの適用](#) 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。

- [View Composer のアップグレード](#)
- [Horizon 接続サーバのアップグレード](#)
- [セキュリティ サーバのアップグレード](#)
- [Cloud Pod アーキテクチャ 環境のアップグレード](#)
- [View Server のアップグレードによる HTML Access の許可](#)
- [vCenter Server のアップグレード](#)
- [デフォルトの SSL 証明書のサムプリントを受け入れる](#)
- [Horizon 7 グループ ポリシー管理用テンプレート ファイルの使用](#)

View Composer のアップグレード

アップグレード中、View は View Composer のプロビジョニング操作とメンテナンス操作をサポートしません。View Server が以前のバージョンを実行している移行期間中、リンク クローン デスクトップのプロビジョニングや

再構成などの操作はサポートされません。View 接続サーバと View Composer のインスタンスをすべてアップグレードした場合のみ、これらの操作を正常に実行できます。

注: View Composer 6.2 の機能を使用してリンク クローン RDS ホストの自動ファームを作成する前に、すべての View コンポーネントを Horizon 6 バージョン 6.2 以降にアップグレードする必要があります。

アップグレードのための vCenter Server および View Composer の準備

vCenter Server と View Composer は同じ仮想マシンまたは物理マシンにインストールされることが多いため、一部の準備作業は両方に該当します。

vSphere を含むアップグレードの準備

最新バージョンの View へのアップグレードに加えて vCenter Server をアップグレードする場合は、『VMware vSphere アップグレード ガイド』を参照して、以下の順序で作業を行う必要があります。

- 1 仮想マシンや物理マシンが、アップグレードする vCenter Server バージョンのシステム要件を満たしていることを確認します。
- 2 現在の View Composer がインストールされている仮想マシンまたは物理マシンが新しいバージョンのセキュリティ要件を満たしていることを確認します。

[View Composer のアップグレード要件](#)を参照してください。

- 3 vCenter Server が仮想マシンにインストールされている場合は、その仮想マシンのスナップショットを作成します。

スナップショットの作成手順については、vSphere Client™ のオンライン ヘルプを参照してください。

- 4 コンピュータ名が 15 文字より長い場合は、15 文字以下の短い名前に変更します。
- 5 vCenter Server データベースと View Composer データベースをバックアップします。

データベースのバックアップ方法については、データベース ベンダーから提供されるマニュアルを参照してください。

- 6 データベース サーバに、使用する予定の vCenter Server のバージョンとの互換性があることを確認します。
たとえば、データベース サーバが Oracle 9i の場合、アップグレードが必要です。

- 7 データベースに新しいバージョンの View Composer との互換性があることを確認します。

View Composer は、vCenter Server でサポートされるデータベース サーバのサブセットをサポートします。vCenter Server で View Composer ではサポートされないデータベース サーバをすでに使用している場合は、引き続き vCenter Server でそのデータベース サーバを使用し、View Composer および View データベース イベント用に別のデータベース サーバをインストールします。

- 8 SSL 証明書を含むフォルダをコピーします。

このフォルダは %ALLUSERSPROFILE%\Application Data\VMware\VMware VirtualCenter にあります。

- 9 vCenter Server がインストールされているマシンの IP アドレスおよびシステム名を記録します。

- 10 すべてのリンク クローン デスクトップ プールについて、View Administrator を使用して新しい仮想マシンのプロビジョニングを無効にします。

View Composer とそのデスクトップ プールとは異なるメンテナンス期間にアップグレードされる場合があるため、両方のコンポーネントがアップグレードされるまでプロビジョニングを延期する必要があります。

- 11 いずれかのデスクトップ プールがログオフ時に OS ディスクを更新するように設定されている場合は、View Administrator を使用してそのプールの [デスクトップ/プール] 設定を編集し、[ログオフ時にマシンを削除または更新] を [なし] に設定します。

この設定を行うと、まだ View Agent がアップグレードされていないデスクトップの更新を新しくアップグレードされた View Composer が試みても、エラーが発生しません。

- 12 いずれかのデスクトップ プールに更新または再構成の操作のスケジュールが設定されている場合は、View Administrator を使用してそれらの操作をキャンセルします。

View Composer のみのアップグレードの準備

View Composer のみをアップグレードして、vCenter Server をアップグレードしない場合は、次の作業を実行する必要があります。

- 1 現在の View Composer がインストールされている仮想マシンまたは物理マシンが新しいバージョンのセキュリティ要件を満たしていることを確認します。

[View Composer のアップグレード要件](#)を参照してください。

- 2 View Composer が仮想マシンにインストールされている場合は、その仮想マシンのスナップショットを作成します。

スナップショットの作成手順については、vSphere Client のオンライン ヘルプを参照してください。

- 3 View Composer データベースをバックアップします。

データベースのバックアップ方法については、データベース ベンダーから提供されるマニュアルを参照してください。

- 4 データベースに新しいバージョンの View Composer との互換性があることを確認します。

View Composer は、vCenter Server でサポートされるデータベース サーバのサブセットをサポートします。vCenter Server で View Composer ではサポートされないデータベース サーバをすでに使用している場合は、引き続き vCenter Server でそのデータベース サーバを使用し、View Composer および View データベース イベント用に別のデータベース サーバをインストールします。

- 5 vCenter Server がインストールされているマシンの IP アドレスおよびシステム名を記録します。

- 6 すべてのリンク クローン デスクトップ プールについて、View Administrator を使用して新しい仮想マシンのプロビジョニングを無効にします。

View Composer とそのデスクトップ プールとは異なるメンテナンス期間にアップグレードされる場合があるため、両方のコンポーネントがアップグレードされるまでプロビジョニングを延期する必要があります。

- 7 いずれかのデスクトップ プールがログオフ時に OS ディスクを更新するように設定されている場合は、View Administrator を使用してそのプールの [デスクトップ/プール] 設定を編集し、[ログオフ時にマシンを削除または更新] を [なし] に設定します。

この設定を行うと、まだ View Agent がアップグレードされていないデスクトップの更新を新しくアップグレードされた View Composer が試みても、エラーが発生しません。

- 8 いずれかのデスクトップ プールに更新または再構成の操作のスケジュールが設定されている場合は、View Administrator を使用してそれらの操作をキャンセルします。

View Composer のアップグレード

最初のメンテナンス期間中に View composer をアップグレードします。すべての View サーバがアップグレードされるまでは、リンク クローン デスクトップのプロビジョニングと再構成などの操作を実行できません。

前提条件

- この手順をいつ実行すべきかを判断します。利用可能なデスクトップメンテナンス期間を選択します。15 ～ 30 分を予定してください。
- [View Composer のみのアップグレードの準備](#)に一覧表示されているタスクを実行します。
- View Composer がインストールされているサーバに CA（証明機関）が署名した TLS/SSL サーバ証明書がインストールされ構成されていることを確認します。View 接続サーバのアップグレード後に、View Composer で CA 署名付き証明書が使用されないと、デフォルトの自己署名証明書は、View Administrator で無効として表示されます。
- インストールとアップグレードを実行する際に使用するホスト上に、管理権限を持つドメイン ユーザー アカウントがあることを確認します。
- スキーマのアップグレードが必要な場合は、インストーラ ウィザードで View Composer データベースをアップグレードするかどうかを指定します。ウィザードが終了したら、SviConfig コマンド ライン ユーティリティを実行してデータベース スキーマを手動でアップグレードし、アップグレードのログを作成することができます。

手順

- 1 View Composer がインストールされている仮想または物理マシンで、View Composer のインストーラをダウンロードして実行します。

インストーラは VMware の Web サイトからダウンロードできます。

インストーラを実行する具体的な手順については、『View インストール ガイド』を参照してください。

- 2 スキーマのアップグレードが必要な場合は、ウィザードでデータベース スキーマをアップグレードするかどうかを指定します。

「Database upgrade completed with warnings(データベースのアップグレードが警告で終了しました)」というメッセージを含むダイアログ ボックスが表示されたら、[OK] をクリックしてメッセージを無視してかまいません。

- 3 ウィザードで View Composer のポート番号を要求されたら、ポート番号が 18443 に設定されていることを確認します。

次のステップ

データベース スキーマの手動アップグレードが必要な場合は、[SviConfig の実行によるデータベースの手動アップグレード](#)を参照してください。

古いバージョンの vCenter Server がある場合、[View Composer から vCenter および ESXi 接続で TLSv1.0 を有効にする](#)を参照してください。

次のメンテナンス期間に、View のアップグレードを続行します。[レプリカ グループ内の接続サーバのアップグレード](#)を参照してください。

View Composer から vCenter および ESXi 接続で TLSv1.0 を有効にする

Horizon 7 以降のコンポーネントでは、TLSv1.0 セキュリティ プロトコルがデフォルトで無効になっています。TLSv1.0 のみをサポートする古いバージョンの vCenter Server が展開環境に含まれている場合、View Composer 7.0 以降のリリースのインストールまたはアップグレード後に、View Composer 接続に対して TLSv1.0 を有効にすることが必要な可能性があります。

vCenter Server 5.0、5.1、および 5.5 の一部の旧メンテナンス リリースは、Horizon 7 以降のリリースではデフォルトで無効になっている TLSv1.0 のみをサポートします。vCenter Server を TLSv1.1 または TLSv1.2 をサポートするバージョンにアップグレードできない場合は、View Composer 接続に対して TLSv1.0 を有効にできます。

ESXi ホストで ESXi 6.0 U1b より前のバージョンが実行されていてアップグレードできない場合は、View Composer から ESXi ホストで TLSv1.0 接続を有効にすることが必要な可能性もあります。

前提条件

- View Composer 7.0 以降のリリースがインストールされていることを確認します。
- View Composer マシンに管理者としてログインして Windows レジストリ エディタを使用できることを確認します。

手順

- 1 View Composer をホストするマシンで、Windows レジストリ エディタ (regedit.exe) を開きます。
- 2 HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client に移動します。
このキーが存在しない場合は作成します。
- 3 値 [Enabled] が存在する場合は削除します。
- 4 [DWORD] 値 [DisabledByDefault] を編集して [0] に設定します。
- 5 VMware Horizon View Composer サービスを再起動します。
これで、View Composer から vCenter への TLSv1.0 接続が有効になりました。
- 6 View Composer マシンの Windows レジストリで、HKLM\SOFTWARE\VMware, Inc.\VMware View Composer に移動します。
- 7 文字列の値 [EnableTLS1.0] を作成または編集して [1] に設定します。
- 8 View Composer ホストが 64 ビット マシンの場合は、HKLM\SOFTWARE\WOW6432Node\VMware, Inc.\VMware View Composer に移動します。
- 9 文字列の値 [EnableTLS1.0] を作成または編集して [1] に設定します。

10 VMware Horizon View Composer サービスを再起動します。

これで、View Composer から ESXi ホストへの TLSv1.0 接続が有効になりました。

View Composer のダイジェスト アクセス認証の有効化

Horizon 7 バージョン 7.0.3 から、View Composer では Web セキュリティのための基本的なアクセス認証方式がデフォルトで有効になりました。セキュリティを強化するために、View Composer でダイジェスト アクセス認証方法を有効にできます。

前提条件

- View Composer 7.0.3 以降のリリースがインストールされていることを確認します。
- 管理者として View Composer マシンにログインできることを確認します。
- 接続サーバ 7.0.3 以降がインストールされていることを確認します。

手順

- 1 View Composer がインストールされているディレクトリに移動します。
- 2 SviWebService.exe.config ファイルを編集します。
- 3 SslPoxBinding 構成オプションを、authenticationScheme="Digest" に設定します。
- 4 SslBasicAtuth 構成オプションを、clientCredentialType="Digest" に設定します。
- 5 SviWebService.exe.config ファイルを保存して閉じます。
- 6 SviConfig.exe.config ファイルを編集します。
- 7 SslSviBinding 構成オプションを、clientCredentialType="Digest" に設定します。
- 8 SviConfig.exe.config ファイルを保存して閉じます。
- 9 View Composer サービスを再起動します。
 - a コマンド プロンプトに `services.msc` を入力して、Windows サービス ツールを起動します。
 - b サービスのリストから、再起動するサービスを右クリックします。たとえば、VMware Horizon Composer 7.0.3 を右クリックします。
 - c [再起動] をクリックします。

View Composer データベースの手動アップグレード

スキーマの更新が必要な場合、View Composer インストーラでデータベースをアップグレードする代わりに、手動でデータベースをアップグレードできます。アップグレード処理を細かく監視する必要がある場合、またはアップグレード作業を異なる役割の複数の IT 管理者に分担させる必要がある場合は、SviConfig ユーティリティを使用できます。

View Composer をデータベース スキーマが更新されているバージョンにアップグレードすると、データベースをアップグレードするためにウィザードを使用するかどうかを尋ねるプロンプトがインストーラにより表示されます。インストーラのウィザードを使用しない場合は、SviConfig ユーティリティを使用してデータベースをアップグレードし、既存のデータを移行する必要があります。

SviConfig コマンド ライン ユーティリティを使用すると、次のような利点があります。

- このユーティリティでは、結果コードが返され、アップグレードが失敗した場合のトラブルシューティングを容易にするデータベース アップグレードのログが作成されます。
- アップグレード作業を分割できます。vSphere または View の管理者は、View Composer インストーラを実行してソフトウェアをアップグレードできます。データベース管理者 (DBA) は、SviConfig を使用して、View Composer データベースをアップグレードできます。
- ソフトウェアのアップグレードとデータベースのアップグレードは、異なるメンテナンス期間に行うことができます。たとえば、サイトのデータベースメンテナンス操作は週末のみに実行し、ソフトウェア保守作業は週の途中で実行することが可能です。

SviConfig の実行によるデータベースの手動アップグレード

SviConfig コマンド ライン ユーティリティを使用すると、View Composer データベースを View Composer ソフトウェアとは別にアップグレードできます。このユーティリティでは、アップグレードが失敗した場合のトラブルシューティングを容易にするログ ファイルも作成されます。

重要: SviConfig ユーティリティは、熟練した View Composer 管理者のみが使用する必要があります。このユーティリティは、View Composer サービスに関連する問題を解決するためのものです。

前提条件

- View Composer データベースをバックアップします。手順については、データベース サーバのマニュアルを参照してください。
- View Composer データベースのデータベース ソース名 (DSN) がわかっているかどうかを確認します。
- このデータベースのデータベース管理者アカウントのユーザー名とパスワードがわかっているかどうかを確認します。

手順

- 1 vCenter Server の仮想マシンまたは物理マシンで、Windows コマンド プロンプトを開き、SviConfig 実行ファイルに移動します。

このファイルは、View Composer アプリケーションと同じ場所にあります。デフォルト パスは C:\Program Files (86)\VMware\VMware View Composer\sviconfig.exe です。

- 2 次のコマンドを入力して VMware View Composer を停止します。

net stop svid

3 SviConfig databaseupgrade コマンドを実行します。

```
sviconfig -operation=databaseupgrade
          -DsnName=target_DSN
          -Username=database_administrator_username
```

例：

```
sviconfig -operation=databaseupgrade -dsname=LinkedClone
          -username=Admin
```

4 入力を求められたらパスワードを入力します。

操作が成功すると、アップグレード手順を示す出力が表示されます。

```
Establishing database connection.
Database connection established successfully.
Upgrading database.
Load data from SVI_VC_CONFIG_ENTRY table.
Update SVI_DEPLOYMENT_GROUP table.
Update SVI_REPLICA table.
Update SVI_SIM_CLONE table.
SviConfig finished successfully.
Database is upgraded successfully.
```

5 次のコマンドを入力して View Composer を開始します。

net start svid

アップグレード プロセスの完全なログが作成され、C:\Users\All Users\VMware\View Composer\vmware-sviconfig.log に保存されます。

次のステップ

データベースのアップグレードが失敗する場合は [View Composer データベース アップグレードの失敗のトラブルシューティング](#) を参照してください。

結果コードが成功を意味する 0 以外の任意の数字の場合は [手動データベース スキーマ更新の結果コード](#) を参照してください。

手動データベース スキーマ更新の結果コード

View Composer データベースを手動でアップグレードすると、sviconfig databaseupgrade コマンドで結果コードが表示されます。

表 3-1. databaseupgrade コマンドの結果コード に sviconfig databaseupgrade の結果コードを示します。

表 3-1. databaseupgrade コマンドの結果コード

| コード | 説明 |
|-----|------------------------|
| 0 | 操作は正常に終了しました。 |
| 1 | 指定された DSN が見つかりませんでした。 |

| コード | 説明 |
|-----|---|
| 2 | 無効なデータベース管理者認証情報が指定されました。 |
| 3 | データベースのドライバがサポートされていません。 |
| 4 | 予期しない問題が発生し、コマンドは完了できませんでした。 |
| 14 | 別のアプリケーションが View Composer サービスを使用しています。コマンドを実行する前にサービスをシャットダウンしてください。 |
| 15 | 復元処理の間に問題が発生しました。詳細については、画面のログ出力を参照してください。 |
| 17 | データベースのデータをアップグレードできません。 |
| 18 | データベース サーバに接続できません。 |

View Composer データベース アップグレードの失敗のトラブルシューティング

View Composer インストーラを使用して、または SviConfig databaseupgrade コマンドを実行して View Composer サービスをアップグレードするときに、View Composer データベースのアップグレード操作が失敗する場合があります。

問題

SviConfig databaseupgrade の操作でエラー コード 17 が表示される、または View Composer インストーラで次の警告メッセージが表示される。

Database upgrade completed with warnings(データベースのアップグレードが警告で終了しました)

原因

データベース アップグレード ソフトウェアは、vCenter Server に接続して、デスクトップについての追加データを取得します。デスクトップが使用できない場合、ESXi ホストが実行されていない場合、または vCenter Server が使用できない場合は、データベースのアップグレードが失敗することがあります。

解決方法

- 1 詳細については、View Composer の SviConfig ログ ファイルを参照してください。

このファイルのデフォルトの場所は C:\Users\All Users\VMware\View Composer\vmware-sviconfig.log です。アップグレード スクリプトは、失敗ごとにメッセージをログに記録します。

- 2 ログの記録を調べて、アップグレードに失敗したデスクトップを特定します。

| オプション | 操作 |
|---------------------|--|
| デスクトップは存在するが使用できない。 | <p>デスクトップを再度使用できるようにします。</p> <p>失敗の原因に応じて、ESXi ホストまたは vCenter Server の再起動、あるいはその他のアクションが必要になる場合があります。</p> |
| デスクトップが存在しない。 | <p>ログ メッセージを無視します。</p> <p>注: 管理者が vSphere でデスクトップ仮想マシンを直接削除した場合、削除したデスクトップが View Administrator では存在するように表示される場合があります。</p> |

3 SviConfig databaseupgrade コマンドを再び実行します。

別のマシンへの View Composer の移行

場合によっては、VMware Horizon View Composer サービスを新しい Windows Server の仮想マシンまたは物理マシンに移行しなければならないことがあります。たとえば、View 展開環境を拡張するために、View Composer と vCenter Server を新しい ESXi ホストまたはクラスタに移行する必要があるかもしれません。さらに、View Composer および vCenter Server を、同じ Windows Server のマシンにインストールする必要はありません。

View Composer を vCenter Server マシンからスタンドアロンマシンに、またはスタンドアロンマシンから vCenter Server マシンに移行できます。

重要: これらのトピックは、最新バージョンの View Composer の別のマシンへの移行に関連しています。これらのタスクを実施する前に、以前のバージョンの View Composer をアップグレードする必要があります。

View Composer の現在のバージョンが最新バージョンのシステム要件を満たさないマシンにインストールされていると、これらの手順は使用できません。View Composer を、このリリースでサポートされる Windows Server オペレーティングシステムがあるシステムに移行した後は、最新バージョンの View Composer へのインプレースアップグレードを実行できます。

■ View Composer 移行に関するガイドライン

VMware Horizon View Composer サービスの移行で行う手順は、既存のリンク クローン仮想マシンを保持するかどうかによって異なります。

■ 既存のデータベースを含む View Composer を移行する

View Composer を別の物理マシンまたは仮想マシンに移行する際に、現在のリンク クローン仮想マシンを保持する場合、新しい VMware Horizon View Composer サービスは引き続き既存の View Composer データベースを使用する必要があります。

■ リンク クローン仮想マシンがない View Composer の移行

現在の VMware Horizon View Composer サービスがリンク クローン仮想マシンを管理していない場合は、RSA 鍵を新しいマシンに移行しなくても、View Composer を新しい物理マシンまたは仮想マシンに移行できます。移行した VMware Horizon View Composer サービスは、元の View Composer データベースに接続できます。または View Composer 用の新しいデータベースを作成できます。

■ RSA 鍵の移行のための Microsoft .NET Framework の準備

既存の View Composer データベースを使用するには、マシン間で RSA 鍵コンテナを移行する必要があります。RSA 鍵コンテナを移行するには、Microsoft .NET Framework と一緒に提供される ASP .NET IIS 登録ツールを使用します。

■ 新しい View Composer サービスへの RSA 鍵コンテナの移行

既存の View Composer データベースを使用するには、既存の VMware Horizon View Composer サービスが存在する移行元の物理マシンまたは仮想マシンから、新しい VMware Horizon View Composer サービスをインストールするマシンに、RSA 鍵コンテナを移行する必要があります。

View Composer 移行に関するガイドライン

VMware Horizon View Composer サービスの移行で行う手順は、既存のリンク クローン仮想マシンを保持するかどうかにによって異なります。

現在の展開でリンク クローン仮想マシンを保持するには、新しい仮想マシンまたは物理マシンにインストールする VMware Horizon View Composer サービスが、既存の View Composer データベースを継続して使用する必要があります。View Composer データベースは、リンク クローンの作成、プロビジョニング、メンテナンス、および削除に必要なデータを含んでいます。

VMware Horizon View Composer サービスを移行するときに、View Composer データベースも新しいマシンに移行できます。

View Composer データベースを移行するかどうかにかかわらず、データベースは VMware Horizon View Composer サービスをインストールする新しいマシンと同じドメインまたは信頼されたドメインの使用可能なマシンに構成する必要があります。

View Composer は RSA 鍵ペアを使用して、View Composer データベースに格納されている認証情報を暗号化および暗号化解除します。このデータ ソースと新しい VMware Horizon View Composer サービスの互換性を確保するには、元の VMware Horizon View Composer サービスで作成した RSA 鍵コンテナを移行する必要があります。RSA 鍵コンテナは、新しいサービスをインストールするマシンにインポートする必要があります。

現在の VMware Horizon View Composer サービスが任意のリンク クローン仮想マシンを管理していない場合、既存の View Composer データベースを使用せずにサービスを移行できます。RSA 鍵は、既存のデータベースを使用するかどうにかかわらず、移行する必要はありません。

注: VMware Horizon View Composer サービスのインスタンスごとに、専用の View Composer データベースが必要です。複数の VMware Horizon View Composer サービスで 1 つの View Composer データベースを共有することはできません。

既存のデータベースを含む View Composer を移行する

View Composer を別の物理マシンまたは仮想マシンに移行する際に、現在のリンク クローン仮想マシンを保持する場合、新しい VMware Horizon View Composer サービスは引き続き既存の View Composer データベースを使用する必要があります。

次のいずれかの方向で View Composer を移行する場合は、この手順に従います。

- vCenter Server マシンからスタンドアロン マシンへ
- スタンドアロン マシンから vCenter Server マシンへ
- スタンドアロン マシンから別のスタンドアロン マシンへ
- vCenter Server マシンから別の vCenter Server マシンへ

VMware Horizon View Composer サービスを移行するときに、View Composer データベースも新しい場所に移行できます。たとえば、現在のデータベースが、移行しようとしている vCenter Server マシン上に配置されている場合、View Composer データベースの移行が必要になることがあります。

VMware Horizon View Composer サービスを新しいマシンにインストールするときは、View Composer データベースに接続するようにサービスを構成する必要があります。

前提条件

- View Composer の移行要件について理解しておきます。[View Composer 移行に関するガイドライン](#)を参照してください。
- RSA 鍵コンテナを新しい VMware Horizon View Composer サービスに移行する手順について理解しておきます。[RSA 鍵の移行のための Microsoft .NET Framework の準備](#)および [新しい View Composer サービスへの RSA 鍵コンテナの移行](#)を参照してください。
- VMware Horizon View Composer サービスのインストールについて理解しておきます。『View インストールガイド』の「View Composer のインストール」を参照してください。
- View Composer 用の SSL 証明書の構成について理解しておきます。『View インストール ガイド』の「View Server 用の SSL 証明書の構成」を参照してください。
- View Administrator での View Composer の構成について理解しておきます。『View 管理ガイド』の View Composer 設定および View Composer ドメインの構成に関するトピックを参照してください。

手順

- 1 VMware Horizon View Composer サービスに関連付けられている vCenter Server インスタンスで、仮想マシンのプロビジョニングを無効にします。
 - a View Administrator で、[View 構成] - [サーバ] を選択します。
 - b [vCenter Servers] タブで、vCenter Server インスタンスを選択し、[プロビジョニングを無効にする] をクリックします。
- 2 (オプション) View Composer データベースを新しい場所に移行します。
この手順を実行する必要がある場合は、移行の手順についてデータベース管理者に問い合わせてください。
- 3 現在のマシンから VMware Horizon View Composer サービスをアンインストールします。
- 4 (オプション) RSA 鍵コンテナを新しいマシンに移行します。
- 5 VMware Horizon View Composer サービスを新しいマシンにインストールします。
インストール中、元の VMware Horizon View Composer サービスで使用されていたデータベースの DSN を指定します。また、そのデータベースに対して、ODBC データ ソース用に提供されたドメイン管理者のユーザー名とパスワードを指定します。

データベースを移行した場合、DSN とデータ ソース情報はデータベースの新しい場所をポイントしている必要があります。データベースを移行したかどうかに関わらず、新しい VMware Horizon View Composer サービスは、リンク クローンに関する元のデータベース情報にアクセスする必要があります。
- 6 新しいマシンで View Composer 用の SSL サーバ証明書を構成します。

元のマシンにインストールした View Composer 用の証明書をコピーするか、新しい証明書をインストールすることができます。

7 View Administrator で、新しい View Composer 設定を構成します。

- a View Administrator で、[View 構成] - [サーバ]を選択します。
- b [vCenter Servers] タブで、View Composer サービスに関連付けられている vCenter Server インスタンスを選択し、[編集] をクリックします。
- c [View Composer Server 設定] ペインで [編集] をクリックして、新しい View Composer 設定を指定します。

新しいマシンに View Composer を vCenter Server と一緒にインストールする場合は、[View Composer を vCenter Server と一緒にインストール] を選択します。

スタンドアロン マシンに View Composer をインストールする場合は、[スタンドアロン View Composer Server] を選択し、View Composer マシンの FQDN と View Composer ユーザーのユーザー名およびパスワードを指定します。

- d 必要に応じて、[ドメイン] ペインで [サーバ情報を検証] をクリックし、View Composer ドメインを追加または編集します。
- e [OK] をクリックします。

リンク クローン仮想マシンがない View Composer の移行

現在の VMware Horizon View Composer サービスがリンク クローン仮想マシンを管理していない場合は、RSA 鍵を新しいマシンに移行しなくても、View Composer を新しい物理マシンまたは仮想マシンに移行できます。移行した VMware Horizon View Composer サービスは、元の View Composer データベースに接続できます。または View Composer 用の新しいデータベースを作成できます。

前提条件

- VMware Horizon View Composer サービスのインストールについて理解しておきます。『View インストールガイド』の「View Composer のインストール」を参照してください。
- View Composer 用の SSL 証明書の構成について理解しておきます。『View インストール ガイド』の「View Server 用の SSL 証明書の構成」を参照してください。
- View Administrator から View Composer を削除する手順について理解しておきます。『View 管理ガイド』の View Administrator からの View Composer の削除に関するトピックを参照してください。

View Composer を削除する前に、View Composer が今後リンク クローン仮想マシンを管理しないことを確認します。リンク クローンが残っている場合は、削除する必要があります。

- View Administrator での View Composer の構成について理解しておきます。『View 管理ガイド』の View Composer 設定および View Composer ドメインの構成に関するトピックを参照してください。

手順

1 View Administrator で、View Composer を View Administrator から削除します。

- a [View 構成] - [サーバ] を選択します。
- b [vCenter Servers] タブで、View Composer サービスに関連付けられている vCenter Server インスタンスを選択し、[編集] をクリックします。

- c [View Composer Server 設定] ペインで、[編集] をクリックします。
 - d [View Composer を使用しない] を選択して、[OK] をクリックします。
- 2 現在のマシンから VMware Horizon View Composer サービスをアンインストールします。
 - 3 VMware Horizon View Composer サービスを新しいマシンにインストールします。
インストール時、元の View Composer データベースまたは新しい View Composer データベースの DSN に接続するように View Composer を構成します。
 - 4 新しいマシンで View Composer 用の SSL サーバ証明書を構成します。
元のマシンにインストールした View Composer 用の証明書をコピーするか、新しい証明書をインストールすることができます。
 - 5 View Administrator で、新しい View Composer 設定を構成します。
 - a View Administrator で、[View 構成] - [サーバ] を選択します。
 - b [vCenter Servers] タブで、View Composer サービスに関連付けられている vCenter Server インスタンスを選択し、[編集] をクリックします。
 - c [View Composer Server 設定] ペインで、[編集] をクリックします。
 - d 新しい View Composer 設定を指定します。

新しいマシンに View Composer を vCenter Server と一緒にインストールする場合は、[View Composer を vCenter Server と一緒にインストール] を選択します。

スタンドアロン マシンに View Composer をインストールする場合は、[スタンドアロン View Composer Server] を選択し、View Composer マシンの FQDN と View Composer ユーザーのユーザー名およびパスワードを指定します。
 - e 必要に応じて、[ドメイン] ペインで [サーバ情報を検証] をクリックし、View Composer ドメインを追加または編集します。
 - f [OK] をクリックします。

RSA 鍵の移行のための Microsoft .NET Framework の準備

既存の View Composer データベースを使用するには、マシン間で RSA 鍵コンテナを移行する必要があります。RSA 鍵コンテナを移行するには、Microsoft .NET Framework と一緒に提供される ASP .NET IIS 登録ツールを使用します。

前提条件

.NET Framework をダウンロードし、ASP.NET IIS 登録ツールについての情報を読みます。<http://www.microsoft.com/net> をご覧ください。

手順

- 1 既存のデータベースに関連付けられた VMware Horizon View Composer サービスがインストールされている物理マシンまたは仮想マシンに .NET Framework をインストールします。

- 2 新しい VMware Horizon View Composer サービスのインストール先マシンに .NET Framework をインストールします。

次のステップ

RSA 鍵コンテナをインストール先マシンに移行します。[新しい View Composer サービスへの RSA 鍵コンテナの移行](#)を参照してください。

新しい View Composer サービスへの RSA 鍵コンテナの移行

既存の View Composer データベースを使用するには、既存の VMware Horizon View Composer サービスが存在する移行元の物理マシンまたは仮想マシンから、新しい VMware Horizon View Composer サービスをインストールするマシンに、RSA 鍵コンテナを移行する必要があります。

新しい VMware Horizon View Composer サービスをインストールする前に、この手順を実行する必要があります。

前提条件

Microsoft .NET Framework および ASP.NET IIS 登録ツールが移行元と移行先のマシンにインストールされていることを確認します。[RSA 鍵の移行のための Microsoft .NET Framework の準備](#)を参照してください。

手順

- 1 既存の VMware Horizon View Composer サービスが存在する移行元マシンで、コマンド プロンプトを開き、%windir%\Microsoft.NET\Framework\v2.0xxxxx ディレクトリに移動します。

- 2 `aspnet_regiis` コマンドを入力して、RSA キー ペアをローカル ファイルに保存します。

```
aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri
```

ASP.NET IIS 登録ツールは RSA 公開/プライベート キーペアを SviKeyContainer コンテナから keys.xml ファイルにエクスポートし、ファイルをローカルに保存します。

- 3 keys.xml ファイルを新しい VMware Horizon View Composer サービスのインストール先マシンにコピーします。
- 4 移行先マシンで、コマンド プロンプトを開き、%windir%\Microsoft.NET\Framework\v2.0xxxxx ディレクトリに移動します。

- 5 `aspnet_regiis` コマンドを入力して、RSA 鍵ペア データを移行します。

```
aspnet_regiis -pi "SviKeyContainer" "path\keys.xml" -exp
```

`path` はエクスポートしたファイルへのパスです。

`-exp` オプションは、エクスポート可能な鍵ペアを作成します。将来的に移行が必要な場合、鍵をこのマシンからエクスポートして別のマシンにインポートできます。以前に `-exp` オプションを使用せずに鍵をこのマシンに移行した場合、将来鍵をエクスポートできるように、`-exp` オプションを使用して再び鍵をインポートできます。

登録ツールは、鍵ペア データをローカルの鍵コンテナにインポートします。

次のステップ

新しい VMware Horizon View Composer サービスを移行先マシンにインストールします。DSN および ODBC データ ソース情報を入力します。これにより、View Composer は元の VMware Horizon View Composer サービスによって使用されていたのと同じデータベース情報に接続できます。インストール手順については、『View のインストール』の「View Composer のインストール」を参照してください。

View Composer を新しいマシンに移行して同じデータベースを使用するための手順を完了します。[既存のデータベースを含む View Composer を移行する](#)を参照してください。

Horizon 接続サーバのアップグレード

展開環境の際にロード バランサを使用して複数の接続サーバ インスタンスを管理する場合は、接続サーバ インフラストラクチャのアップグレードをゼロ ダウンタイムで実行できます。

注: Horizon 6 バージョン 6.2 の機能を使用してデスクトップ プールのクローンを作成する前に、ポッド内のすべての接続サーバ インスタンスを Horizon 6 バージョン 6.2 以降にアップグレードする必要があります。

フレッシュ インストールを実行するか、すべての接続サーバを Horizon 7 バージョン 7.2 にアップグレードした後は、LDAP データの保護に使用されるキーが変更されたため、Horizon 7 バージョン 7.2 より前のバージョンに接続サーバ インスタンスをダウングレードすることはできません。

Horizon 7 バージョン 7.2 へのアップグレードを計画するときに、接続サーバ インスタンスをダウングレードする可能性がある場合には、アップグレードの開始前に接続サーバ インスタンスをバックアップする必要があります。接続サーバ インスタンスをダウングレードする必要がある場合には、すべての接続サーバ インスタンスをダウングレードし、最後にダウングレードした接続サーバにバックアップを適用する必要があります。

アップグレードのための接続サーバの準備

接続サーバをアップグレードする場合、または接続サーバが依存する vSphere コンポーネントのいずれかをアップグレードする場合は、正常にアップグレードできるよう事前にいくつかの作業を実行する必要があります。

レプリカ グループ内の 1 つのインスタンスにのみ実行するタスク

接続サーバ インスタンスのアップグレードを開始する前に、いずれか 1 つのインスタンスについてのみ次のタスクを実行します。インスタンスは複製されるため、1 つのインスタンスの設定はその他のインスタンスの設定と同じです。

- 接続サーバが仮想マシンにインストールされている場合は、その仮想マシンのスナップショットを作成します。
スナップショットの作成手順については、vSphere Client のオンライン ヘルプを参照してください。このスナップショットに戻す必要があり、レプリカ グループ内に他にも接続サーバ インスタンスがある場合は、マスターをスナップショットに戻す前に、これらのインスタンスをアンインストールする必要があります。戻した後で、レプリカ インスタンスを再インストールして、その戻したインスタンスを参照します。

このスナップショットに「アップグレード準備作業」などのラベルを付けます。
- Horizon Administrator を開き、すべてのグローバル設定およびデスクトップとプールの設定を記録します（[インベントリ] ツリーの [プール] セクションと [デスクトップ] セクション、および [View 構成] ツリーの [グローバル設定] セクション）。

たとえば、該当する設定のスクリーン ショットを撮ります。

- 展開環境で現在ローカル モード機能を使用している場合は、エンド ユーザーにローカル モード デスクトップにチェックインするように求めるか、または Horizon Administrator を使用してローカル モード デスクトップをロールバックすることによって、どのデスクトップもチェックアウト状態として Horizon Administrator に表示されないようにします。

重要: 接続サーバ インストーラを実行してアップグレードをインストールするときにローカル モードのデスクトップがチェックアウトされると、アップグレードは失敗します。

- 展開環境で現在ローカル モード機能を使用している場合は、Horizon Administrator を開き、[View 構成] - [サーバ] の順に移動し、すべての転送サーバ インスタンスを削除します。
- vdmexport.exe ユーティリティを使用して、LDAP データベースをバックアップします。

手順については、現在使用しているバージョンの『View 管理』ドキュメントを参照してください。

アップグレード直前に各インスタンスに対して実行するタスク

- 現在の接続サーバ インスタンスがインストールされている仮想マシンまたは物理マシンが、新しいバージョンのシステム要件を満たしていることを確認します。

[Horizon 接続サーバの要件](#)を参照してください。

- 接続サーバがインストールされているマシンの IP アドレスおよびシステム名を記録します。
- 接続サーバ上の View データベースに対して実行されるバッチ ファイルまたはスクリプトが社内で作成されているかどうかを確認し、作成されている場合はその名前と場所を記録します。
- Horizon Administrator を開き、このインスタンス固有のすべての設定を記録します。

たとえば、[View 構成] - [サーバ] - [接続サーバ] に移動し、テーブルから接続サーバ インスタンスを選択して [編集] をクリックします。[接続サーバ設定の編集] ダイアログ ボックスの各タブのスクリーン ショットを撮ります。

レプリカ グループ内の接続サーバのアップグレード

この手順では、セキュリティ サーバとペアになっていない接続サーバ インスタンスのアップグレードについて説明します。たとえば、会社のファイアウォール内のクライアントへの接続用として構成された接続サーバに対して、この手順が適用されます。

セキュリティ サーバとペアになっている接続サーバ インスタンスについては、[View セキュリティ サーバとペアになっている View 接続サーバのアップグレード](#)で説明する手順を参照してください。

注: この手順では、インプレース アップグレードについて説明します。異なるマシンに移行するには、[別のマシンでの最新バージョンの接続サーバへのアップグレード](#)を参照してください。

前提条件

- この手順をいつ実行すべきかを判断します。利用可能なデスクトップメンテナンス期間を選択します。このアップグレードにかかる時間は、グループ内の接続サーバ インスタンスの数によって決まります。1 インスタンスにつき 15 ～ 30 分を予定してください。

- View Composer を使用する場合、View Composer がアップグレードされていることを確認してください。[View Composer のアップグレード](#)を参照してください。接続サーバをアップグレード後は、Horizon Administrator を使用して View Composer を追加する必要があります。
- Horizon 7 のセキュリティ関連の要件について理解し、これらの要件を満たしていることを確認します。[View 接続サーバのアップグレード要件](#)を参照してください。証明書の失効情報を含む CA 署名付き SSL サーバ証明書を取得およびインストールし、[セキュリティが強化された Windows ファイアウォール] を [オン] に設定し、IPsec をサポートするようにバックエンドのファイアウォールを構成する必要がある場合があります。
- vCenter Server がインストールされ、ているサーバに CA（証明機関）署名付き SSL サーバ証明書がインストールされ、構成されていることを確認します。接続サーバをアップグレードした後に、認証局 (CA) 署名付き証明書を vCenter Server が使用しないと、デフォルトの自己署名証明書が Horizon Administrator で無効として表示され、vCenter Server が利用できないというメッセージが表示されます。
- [アップグレードのための接続サーバの準備](#)に一覧表示されているタスクを実行します。

重要: 接続サーバ インストーラを実行してアップグレードをインストールするときにローカル モードのデスクトップがチェックアウトされると、アップグレードは失敗します。

- 新しいバージョンに有効なライセンスがあることを確認します。

注: バージョン 6.0.x または 6.1.x から 6.2 にアップグレードする場合は、以前のライセンスが引き続き機能し、使用モデルが[同時ユーザー]に設定されます。Horizon 6 バージョン 6.2 から、Named User と呼ばれる新しいライセンス モデルが追加されました。オプションとして、ライセンス モデルを [Named User] に変更できます。詳細については、<http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf> を参照してください。

- インストールとアップグレードを実行する際に使用するホスト上に、管理権限を持つドメイン ユーザー アカウントがあることを確認します。
- vdmexport.exe ユーティリティについて詳しくない場合は、『View 管理』ドキュメントの使用手順を印刷してください。このユーティリティは、アップグレード手順の一環として View LDAP データベースをバックアップするために使用します。

既存のロード バランサの構成を変更する必要はありません。

手順

- 1 ロード バランサを使用して接続サーバ インスタンスのグループを管理する場合、アップグレードする接続サーバ インスタンスをホストするサーバを無効にします。
- 2 Horizon Administrator にログインし、アップグレードする接続サーバ インスタンスを無効にします。
 - a [View 構成] - [サーバ] に移動し、[接続サーバ] タブをクリックします。
 - b リストで接続サーバ インスタンスを選択し、表の上にある [無効化] ボタンをクリックします。
 - c [OK] をクリックしてサーバの無効化を確定します。

- 3 接続サーバ インスタンスのホストで、接続サーバの新しいバージョンのインストーラをダウンロードして実行します。

インストーラのファイル名は、VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe です。xxxxxx は、ビルド番号であり、y.y.y はバージョン番号です。アップグレードを実行する前にサービスを停止する必要はありません。インストーラは必要に応じてサービスの停止と再起動を行います。実際、View LDAP データベースをアップグレードするために VMwareVDMDS サービスは実行されている必要があります。

旧バージョンがすでにインストールされているかどうかはインストーラによって判別され、アップグレードが実行されます。新規インストールの場合は、インストーラに表示されるインストール オプションの数が少なくなります。

View LDAP もアップグレードされます。

注: アップグレードの前に、インストーラは、複製ステータス チェックを実行して、サーバが複製されたグループ内の他のサーバと通信できるかどうかと、サーバがグループ内の他のサーバから LDAP アップデートを取得できるかどうかを判断します。ステータス チェックが失敗すると、アップグレードは続行されません。

- 4 インストーラ ウィザードが閉じた後、VMware Horizon 接続サーバ サービスが再起動したことを確認します。
- 5 Horizon Administrator にログインし、アップグレードした接続サーバ インスタンスを有効にします。
 - a [View 構成] - [サーバ] に移動し、[接続サーバ] タブをクリックします。
 - b リストで接続サーバ インスタンスを選択し、表の上にある [有効化] ボタンをクリックします。
 - c [バージョン] 列に新しいバージョンが表示されていることを確認します。
- 6 [View 構成] - [製品のライセンスと使用状況] に移動し、[ライセンスを編集] をクリックして、ライセンス キーを入力し、[OK] をクリックします。
- 7 ロード バランサを使用してこの接続サーバ インスタンスを管理する場合、アップグレードしたサーバを有効にします。
- 8 リモート デスクトップにログインできることを確認します。
- 9 前の手順を繰り返して、グループ内の各接続サーバ インスタンスをアップグレードします。

重要: レプリカ グループにあるすべての接続サーバ インスタンスをアップグレードしないと、Horizon Administrator のダッシュボードの健全性インジケータで、1 つまたは複数のインスタンスのステータスがエラーになる場合があります。バージョンが異なると提供されるデータの種類も異なるために、この状況が発生します。この問題を解決するには、レプリカ グループにあるすべてのインスタンスをアップグレードします。

- 10 vdmexport.exe ユーティリティを使用して、新しくアップグレードされた View LDAP データベースをバックアップします。

レプリカ グループ内に接続サーバ インスタンスが複数存在する場合は、1 つのインスタンスからデータをエクスポートするだけでかまいません。

- 11 Horizon Administrator にログインし、ダッシュボードを調べて、vCenter Server と View Composer アイコンが緑になっていることを確認します。

これらのアイコンのいずれかが赤になっており、[無効な証明書が検出されました]ダイアログ ボックスが表示される場合、[検証]をクリックして、「次の手順」で説明されているように信頼されていない証明書の指紋を受け入れるか、CA によって署名された有効な SSL 証明書をインストールします。

vCenter Server のデフォルト証明書の置換の詳細については、『VMware vSphere Examples and Scenarios』ドキュメントを参照してください。

- 12 接続サーバインスタンスのダッシュボード アイコンも緑であることを確認します。

いずれかのインスタンスのアイコンが赤の場合は、インスタンスをクリックして、複製ステータスを確認します。次のいずれかの理由で、複製が失敗することがあります。

- ファイアウォールによって通信がブロックされている
- 接続サーバ インスタンスで VMware VDMDS サービスが停止している可能性がある。
- VMware VDMDS DSA オプションによって複製がブロックされている
- ネットワークの問題が発生している

次のステップ

vCenter Server または View Composer のデフォルト、つまり自己署名証明書を使用するには、[デフォルトの SSL 証明書のサムプリントを受け入れる](#)を参照してください。

古いバージョンの vCenter Server がある場合、[接続サーバから vCenter 接続で TLSv1.0 を有効にする](#)を参照してください。

1 つ以上の接続サーバ インスタンスでアップグレードが失敗する場合は、[接続サーバをスナップショットに戻した後のレプリカ グループの作成](#)を参照してください。

重要: JMS メッセージに拡張されたメッセージセキュリティ モードを使用する場合、ファイアウォールにより接続サーバ インスタンスが、デスクトップおよびセキュリティ サーバから 4002 ポートに入ってくる JMS トラフィックを受信できるようになっているか確認します。また、ポート 4101 を開いて他の接続サーバ インスタンスからの通信を受け入れます。

パフォーマンス データを監視するようにデータ コレクタ セットが構成されているサーバに接続サーバを再インストールしてある場合は、データ コレクタ セットを停止して再起動してください。

接続サーバから vCenter 接続で TLSv1.0 を有効にする

Horizon 7 以降のコンポーネントでは、TLSv1.0 セキュリティ プロトコルがデフォルトで無効になっています。TLSv1.0 のみをサポートする古いバージョンの vCenter Server が展開環境に含まれている場合、接続サーバ 7.0 以降のリリースのインストールまたはアップグレード後に、接続サーバへの接続に対して TLSv1.0 を有効にすることが必要な可能性があります。

vCenter Server 5.1 および 5.5 の一部の旧メンテナンス リリースは、Horizon 7 以降のリリースではデフォルトで無効になっている TLSv1.0 のみをサポートします。vCenter Server を TLSv1.1 または TLSv1.2 をサポートするバージョンにアップグレードできない場合は、接続サーバへの接続に対して TLSv1.0 を有効にできます。

前提条件

- Horizon 7 にアップグレードする場合は、アップグレード前にこの手順を実行して、サービスの再起動回数を最小限に抑えます。VMware Horizon View 接続サーバのアップグレード中にサービスが再起動され、この手順で説明されている構成の変更を適用するときに再起動が必要になります。この手順を実行する前にアップグレードを行うと、サービスをもう一度再起動する必要があります。
- お使いのバージョンの Windows オペレーティング システムでの ADSI Edit ユーティリティの使用方法については、Microsoft TechNet Web サイトを参照してください。

手順

- 1 接続サーバ ホスト上で ADSI Edit ユーティリティを起動します。
- 2 コンソール ツリーで、[接続] を選択します。
- 3 [識別名または命名規則を選択または入力] テキスト ボックスに、識別名「**DC=vdi, DC=vmware, DC=int**」を入力します。
- 4 [コンピュータ] ペインで、**localhost:389** を選択または入力するか、接続サーバ ホストの完全修飾ドメイン名 (FQDN) を入力し、続いてポート 389 を入力します。

例：**localhost:389** または **mycomputer.example.com:389**

- 5 [ADSI Edit] ツリーを展開し、[OU=Properties] を展開して [OU=Global] を選択し、右ペインで [CN=Common] をダブルクリックします。
- 6 [プロパティ] ダイアログ ボックスで、[pae-ClientSSLSecureProtocols] 属性を編集して次の値を追加します。

\LIST:TLSv1.2,TLSv1.1,TLSv1

必ず行の先頭にバック スラッシュを含めてください。

- 7 [OK] をクリックします。
- 8 新規インストールの場合に構成の変更を適用するには、各接続サーバ インスタンスで VMware Horizon View 接続サーバ サービスを再起動します。

アップグレードを実行する場合は、アップグレードのプロセスによって自動的にサービスが再起動されるため、サービスを再起動する必要はありません。

別のマシンでの最新バージョンの接続サーバへのアップグレード

アップグレードの一部として、接続サーバを新しいマシンに移行できます。

前提条件

- 少なくとも 1 つの既存の接続サーバ インスタンスを最新バージョンにアップグレードします。[レプリカ グループ内の接続サーバのアップグレード](#)を参照してください。このアップグレードの間に、既存の View LDAP がアップグレードされます。
- 新しい物理マシンまたは仮想マシンが接続サーバのインストールに対するシステム要件を満たしていることを確認します。「[Horizon 接続サーバでサポートされるオペレーティング システムおよび Horizon 接続サーバのハードウェア要件](#)」を参照してください。

- Horizon 7 のセキュリティ関連の要件について理解し、これらの要件を満たしていることを確認します。[View 接続サーバのアップグレード要件](#)を参照してください。
- この手順をいつ実行すべきかを判断します。利用可能なデスクトップメンテナンス期間を選択します。1 インスタンスにつき 15 ～ 30 分を予定してください。
- インストーラの実行に使用するホスト上に管理者権限のあるドメイン ユーザー アカウントがあることを確認します。
- レプリカ インスタンスをインストールするための手順をよく理解してください。『View のインストール』ドキュメントを参照してください。この手順の一部としてレプリカ インスタンスをインストールします。

既存のロード バランサの構成を変更する必要はありません。

手順

- 1 接続サーバのアップグレードされたインスタンスが実行されていて、接続サーバをインストールする予定の新しいマシンにアクセスできることを確認します。

新しいホストに接続サーバをインストールするときは、この既存のインスタンスを指定します。
- 2 新しいマシンで、接続サーバのレプリカ インスタンスをインストールします。

新しいインスタンスの View LDAP は、アップグレードされたソース インスタンスのものを複製します。
- 3 必要に応じて、Windows の [プログラムの追加と削除] ユーティリティを使用して、古いホストから接続サーバをアンインストールします。
- 4 Horizon Administrator で、[View 構成] - [サーバ] - [接続サーバ] タブに移動し、アンインストールした接続サーバインスタンスがまだリストに表示されるかどうかを調べます。
- 5 アンインストールした接続サーバ インスタンスがまだリストに表示される場合は、`vdadmin` コマンドを使用して削除します。

```
vdadmin.exe -S -s server_name -r
```

この例で、`server_name` は接続サーバ ホストのホスト名または IP アドレスです。`vdadmin` コマンドラインツールの詳細については、『View 管理』ドキュメントを参照してください。

接続サーバの新しいインスタンスがグループに追加されて、古いインスタンスが削除されます。

次のステップ

古いバージョンの vCenter Server がある場合、[接続サーバから vCenter 接続で TLSv1.0 を有効にする](#)を参照してください。

残りの Horizon 7 サーバ コンポーネントをアップグレードします。

パフォーマンス データを監視するようにデータ コレクタ セットが構成されているサーバに接続サーバを再インストールしてある場合は、データ コレクタ セットを停止して再起動してください。

接続サーバをスナップショットに戻した後のレプリカ グループの作成

アップグレードが失敗した場合、または他の理由で接続サーバをホストする仮想マシンをスナップショットに戻す必要がある場合は、グループ内の他の接続サーバ インスタンスをアンインストールして、レプリカ グループを再作成する必要があります。

1 台の接続サーバ仮想マシンをスナップショットに戻した場合、その仮想マシンのデータベースの View LDAP オブジェクトは、他のレプリカ インスタンスのデータベースの View LDAP オブジェクトと一致しなくなっています。スナップショットに戻した後、次のイベントが Windows イベント ログ、VMwareVDMDS イベント ログ（イベント ID 2103）に記録されます。Active Directory ライトウェイト ディレクトリ サービス データベースは、サポートされていない復元方法を使って復元されました。戻された仮想マシンは View LDAP の複製を停止します。

スナップショットに戻す必要がある場合は、他の接続サーバ インスタンスをアンインストールし、これらの仮想マシンの View LDAP をアンインストールした後、レプリカ インスタンスを再インストールする必要があります。

前提条件

どの接続サーバ インスタンスを新しい標準つまりマスターの接続サーバにするかを決定します。この接続サーバに必要な Horizon 7 構成データが含まれます。

手順

- 1 新しい標準の接続サーバ インスタンスとして選択したもの以外のすべての接続サーバ インスタンスで、接続サーバおよび View LDAP インスタンスをアンインストールします。

View LDAP インスタンスは、AD LDS Instance VMwareVDMDS と呼ばれます。

- 2 標準つまりマスターの接続サーバ インスタンスをホストする仮想マシンでコマンド プロンプトを開き、次のコマンドを入力して、複製が無効になっていないことを確認します。

```
repadmin /options localhost:389 -DISABLE_OUTBOUND_REPL -DISABLE_INBOUND_REPL
```

- 3 レプリカの接続サーバ インスタンスをホストする仮想マシンで、接続サーバ インストーラを実行し、[View レプリカ サーバ] インストール オプションを選択して、標準の接続サーバ インスタンスのホスト名または IP アドレスを指定します。

接続サーバ インスタンスのレプリカ グループが再作成され、その View LDAP オブジェクトが一致するようになります。

セキュリティ サーバのアップグレード

複数のセキュリティ サーバの管理にロード バランサを使用している場合は、ダウンタイムを設けずに接続サーバのインフラストラクチャのアップグレードを行うことができます。

注: セキュリティ サーバの代わりに Unified Access Gateway アプライアンスを使用するには、接続サーバ インスタンスを Horizon 6 バージョン 6.2 以降にアップグレードしてから、Unified Access Gateway アプライアンスをインストールして接続サーバ インスタンス、またはインスタンスの前に配置しているロード バランサを参照するように設定する必要があります。詳細については、『Unified Access Gateway の導入および設定』を参照してください。

アップグレードのための View セキュリティ サーバの準備

セキュリティ サーバをアップグレードする前に、次のタスクを実行してバックアップを作成し、構成設定を記録します。

- 現在のセキュリティ サーバがインストールされている仮想マシンまたは物理マシンが新しいバージョンのシステム要件を満たしていることを確認します。

[Horizon 接続サーバの要件](#)を参照してください。

- セキュリティ サーバが仮想マシンにインストールされている場合は、その仮想マシンのスナップショットを作成します。

スナップショットの作成手順については、vSphere Client のオンライン ヘルプを参照してください。このスナップショットに「アップグレード準備作業」などのラベルを付けます。

- View Administrator を開き、このセキュリティ サーバの設定を記録します。[View 構成] - [サーバ] に移動し、[セキュリティ サーバ] タブをクリックします。

たとえば、セキュリティ サーバを選択して [編集] をクリックし、設定のスクリーンショットを撮ります。

- セキュリティ サーバがインストールされているマシンの IP アドレスおよびシステム名を記録します。
- セキュリティ サーバにロード バランサを使用する場合は、ロード バランサの構成設定を記録します。

注: このトピックでは、View Administrator の [セキュリティ サーバ] タブから使用できる [アップグレードまたは再インストールの準備] コマンドについては説明していません。このコマンドはセキュリティ サーバから IPsec ルールを削除し、これによってセキュリティ サーバとペアになっている View 接続サーバ インスタンスの間のすべての通信を停止します。このため、アップグレードの手順では、セキュリティ サーバをアップグレードする直前にこのコマンドを使用します。この操作については、[View セキュリティ サーバとペアになっている View 接続サーバのアップグレード](#)を参照してください。

View セキュリティ サーバとペアになっている View 接続サーバのアップグレード

アップグレードする予定の View 接続サーバ インスタンスがセキュリティ サーバとペアになっている場合は、この手順を使用します。

この手順では、セキュリティ サーバと View 接続サーバ インスタンスのペア 1 つをアップグレードした上で、次のセキュリティ サーバと View 接続サーバ インスタンスのペアのアップグレードに進みます。この方法によって、ゼロダウンタイムが実現されます。インスタンスがセキュリティ サーバとペアになっていない場合は、[レプリカ グループ内の接続サーバのアップグレード](#)の手順を使用します。

この手順では、まず View 接続サーバ インスタンスをアップグレードします。View 接続サーバをアップグレードした後は、セキュリティ サーバの IPsec ルールを削除してから、セキュリティ サーバをアップグレードします。アクティブなセキュリティ サーバに対して IPsec ルールを削除すると、セキュリティ サーバのすべての通信は、セキュリティ サーバのアップグレードまたは再インストールまで失われます。

デフォルトでは、セキュリティ サーバとそのペアの View 接続サーバ インスタンス間の通信は IPsec ルールによって制御されています。アップグレードまたは再インストールの前に IPsec ルールが削除されない場合、セキュリティ サーバと View 接続サーバの間のペアリングが失敗し、アップグレード後に新しい IPsec ルールのセットを確立できません。

前提条件

- この手順をいつ実行すべきかを判断します。利用可能なデスクトップメンテナンス期間を選択します。各セキュリティ サーバとそのペアの View 接続サーバ インスタンスにつき 15 ～ 30 分を予定してください。
- View Composer を使用する場合、View Composer がアップグレードされていることを確認してください。以下を参照してください。 [View Composer のアップグレード](#)。View 接続サーバをアップグレード後は、View Administrator を使用して View Composer を追加する必要があります。
- View のセキュリティ関連の要件について理解し、これらの要件を満たしていることを確認します。 [View 接続サーバのアップグレード要件](#) を参照してください。証明書の失効情報を含む CA 署名付き SSL サーバ証明書を取得およびインストールし、[セキュリティが強化された Windows ファイアウォール] を [オン] に設定し、IPsec をサポートするようにバックエンドのファイアウォールを構成する必要がある場合があります。
- 現在のセキュリティ サーバと View 接続サーバ インスタンスがインストールされている仮想マシンまたは物理マシンがシステム要件を満たしていることを確認します。

[Horizon 接続サーバの要件](#) を参照してください。

- [アップグレードのための接続サーバの準備](#) に一覧表示されているタスクを実行します。

重要: View 接続サーバ インストーラを実行してアップグレードをインストールするときにローカル モードのデスクトップがチェックアウトされると、アップグレードは失敗します。

- 新しいバージョンのライセンスがあることを確認します。
- インストーラとアップグレードを実行する際に使用するホストに対して管理権限のあるユーザー アカウントを持っていることを確認します。
- セキュリティ サーバのペアリング パスワードを構成していない場合は、最新バージョンの View Administrator を使用して構成します。インストール時にインストール プログラムでこのパスワードを入力するように求められます。『View のインストール』ドキュメントにあるトピック「セキュリティ サーバのペアリング パスワードの構成」を参照してください。

手順

- 1 ロード バランサを使用して接続サーバ インスタンスとペアになっているセキュリティ サーバを管理する場合、アップグレードする接続サーバ インスタンスとペアになっているセキュリティ サーバを無効にします。
- 2 このセキュリティ サーバとペアになっている View 接続サーバ インスタンスをアップグレードします。

[レプリカ グループ内の接続サーバのアップグレード](#) の手順 2 ～ 6 に従って操作します。

- 3 アップグレードした View 接続サーバ インスタンスとペアになっているセキュリティ サーバの IPsec ルールを削除します。

- a View Administrator で、[View 構成] - [サーバ] をクリックします。
- b [セキュリティ サーバ] タブで、セキュリティ サーバを選択し、[その他のコマンド] - [アップグレードまたは再インストールの準備] をクリックします。

セキュリティ サーバをインストールする前に IPsec ルールを無効にした場合は、この設定は無効です。この場合、再インストールまたはアップグレード前に IPsec ルールを削除する必要はありません。

- c [OK] をクリックします。

IPsec ルールが削除され、[アップグレードまたは再インストールを準備] 設定が無効になります。つまりセキュリティ サーバを再インストールまたはアップグレードできます。

- 4 セキュリティ サーバのホストで、View 接続サーバの最新バージョンのインストーラをダウンロードして実行します。

インストーラのファイル名は、VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe です。xxxxxx は、ビルド番号であり、y.y.y はバージョン番号です。旧バージョンがすでにインストールされているかどうかによって判別され、アップグレードが実行されます。新規インストールの場合は、インストーラに表示されるインストール オプションの数が少なくなります。

セキュリティ サーバのペアリング パスワードを入力するように求められます。

セキュリティ サーバ サービスが停止したことを通知するメッセージ ボックスを消去するように求められる場合があります。インストーラはアップグレードの準備のためにサービスを停止します。

- 5 インストーラ ウィザードの終了後に、VMware Horizon View セキュリティ サーバ サービスが開始されていることを確認します。
- 6 このセキュリティ サーバの管理にロード バランサを使用している場合は、このサーバを負荷分散グループに戻します。
- 7 View Administrator にログインして、ダッシュボードでセキュリティ サーバを選択し、セキュリティ サーバが最新バージョンになっていることを確認します。
- 8 リモート デスクトップにログインできることを確認します。
- 9 View Administrator で [View 構成] - [サーバ] - [セキュリティ サーバ] タブに移動します。

自動化されたセキュリティ サーバ ペアリング メカニズムでは、完全なシステム名が、セキュリティ サーバが最初に作成されたときに割り当てられた名前と一致しない場合、[セキュリティ サーバ] の一覧に重複したエントリが作成される場合があります。

- 10 vdmexport.exe ユーティリティを使用して、新しくアップグレードされた View LDAP データベースをバックアップします。

レプリカ グループ内に接続サーバ インスタンスが複数存在する場合は、1 つのインスタンスからデータをエクスポートするだけでかまいません。

- Horizon Administrator にログインし、ダッシュボードを調べて、vCenter Server と View Composer アイコンが緑になっていることを確認します。

これらのアイコンのいずれかが赤になっており、[無効な証明書が検出されました]ダイアログ ボックスが表示される場合、[検証]をクリックして、「次の手順」で説明されているように信頼されていない証明書の指紋を受け入れるか、CA によって署名された有効な SSL 証明書をインストールします。

vCenter Server のデフォルト証明書の置換の詳細については、『VMware vSphere Examples and Scenarios』ドキュメントを参照してください。

- 接続サーバ インスタンスのダッシュボード アイコンも緑であることを確認します。

いずれかのインスタンスのアイコンが赤の場合は、インスタンスをクリックして、複製ステータスを確認します。次のいずれかの理由で、複製が失敗することがあります。

- ファイアウォールによって通信がブロックされている
- 接続サーバ インスタンスで VMware VDMDS サービスが停止している可能性がある。
- VMware VDMDS DSA オプションによって複製がブロックされている
- ネットワークの問題が発生している

次のステップ

vCenter Server または View Composer のデフォルト、つまり自己署名証明書を使用するには、[デフォルトの SSL 証明書のサムプリントを受け入れる](#)を参照してください。

1 つ以上の View 接続サーバ インスタンスでアップグレードが失敗する場合は、[接続サーバをスナップショットに戻した後のレプリカ グループの作成](#)を参照してください。

重要: JMS メッセージに拡張されたメッセージセキュリティ モードを使用する場合、ファイアウォールにより接続サーバ インスタンスが、デスクトップおよびセキュリティ サーバから 4002 ポートに入ってくる JMS トラフィックを受信できるようになっているか確認します。また、ポート 4101 を開いて他の接続サーバ インスタンスからの通信を受け入れます。

パフォーマンス データを監視するようにデータ コレクタ セットが構成されているサーバに接続サーバを再インストールしてある場合は、データ コレクタ セットを停止して再起動してください。

Cloud Pod アーキテクチャ 環境のアップグレード

Cloud Pod アーキテクチャ 機能は、標準の Horizon 7 コンポーネントを使用してクロスデータセンター管理を提供しています。Cloud Pod アーキテクチャ 機能を使用することで、複数のポッドをまとめてリンクし、デスクトップとアプリケーションの仲介および管理のための単一の大規模環境を形成できます。ポッドは、複数の接続サーバ インスタンス、共有ストレージ、データベース サーバ、vSphere およびデスクトップやアプリケーション プールのホストに必要なネットワーク インフラストラクチャで構成されます。

次の手順で Cloud Pod アーキテクチャ 環境をアップグレードします。

- 1 接続サーバ インスタンスを 1 つずつアップグレードする通常の手順に従って、ポッド内のすべての接続サーバ インスタンスをアップグレードします。

2 ポッド フェデレーション内の他のポッドにも同じ手順を繰り返し、各ポッドを1つずつアップグレードします。

アップグレード中は、Horizon 7 の最新バージョンを使用する接続サーバ インスタンスと、以前のバージョンを使用する接続サーバ インスタンスが混在する状態になります。このような異なるバージョンが混在する環境は、Horizon 7 バージョン 7.4 でサポートされますが、新機能は動作しません。たとえば、アップグレード済みのサーバ上の Horizon Administrator では表示される新機能がアップグレードされていないサーバ上の Horizon Administrator では表示されません。

Cloud Pod アーキテクチャ 環境の設計とセットアップについては、『Horizon 7 での Cloud Pod アーキテクチャの管理』を参照してください。

View Server のアップグレードによる HTML Access の許可

ロード バランサの背後、または Access Point などのゲートウェイの背後に存在する View 接続サーバ インスタンスまたはセキュリティ サーバをアップグレードするときは、HTML Access を引き続き使用するように構成を変更する必要があります。

詳細については、『View のインストール』ドキュメントの「ロード バランサでの HTML Access の許可」および「ゲートウェイでの HTML Access の許可」を参照してください。

vCenter Server のアップグレード

vCenter Server のアップグレードは、その他の View Server コンポーネントをアップグレードするのと同じメンテナンス期間に実行します。vCenter Server をアップグレードする前に、View データを一部バックアップする必要があります。アップグレード後、View Composer が同じサーバ上で実行されている場合、View Composer サービスを再起動する必要があります。

注: vCenter Server のアップグレード中に、既存のリモート デスクトップとアプリケーションのセッションは切断されませんが、次の機能を使用できません。

- プロビジョニング状態のリモート デスクトップはパワーオンされません。
- 新しいデスクトップは起動されません。
- View Composer の操作は許可されません。

前提条件

- この手順をいつ実行すべきかを判断します。利用可能なデスクトップメンテナンス期間を選択します。所要時間については、『VMware vSphere アップグレード ガイド』を参照してください。
- vCenter Server データベースと View Composer データベースをバックアップします。
- `vdmexport.exe` ユーティリティを使用して、View 接続サーバ インスタンスから View LDAP データベースをバックアップします。

手順については、『View 管理者ガイド』を参照してください。レプリカ グループ内に View 接続サーバ インスタンスが複数存在する場合は、1 つのインスタンスからデータをエクスポートするだけでかまいません。

- [vSphere を含むアップグレードの準備](#)に一覧表示されている作業を実行します。

- vCenter Server がインストールされ、ているサーバに CA（証明機関）署名付き SSL サーバ証明書がインストールされ、構成されていることを確認します。View 接続サーバをアップグレードした後に、CA 署名付き証明書を vCenter Server が使用しないと、デフォルトの自己署名証明書が View Administrator で無効として表示され、vCenter Server が利用できないというメッセージが表示されます。
- アップグレード後の vSphere のバージョンに対応しているガイドのバージョンを参照して、『VMware vSphere アップグレード ガイド』に一覧表示されている前提条件を完全に満たします。

手順

- 1 『vCenter Server アップグレード ガイド VMware vSphere』に説明されているとおりに、をアップグレードします。

重要: クラスタに、Virtual SAN データストアが含まれる場合は、『VMware Virtual SAN の管理』ドキュメントの Virtual SAN クラスタのアップグレードに関する章も参照してください。この章には vCenter Server のアップグレードについてのトピックが含まれています。

- 2 View Composer が同じホストにインストールされている場合、View Composer サービスを再起動します。
- 3 View Administrator にログインし、ダッシュボードを調べて、vCenter Server と View Composer アイコンが緑になっていることを確認します。

これらのアイコンのいずれかが赤になっており、[無効な証明書が検出されました]ダイアログ ボックスが表示される場合、[検証]をクリックして、「次の手順」で説明されているように信頼されていない証明書の指紋を受け入れるか、CA によって署名された有効な SSL 証明書をインストールします。

vCenter Server のデフォルト証明書の置換の詳細については、『VMware vSphere Examples and Scenarios』ドキュメントを参照してください。

次のステップ

vCenter Server または View Composer のデフォルト、つまり自己署名証明書を使用するには、[デフォルトの SSL 証明書のサンプリントを受け入れる](#)を参照してください。

View Server コンポーネントのアップグレードが終了している場合は、次のメンテナンス期間に、View のアップグレードを続行します。

- vSphere コンポーネントもアップグレードしている場合は、[4 章 ESXi ホストおよび仮想マシンのアップグレード](#)を参照してください。
- View コンポーネントのみをアップグレードする場合は、[View Agent または Horizon Agent のアップグレード](#)を参照してください。

デフォルトの SSL 証明書のサンプリントを受け入れる

vCenter Server および View Composer インスタンスを Horizon 7 に追加する場合、vCenter Server および View Composer インスタンス用に使用される SSL 証明書が有効で、接続サーバによって信頼されていることを確認する必要があります。vCenter Server および View Composer でインストールされるデフォルトの証明書が存在する場合、これらの証明書のサンプリントを受け入れるかどうかを決定する必要があります。

vCenter Server または View Composer インスタンスが CA によって署名された証明書で構成され、ルート証明書が接続サーバによって信頼される場合、この証明書のサムプリントを受け入れる必要はありません。操作は何も必要ありません。

デフォルト証明書を CA によって署名された証明書に置換するにもかかわらず接続サーバがルート証明書を信頼していない場合、証明書のサムプリントを受け入れるかどうかを決定する必要があります。サムプリントとは、証明書の暗号化ハッシュです。サムプリントは、提示された証明書が以前に受け入れられた証明書など、別の証明書と同じものであるかどうかを素早く判別するために使用されます。

注: 同じ Windows Server ホストに vCenter Server と View Composer をインストールする場合、同じ SSL 証明書を使用できますが、各コンポーネントで証明書を個別に構成する必要があります。

SSL 証明書の構成の詳細については、『View のインストール』ドキュメントの「View Server の SSL 証明書の構成」を参照してください。

まず、Horizon Administrator で vCenter Server の追加ウィザードを使用して、vCenter Server と View Composer を追加します。証明書が信頼されておらず、サムプリントを受け入れなければ、vCenter Server および View Composer を追加できません。

これらのサーバが追加されたら、[vCenter Server の編集] ダイアログ ボックスで再構成できます。

注: 旧リリースからアップグレードする場合、そして vCenter Server または View Composer 証明書が信頼されていない場合、または信頼されている証明書を信頼されていない証明書と置き換える場合は、証明書のサムプリントを受け入れる必要もあります。

Horizon Administrator ダッシュボードで、vCenter Server または View Composer のアイコンが赤に変わり、[無効な証明書が検出されました] ダイアログ ボックスが表示されます。[検証] をクリックして、表示される手順に従う必要があります。

同様に Horizon Administrator では、接続サーバ インスタンスごとに使用する SAML 認証システムを構成できます。SAML サーバの証明書が接続サーバによって信頼されていない場合、証明書のサムプリントを受け入れるかどうかを決定する必要があります。サムプリントを受け入れなければ、Horizon 7 で SAML 認証システムを構成できません。SAML 認証システムが構成されると、[View 接続サーバの編集] ダイアログ ボックスで再構成できます。

手順

- 1 Horizon Administrator で [無効な証明書が検出されました] ダイアログ ボックスが表示されたら、[証明書を表示] をクリックします。
- 2 [証明書情報] ウィンドウで証明書のサムプリントを調べます。
- 3 vCenter Server または View Composer インスタンス用に構成された証明書のサムプリントを調べます。
 - a vCenter Server または View Composer ホストで、MMC スナップインを開始し、Windows 証明書ストアを開きます。
 - b vCenter Server または View Composer の証明書に移動します。
 - c [証明書の詳細] タブをクリックして証明書のサムプリントを表示します。

同様に、SAML 認証システムの証明書のサムプリントを調べます。必要に応じて、SAML 認証システム ホストで上記の手順を行います。

- 4 [証明書情報] ウィンドウのサムプリント (two occurrences)が vCenter Server または View Composer インスタンスのサムプリント (two occurrences)と一致することを確認します。

同様に、SAML 認証システムについてもサムプリントが一致するかどうかを調べます。

- 5 証明書のサムプリントを受け入れるかどうかを決定します。

| オプション | 説明 |
|------------------|--|
| サムプリントが一致しています。 | [許可] をクリックしてデフォルト証明書を使用します。 |
| サムプリントが一致していません。 | [拒否] をクリックします。 一致しない証明書のトラブルシューティングを行います。たとえば、vCenter Server または View Composer で正しくない IP アドレスを指定した可能性があります。 |

Horizon 7 グループ ポリシー管理用テンプレート ファイルの使用

Horizon 7 には、コンポーネント固有のグループ ポリシー管理用 ADMX テンプレート ファイルがいくつか含まれています。ADMX テンプレート ファイル内のポリシー設定を Active Directory 内の新しい GPO または既存の GPO に追加することによって、リモート デスクトップとアプリケーションを最適化し、セキュリティ保護することができます。

Horizon 7 のグループ ポリシー設定を提供する ADMX ファイルはすべて、VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip という .zip バンドル ファイル内にあります。x.x.xはバージョン、yyyyyyはビルド番号です。このファイルは、<https://my.vmware.com/web/vmware/downloads> の VMware ダウンロード サイトからダウンロードできます。[Desktop & End-User Computing (デスクトップおよびエンドユーザー コンピューティング)] で VMware Horizon 7 のダウンロードを選択します。これには .zip バンドル ファイルが含まれます。

グループ ポリシーをアップグレードするには、Active Directory サーバのグループ ポリシー オブジェクト エディタを使用して、新しいバージョンのテンプレート ファイルを追加します。

Horizon 7 ADMX テンプレート ファイルには、コンピュータの設定とユーザーの設定の両方のグループ ポリシーが含まれます。

- コンピュータの構成ポリシーは、だれがデスクトップに接続するかにはかかわらず、すべてのリモート デスクトップに適用されるポリシーを設定します。
- ユーザーの構成ポリシーは、ユーザーが接続するリモート デスクトップやアプリケーションにはかかわらず、すべてのユーザーに適用されるポリシーを構成します。ユーザーの構成ポリシーは、対応するコンピュータの構成ポリシーより優先されます。

Microsoft Windows は、デスクトップの起動時とユーザーのログイン時にポリシーを適用します。

ESXi ホストおよび仮想マシンのアップグレード

ESXi ホストおよび仮想マシンをアップグレードする作業は、View アップグレードのこの中盤で最も時間のかかる部分です。

以下の手順では、2 番目およびそれ以降のメンテナンス期間の間に実行が必要な作業の概要について説明します。一部の作業の実行には、『VMware vSphere アップグレード ガイド』および『View 管理ガイド』に記載されている手順が必要になる場合があります。

vCenter Server および ESXi のバージョンと互換性があるバージョンについての詳細は、http://www.vmware.com/resources/compatibility/sim/interop_matrix.php の VMware 製品の互換性一覧を参照してください。

重要: 次の表では、特定の仮想マシン ハードウェアに依存するため、仮想マシンのアップグレードが必要になる場合がある View 機能について説明します。

表 4-1. 特定の機能に必要な仮想マシン ハードウェア バージョン

| 機能 | 仮想ハードウェア バージョン | 対応する vSphere バージョン |
|---|----------------|-------------------------|
| リンク クローン プールのスペース効率的なディスク形式 | 9 以降 | vSphere 5.1 以降 |
| VMware [®] Virtual SAN [™] データストア、第 1 バージョン | 10 以降 | vSphere 5.5 Update 1 以降 |
| VMware Virtual SAN データストア、第 2 バージョン | 11 以降 | vSphere 6.0 以降 |
| VMware Virtual Volumes データストア | 11 以降 | vSphere 6.0 以降 |
| ネイティブ NFS スナップショット テクノロジ (VAAI) | 9 以降 | vSphere 5.1 以降 |
| Virtual Shared Graphics Acceleration | 8 以降 | vSphere 5.0 以降 |
| Virtual Dedicated Graphics Acceleration | 9 以降 | vSphere 5.1 以降 |
| NVIDIA GRID vGPU Graphics Acceleration | 11 以降 | vSphere 6.0 以降 |

前提条件

- [レプリカ グループ内の接続サーバのアップグレード](#)に説明されている手順を実行します。
- 『ESXi アップグレード ガイド VMware vSphere』に記載されている のアップグレード準備作業を実行します。

手順

1 ESXi ホストを 1 クラスタずつアップグレードします。

手順については、『VMware vSphere アップグレード ガイド』を参照してください。クラスタに、Virtual SAN データストアが含まれる場合は、『VMware Virtual SAN の管理』ドキュメントの Virtual SAN クラスタのアップグレードに関する章も参照してください。この章には、ESXi ホストのアップグレードに関するトピックが含まれます。

クラスタが多数ある場合は、この手順を完了するために複数のメンテナンス期間が必要となることがあります。ESXi ホストのアップグレードでは、次の作業を実行する場合があります。

- a VMware vSphere[®] vMotion[®] を使用して、仮想マシンを ESXi ホストの外に移動します。
- b ホストをメンテナンスモードにします。
- c アップグレードを実行します。
- d vMotion を使用して、仮想マシンをホスト上に戻します。
- e ESXi ホストのアップグレード後の作業を実行します。

前提条件で示したように、すべてのホストはクラスタのメンバーである必要があります。

- 2 アップグレードしたホストが自動的に vCenter Server に再接続されない場合は、vSphere Client を使用してホストを vCenter Server に再接続します。
- 3 View Composer を使用する場合は、すべての ESXi ホストをアップグレードした後、vCenter Server ホストで View Composer サービスを再起動します。
- 4 (オプション) すべての親仮想マシン上の VMware Tools[™] および仮想マシンと、仮想マシン テンプレート、および View 接続サーバインスタンスなどの View Server コンポーネントをホストしている仮想マシンをアップグレードします。

- a 『VMware vSphere アップグレード ガイド』の説明に従って、ダウンタイムの計画を立てます。
- b VMware Tools を更新し、リモート デスクトップのソースとして使用される仮想マシンの仮想マシン ハードウェアをアップグレードします。

VMware vSphere[®] Update Manager[™] を使用しない場合の詳しい手順については、『VMware vSphere 仮想マシン管理』ドキュメントの仮想マシンのアップグレードに関する章を参照してください。

VMware vSphere Update Manager を使用すると、特定のフォルダ内にあるすべての仮想マシンで、VMware Tools の次に仮想ハードウェア バージョンという正しい順序で更新できます。『VMware vSphere アップグレード ガイド』を参照してください。

- 5 (オプション) 各仮想マシンで完全クローン デスクトップを使用する場合は、VMware Tools とリモート デスクトップのソースとして使用される仮想マシンの仮想ハードウェアをアップグレードします。

VMware vSphere[®] Update Manager[™] を使用しない場合の詳しい手順については、『VMware vSphere 仮想マシン管理』ドキュメントの仮想マシンのアップグレードに関する章を参照してください。

vSphere Update Manager を使用すると、特定のフォルダ内にあるすべての仮想マシンで、VMware Tools の次に仮想マシンのハードウェア バージョンという正しい順序でアップデートを実行できます。『VMware vSphere アップグレード ガイド』を参照してください。

次のステップ

エージェント ソフトウェアをアップグレードします。[View Agent](#) または [Horizon Agent](#) のアップグレードを参照してください。

リモート デスクトップおよび Horizon Client のアップグレード

5

アップグレードできるリモート デスクトップおよびクライアント コンポーネントとして、リモート デスクトップと Microsoft RDS ホストのオペレーティング システム内で実行しているサポート対象のデスクトップおよびモバイル クライアント プラットフォームの Horizon Client、VMware パートナーから提供されるシン クライアント、および Horizon Agent があります。

重要: この章には、Linux 仮想マシンでの Horizon Agent のアップグレードに関する情報は含まれません。この情報については、Horizon 7 for Linux デスクトップのセットアップ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。

- リモート デスクトップのアップグレードのためのセキュリティ関連の要件
- セッション ベースのデスクトップを提供する RDS ホストのアップグレード
- View Agent または Horizon Agent のアップグレード
- View Composer デスクトップ プールのアップグレード
- クライアント アプリケーションのアップグレード

リモート デスクトップのアップグレードのためのセキュリティ関連 の要件

View コンポーネントでは、RC4、SSLv3、および TLSv1.0 はデフォルトで無効になっています。リモート デスクトップで RC4、SSLv3、または TLSv1.0 を再び有効にする必要がある場合は、『View セキュリティ』ドキュメントの「View で無効化された古いプロトコルと暗号化方式」を参照してください。

View Agent、Horizon Agent、および Horizon Client のセキュリティ機能の詳細については、『Horizon Client および Agent のセキュリティ』ドキュメントを参照してください。

セッション ベースのデスクトップを提供する RDS ホストのアップ グレード

Windows Server 2008 R2 以上のオペレーティング システムを搭載した RDS ホストの場合、View Agent または Horizon Agent ソフトウェアをアップグレードして、RDS ホストでリモート デスクトップと Windows ベースのリモート アプリケーションを提供できるようにプール設定を編集できます。

VMware Horizon 6.0 以降のリリースを使用すると、Microsoft RDS ホストを使用してリモート デスクトップに加えてリモート アプリケーションを提供できます。この追加の機能によって、以前非表示にされたサーバ ファーム名が Horizon Administrator で表示されます。

前提条件

- レプリカ グループにある 1 つ以上の Horizon 接続サーバ インスタンスがアップグレードされていることを確認します。安全な JMS ペアリング メカニズムが Horizon Agent で動作するように、接続サーバを最初にアップグレードする必要があります。
- 現在リモート デスクトップをホストしている RDS ホストが Windows Server 2008 R2、Windows Server 2012 または Windows Server 2012 R2 で実行されていることを確認します。Windows Server 2008 (ターミナル サービス) は View の以前のバージョンではサポート対象のオペレーティング システムでしたが、このリリースではサポートされません。サポートされた Windows Server オペレーティング システムがない場合、アップグレードではなく新規インストールを実行する必要があります。サポートされているオペレーティング システムの一覧については、[Horizon Agent でサポートされるオペレーティング システム](#) を参照してください。
- RDS ホスト ロールがオペレーティング システムにインストールされていることを確認します。『Horizon 7 での公開されたデスクトップとアプリケーションのセットアップ』ドキュメントで「Windows Server 2008 R2 へのリモート デスクトップ サービスのインストール」の手順を参照してください。
- Horizon Agent インストーラを実行する手順を理解しておいてください。『Horizon 7 での公開されたデスクトップとアプリケーションのセットアップ』（Horizon Administrator で [ヘルプ] ボタンをクリックして表示）の「リモート デスクトップ サービス ホストへの Horizon Agent のインストール」の手順を参照してください。
- すべてのリモート デスクトップとリモート アプリケーションからログアウトしていることを確認します。
- インストールとアップグレードを実行する際に使用するホスト上に、管理権限を持つドメイン ユーザー アカウントがあることを確認します。

手順

- 1 Horizon Administrator で、デスクトップ プール設定を編集してプールを無効にします。
[カタログ] - [デスクトップ プール] からプールを選択して、[編集] をクリックします。
- 2 RDS ホストで、新しいバージョンの Horizon Agent のインストーラをダウンロードして実行します。
インストーラは VMware の Web サイトからダウンロードできます。
- 3 Horizon Administrator で、ファーム設定を編集して [PCoIP] または [VMware Blast] をデフォルトの表示プロトコルに設定します。
[リソース] - [ファーム] からファームを選択して、[編集] をクリックします。
エンド ユーザーがプロトコルを選択できるようにする設定を使用することもできます。リモート アプリケーションを使用するには、プロトコルは PCoIP または VMware Blast である必要があります。リモート アプリケーションは RDP ではサポートされません。
- 4 Horizon Administrator で、デスクトップ プール設定を編集してプールを有効にします。

このホストはリモート デスクトップに加えてリモート アプリケーションも提供できるようになりました。Horizon Administrator で、[カタログ] - [デスクトップ プール] に移動すると、プールのタイプが [RDS デスクトップ プール]

と表示されています。[リソース]-[ファーム]に移動すると、プール ID に対応するファーム ID がリストに表示されています。

次のステップ

クライアントをアップグレードします。[クライアント アプリケーションのアップグレード](#)を参照してください。

View Agent または Horizon Agent のアップグレード

エージェント ソフトウェアのアップグレード方法は、デスクトップ ソースの種類によって決まります。

注: 仮想マシン デスクトップ内のオペレーティング システムを Windows 8 から Windows 8.1 にアップグレードするには、Horizon Agent をアンインストールし、オペレーティング システムを Windows 8 から Windows 8.1 にアップグレードし、次に Horizon Agent を再インストールします。代わりに、Windows 8.1 を新規インストールしてから Horizon Agent をインストールできます。

ここでは、デスクトップ ソースとして使用される仮想マシンでエージェント ソフトウェアからアップグレードするために実行が必要な作業の概要について説明します。一部の作業の実行には、vSphere Client のオンライン ヘルプ または『Horizon 7 での仮想デスクトップのセットアップ』（Horizon Administrator で [ヘルプ] ボタンをクリックして表示）に記載されている手順が必要になる場合があります。ターミナル サービス ホストまたは Microsoft RDS ホスト上のエージェント ソフトウェアをアップグレードする場合は、[セッション ベースのデスクトップを提供する RDS ホストのアップグレード](#)を参照してください。Linux 仮想マシン上のエージェント ソフトウェアをアップグレードするには、別途『Horizon 7 for Linux デスクトップのセットアップ』ドキュメントを参照してください。

インスタント クローンの展開を予定している場合は、この手順を使用して、インスタントクローン デスクトップ プールの親仮想マシンを作成できます。親仮想マシンで Horizon Agent をアップグレードするときは、インスタントクローン デスクトップ プールに適切なオプションを選択するだけです。

重要: Horizon Agent インストーラには、現在、Remote Experience Agent (VMware Horizon™View™ Feature Pack の一部だったもの) に以前含まれていたコンポーネントがすべて含まれています。Remote Experience Agent でインストールされた機能をアップグレードするには、Horizon Agent インストーラを実行してください。このインストーラを実行すると、Remote Experience Agent が削除され、次にアップグレードが行われます。何らかの理由で Remote Experience Agent を手動で削除する場合は、Horizon Agent の新バージョンのインストーラを実行する前に削除してください。

前提条件

- レプリカ グループにある少なくとも 1 つの View 接続サーバ インスタンスがアップグレードされていることを確認します。安全な JMS ペアリング メカニズムが Horizon Agent で動作するように、View 接続サーバを最初にアップグレードする必要があります。
- ESXi ホストおよび仮想マシンをアップグレードする場合は、[4 章 ESXi ホストおよび仮想マシンのアップグレード](#)に説明されている手順を実行します。
- インストールとアップグレードを実行する際に使用するホスト上に、管理権限を持つドメイン ユーザー アカウントがあることを確認します。

手順

- 1 インスタント クローンまたは View Composer のリンク クローンを展開する予定の場合は、親仮想マシンでエージェント ソフトウェアをアップグレードし、テスト用デスクトップ プールを作成します。

- a 親仮想マシンで Horizon Agent のインストーラの新しいバージョンをダウンロードして実行します。

インストーラは VMware の Web サイトからダウンロードできます。

- b この仮想マシンから、小さなデスクトップ プールを作成します。
- c 作成したデスクトップ プールから仮想マシン デスクトップをテストして、あらゆる使用方法のシナリオが正常に機能することを確認します。

たとえば、1 つの仮想マシン デスクトップを含むデスクトップ プールを作成し、Horizon Client を使用してそのデスクトップにログインできることを確認します。

Horizon Agent インストーラを実行してデスクトップ プールを作成する手順については、『Horizon 7 での仮想デスクトップのセットアップ』（Horizon Administrator の [ヘルプ] ボタンをクリックして表示）を参照してください。

重要: View 5.1.x 以前からアップグレードする場合に、Sysprep を使用していて、エンド ユーザーが USB デバイスをリモート デスクトップに接続する場合は、<http://kb.vmware.com/kb/2051801> の VMware ナレッジベースに記載の手順に従う必要があります。この手順に従わない場合、エージェント ソフトウェアをアップグレードした後に USB リダイレクト機能が動作しないことがあります。

- 2 別の親仮想マシンおよび仮想マシン テンプレート上で、Horizon Agent の新しいバージョンのインストーラをダウンロードして実行します。

Horizon Agent インストーラを実行してデスクトップ プールを作成する手順については、『Horizon 7 での仮想デスクトップのセットアップ』（Horizon Administrator の [ヘルプ] ボタンをクリックして表示）を参照してください。

- 3 インスタントクローンまたは View Composer のリンククローン デスクトップ プールの作成を予定している場合は、アップグレードされる各親仮想マシンのスナップショットを作成します。

新しいスナップショットを使用して、インスタントクローンまたはリンククローン デスクトップ プールを作成するか、または既存のリンククローン デスクトップ プールを再構成します。

スナップショットの作成手順については、vSphere Client のオンライン ヘルプを参照してください。

- 4 完全クローン デスクトップを使用する場合、あるいは個別のデスクトップまたは手動プールの一部として追加した他の仮想マシンを使用する場合は、ソフトウェアのアップグレードに通常使用している任意の他社製ツールを使用して、エージェント ソフトウェアをアップグレードしてください。

- 5 インスタントクローンまたはリンククローン プールではない自動または手動の Windows 7 および 8 プールの場合、3D レンダリング機能をオンにするには、プールを編集し、仮想マシン デスクトップのパワーオフとパワーオンを実行します。

- a 次のプール設定を構成します。

- プールが PCoIP 表示プロトコルまたは VMware Blast 表示プロトコルを使用するように設定します。
- [ユーザーがプロトコルを選択できるようにする] を [いいえ] に設定します。
- [3D Rendering (3D レンダリング)] 機能をオンにします。

- b 各仮想マシンをパワーオフしてから再度パワーオンします。

仮想マシンのパワーオフとパワーオンを実行する代わりに再起動した場合、この設定は有効になりません。

- 6 Microsoft RDS ホストとして物理 PC または仮想マシンを使用し、リモート デスクトップまたはアプリケーションを提供する場合、これらマシン上で Horizon Agent の新しいバージョンのインストーラをダウンロードして実行します。

インストーラは VMware の Web サイトからダウンロードできます。

重要: 仮想マシンの RDS ホストでインストーラを実行するときは、[View Composer Agent] コンポーネントの選択が解除されています。アップグレード中は、このコンポーネントを選択しないでください。このコンポーネントを使用して自動ファーム (Horizon 6 バージョン 6.2 で導入された機能) を作成する場合は、以前のバージョンのエージェント ソフトウェアをアンインストールしてから、[View Composer Agent] コンポーネントを選択した状態で新しいバージョンをインストールします。

- 7 物理 PC をデスクトップソースとして使用する場合は、これらの物理マシンに Horizon Agent の新しいバージョンのインストーラをダウンロードして実行します。

インストーラは VMware の Web サイトからダウンロードできます。

- 8 アップグレードされていない Horizon Client を使用して、アップグレード済みのリモート デスクトップソースに旧クライアント ソフトウェアでログインできることを確認します。

次のステップ

View Composer デスクトップ プールを使用している場合は、プールを再構成または再作成します。[View Composer デスクトップ プールのアップグレード](#)を参照してください。

クライアントをアップグレードします。[クライアント アプリケーションのアップグレード](#)を参照してください。

View Composer デスクトップ プールのアップグレード

View のアップグレードの最終段階には、その一環として View Composer デスクトップ プールのアップグレードが含まれます。

View Composer で作成されたプールをアップグレードする場合は、親仮想マシンで Horizon Agent をアップグレードした後で取得したスナップショットを使用する必要があります。

重要: View Composer のリンク クローンを使用して vSphere 5.1 以降の仮想マシンで利用できる領域再利用機能を使用する場合、この手順の実行に加えて、View LDAP および View Administrator で特定の設定を行う必要があります。作業の完全なリストについては、[領域を再利用するためにデスクトップ プールをアップグレードする作業](#)を参照してください。

注: 仮想ハードウェア バージョン 8 以降へのアップグレードなど、vSphere 5 以降に含まれる仮想ハードウェア バージョンもアップグレードしている場合、アップグレードされた親仮想マシンのスナップショットが、リンク クローン プールにある残りの仮想マシンの仮想ハードウェア バージョンのアップグレードに使用されます。

この方法によるアップグレードでは、上位のバージョンへの仮想ハードウェア バージョン（または互換性のあるレベル）のアップグレードがサポートされます。しかし、現在のバージョンよりも低いハードウェア バージョンにリンク クローンを再構成することはできません。たとえば、ハードウェア バージョン 7 の親仮想マシンにハードウェア バージョン 8 のクローンを再構成することはできません。

前提条件

- [View Composer のアップグレード](#)に説明されている手順を実行します。
- [レプリカ グループ内の接続サーバのアップグレード](#)に説明されている手順を実行します。
- ESXi ホストおよび仮想マシンをアップグレードする場合は、[4 章 ESXi ホストおよび仮想マシンのアップグレード](#)に説明されている手順を実行します。

さまざまな新機能に必要な vSphere バージョンの詳細については、「[表 4-1. 特定の機能に必要な仮想マシン ハードウェア バージョン](#)」を参照してください。

- 親仮想マシンのエージェントをアップグレードする場合は、[View Agent または Horizon Agent のアップグレード](#)に説明されている手順を実行します。

重要: View 5.1.x 以前からアップグレードする場合に、Sysprep を使用していて、エンド ユーザーが USB デバイスをリモート デスクトップに接続する場合は、<http://kb.vmware.com/kb/2051801> の VMware ナレッジベースに記載の手順に従う必要があります。この手順に従わない場合、エージェント ソフトウェアをアップグレードした後に USB リダイレクト機能が動作しないことがあります。

- デスクトップ プールの再作成および再構成によってストレージ アレイおよび ESXi ホストに負担がかからないように、メンテナンス期間を慎重に計画してください。

手順

- 1 アップグレードの準備作業で新規仮想マシンのプロビジョニングを無効にした場合は、再度プロビジョニングを有効にします。
- 2 3D レンダリング機能をオンにするには、プールを編集し、次の設定を構成します。
 - プールが PCoIP 表示プロトコルまたは VMware Blast 表示プロトコルを使用するように設定します。
 - [ユーザーがプロトコルを選択できるようにする] を [いいえ] に設定します。
 - [3D レンダリング] 機能をオンにします。

- 3 vSphere 5.1 仮想マシンで利用できる領域再利用機能を有効化するには、プール設定の [詳細なストレージ] セクションで [仮想マシンディスク領域を再利用] を選択し、領域再利用のしきい値を 1GB に設定します。
- 4 vSphere 5.0 以降の仮想マシンで利用できる View Storage Accelerator を有効にするには、プール設定の [詳細なストレージ] セクションで [View Storage Accelerator を使用] チェックボックスがオンになっていることを確認します。

View Storage Accelerator は、一般的な仮想マシンのディスク データをキャッシュすることを ESXi のホストに許可することによって、ブート ストームやウイルス対策スキャンの I/O ストーム中にパフォーマンスを改善できます。

重要: この機能は、デフォルトでオンになっています。View Storage Accelerator では、ESXi ホストごとに 1GB の RAM が必要です。

- 5 親仮想マシンのアップグレード後に作成したスナップショットを使用して、デスクトップ プールを再構築します。
- 6 アップグレードの準備作業でプールの [ログオフ時に OS ディスクを更新] 設定を [なし] に変更した場合は、適切な更新ポリシーに合わせて設定を元に戻します。
- 7 いずれかのデスクトップ プールについて更新または再構成の操作をキャンセルした場合は、再度作業をスケジュールします。

次のステップ

クライアントをアップグレードします。[クライアント アプリケーションのアップグレード](#)を参照してください。

使用するセットアップに適用する「[6 章 View セットアップで新機能を有効にするためのアップグレード後タスク](#)」に一覧されているタスクを実行します。

クライアント アプリケーションのアップグレード

View のアップグレードの最終段階では、最新バージョンの Horizon Client にアップグレードするとともに、シンクライアント デバイスを使用する場合にはそれらのデバイスのファームウェアをアップグレードします。

Horizon Client のローカル モード機能は削除されました。代わりに、VMware Horizon 7 に含まれている Mirage を使用することをお勧めします。詳細については、https://www.vmware.com/support/pubs/view_pubs.html で入手可能な View リリース ノートを参照してください。

重要: アップグレードでは、まず、クライアント アプリケーションの旧バージョンを削除せずに Horizon Client インストーラの新しいバージョンを実行します。エンド ユーザーが Windows ベースの View Client 4.6.0 以前のバージョンを使用している場合、最新の Horizon Client インストーラをダウンロードして実行する前にそのクライアント ソフトウェアを削除するように指示してください。

前提条件

- View 接続サーバや View Composer などのサーバ コンポーネントのアップグレード手順を完了します。[3 章 View Server コンポーネントのアップグレード](#)を参照してください。
- インストーラとアップグレードを実行する際に使用するホスト上に、管理権限を持つドメイン ユーザー アカウントがあることを確認します。

- クライアント デスクトップ、ラップトップ、タブレット、または電話が、Horizon Client のオペレーティング システム要件およびハードウェア要件を満たしていることを確認します。特定のタイプのデスクトップまたはモバイル クライアント デバイスについては、『Horizon Client の使用』を参照してください。https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html をご覧ください。

手順

- 1 最新バージョンの Horizon Client にアップグレードするようにエンド ユーザーに指示します。

| オプション | アクション |
|------------------------------|---|
| Horizon Client | <p>Horizon Client のインストーラをダウンロードしてエンド ユーザーに送信するか、Web サイトに掲示した後、インストーラをダウンロードして実行するようにエンド ユーザーに依頼します。https://www.vmware.com/go/viewclients の VMware Web サイトからインストーラをダウンロードできます。</p> <p>モバイル クライアントの場合は、その代わりに Apple App Store、Google Play、Amazon、および Windows ストアを含むアプリを販売する他の Web サイトから最新バージョンの Horizon Client を入手するようにエンド ユーザーに指示することもできます。</p> |
| VMware Horizon ユーザー Web ポータル | <p>エンド ユーザーは、ブラウザを開いて、View 接続サーバ インスタンスに移動できます。表示される Web ページは VMware Horizon ユーザー Web ポータルと呼ばれます。このページには、Horizon Client のインストーラ ファイルをダウンロードするためのリンクが含まれています。</p> <p>注: この Web ページのデフォルトのリンクでは、Horizon Client のダウンロード サイトが指定されています。デフォルトのリンクの指定先は自由に変更できます。エンド ユーザー用の VMware Horizon Web ポータル ページの構成を参照してください。</p> |
| シン クライアント | <p>エンド ユーザーのクライアント デバイスで、シン クライアントのファームウェアをアップグレードし、新しい Horizon Client ソフトウェアをインストールします。シン クライアントおよびゼロ クライアントは、VMware のパートナーから提供されます。</p> |

- 2 エンド ユーザーに各自のリモート デスクトップにログインおよび接続できることを確認してもらいます。

View セットアップで新機能を有効にするためのアップグレード後タスク

デスクトップおよびアプリケーション プール用のサーバ、仮想マシン、およびエージェント ソフトウェアのアップグレードが完了したら、セットアップを構成して特定の新機能を活用できるようになります。

この章のトピックに記載されているタスクに加えて、該当する場合は、View Administrator を使用してデスクトップ プール用のストレージの詳細オプションを編集したり、透過的なページ共有の範囲を変更したりすることができます。セキュリティ上の予防措置として、ESXi ホスト上の仮想マシン間でのメモリ共有はデフォルトで行えません。詳細については、『View 管理』ドキュメントの「既存のデスクトップ プールの設定の変更」というトピック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。

- JMS メッセージ セキュリティ モードを拡張済みに変更する
- 領域を再利用するためにデスクトップ プールをアップグレードする作業
- VMware Virtual SAN データストアを使用する場合のアップグレード作業
- エンド ユーザー用の VMware Horizon Web ポータル ページの構成

JMS メッセージ セキュリティ モードを拡張済みに変更する

アップグレードする場合、前のバージョンで使用していた既存の JMS メッセージ セキュリティ モード設定は維持されます。Horizon 6 バージョン 6.1 以降、View Administrator を使用してこの設定を [拡張済み] に変更できます。

この手順は、View Administrator を使用してメッセージ セキュリティ モードを [拡張済み] に変更する方法と、すべての View コンポーネントでの変更の進行状況を監視する方法について示します。または、`vdmutil` コマンドラインユーティリティを使用してモードを変更し、進行状況を監視することもできます。『View 管理』ドキュメントを参照してください。

注: Horizon 6 バージョン 6.2 以降のリリースでは、View セキュリティ サーバの代わりに Access Point アプライアンスを使用できます。Access Point は、標準の HTTP(S) プロトコルを使用して View 接続サーバと通信します。JMS、IPsec、および AJP13 は使用されません。

View セキュリティ サーバの代わりに Access Point アプライアンスを使用するには、View 接続サーバ インスタンスをバージョン 6.2 以降にアップグレードしてから、Access Point アプライアンスをインストールし、View 接続サーバ インスタンスまたはインスタンスに使用するロード バランサを参照するように構成する必要があります。詳細については、Unified Access Gateway の導入および設定を参照してください。

前提条件

すべての View 接続サーバ インスタンス、セキュリティ サーバ、および View デスクトップを Horizon 6 バージョン 6.1 以降のリリースにアップグレードしたことを確認します。Horizon 6 バージョン 6.1 よりも前の View コンポーネントは、拡張済みモードを使用する View 接続サーバ 6.1 インスタンスと通信することができません。

手順

- 1 バックエンド ファイアウォール ルールを、セキュリティ サーバがポート 4002 で JMS トラフィックを View 接続サーバ インスタンスに送信することを許可するように構成します。
- 2 View Administrator で、[View 構成] - [グローバル設定] に移動して、[セキュリティ] タブで [メッセージ セキュリティ モード] を [拡張済み] に設定します。
- 3 ポッド内のすべての View 接続サーバ ホストの VMware Horizon View Message Bus コンポーネント サービスを手動で再起動するか、View 接続サーバ インスタンスを再起動します。

サービスが再起動されると、View 接続サーバ インスタンスによってモードが [拡張済み] に変更され、すべてのデスクトップおよびセキュリティ サーバ上のメッセージ セキュリティ モードが再構成されます。

- 4 View Administrator で進行状況を監視するには、[View 構成] - [グローバル設定] に移動します。

すべてのコンポーネントで [拡張済み] モードへの移行が行われたら、[セキュリティ] タブの [拡張セキュリティのステータス] 項目に [拡張済み] が表示されます。

サーバがクライアントと通信すると、サーバは拡張メッセージ セキュリティ モードを使用するようにクライアントを構成します。

領域を再利用するためにデスクトップ プールをアップグレードする作業

vSphere 5.1 以降では、Horizon 7 が効率的なディスク形式でリンク クローン仮想マシンを作成します。この形式により、ESXi ホストはリンク クローンの未使用のディスク領域を再利用することができます。この機能を使用するためのプールのアップグレードでは、vCenter Server、View LDAP およびプールの設定の変更、そしてプールの再構成を行います。

注: 仮想マシンのデスクトップが Virtual SAN データストアまたは Virtual Volumes データストアでホストされている場合、領域再利用機能はサポートされません。

領域再利用機能は、仮想マシンで使用されるディスク領域量を削減しますが、使用されない領域だけを再利用できます。この機能は、最適化されていない仮想マシンで作成されたディスク領域を再利用できません。オペレーティングシステム イメージを最適化するために、インデクサ サービス、デフラグメント サービス、および復元ポイントなどの Windows サービスをオフにできます。詳細については、『Horizon 7 での仮想デスクトップのセットアップ』の「Windows ゲスト OS のパフォーマンスの最適化」「Windows 7 および Windows 8 ゲスト OS のパフォーマンスの最適化」および「リンク クローン デスクトップ用の Windows 7 および Windows 8 の最適化」を参照してください。

重要: この手順には、デスクトップ プールの再構成が関わるので、エンド ユーザーがオペレーティングシステム ディスクに行った変更は失われます。

- 1 プール内に、VMware vSphere 5.1 以降のバージョンでない vCenter Server インスタンスや ESXi ホストがある場合は、それらを 5.1 以降にアップグレードします。

手順については、『VMware vSphere アップグレード ガイド』を参照してください。

- 2 プール内に、VMware vSphere 5.1（仮想ハードウェア バージョン 9）以降でない仮想マシンがある場合は、それらをアップグレードします。

- 親仮想マシンで、VMware Tools を最新の VMware vSphere 5.1 以降のバージョンにアップグレードし、仮想マシンを最新のバージョンにアップグレードします。これは、仮想ハードウェア バージョン 9 以降である必要があります。

手順については、『VMware vSphere アップグレード ガイド』を参照してください。

- 親仮想マシンのスナップショットを作成します。スナップショットの作成手順については、vSphere Client のオンライン ヘルプを参照してください。
- デスクトップ プールを再構成するために作成した親仮想マシンのスナップショットを使用します。プールの再構成の手順については、Horizon Administrator の [ヘルプ] ボタンをクリックします。

アップグレードした仮想マシンのスナップショットからのプールの再構成は、リンク クローン プールですべての仮想マシンをアップグレードするひとつの方法です。仮想マシンを 1 つずつアップグレードすることもできます。

- 3 仮想マシンで使用されたディスク 形式をアップグレードします。

- 接続サーバ ホストでは、ADSIEdit を使用してプールに対応するサーバ グループに移動し、[pae-UseSparseFormat] フィールドの値を [0] から [1] に変更します。
- デスクトップ プールを再構成します。

- 4 vCenter Server 設定を編集するために Horizon Administrator を使用し、[ストレージ] タブに移動し、[VM ディスク容量を再利用] を選択します。

サーバ設定の編集の手順については、Horizon Administrator の [ヘルプ] ボタンをクリックします。

- 5 プール設定を編集するために Horizon Administrator を使用し、[詳細なストレージ] セクションに移動し、[VM ディスク容量を再利用] を選択し、容量再利用のしきい値を 1 GB に設定します。

VMware Virtual SAN データストアを使用する場合のアップグレード作業

vSphere 5.5 Update 1 以降では、高性能なストレージとポリシー ベースの管理のために Virtual SAN 機能を使用できます。

Virtual SAN では、vSphere ホストのクラスタで使用できるローカルで接続された物理ストレージディスクが、1 つの仮想データストアとして集約されます。このデータストアは、デスクトップ プールを作成するときに指定します。仮想マシン ファイル、レプリカ、ユーザー データ、オペレーティング システム ファイルなどの各種コンポーネントは、適切な半導体ディスク ドライブ (SSD) ディスクまたは直接接続されたハードディスク (HDD) に配置されます。

容量、パフォーマンス、可用性などの仮想マシン ストレージ要件は、使用されているプール設定に応じて、View によってデフォルト ストレージ ポリシー プロファイルの形で定義されます。ストレージは、割り当てられたポリシーに従ってプロビジョニングされ、自動的に設定されます。

注: 仮想マシンのデスクトップが Virtual SAN データストアでホストされている場合、領域再利用機能はサポートされません。

Non-Virtual SAN データストアから Virtual SAN データストアへのアップグレード

VMware Virtual SAN データストアを使用するためのプールのアップグレードでは、プール設定を変更してからプールを再分散します。

この手順に示されるタスクでは、non-Virtual SAN データストアから Virtual SAN データストアにアップグレードする方法について説明します。vSphere 5.5 以前のクラスタの Virtual SAN データストア (Tech Preview 機能) からのアップグレードはサポートされません。

重要: この手順には、デスクトップ プールの再構成が関わるので、エンド ユーザーがオペレーティング システム ディスクに行った変更は失われます。

前提条件

- プールに使用されているクラスタ内のすべての ESXi ホストが 5.5 Update 1 以降にアップグレードされていることと、それらが Virtual SAN 機能のシステム要件を満たしていることを確認します。vSphere 6.0 以降のリリースで利用可能な Virtual SAN 機能には、vSphere 5.5 Update 1 の機能と比較して多くのパフォーマンス向上があるため、VMware は vSphere 6.0 以降にアップグレードすることを推奨します。vSphere 6.0 では、この機能により広範囲にわたる HCL (ハードウェア互換性) サポートも含まれています。

アップグレードについては、「[4 章 ESXi ホストおよび仮想マシンのアップグレード](#)」および『VMware vSphere アップグレードガイド』を参照してください。Virtual SAN 要件およびアップグレードについては、『VMware Virtual SAN の管理』ドキュメントを参照してください。

- vCenter Server で、次の権限が Composer のロールに追加されていることを確認します。

Profile-Driven Storage: All
Folder: Create Folder & Delete Folder
Host: Configuration: Advanced settings

手順

- 1 vCenter Server 5.5 Update 1 以降を使用し、vSphere クラスタの Virtual SAN を有効にします。

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。

- 2 [View Composer デスクトップ プールのアップグレード](#)の説明に従って、デスクトップ プールを最新バージョンにアップグレードします。

このプロセスでは、Horizon Agent の最新バージョンを親仮想マシンにインストールし、スナップショットを作成します。

- 3 作成した親仮想マシンのスナップショットを使用し、non-Virtual SAN データストア上にプールを再構成します。

プールの再構成の手順については、View Administrator の [ヘルプ] ボタンをクリックします。

- 4 新たにアップグレードしたデスクトップ プールのプール設定を編集して、[VMware Virtual SAN を使用する] プール設定を有効にし、データストアを non-Virtual SAN データベースから Virtual SAN データストアに変更して、[Rebalance] コマンドを実行します。

サーバ設定の編集と [Rebalance] コマンドの実行の手順については、View Administrator の [ヘルプ] ボタンをクリックして確認してください。

Virtual SAN Disk Format バージョン 1 からのアップグレード

VMware vSphere 5.5 Update 1 から vSphere 6.0 以降のリリースにアップグレード後は、Virtual SAN ディスク形式もアップグレードする必要があります。

vSphere 6.0 以降のリリースで利用可能な Virtual SAN 機能には、vSphere 5.5 Update 1 の機能と比較して多くのパフォーマンス改善点が含まれているため、VMware は vSphere 6.0 以降にアップグレードすることを推奨します。vSphere 6.0 では、この機能により広範囲にわたる HCL（ハードウェア互換性）サポートも含まれています。

重要: この手順では、現在 vSphere 5.5 Update 1 以降のアップデート リリースで利用可能な Virtual SAN データストアのデスクトップ プールがある場合の Virtual SAN のアップグレード プロセスを説明しています。現在デスクトップ プールで Virtual SAN データストアが使用されていない場合、『[Non-Virtual SAN データストアから Virtual SAN データストアへのアップグレード](#)』を参照してください。

VMware Virtual SAN データストアのアップグレードは、各 ESXi ホストでの vSphere ソフトウェアのアップグレードと、その後ディスク グループごとのディスク形式のアップグレードを含む複数フェーズのプロセスです。

vSphere 6 ドキュメント『VMware Virtual SAN の管理』の章全体は、アップグレード プロセスにあてられています。次の処理の手順では、vCenter Server の ESXi ホスト レベルおよび View Administrator のデスクトップ プール レベルで行うタスクの順番について概要を説明します。

前提条件

- デスクトップ プールで View Agent 6.0 以降のバージョンが使用されているのを確認します。Virtual SAN データストアの仮想マシンで View Agent 5.3.x が使用される場合は、『[Virtual SAN データストア上の Horizon View 5.3.x からのアップグレード](#)』を参照してください。

- vCenter Server で、次の権限が Composer のロールに追加されていることを確認します。

```
Profile-Driven Storage: All
Folder: Create Folder & Delete Folder
Host: Configuration: Advanced settings
```

- Virtual SAN アップグレード プロセスについて理解しておきます。『VMware Virtual SAN の管理』の Virtual SAN のアップグレードに関する章を参照してください。ドキュメントは <https://www.vmware.com/support/pubs/virtual-san-pubs.html> から利用できます。

手順

- 1 vSphere 6.0 ドキュメント センターで利用可能な『VMware Virtual SAN の管理』ドキュメントの Virtual SAN クラスタのアップグレードに関する章にしたがって、vCenter Server と ESXi ホストを vSphere 6 以降にアップグレードします。

この時点では、デスクトップ プールはまだ Virtual SAN disk format 1 を使用しており、仮想マシンと VMware Tools はまだ vSphere 6.0 virtual hardware version 11 にアップグレードされていません。

- 2 「View Agent または Horizon Agent のアップグレード」と「View Composer デスクトップ プールのアップグレード」の説明に従って、デスクトップ プールを最新バージョンにアップグレードします。

このプロセスには、親仮想マシンの Horizon Agent、仮想マシン テンプレート、またはプールの完全クローン仮想マシンの最新バージョン インストールが含まれています。リンク クローン プールの場合、プロセスにはスナップショットの作成とプールの再構成も含まれています。

これで、デスクトップ プールの仮想マシンには View Agent 6.1 以降がインストールされ、仮想マシンは vSphere 5.5 Update 1 で利用可能な Virtual SAN データストアに残ります。この時点で、デスクトップ プールは Virtual SAN disk format 1 を使用しています。

- 3 Virtual SAN ディスク形式をバージョン 1 からバージョン 2 にアップグレードします。

詳細な手順については、『VMware Virtual SAN の管理』のアップグレードに関する章のトピック「Virtual SAN ディスク形式のアップグレード」を参照してください。ドキュメントは <https://www.vmware.com/support/pubs/virtual-san-pubs.html> から利用できます。

このアップグレードにはコマンドライン RVC ツールを使用できます。また、vSphere 6 Update 1 を使用している場合は vSphere Web Client を使用できます。Ruby vSphere Console (RVC) は VMware ESXi ホストおよび vCenter Server 用の Ruby ベースのコマンドライン コンソールです。RVC は Windows および Linux 両方のバージョンの vCenter Server に同梱されます。RVC コマンドの使用の詳細については、『RVC コマンドライン リファレンス ガイド』を参照してください。

- 4 親仮想マシン、仮想マシン テンプレートまたはプールの完全クローン仮想マシン上でクラスタの全 ESXi ホストに対しディスクがアップグレードされたら、次のタスクを順番に完了させます。

- a 親仮想マシンが Virtual SAN データストア上にある場合は、すべてのスナップショットを削除します。

すべての以前の **redo log** ベース スナップショットが削除されないと、仮想マシンでは Virtual SAN format 2 で利用可能な新しいスナップショットを使用開始できません。仮想マシンが Virtual SAN データストア上にない場合、スナップショットを削除する必要はありません。

- b 仮想マシン ハードウェアをバージョン 11 にアップグレードし、VMware Tools をアップグレードします。

- 5 リンク クローン プールの場合、新しいスナップショットを作成し、その新しいスナップショットを使用して、デスクトップ プールを再構成します。

以上で、デスクトップ プールは Virtual SAN disk format 2 を使用するようになります。

Virtual SAN データストア上の Horizon View 5.3.x からのアップグレード

Horizon 6.0 () では、Virtual SAN 向けにいくつかの新しいデフォルトのストレージ ポリシーが導入されました。デスクトップ プールをアップグレードしても、View 5.3.x によって Virtual SAN 上で作成された既存の仮想マシン デスクトップにこれらのポリシーは自動的に適用されません。

また、View 5.3.x からアップグレードする場合、プールが Virtual SAN データストア上にあっても、[VMware Virtual SAN を使用する] プール設定は自動的に有効化されません。次のアップグレード オプションがあります。

- アップグレード後、VMware vSphere 5.5 Update 1 を引き続き使用する場合、View 5.3.x で使用したデフォルトのストレージ ポリシーを使用します。このオプションを選択する場合は、[VMware Virtual SAN を使用する] が有効になるようにプール設定を編集します。
- このトピックで説明している手順を使って、デスクトップ プールで新しいデフォルトのストレージ ポリシーが使用されるようにします。この手順では、non-Virtual SAN データストアへのデスクトップ プールを再分散してから、アップグレードを行って Virtual SAN データストアに対して再分散して戻します。

重要: この手順に示されるタスクでは、VMware vSphere 5.5 Update 1 クラスタ上の Virtual SAN データストアを使用して、View 5.3.x デスクトップ プールをアップグレードする方法について説明します。Virtual SAN データストア (Tech Preview 機能) からのアップグレードは、VMware vSphere 5.5 以前のクラスタではサポートされません。

また、この手順にはデスクトップ プールの再構成に関わるため、エンド ユーザーがオペレーティング システム ディスクに対して行った変更はすべて失われます。

前提条件

- プール内のすべての仮想マシンが VMware vSphere 5.5 Update 1 以降の仮想マシンであることを確認します。vSphere 6.0 以降のリリースで利用可能な Virtual SAN 機能には、vSphere 5.5 Update 1 の機能と比較して多くのパフォーマンス向上があるため、VMware は VMware vSphere 6.0 以降にアップグレードすることを推奨します。vSphere 6.0 では、この機能により広範囲にわたる HCL (ハードウェア互換性) サポートも含まれています。

アップグレードの詳細については、[4 章 ESXi ホストおよび仮想マシンのアップグレード](#)および『VMware vSphere アップグレード ガイド』を参照してください。Virtual SAN 要件およびアップグレードについては、『VMware Virtual SAN の管理』ドキュメントを参照してください。

- vCenter Server で、次の権限が Composer のロールに追加されていることを確認します。

```
Profile-Driven Storage: All
Folder: Create Folder & Delete Folder
Host: Configuration: Advanced settings
```

手順

- 1 データストアを Virtual SAN データストアから non-Virtual SAN データストアに変更するため、デスクトッププールのプール設定を編集して、[Rebalance] コマンドを実行します。

サーバ設定の編集と [Rebalance] コマンドの実行の手順については、View Administrator の [ヘルプ] ボタンをクリックして確認してください。

- 2 [View Composer デスクトップ プールのアップグレード](#)の説明に従って、デスクトップ プールを最新バージョンにアップグレードします。

このプロセスでは、Horizon Agent の最新バージョンを親仮想マシンにインストールし、スナップショットを作成します。

- 3 作成した親仮想マシンのスナップショットを使用し、non-Virtual SAN データストア上にプールを再構成します。

プールの再構成の手順については、View Administrator の [ヘルプ] ボタンをクリックします。

- 4 新たにアップグレードしたデスクトップ プールの設定を編集してデータストアを non-Virtual SAN データストアから Virtual SAN データストアに変更し、[Rebalance] コマンドを実行します。

次のステップ

Virtual SAN 1 ではなく Virtual SAN 2 を使用するため、仮想マシンを VMware vSphere 6.0 へアップグレードした場合、「[Virtual SAN Disk Format バージョン 1 からのアップグレード](#)」を参照してください。

エンド ユーザー用の VMware Horizon Web ポータル ページの構成

この Web ページを構成して、Horizon Client ダウンロード用のアイコン、または HTML Access 経由でリモート デスクトップに接続するアイコンの表示と非表示を切り替えることができます。このページの他のリンクも構成できます。

デフォルトでは、Web ポータル ページに、ネイティブ Horizon Client のダウンロードおよびインストールのアイコンと、HTML Access 経由で接続するためのアイコンの両方が表示されます。使用されるダウンロード リンクは、`portal-links-html-access.properties` ファイルで定義されているデフォルト値で決定されます。

ただし、社内の Web サーバへのリンクを表示したり、特定のクライアント バージョンをサーバで使用できるようにした方がよい場合もあります。`portal-links-html-access.properties` ファイルの内容を変更して、別のダウンロード URL を示すようにポータル ページを再構成できます。このファイルが使用できない、または空白であり、`oslinks.properties` ファイルが存在する場合は、`oslinks.properties` ファイルを使用して、インストーラ ファイルのリンクの値が決定されます。

oslinks.properties ファイルは、*installation-directory*\VMware\VMware View\Server\broker\webapps\portal\WEB-INF フォルダにインストールされます。HTML Access セッションでこのファイルが見つからない場合、このダウンロードリンクによって、ユーザーはデフォルトで <https://www.vmware.com/go/viewclients> にアクセスします。このファイルには、次のデフォルト値が含まれます。

```
link.download=https://www.vmware.com/go/viewclients
# download Links for particular platforms
link.win32=https://www.vmware.com/go/viewclients#win32
link.win64=https://www.vmware.com/go/viewclients#win64
link.linux32=https://www.vmware.com/go/viewclients#linux32
link.linux64=https://www.vmware.com/go/viewclients#linux64
link.mac=https://www.vmware.com/go/viewclients#mac
link.ios=https://itunes.apple.com/us/app/vmware-view-for-ipad/id417993697
link.android=https://play.google.com/store/apps/details?id=com.vmware.view.client.android
link.chromeos=https://chrome.google.com/webstore/detail/vmware-horizonclient/
pckbpdplfajmgaipljfamclkinbjdnma
link.winmobile=https://www.microsoft.com/en-us/store/p/vmware-horizon-client/9nblggh51p19
```

特定のクライアント オペレーティング システム用のインストーラ リンクは、portal-links-html-access.properties または oslinks.properties ファイルのいずれかで作成できます。たとえば、Mac OS X システムからポータル ページを参照すると、ネイティブ Mac OS X インストーラのリンクが表示されます。Windows や Linux クライアントの場合、32 ビット版インストーラのリンクと 64 ビット版インストーラのリンクを個別に作成できます。

重要: View 接続サーバ 5.x 以前のリリースからのアップグレードで HTML Access コンポーネントをインストールしておらず、Horizon Client ダウンロード用の社内サーバを指定するポータル ページを編集してある場合、これらのカスタマイズは View 接続サーバ 6.0 以降をインストールすると非表示になることがあります。Horizon 6 以降では、HTML Access コンポーネントが View 接続サーバのアップグレード時に自動的にインストールされます。

View 5.x 用に別途 HTML Access コンポーネントをインストールした場合は、Web ページに行ったカスタマイズはすべて保持されています。HTML Access コンポーネントをインストールしなかった場合、カスタマイズはすべて非表示になります。以前のリリース用のカスタマイズは、使用されなくなった portal-links.properties ファイルに入っています。

手順

- 1 View 接続サーバ ホストで、テキスト エディタを使用して portal-links-html-access.properties ファイルを開きます。

このファイルの場所は *CommonAppDataFolder*\VMware\VDM\portal\portal-links-html-access.properties です。Windows Server 2008 オペレーティング システムでは、*CommonAppDataFolder* ディレクトリは C:\ProgramData です。Windows Explorer で C:\ProgramData フォルダを表示するには、[フォルダ オプション] ダイアログ ボックスを使用して非表示のフォルダを表示する必要があります。

portal-links-html-access.properties ファイルが存在せず、oslinks.properties ファイルが存在する場合は、<installation-directory>\VMware\VMware View\Server\broker\webapps\portal\WEB-INF\oslinks.properties ファイルを開いて、特定のインストーラ ファイルをダウンロードするために使用する URL を変更します。

注: portal-links.properties ファイル (portal-links-html-access.properties ファイルと同じ *CommonAppDataFolder\VMware\VDM\portal* ディレクトリにある) に入っている View 5.x 以前用のカスタマイズです。

2 構成プロパティを編集し、適切に設定します。

デフォルトでは、インストーラ アイコンと HTML Access アイコンの両方が有効で、リンクは VMware Web サイトのクライアント ダウンロード ページを参照します。アイコンを無効にする (Web ページからアイコンを削除する) には、プロパティを `false` に設定します。

注: oslinks.properties ファイルは、特定のインストーラ ファイルへのリンクの構成にのみ使用できます。下記に表示される他のオプションはサポートされません。

| オプション | プロパティ設定 |
|---|---|
| HTML Access を無効にする | <p><code>enable.webclient=false</code></p> <p>このオプションが <code>false</code> に設定されているにもかかわらず <code>enable.download</code> オプションが <code>true</code> に設定されていると、ユーザーは Web ページでネイティブの Horizon Client インストーラのダウンロードを求められます。両オプションが <code>false</code> に設定されていると、次のメッセージが表示されます。「この接続サーバへのアクセスについての説明は、ローカルの管理者にお問い合わせください。」</p> |
| Horizon Client のダウンロードを無効にする | <p><code>enable.download=false</code></p> <p>このオプションが <code>false</code> に設定されているにもかかわらず <code>enable.webclient</code> オプションが <code>true</code> に設定されていると、ユーザーに HTML Access のログイン Web ページが表示されます。両オプションが <code>false</code> に設定されていると、次のメッセージが表示されます。「この接続サーバへのアクセスについての説明は、ローカルの管理者にお問い合わせください。」</p> |
| Horizon Client をダウンロードするための Web ページの URL を変更します | <p><code>link.download=https:// url-of-web-server</code></p> <p>独自の Web ページを作成する予定がある場合は、このプロパティを使用します。</p> |

| オプション | プロパティ設定 |
|----------------------------------|---|
| 特定のインストーラ用のリンクを作成する | <p>以下に示すのは完全 URL の例ですが、インストーラ ファイルが次の手順の説明のように View 接続サーバの C:\Program Files\VMware\VMware View\Server\broker\webapps\ ディレクトリの downloads ディレクトリにある場合は、相対 URL を使用できます。</p> <ul style="list-style-type: none"> ■ インストーラをダウンロードするための一般的なリンク : <pre>link.download=https://server/downloads</pre> ■ 32 ビット Windows インストーラ : <pre>link.win32=https://server/downloads/VMware-Horizon-Client-x86-build#.exe</pre> ■ 64 ビット Windows インストーラ : <pre>link.win64=https://server/downloads/VMware-Horizon-Client-x86_64-build#.exe</pre> ■ Windows Phone インストーラ : <pre>link.winmobile=https://server/downloads/VMware-Horizon-Client-build#.appx</pre> ■ 32 ビット Linux インストーラ : <pre>link.linux32=https://server/downloads/VMware-Horizon-Client-build#.x86.bundle</pre> ■ 64 ビット Linux インストーラ : <pre>link.linux64=https://server/downloads/VMware-Horizon-Client-build#.x64.bundle</pre> ■ Mac OS X インストーラ : <pre>link.mac=https://server/downloads/VMware-Horizon-Client-build#.dmg</pre> ■ iOS インストーラ: <pre>link.ios=https://server/downloads/VMware-Horizon-Client-iPhoneOS-build#.ipa</pre> ■ Android インストーラ : <pre>link.android=https://server/downloads/VMware-Horizon-Client-AndroidOS-build#.apk</pre> ■ Chrome OS インストーラ : <pre>link.chromeos=https://server/downloads/VMware-Horizon-Client-ChromeOS-build#.apk</pre> |
| ログイン ページの [ヘルプ] リンクの URL を変更します。 | <pre>link.help</pre> <p>デフォルトでは、このリンクは VMware の Web サイトにホストされているヘルプ システムを参照します。[ヘルプ] リンクが、ログイン ページの下部に表示されます。</p> |

- 3 ユーザーに VMware Web サイト以外の場所からインストーラをダウンロードさせるには、インストーラ ファイルを置くことになる HTTP サーバにインストーラ ファイルを配置します。

この場所は、前の手順の `portal-links-html-access.properties` ファイルまたは `oslinks.properties` ファイルで指定した URL に対応している必要があります。たとえば、View 接続サーバホストの `downloads` ディレクトリにファイルを配置するには、以下のパスを使用します。

```
C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
```

これで、インストーラ ファイルに対するリンクで `/downloads/client-installer-file-name` というフォーマットの相対 URL を使用できます。

- 4 View Web コンポーネント サービスを再起動します。

View パッチの適用

パッチ リリースには、View コンポーネント（View Composer、View 接続サーバ、Horizon Agent、およびさまざまなクライアント）のインストーラ ファイルが含まれている場合があります。適用する必要があるパッチ コンポーネントは、View のデプロイで必要されるバグ修正によって異なります。

必要とされるバグ修正によっては、次の順番で該当する View コンポーネントをインストールします。

- 1 View Composer
- 2 View 接続サーバ
- 3 Horizon Agent
- 4 Horizon Client

この章には、次のトピックが含まれています。

- [View Composer へのパッチの適用](#)
- [View 接続サーバへのパッチの適用](#)
- [View Agent または Horizon Agent へのパッチの適用](#)
- [Horizon Client のパッチの適用](#)

View Composer へのパッチの適用

パッチを適用するには、パッチ バージョンのインストーラをダウンロードして実行します。パッチ リリースによっては、View Composer 用のパッチが含まれていない場合もあります。

前提条件

- この手順をいつ実行すべきかを判断します。利用可能なデスクトップメンテナンス期間を選択します。パッチ バージョンのインストールには 15 ～ 30 分を予定してください。
- パッチ インストーラの実行に使用するホスト上に管理者権限のあるドメイン ユーザー アカウントがあることを確認します。
- View Composer が仮想マシンにインストールされている場合は、その仮想マシンのスナップショットを作成します。
スナップショットの作成手順については、vSphere Client のオンライン ヘルプを参照してください。
- vCenter Server データベースと View Composer データベースをバックアップします。

データベースのバックアップ方法については、データベース ベンダーから提供されるマニュアルを参照してください。

- すべてのリンク クローン デスクトップ プールについて、新しい仮想マシンのプロビジョニングを無効にします。
- いずれかのデスクトップ プールに更新または再構成の操作のスケジュールが設定されている場合は、それらの操作をキャンセルします。

手順

- 1 View Composer をホストする仮想マシンで、View Composer のパッチ バージョンのインストーラ ファイルをダウンロードします。

このダウンロードに関する手順については、VMware の担当者までお問い合わせください。

- 2 View Composer のパッチ リリース用にダウンロードしたインストーラを実行します。

注: Horizon 6 バージョン 6.2 以降のリリースでは、パッチをインストールする前に以前のバージョンをアンインストールする必要がなくなりました。

- 3 インストーラ ウィザードが閉じた後、VMware Horizon View Composer サービスが再起動することを確認します。
- 4 必要な場合は、親仮想マシン上で Horizon Agent のパッチを適用し、テスト用のデスクトップ プールを作成します。

- a 親仮想マシンで Horizon Agent のパッチ インストーラをダウンロードして実行します。

このダウンロードに関する手順については、VMware の担当者までお問い合わせください。

- b この仮想マシンから、小さなリンク クローン デスクトップ プールを作成します。

- c 作成したデスクトップ プールから仮想デスクトップをテストして、あらゆる使用方法のシナリオが正常に機能することを確認します。

たとえば、1 つの仮想デスクトップを含むデスクトップ プールを作成し、Horizon Client を使用してそのデスクトップにログインできることを確認します。

Horizon Agent インストーラを実行してデスクトップ プールを作成する手順については、『Horizon 7 での仮想デスクトップのセットアップ』（Horizon Administrator の [ヘルプ] ボタンをクリックして表示）を参照してください。

- d テスト デスクトップ プール内の仮想デスクトップが期待どおりに機能することを確認します。

次のステップ

必要に応じて、View 接続サーバにパッチを適用します。

View 接続サーバへのパッチの適用

パッチを適用するには、パッチ バージョンのインストーラをダウンロードして実行します。

前提条件

- この手順をいつ実行すべきかを判断します。利用可能なデスクトップメンテナンス期間を選択します。この処理に必要な時間は、グループ内の View 接続サーバ インスタンスの数によって決まります。1 インスタンスにつき 15 ～ 30 分を予定してください。
- パッチ インストーラの実行に使用するホスト上に管理者権限のあるドメイン ユーザー アカウントがあることを確認します。

手順

- 1 View 接続サーバが仮想マシンにインストールされている場合は、その仮想マシンのスナップショットを作成します。

スナップショットの作成手順については、vSphere Client のオンライン ヘルプを参照してください。
- 2 複製されたグループにある View 接続サーバ インスタンスの 1 つで、View 接続サーバのパッチ バージョン用のインストーラ ファイルをダウンロードします。

このダウンロードに関する手順については、VMware の担当者までお問い合わせください。
- 3 View 接続サーバのパッチ リリース用にダウンロードしたインストーラを実行します。

インストーラの実行については、『View インストール ガイド』を参照してください。

注: Horizon 6 バージョン 6.2 以降のリリースでは、パッチをインストールする前に以前のバージョンをアンインストールする必要がなくなりました。

- 4 インストール ウィザードのプロンプトに従って操作し、既存の ADAM インスタンスを使用してインストールを続行するかどうか確認を求められたら、[OK] をクリックします。
- 5 インストーラ ウィザードが閉じた後、VMware Horizon View 接続サーバ サービスが再起動したことを確認します。
- 6 レプリカ グループ内の他の View 接続サーバ インスタンスについても、前の手順を繰り返します。
- 7 この手順を View セキュリティ サーバで繰り返します。

次のステップ

1 つ以上の View 接続サーバ インスタンスでパッチの適用が失敗する場合は、[接続サーバをスナップショットに戻した後のレプリカ グループの作成](#)を参照してください。

必要に応じて、View Agent にパッチを適用します。

View Agent または Horizon Agent へのパッチの適用

パッチを適用するには、パッチ バージョンのインストーラをダウンロードして実行します。

次の手順は、リンク クローン デスクトップ プールについては親仮想マシンで、完全なクローン プールでは各仮想マシン デスクトップで、1 つの仮想マシン デスクトップのみを含むプールについては個々のデスクトップ仮想マシンで、実行する必要があります。

前提条件

パッチ インストーラの実行に使用するホスト上に管理者権限のあるドメイン ユーザー アカウントがあることを確認します。

手順

- 1 すべての親仮想マシン、完全クローンのテンプレートに使用される仮想マシン、プールにある完全クローン、手動で追加された個々の仮想マシンで、View Agent (Horizon 6) または Horizon Agent (Horizon 7) のパッチ バージョンのインストーラ ファイルをダウンロードします。

このダウンロードに関する手順については、VMware の担当者までお問い合わせください。

- 2 View Agent または Horizon Agent のパッチ リリース用にダウンロードしたインストーラを実行します。

注: Horizon 6 バージョン 6.2 以降のリリースでは、パッチをインストールする前に、前バージョンをアンインストールする必要はありません。

- 3 View Composer へのパッチ適用の準備作業で新規仮想マシンのプロビジョニングを無効にした場合は、再度プロビジョニングを有効にします。
- 4 リンク クローン デスクトップ プールを作成するために使用される親仮想マシンについては、仮想マシンのスナップショットを取得します。
スナップショットの作成の詳細については、vSphere Client のオンライン ヘルプを参照してください。
- 5 リンク クローン デスクトップ プールでは、作成したスナップショットを使用してデスクトップ プールを再構成します。
- 6 パッチが適用されたデスクトップ プールに Horizon Client を使用してログインできることを確認します。
- 7 いずれかのリンク クローン デスクトップ プールについて更新または再構成の操作をキャンセルした場合は、再度作業をスケジュールします。

Horizon Client のパッチの適用

デスクトップ クライアントデバイスでパッチを適用するには、パッチ バージョンのインストーラをダウンロードして実行します。モバイル クライアントでパッチを適用する場合には、Google Play、Windows ストア、または Apple App Store などのアプリを販売する Web サイトから更新をインストールします。

手順

- 1 各クライアント システムで、Horizon Client のパッチ バージョンのインストーラ ファイルをダウンロードします。

このダウンロードに関する手順については、VMware の担当者までお問い合わせください。または、クライアント ダウンロード ページ <http://www.vmware.com/go/viewclients> でご確認ください。すでに述べたように、一部のクライアントについては、アプリ ストアからパッチ リリースを入手できます。

- 2 クライアント デバイスが Mac または Linux デスクトップまたはラップトップである場合は、デバイスから現在のバージョンのクライアント ソフトウェアを削除します。

各デバイス特有の方法でアプリケーションを削除してください。

注: Horizon Client 3.5 for Windows 以降のリリースでは、Windows クライアントのパッチをインストールする前に、前バージョンをアンインストールする必要はありません。Horizon Client 4.1 for Windows 以降のリリースでは、アップグレード Horizon Client オンライン機能を有効にして、Windows クライアントの Horizon Client をオンラインでアップグレードできます。Horizon Client for Mac 4.4 以降では、アップグレード Horizon Client オンライン機能を有効にして、Mac クライアントの Horizon Client をオンラインでアップグレードできます。

- 3 必要な場合には、Horizon Client のパッチ リリース用にダウンロードしたインストーラを実行します。

Apple App Store や Google Play からパッチを入手した場合には、アプリは、通常ダウンロードしたときにインストールされるため、インストーラを実行する必要はありません。

- 4 パッチが適用されたデスクトップ プールに新しくパッチが適用された Horizon Client でログインできることを確認します。

View 環境における vSphere コンポーネントの個別アップグレード

8

View コンポーネントとは別に vSphere コンポーネントを個別にアップグレードする場合は、一部の View データをバックアップし、一部の View ソフトウェアを再インストールする必要があります。

View コンポーネントと vSphere コンポーネントの統合アップグレードを実行する代わりに、最初にすべての View コンポーネントをアップグレードしてから vSphere コンポーネントをアップグレードしたり、その逆の順序でアップグレードしたりすることができます。vSphere の新しいバージョンまたは更新がリリースされたときに、vSphere コンポーネントのみをアップグレードすることもできます。

View コンポーネントとは別に vSphere コンポーネントを個別にアップグレードする場合、次の追加タスクを実行する必要があります。

- 1 vCenter Server をアップグレードする前に、vCenter Server データベースと View Composer データベースをバックアップします。
- 2 vCenter Server をアップグレードする前に、`vdmexport.exe` ユーティリティを使用して、View 接続サーバインスタンスから View LDAP データベースをバックアップします。

手順については、『View 管理者ガイド』を参照してください。レプリカ グループ内に View 接続サーバインスタンスが複数存在する場合は、1 つのインスタンスからデータをエクスポートするだけでかまいません。

- 3 View Composer を使用する場合は、特定の vCenter Server インスタンスで管理されているすべての ESXi ホストをアップグレードした後、そのホストで View Composer サービスを再起動します。
- 4 リモート デスクトップとして使用されている仮想マシンの VMware Tools をアップグレードした後、Horizon Agent を再インストールします。

Horizon Agent を再インストールすると、仮想マシンのドライバとその他の View コンポーネントとの互換性が引き続き確保されます。

Horizon Agent インストーラを実行する手順については、『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントを参照してください。