

Horizon 7 のアップグレード

2020 年 3 月

VMware Horizon 7 7.12



vmware®

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

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

ヴィ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 © 2009-2020 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

目次

Horizon 7 7.12 へのアップグレード	5
1 Horizon 7 のアップグレードの概要	6
2 Extended Service Branch の適用	9
3 クライアント アプリケーションのアップグレード	10
4 Horizon 7 Server をアップグレードする場合のシステム要件	12
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	12
View Composer の要件	13
View Composer でサポートされるオペレーティング システム	13
スタンドアロン View Composer のハードウェア要件	14
View Composer およびイベント データベースのデータベース要件	14
View Composer のアップグレード要件	15
Horizon 接続サーバの要件	16
Horizon 接続サーバのハードウェア要件	16
Horizon Connection Server でサポートされるオペレーティング システム	17
Horizon 接続サーバのアップグレード要件	17
Horizon Agent の要件と考慮事項	19
5 Horizon 7 Server コンポーネントのアップグレード	20
View Composer のアップグレード	20
アップグレードのための vCenter Server および View Composer の準備	21
View Composer のアップグレード	23
View Composer から vCenter および ESXi 接続で TLSv1.0 を有効にする	24
View Composer のダイジェスト アクセス認証の有効化	25
View Composer データベースの手動アップグレード	25
別のマシンへの View Composer の移行	28
Horizon Connection Server のアップグレード	35
アップグレードのための接続サーバの準備	35
レプリカ グループ内の接続サーバのアップグレード	36
接続サーバから vCenter 接続で TLSv1.0 を有効にする	39
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	40
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	41
セキュリティ サーバのアップグレード	42
アップグレードのためのセキュリティ サーバの準備	42
セキュリティ サーバとペアになっている接続サーバのアップグレード	43

Unified Access Gateway アプライアンスとセキュリティ サーバの置換	46
登録サーバのアップグレード	47
クラウド ポッド アーキテクチャ 環境のアップグレード	47
Horizon 7 Server のアップグレードによる HTML Access の許可	48
vCenter Server のアップグレード	48
デフォルトの TLS 証明書のサムプリントを受け入れる	50
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	51

6 ESXi ホストおよび仮想マシンのアップグレード 53

7 公開デスクトップと仮想デスクトップのアップグレード 56

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	56
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	56
View Agent または Horizon Agent のアップグレード	58
View Composer デスクトップ プールのアップグレード	61
インスタント クローン デスクトップ プールのアップグレード	62

8 Horizon 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 65

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	65
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	66
VMware vSAN データストアを使用する場合のアップグレード作業	68
non-vSAN データストアから vSAN データストアへのアップグレード	68
vSAN disk format 1 からのアップグレード	69
vSAN データストア上の Horizon View 5.3.x からのアップグレード	71
エンド ユーザー用の VMware Horizon Web ポータル ページの構成	72

9 Horizon 7 環境における vSphere コンポーネントの個別アップグレード 77

Horizon 7 7.12 へのアップグレード

『Horizon 7 のアップグレード』では、最新メンテナンス リリースの 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。Horizon 7 メンテナンス リリースにアップグレードするときも、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、Horizon 7 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。

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。

Horizon 7 のアップグレードの概要

1

Horizon 7 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。Horizon Connection Server および他の Horizon 7 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、Horizon 7 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。Horizon 7 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。Horizon 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、『Horizon 7 のインストール』ドキュメントで「FIPS モードでの Horizon 7 のインストール」を参照してください。

アップグレード中、Horizon 7 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。Horizon 7 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。Connection Server 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。

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 Horizon 7 のコンポーネントによって異なります。

- 1 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。[3 章 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。
- 2 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ります。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。

- 3 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。

- 4 Connection Server 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 Connection Server 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。

- 5 セキュリティ サーバとペアになっていない Connection Server 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 Connection Server 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、Connection Server インスタンスのアップグレード時に負荷が分散されている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： Connection Server 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 Connection Server 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。

- 6 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。

- 7 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 Connection Server 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。[セキュリティ サーバとペアになっている接続サーバのアップグレード](#)を参照してください。

- 8 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。

- 9 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。

- 10 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。[6 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。

- 11 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。
- 12 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。
- 13 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。
- 14 クラウド ポッド アーキテクチャの機能を使用する場合は、[クラウド ポッド 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 転送サーバ インスタンスと 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://docs.vmware.com/jp/VMware-Horizon-7/index.html> で入手可能な Horizon 7 リリース ノートを参照してください。

Extended Service Branch の適用

2

拡張サービスブランチ (ESB) は、Horizon 7、VMware App Volumes、VMware Dynamic Environment Manager で使用可能なオプションです。これは、累積的な修正、重要なバグ修正、セキュリティ修正を含む定期的なサービスパック (SP) のアップデートを提供します。

Horizon の最新バージョンにアップグレードせずに同じバージョンを使用する場合は、ESB をデプロイすると、引き続きバグやセキュリティの修正を迅速に取得できます。SP の更新には新しい機能は含まれません。重要な環境で安定した Horizon プラットフォームを利用できます。

コアとなる Horizon プラットフォーム、VMware App Volumes、VMware Dynamic Environment Manager に対して、個別の ESB が年に 1 回利用できます。ESB の期間は 24 か月で、その間に 3 回の SP 更新を予定しています。SP1 は初期リリースの 6 か月後にリリースされます。SP2 は SP1 の 3 か月後、SP3 は SP2 の 6 か月後にリリースされます。

詳細については、<https://kb.vmware.com/s/article/52845> にある「FAQ: Horizon 7, App Volumes, DEM Extended Service Branches (ESB)」を参照してください。

クライアント アプリケーションのアップグレード

3

Horizon Client の最新バージョンにアップグレードします。シン クライアント デバイスを使用する場合は、こ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。

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 Horizon 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

- 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、管理者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://docs.vmware.com/jp/VMware-Horizon-Client/index.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 サイトに掲載した後、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、Connection Server 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。

Horizon 7 Server をアップグレードする場合のシステム要件

4

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 の要件と考慮事項](#)

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/jp/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 Connection Server と Horizon Agent との互換性は、Connection Server 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。Horizon Agent を管理する Connection Server のバージョンに合わせて、できるだけ早く 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 4-1. 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

	Connection Server : 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
Connection Server 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	アップグレード中 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。Horizon 7 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。Connection Server 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 4-2. 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

表 4-2. View Composer がサポートするオペレーティング システム (続き)

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 2016	64 ビット	Standard Datacenter
Windows Server 2019	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。

Windows Server 2016 または Windows Server 2019 仮想マシンでの View Composer のインストールのトラブルシューティングについては、VMware ナレッジベースの記事 <https://kb.vmware.com/s/article/59633> 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 4-3. 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。Horizon イベントに関する Horizon Connection Server 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、認証局 (CA) が署名した TLS 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 TLS 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、『Horizon 7 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 Horizon 7 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、『Horizon 7 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、『Horizon 7 のセキュリティ』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。『Horizon 7 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 4-4. 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 Connection Server でサポートされるオペレーティング システム

Horizon Connection Server 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 Connection Server 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 4-5. Horizon Connection Server 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
Windows Server 2019	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。

Horizon 接続サーバのアップグレード要件

Horizon 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。

- 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。
- 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、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。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、Administrators 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。Horizon 7 ではこのアカウントのみに、複製された接続サーバ インスタンスをインストールする権限を含むすべての Horizon 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。
- 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 Horizon 7 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

- 接続サーバでは、認証局 (CA) によって署名され、クライアントが検証可能な TLS 証明書が必要です。接続サーバをインストールすると、認証局 (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、Horizon 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 TLS 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、『Horizon 7 のインストール』の「Horizon 7 Server 用の TLS 証明書の構成」を参照してください。また、『Horizon 7 の TLS 証明書設定のシナリオ』も参照してください。このドキュメントには、ロード バランシングと SSL 接続の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が記載されています。

注： 元のサーバに認証局 (CA) によって署名された TLS 証明書がすでにある場合は、アップグレード中に、既存の認証局 (CA) 署名付き証明書を Horizon 7 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 Horizon 7 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、『Horizon 7 のインストール』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、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、『Horizon 7 の管理』の「Horizon 7 サーバ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 サーバをこの接続サーバ インスタンスとペアにする場合、[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。『Horizon 7 のインストール』ドキュメント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、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。
- バージョン 6.2 より前の View Agent を使用する Horizon 7 Server 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 Server 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、『Horizon 7 のインストール』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 の要件と考慮事項

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 사용됩니다。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 ポリシーをセットアップする手順については、『Horizon 7 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。

Horizon 7 Server コンポーネントのアップグレード

5

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、Horizon Connection Server、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。

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 Connection Server 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](#)
- [登録サーバのアップグレード](#)
- [クラウド ポッド アーキテクチャ 環境のアップグレード](#)
- [Horizon 7 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 TLS 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、Horizon 7 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。Horizon 7 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。Horizon Connection Server 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 Horizon 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 Horizon 7 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 Horizon 7 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 TLS 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 クローンとインスタント クローンのデスクトップ プールについて、Horizon 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。

リンク クローンの場合、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 リンク クローンまたはインスタント クローンのデスクトップ プールがログアウト時に OS ディスクを更新するように設定されている場合は、Horizon 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。

リンク クローンの場合、この設定を行うと、まだ Horizon 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 リンク クローンまたはインスタント クローンのデスクトップ プールに更新、再構成またはイメージ プッシュ操作のスケジュールが設定されている場合は、Horizon Administrator を使用して、こ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 Horizon 7 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、Horizon 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 プールがログアウト時に OS ディスクを更新するように設定されている場合は、Horizon 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、Horizon Administrator を使用して、こ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 Horizon 7 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。Horizon Connection Server のアップグレード後に、View Composer で認証局 (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、Horizon 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、『Horizon 7 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、Horizon 7 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 SslBasicAuth 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 Horizon 7 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 -dsnname=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 svuid

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 5-1. 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 5-1. 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。
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。

表 5-1. databaseupgrade コマンドの結果コード（続き）

コード	説明
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	アクション
デスクトップは存在するが使用できない。	デスクトップを再度使用できるようにします。 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。
デスクトップが存在しない。	ログ メッセージを無視します。 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 Horizon Administrator では存在するように表示される場合があります。

- 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、Horizon 7 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かにかかわらず、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。

- Horizon 7 のインストールを参照して、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。
- Horizon 7 のインストールを参照して、View Composer での TLS 証明書の構成について理解しておきます。
- Horizon Administrator での View Composer の構成について理解しておきます。Horizon 7 の管理の 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。
- ベスト プラクティスとして、View Composer の移行に使用する移行元と移行先のマシンが同一で、同じ管理者の認証情報を共有していることを確認します。スタンドアローン マシンからすでに View Composer がインストールされている vCenter Server マシンに View Composer を移行した場合、2 台のマシンで使用する認証情報が異なると、View Composer の構成が失敗する可能性があります。

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 Horizon Administrator で、[View 構成] - [サーバ] の順に選択します。
 - 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 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 Horizon Administrator で、新しい View Composer の設定を指定します。
 - a Horizon Administrator で、[View 構成] - [サーバ] の順に選択します。
 - 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

- 『Horizon 7 のインストール』を参照して、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。
 - 『Horizon 7 のインストール』を参照して、View Composer での TLS 証明書の構成について理解しておきます。
 - Horizon Administrator から View Composer を削除する手順について理解しておきます。『Horizon 7 の管理』で、Horizon 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。
- Horizon Administrator での View Composer の構成について理解しておきます。『Horizon 7 の管理』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 Horizon Administrator で、Horizon Administrator から View Composer を削除します。
 - a [View 構成] - [サーバ] の順に選択します。
 - 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 TLS 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 Horizon Administrator で、新しい View Composer の設定を指定します。

a Horizon Administrator で、[View 構成] - [サーバ] の順に選択します。

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 パブリック/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 キー 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のパスです。

-exp オプションは、エクスポート可能なキー 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、キー 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、Horizon 7 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 Connection Server 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 Connection Server インスタンスを管理する場合は、Connection Server 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 Connection Server 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 Connection Server 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 Connection Server 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、Connection Server 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 Connection Server インスタンスをバックアップする必要があります。Connection Server 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 Connection Server 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 Connection Server にバックアップを適用する必要があります。

Horizon 7 バージョン 7.8 よりも前の Horizon 7 からアップグレードすると、一部のユーザー認証設定が変更されます。これらのユーザー認証設定がユーザー エクスペリエンスに及ぼす影響は、クライアントによって異なります。<https://docs.vmware.com/jp/VMware-Horizon-Client/index.html> にある Horizon Client のマニュアルを参照してください。変更を行う前に、操作性とセキュリティへのユーザー認証設定の影響を理解しておく必要があります。『Horizon 7 のセキュリティ』の「ユーザー認証のセキュリティ関連のサーバ設定」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

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。

- 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『Horizon 7 の管理』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、[セキュリティ サーバとペアになっている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。

アップグレードの完了後、接続サーバを再起動する必要はありません。

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。
[Horizon 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。
- 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、『Horizon 7 の管理』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。
 - a Horizon Administrator にログインします。
 - b [View 構成] - [サーバ] の順に移動し、[接続サーバ] タブをクリックします。
 - c 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。
 - d [OK] をクリックしてサーバの無効化を確定します。
- 2 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。

- 3 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。
- 4 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] の順に移動し、[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。
- 5 [View 構成] - [製品のライセンスと使用状況] の順に移動し、[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。
- 6 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。
- 7 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。
- 8 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。

- 9 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。

- 10 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。

11 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 VDMS 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 TLS 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。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 Connection Server 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。[Horizon 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。『Horizon 7 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、vdmadmin コマンドを使用して削除します。

```
vdmadmin.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。vdmadmin コマンド ライン ツールの詳細については、『Horizon 7 の管理』ドキュメントを参照してください。

結果

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。

結果

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 アプライアンスとセキュリティ サーバの置換](#)を参照してください。

アップグレードのためのセキュリティ 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、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。

- Horizon 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 バランサの設定を記録します。

注： このトピックでは、Horizon 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、[セキュリティ サーバとペアになっている接続サーバのアップグレード](#)を参照してください。

セキュリティ サーバとペアになっている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、接続サーバ インスタンスをアップグレードします。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。[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。
[Horizon 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 認証局 (CA) 署名付き TLS 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。
- 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 サーバとペアにする接続サーバのインスタンスが、セキュリティ サーバをインストールする予定のコンピュータからアクセスできることを確認します。

注： 接続サーバを Horizon 7 バージョン 7.5 にアップグレードした場合、IPsec が無効になっているセキュリティ サーバを再インストールする必要があります。セキュリティ サーバの IP アドレスが変更された場合、再インストールする必要があります。セキュリティ サーバが動的 NAT の背後にある場合、セキュリティ サーバのペアリングが正しく機能しません。

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 Horizon Administrator で、[View 構成] - [サーバ] の順にクリックします。
 - 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 Horizon Administrator の最新バージョンを使用して、セキュリティ サーバのペアリング パスワードを設定します。『Horizon 7 のインストール』の「セキュリティ サーバのペアリング パスワードの設定」を参照してください。

- 5 セキュリティ サーバのホストで、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。

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。

- 6 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。
- 7 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。
- 8 Horizon 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。
- 9 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。
- 10 Horizon Administrator で [View 構成] - [サーバ] - [セキュリティ サーバ] タブの順に移動し、重複したセキュリティ サーバをリストから削除します。

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。

- 11 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。

- 12 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。

- 13 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 VDMS 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 TLS 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。

Unified Access Gateway アプライアンスとセキュリティ サーバの置換

セキュリティ サーバを Unified Access Gateway アプライアンスと置き換えることができます。

前提条件

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。

手順

- 1 セキュリティ サーバ ソフトウェアをアンインストールします。
- 2 セキュリティ サーバの IPsec 設定を削除します。『Horizon 7 のインストール』の「セキュリティ サーバの IPsec ルールの削除」を参照してください。
- 3 セキュリティ サーバの LDAP エントリを削除します。『Horizon 7 の管理』の「-S オプションを使用した接続サーバ インスタンスまたはセキュリティ サーバのエントリの削除」を参照してください。
- 4 Horizon Administrator で、Unified Access Gateway アプライアンスに登録します。
- 5 Unified Access Gateway と接続サーバ間のネットワーク ファイアウォールで、削除されたセキュリティ サーバに関連付けられているファイアウォール ルールを削除し、受信 Unified Access Gateway に関連付けられているファイアウォール ルールを追加します。Unified Access Gateway は、TCP ポート 443 で接続サーバと通信する必要があります。

接続サーバに対するセキュリティ サーバのバックエンド ファイアウォール ルールは次のとおりです。

送信元	デフォルトポート	プロトコル	送信先	デフォルトポート	注
セキュリティサーバ	UDP 500	ISAKMP	接続サーバ	UDP 500	IPsec フェーズ 1 ネゴシエーション。
セキュリティサーバ	UDP 4500	NAT-T	接続サーバ	UDP 4500	NAT を使用する場合のカプセル化された AJP13 トラフィック。
セキュリティサーバ		ESP	接続サーバ		NAT トラバーサルが必要ない場合のカプセル化された AJP13 トラフィック。ESP は IP プロトコル 50 です。ポート番号は指定されていません。
セキュリティサーバ		AJP13	接続サーバ	TCP 8009	IPsec を使用しない AJP13 トラフィックとペアリング時。
セキュリティサーバ		JMS	接続サーバ	TCP 4001	キー ネゴシエーションのメッセージ チャンネル。
セキュリティサーバ		JMS-TLS	接続サーバ	TCP 4002	管理用のメッセージ チャンネル。

6 Unified Access Gateway アプライアンスを設定して起動します。

<https://docs.vmware.com/jp/Unified-Access-Gateway/index.html> にある『VMware Unified Access Gateway の導入および設定』を参照してください。

登録サーバのアップグレード

以前のバージョンの登録サーバがインストールされている仮想マシンで、Connection Server インストーラの最新バージョンを実行して登録サーバをアップグレードできます。また、以前のバージョンの登録サーバをアンインストールして、最新バージョンの Connection Server インストーラを実行し、Horizon 7 登録サーバ オプションを選択して最新バージョンをインストールすることもできます。

登録サーバはステートレスです。True SSO に関連する設定は登録サーバで保持されません。登録サーバが実行され、Connection Server が正常に登録サーバに接続したときに、登録サーバは Connection Server から True SSO の設定を受け取ります。

注： アップグレード後は、ペアリング証明書を Connection Server から登録サーバの Windows 証明書ストアに手動でインポートする必要はありません。以前に手動でインポートしたペアリング証明書は、アンインストールまたはアップグレード プロセスで削除されません。アップグレード後に登録サーバが実行されている場合、Connection Server に正常に接続され、以前にインポートされたペアリング証明書が再利用されます。

クラウド ポッド アーキテクチャ 環境のアップグレード

クラウド ポッド 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。クラウド ポッド 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 クラウド ポッド 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。

クラウド ポッド 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 でのクラウド ポッド アーキテクチャの管理』を参照してください。

Horizon 7 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 Unified Access Gateway などのゲートウェイの背後に存在する接続サーバ 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、『Horizon 7 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 Horizon 7 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、Horizon 7 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、vCenter Server のアップグレード中は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、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、『Horizon 7 の管理』ドキュメントを参照してください。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。

- **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 認証局 (CA) 署名付き TLS 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。
- インスタント クローンの使用中に vCenter Server をアップグレードする場合は、VMware のナレッジベースの記事 <https://kb.vmware.com/s/article/52573> にある手順を参照してください。

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 vSAN データストアが含まれている場合は、『VMware vSAN の管理』で、vSAN クラスタのアップグレードに関する章を参照してください。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 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。

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 TLS 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。

Horizon 7 Server コンポーネントのアップグレードが完了している場合は、次のメンテナンス期間に、Horizon 7 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、[6 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。
- Horizon 7 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 TLS 証明書のサム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 TLS 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。

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 TLS 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。

TLS 証明書の構成の詳細については、『Horizon 7 のインストール』ドキュメントの「View Server の TLS 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。Horizon Administrator で、[View 構成] - [サーバ] の順にクリックし、View Composer サービスに関連付けられた vCenter Server のエントリを編集します。vCenter Server の設定で [編集] をクリックし、プロンプトに従って自己署名証明書を確認して同意します。

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、[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 ポリシー設定用のすべての ADMX ファイルは、VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip に含まれています。x.x.x はバージョン番号、yyyyyyy 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 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

6

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、Horizon 7 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『Horizon 7 の管理』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 Horizon 7 機能について説明します。

表 6-1. 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 [®] vSAN [®] データストア、第 1 バージョン	10 以降	vSphere 5.5 Update 1 以降
VMware vSAN 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 vSAN データストアが含まれている場合は、『VMware vSAN の管理』で、vSAN クラスタのアップグレードに関する章を参照してください。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、および接続サーバ インスタンスなどの Horizon 7 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。

公開デスクトップと仮想デスクトップ のアップグレード

7

公開デスクトップと仮想デスクトップの他に、仮想デスクトップまたは公開されたデスクトップ、Microsoft RDS ホストのオペレーティング システム内で実行されている Horizon Agent をアップグレードします。

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。

- 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
- インスタント クローン デスクトップ プールのアップグレード

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

Horizon 7 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。仮想デスクトップまたは公開デスクトップで RC4、SSLv3、または TLSv1.0 を再び有効にする必要がある場合は、『Horizon 7 のセキュリティ』ドキュメントの「Horizon 7 で無効に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 Horizon 7 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 の要件と考慮事項](#) 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。

結果

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。[3 章 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 にアップデートするには、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 にアップデートしてから 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ます。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 Connection Server インスタンスがすべて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、すべての Connection Server インスタンス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、[6 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。

重要： デスクトップで使用するように設定された Windows Server オペレーティング システムで、アップグレード中に Horizon Agent インストール モードを変更しない場合は、Horizon Agent インストーラで [デスクトップ モード] を選択して続行します。モードを変更する場合は、[RDS モード] を選択し、インストーラの指示に従ってアップグレードを続行します。

- 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。[3 章 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

Horizon 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使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 Horizon 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、[6 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 6-1. 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 仮想マシンで使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使用できる 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。[3 章 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「[8 章 Horizon 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。

インスタント クローン デスクトップ プールのアップグレード

vCenter Server を vSphere 6.7 にアップグレードする場合は、インスタント クローン デスクトップ プールもアップグレードする必要があります。

前提条件

- Horizon 7 バージョン 7.5 以降にアップグレードする場合のシステム要件を満たしていることを確認します。
- [Horizon Connection Server のアップグレード](#)で説明する手順を確認します。
- 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。

- 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。

注： vCenter Server を vSphere 6.7 にアップグレードする場合、クラスタ内のすべてまたは一部の ESXi ホストを vSphere 6.7 にアップグレードする必要があります。この操作を行わないと、インスタント クローン デスクトップ プールが正しくプロビジョニングされません。

- アップグレードする ESXi ホストを確認し、既存のデスクトップ プールに十分なホストがオンライン状態になっていることを確認します。

手順

- 1 Horizon Agent を Horizon 7 バージョン 7.5 以降にアップグレードする親仮想マシンのスナップショットを作成します。このスナップショットは、インスタント クローンのマスター イメージになります。
- 2 クラスタの Storage Distributed Resource Scheduler (DRS) の移行しきい値を 3 に設定します。
- 3 インスタント クローン デスクトップ プールを無効にします。
- 4 vCenter Server を vSphere 6.7 にアップグレードします。
- 5 アップグレードするホストをメンテナンス モードにするには、次のいずれかのオプションを選択します。
 - vSphere Web Client から直接ホストをメンテナンス モードにし、vSphere 6.7 にアップグレードします。アップグレードの完了後、vSphere Web Client でメンテナンス モードを終了します。
 - `icmaint.cmd` ユーティリティで、[ON] オプションを使用して、メンテナンスするホストにマークを設定します。メンテナンス用のホストをマークすると、vCenter Server で親仮想マシンになるマスター イメージが ESXi ホストから削除されます。ホストをメンテナンス モードにして、vSphere 6.7 ESXi にアップグレードします。アップグレードが完了したら、ホストのメンテナンス モードを終了します。次に、`icmaint.cmd` で [OFF] オプションを使用して、メンテナンスしたホストのマークを解除します。

注： デスクトップ プールのプロビジョニングを再開できるように、少なくとも 1 台のホストをアップグレードする必要があります。その後、他のすべてのホストをアップグレードする必要があります。

- 6 インスタント クローン デスクトップ プールを有効にします。
- 7 新しいスナップショットを使用するインスタント クローン デスクトップ プールごとにプッシュイメージ操作を実行します。

プロビジョニングに使用されるのは、vSphere 6.7 ESXi にアップグレードされたホストだけです。プッシュイメージの操作中に作成されたインスタント クローンが、vSphere 6.7 がない他のホストに移動する場合があります。

- 8 クラスタ内のすべてのホストが vSphere 6.7 にアップグレードされていることを確認します。
- 9 親仮想マシンを、前のバージョンから ESXi 6.7 以降 と互換性のあるバージョン（バージョン 14 の仮想マシン）にアップグレードする場合は、親仮想マシンで VMware Tools をアップグレードします。親仮想マシンの新しいスナップショットを作成します。これは、インスタント クローンのマスター イメージになります。次に、このマスター イメージの以前のバージョンを使用しているすべてのインスタント クローン デスクトップ プールにプッシュイメージ操作を実行する必要があります。

- 10 分散仮想スイッチ (vDS) をアップグレードする場合は、親仮想マシンをパワーオン状態にして、ネットワークに問題がないことを確認します。vDS のアップグレードをアップグレードしたら、新しい親仮想マシンのスナップショットを作成し、すべてのインスタント クローン デスクトップ プールでプッシュ イメージ操作を実行する必要があります。

Horizon 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

8

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、Horizon 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、『Horizon 7 の管理』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 vSAN 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 以降では、Horizon 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、Horizon 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 Horizon 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。『Horizon 7 の管理』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、Horizon 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。

Horizon 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、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、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 Horizon Connection Server インスタンス、セキュリティ サーバ、および Horizon 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 Horizon Administrator で、[View 構成] - [グローバル設定] の順に移動して、[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接続サーバ ホストの VMware Horizon Message Bus コンポーネント サービスを手動で再起動するか、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、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 Horizon Administrator で進行状況を監視するには、[View 構成] - [グローバル設定] の順に移動します。
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。

結果

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 vSAN 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 プールの再構成に関わるので、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 vSphere5.1 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 vSphere5.1（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-UseSeSparseFormat] 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 vSAN 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 vSAN 機能を使用できます。

vSAN 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、Horizon 7 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 vSAN 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-vSAN データストアから vSAN データストアへのアップグレード

VMware vSAN 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-vSAN データストアから vSAN 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 vSAN 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いることと、それらが vSAN 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 vSAN 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、[6 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。vSAN の要件とアップグレードの詳細については、『VMware vSAN の管理』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 vSAN 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-vSAN 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、Horizon 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-vSAN データベースから vSAN 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、Horizon Administrator の [ヘルプ] ボタンをクリックして確認してください。

vSAN disk format 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、vSAN 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 vSAN 機能には、vSphere 5.5 Update 1 の機能と比較してパフォーマンスが大きく向上しているため、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 vSAN データストアのデスクトップ プールがある場合の vSAN 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 vSAN データストアが使用されていない場合、[non-vSAN データストアから vSAN 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 vSAN 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 vSAN 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。vSAN 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、[vSAN 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
```

- vSAN アップグレード プロセスについて理解しておきます。<https://docs.vmware.com/jp/VMware-vSAN/index.html> にある『VMware vSAN の管理』で、vSAN のアップグレードに関する章を参照してください。

手順

- 1 vSphere 6.0 ドキュメント センターで利用可能な『VMware vSAN の管理』ドキュメントの vSAN クラスターのアップグレードに関する章に従って、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 vSAN disk format 1 を使用しており、仮想マシンと VMware Tools はまだ vSphere 6.0 仮想ハードウェア バージョン 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 vSAN 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 vSAN disk format 1 を使用しています。

- 3 vSAN 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 vSAN の管理』のアップグレードに関する章のトピック「vSAN 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://docs.vmware.com/jp/VMware-vSAN/index.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ーの全 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 vSAN 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 vSAN 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 vSAN 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。

結果

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

vSAN 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、vSAN 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、Horizon 7 5.3.x によって vSAN 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、Horizon 7 5.3.x からアップグレードする場合、プールが vSAN 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にされません。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、Horizon 7 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-vSAN 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 vSAN 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 vSAN データストアを使用して、Horizon 7 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。VMware vSphere 5.5 以前のクラスタの vSAN 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。

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。VMware vSphere 6.0 以降のリリースで利用可能な vSAN 機能には、vSphere 5.5 Update 1 の機能と比較してパフォーマンスが大きく向上しているため、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。

アップグレードの詳細については、[6 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。vSAN の要件とアップグレードの詳細については、『VMware vSAN の管理』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 vSAN データストアから non-vSAN 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-vSAN 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-vSAN データストアから vSAN 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

vSAN 1 ではなく vSAN 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、[vSAN disk format 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

Horizon Client ダウンロード用のアイコン、HTML Access 経由でリモート デスクトップに接続するアイコン、その他のリンクを表示したり、非表示にするように、VMware Horizon Web ポータル ページを設定できます。

デフォルトでは、VMware HorizonWeb ポータル ページに、Horizon Client のダウンロード/インストールを行うアイコンと、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。portal-links-html-access.properties ファイルで定義されているデフォルト値により、VMware Horizon Web ポータル ページに表示されるダウンロード リンクが決まります。

VMware Horizon Web ポータル ページに社内の Web サーバへのリンクを表示したり、サーバで特定のクライアント バージョンを使用できるようにしたい場合もあります。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 VMware Horizon Web ポータル ページを再設定できます。このファイルが使用できないか空白で、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 ディレクトリ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/
pckbpdplfajmgaip1jfamclkinbjdnma
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定義できます。たとえば、macOS システムから VMware Horizon Web ポータル ページを参照すると、Horizon Client for Mac インストーラのリンクが表示されます。Windows または Linux クライアントの場合は、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。

手順

- 1 Connection Server ホストで、テキスト エディタを使用して *CommonAppDataFolder*\VMware\VDM\portal\portal-links-html-access.properties ディレクトリの portal-links-html-access.properties ファイルを開きます。

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します。

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。

2 構成プロパティを編集します。

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。

オプション	プロパティ設定
HTML Access を無効にする	<code>enable.webclient=false</code> 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 Connection Server 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。」
Horizon Client のダウンロードを無効にする	<code>enable.download=false</code> 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 Connection Server 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。」
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	<code>link.download=https://url-of-web-server</code> 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。

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 data-bbox="635 226 1425 348">以下に示すのは完全 URL の例です。インストーラ ファイルを Connection Server ホストの C:\Program Files\VMware\VMware View\Server\broker\webapps\ ディレクトリの downloads ディレクトリに配置する場合は、次の手順の説明のように相対 URL を使用できます。</p> <ul style="list-style-type: none"> <li data-bbox="635 359 1425 457">■ 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 : <div data-bbox="671 415 1425 457">link.download=https://<i>server</i>/downloads</div> <li data-bbox="635 468 1425 600">■ 32 ビット Windows インストーラ : <div data-bbox="671 527 1425 600">link.win32=https://<i>server</i>/downloads/VMware-Horizon-Client-x86-build#.exe</div> <li data-bbox="635 611 1425 743">■ 64 ビット Windows インストーラ : <div data-bbox="671 669 1425 743">link.win64=https://<i>server</i>/downloads/VMware-Horizon-Client-x86_64-build#.exe</div> <li data-bbox="635 753 1425 873">■ Windows Phone インストーラ : <div data-bbox="671 812 1425 873">link.winmobile=https://<i>server</i>/downloads/VMware-Horizon-Client-build#.appx</div> <li data-bbox="635 884 1425 1016">■ 32 ビット Linux インストーラ : <div data-bbox="671 942 1425 1016">link.linux32=https://<i>server</i>/downloads/VMware-Horizon-Client-build#.x86.bundle</div> <li data-bbox="635 1026 1425 1159">■ 64 ビット Linux インストーラ : <div data-bbox="671 1085 1425 1159">link.linux64=https://<i>server</i>/downloads/VMware-Horizon-Client-build#.x64.bundle</div> <li data-bbox="635 1169 1425 1289">■ Mac OS X インストーラ : <div data-bbox="671 1228 1425 1289">link.mac=https://<i>server</i>/downloads/VMware-Horizon-Client-build#.dmg</div> <li data-bbox="635 1299 1425 1432">■ iOS インストーラ: <div data-bbox="671 1358 1425 1432">link.ios=https://<i>server</i>/downloads/VMware-Horizon-Client-iPhoneOS-build#.ipa</div> <li data-bbox="635 1442 1425 1562">■ Android インストーラ : <div data-bbox="671 1501 1425 1562">link.android=https://<i>server</i>/downloads/VMware-Horizon-Client-AndroidOS-build#.apk</div> <li data-bbox="635 1572 1425 1705">■ Chrome OS インストーラ : <div data-bbox="671 1631 1425 1705">link.chromeos=https://<i>server</i>/downloads/VMware-Horizon-Client-ChromeOS-build#.apk</div>
ログイン ページの [ヘルプ] リンクの URL を変更します。	<div data-bbox="635 1728 1425 1749">link.help</div> <p data-bbox="635 1759 1425 1812">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、Connection Server 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` という形式の相対 URL を使用できます。

- 4 Horizon Web コンポーネント サービスを再起動します。

Horizon 7 環境における vSphere コンポーネントの個別アップグレード

9

Horizon 7 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 Horizon 7 データをバックアップし、一部の Horizon 7 ソフトウェアを再インストールする必要があります。

Horizon 7 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 Horizon 7 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。

Horizon 7 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、Horizon Connection Server インスタンスから Horizon LDAP データベースをバックアップします。

手順については、『Horizon 7 の管理』ドキュメントを参照してください。レプリカ グループ内に接続サーバー 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のみ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 Horizon 7 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。