Horizon 7 の管理

2018 年 9 月 6 日
VMware Horizon 7 7.6

vmware®

最新の技術ドキュメントは VMware の Web サイト（https://docs.vmware.com/jp/）にあります
このドキュメントに関するご意見およびご感想がある場合は、docfeedback@vmware.com までお送りください。

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

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

目次

Horizon 7 管理

『Horizon 7 の管理』では、Horizon Administrator での Horizon 接続サーバの構成、管理者の作成、ユーザー認証の設定、ポリシーの構成、VMware ThinApp® アプリケーションの管理方法など、VMware Horizon® 7 を構成および管理する方法について説明します。また、Horizon 7 コンポーネントを保守およびトラブルシューティングする方法についても説明します。

対象読者

本書に記載されている情報は、VMware Horizon 7 を構成および管理するすべての方を対象としています。本書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 Windows または Linux システム管理者向けに書かれています。

1 Horizon Administrator の使用

Horizon Administrator は、View 接続サーバを構成し、リモート デスクトップおよびアプリケーションを管理するための Web インターフェイスです。

Horizon Administrator、コマンドレット、および `vdmadmin` で実行できる操作の比較については、『Horizon 7 の統合』 ドキュメントを参照してください。

この章では次のトピックについて説明します。

Horizon Administrator と Horizon 接続サーバ

Horizon Administrator では Horizon 7 の Web ベースの管理インターフェイスが提供されます。

Horizon 接続サーバは、レプリカ サーバまたはセキュリティ サーバとして機能する複数のインスタンスを持つことができます。Horizon 7 の展開環境によっては、接続サーバの各インスタンスで Horizon Administrator インターフェイスを使用できます。

接続サーバで Horizon Administrator を使用する場合、次のベスト プラクティスを使用します。

- 接続サーバのホスト名と IP アドレスを使用して、Horizon Administrator にログインします。Horizon Administrator インターフェイスを使用して、接続サーバおよび関連するセキュリティ サーバやレプリカ サーバを管理します。
- ポッド環境では、すべての管理者が同じ接続サーバのホスト名と IP アドレスを使用して Horizon Administrator にログインしていることを確認します。ロード バランサのホスト名と IP アドレスを使用して、Horizon Administrator の Web ページにアクセスしないでください。

注　セキュリティ サーバではなく、Unified Access Gateway アプライアンスを使用する場合は、Unified Access Gateway REST API を使用して Unified Access Gateway アプライアンスを管理する必要があります。Unified Access Gateway の以前のバージョンには、Access Point という名前が付けられます。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。

Horizon Administrator へのログイン

初期設定タスクを実行するには、Horizon Administrator にログインする必要があります。Horizon Administrator には、安全な接続 (TLS) を使用してアクセスします。

開始する前に

- Horizon 接続サーバが専用コンピュータにインストールされていることを確認します。
- Horizon Administrator でサポートされている Web ブラウザを使用していることを確認します。Horizon Administrator の要件については、『Horizon 7 のインストール』 ドキュメントを参照してください。

手順

1 Web ブラウザを開き、次の URL を入力します。<server> は、接続サーバ インスタンスのホスト名です。

`https://<server>/admin`

注 ホスト名が解決できないときに接続サーバ インスタンスにアクセスする必要がある場合は、IP アドレスを使用できます。ただし、通信するホストは、接続サーバ インスタンスに対して構成された TLS 証明書に一致しないため、アクセスがブロックされたりアクセスのセキュリティが低下したりします。

Horizon Administrator へのアクセスは、接続サーバ コンピュータで構成されている証明書のタイプによって異なります。

接続サーバ ホストで Web ブラウザを開く場合、**`https://localhost`** ではなく、**`https://127.0.0.1`** を使用して接続します。この方法で `localhost` 解決における潜在的な DNS 攻撃を回避することにより、セキュリティが向上します。

オプション	説明
View 接続サーバ用に CA によって署名された証明書を構成しています。	最初に接続するときに、Web ブラウザで Horizon Administrator が表示されます。
View 接続サーバによって提供されたデフォルトの自己署名証明書が構成されます。	最初に接続したときに、Web ブラウザによって、アドレスに関連付けられているセキュリティ証明書が、信頼された証明機関から発行されていないことを警告するページが表示される場合があります。 [無視] をクリックして、現在の TLS 証明書の使用を続けます。

2 管理者ロールを持つアカウントを使用してログインします。

スタンドアローンの接続サーバ インスタンス、または複製されたグループにおける最初の接続サーバ インスタンスをインストールするときに、管理者ロールの初期割り当てを行います。デフォルトでは、接続サーバのインストールに使用するアカウントが選択されていますが、このアカウントを Administrators ローカル グループまたはドメイン グローバル グループに変更できます。

Administrators ローカル グループを選択した場合は、このグループに追加されたドメイン ユーザーを直接またはグループ メンバーシップ経由で使用できます。このグループに追加されたローカル ユーザーは使用できません。

Horizon Administrator にログインした後、[View 構成] - [管理者] を使用して、管理者ロールを持つユーザーおよびグループのリストを変更できます。

Horizon Administrator インターフェイスの使用のヒント

Horizon Administrator のユーザー インターフェイス機能を使用すると、Horizon ページ内を移動したり、Horizon オブジェクトの検索、フィルタ処理、および並べ替えを行うことができます。

Horizon Administrator には、多くの一般的なユーザー インターフェイス機能があります。たとえば、各ページの左側のナビゲーション ペインから、Horizon Administrator のその他のページに直接移動できます。検索フィルタでは、検索対象のオブジェクトに関連するフィルタ条件を選択できます。

次の表に、Horizon Administrator の使用に役立つ別の機能を示します。

表 1-1. Horizon Administrator のナビゲーションおよび表示機能

Horizon Administrator の機能	説明
Horizon Administrator ページで前および次に移動	以前表示した Horizon Administrator ページに戻るには、ブラウザの [戻る] ボタンをクリックします。現在のページに戻るには、[進む] ボタンをクリックします。 Horizon Administrator ウィザードまたはダイアログ ボックスの使用中にブラウザの [戻る] ボタンをクリックすると、Horizon Administrator のメイン ページに戻ります。ウィザードまたはダイアログに入力した情報は失われます。 View 5.1 より前のバージョンでは、ブラウザの [戻る] ボタンや [進む] ボタンを使用して Horizon Administrator 内を移動できません。ナビゲーションのため、Horizon Administrator ウィンドウ内に独自の [戻る] ボタンと [進む] ボタンがありました。これらのボタンは View 5.1 リリースで削除されました。
Horizon Administrator ページのブックマーク	ブラウザで Horizon Administrator ページをブックマークできます。
複数列の並べ替え	複数列の並べ替えを使用して、さまざまな方法で Horizon オブジェクトを並べ替えることができます。 Horizon Administrator の表の一番上の行にある見出しをクリックして、その見出しに基づいて Horizon オブジェクトをアルファベット順に並べ替えます。 たとえば [リソース] - [マシン] ページの順に移動して [デスクトップ プール] をクリックすると、デスクトップを含むプールに基づいてデスクトップを並べ替えることができます。 [1] が見出しの隣に表示されます。これはその列が一次的な並べ替え列であることを示します。見出しを再びクリックすると、並べ替え順序を逆にすることができます。並べ替え順序は、上または下矢印によって示されます。 二次的な項目によって Horizon オブジェクトを並べ替えるには、Ctrl キーを押しながら別の見出しをクリックします。 たとえば、マシン表では、[ユーザー] をクリックして、デスクトップが割り当てられたユーザーに基づいて二次的な並べ替えを実行できます。二次的な見出しの隣には [2] が表示されます。この例では、デスクトップはプールによって並べ替えられ、各プール内ではユーザーによって並べ替えられます。 Ctrl キーを押しながら続けてクリックすると、表内のすべての列を重要性の高い順に並べ替えることができます。 並べ替え項目の選択を解除するには、Ctrl + Shift キーを押しながらクリックします。 たとえば、特定の状態で、特定のデータソースに保存されている、プール内のデスクトップを表示できます。[リソース] - [マシン] の順に選択して、[データストア] 見出しをクリックし、Ctrl キーを押しながら [ステータス] 見出しをクリックすることができます。

表 1-1. Horizon Administrator のナビゲーションおよび表示機能 (続き)

Horizon Administrator の機能	説明
表の列のカスタマイズ	選択した列を非表示にしたり、最初の列をロックするなど、Horizon Administrator の表の列の表示をカスタマイズできます。この機能を使用すると、[カタログ] - [デスクトップ プール] の順に移動して、多くの列を含む大きな表の表示を管理できます。 列のヘッダを右クリックすると、次のアクションを実行できるコンテキスト メニューが表示されます。 ■ 選択した列を非表示。 ■ 列をカスタマイズ。ダイアログに表内のすべての列が表示されます。表示または非表示にする列を選択できます。 ■ 最初の列をロック。このオプションにより、多くの列を含む表を横にスクロールするときに、左側の列が表示されたままになります。たとえば、[カタログ] - [デスクトップ プール] ページの順に移動して、横にスクロールして他のデスクトップの特性を表示するときに、デスクトップ ID は表示されたままになります。
Horizon オブジェクトの選択および Horizon オブジェクトの詳細の表示	Horizon オブジェクトが表示される Horizon Administrator の表で、オブジェクトを選択したり、オブジェクトの詳細を表示したりできます。 ■ オブジェクトを選択するには、表のオブジェクトの行内をクリックします。ページの上部にある、オブジェクトを管理するメニューとコマンドがアクティブになります。 ■ オブジェクトの詳細を表示するには、オブジェクトの行の左セルをダブルクリックします。新しいページに、オブジェクトの詳細が表示されます。 たとえば、[カタログ] - [デスクトップ プール] ページの順に移動して個々のプールの行内をクリックすると、プールに関連するコマンドが有効になります。 左の列の [ID] セルをダブルクリックすると、プールに関する詳細を含む新しいページが表示されます。
詳細表示のためのダイアログ ボックスの展開	Horizon Administrator ダイアログ ボックスを展開して、表の列にデスクトップ名やユーザー名などの詳細を表示できます。 ダイアログ ボックスを展開するには、ダイアログ ボックスの右下隅のドットの上にマウスを置き、角をドラッグします。
Horizon オブジェクトのコンテキスト メニューの表示	Horizon Administrator の表で Horizon オブジェクトを右クリックして、コンテキスト メニューを表示できます。コンテキスト メニューから、選択した Horizon オブジェクトで動作するコマンドにアクセスできます。 たとえば、[カタログ] - [デスクトップ プール] ページの順に移動して、デスクトップ プールを右クリックして、[追加]、[編集]、[削除]、[プロビジョニングを無効（有効）にする] などのコマンドを表示できます。

Horizon Administrator でのテキスト表示のトラブルシューティング

Web ブラウザが Windows 以外のオペレーティング システム（Linux、UNIX、Mac OS など）で実行されている場合、Horizon Administrator でテキストが正しく表示されません。

問題

Horizon Administrator インターフェイスのテキストが正しく表示されません。たとえば、単語の中央にスペースが表示されます。

原因

Horizon Administrator には、Microsoft 固有のフォントが必要です。

解決方法

コンピュータに Microsoft 固有のフォントをインストールします。

現在、Microsoft の Web サイトでは Microsoft フォントが配布されていませんが、独立系の Web サイトからダウンロードできます。

Horizon 接続サーバの構成

2

Horizon 接続サーバをインストールし初期構成を実行後、vCenter Server インスタンスおよび View Composer サービスを Horizon 7 環境に追加し、管理者責任を委任するためのロールを設定して、構成データのバックアップをスケジューリングできます。

この章では次のトピックについて説明します。

vCenter Server および View Composer の構成

仮想マシンをリモート デスクトップとして使用するには、vCenter Server と通信するように View を構成する必要があります。リンク クローン デスクトップ プールを作成および管理するには、Horizon Administrator で View Composer 設定を構成する必要があります。

Horizon 7 用のストレージも構成できます。ESXi ホストに対して、リンク クローン仮想マシンでディスク容量を再利用するように構成できます。ESXi ホストで仮想マシンのデータをキャッシュできるようにするには、vCenter Server の View Storage Accelerator を有効にする必要があります。

View Composer AD 操作のユーザー アカウントの作成

View Composer を使用する場合、View Composer が Active Directory で特定の操作を実行できるようになるユーザー アカウントを、Active Directory で作成する必要があります。View Composer では、リンク クローン仮想マシンを Active Directory ドメインに参加させるためにこのアカウントが必要です。

セキュリティのため、View Composer で使用するためのユーザー アカウントを別に作成する必要があります。別のアカウントを作成することで、他の目的のために定義されている追加権限がアカウントに付与されないようにすることができます。このアカウントには、指定された Active Directory コンテナ内のコンピュータ オブジェクトを追加および削除するために必要な最小限の権限を付与できます。たとえば、View Composer アカウントにはドメイン管理者権限は必要ありません。

手順

1 Active Directory で、接続サーバ ホストと同じドメインまたは信頼されたドメインにユーザー アカウントを作成します。

2 リンク クローン コンピュータ アカウントを中に作成する、またはリンク クローン コンピュータ アカウントを移動する先の Active Directory コンテナで、[コンピュータ オブジェクトの作成] 権限、[コンピュータ オブジェクトの削除] 権限、および [すべてのプロパティの書き込み] 権限をアカウントに追加します。

次のリストでは、ユーザー アカウントに必要なすべての権限を示します。デフォルトで割り当てられる権限も含まれます。

- 内容の一覧表示
- すべてのプロパティの読み取り
- すべてのプロパティの書き込み
- アクセス許可の読み取り
- パスワードのリセット
- コンピュータ オブジェクトの作成
- コンピュータ オブジェクトの削除

注 デスクトップ プールの[Allow reuse of pre-existing computer accounts]設定を選択する場合、必要な権限はより少なくなります。次の権限がユーザー アカウントに割り当てられていることを確認します。

- 内容の一覧表示
- すべてのプロパティの読み取り
- アクセス許可の読み取り
- パスワードのリセット

3 ユーザー アカウントの権限が Active Directory コンテナおよびコンテナのすべての子オブジェクトに適用されることを確認します。

次に進む前に

[vCenter Server を追加] ウィザードで View Composer ドメインを構成時、およびリンク クローン デスクトップ プールを構成して展開する際に、Horizon Administrator でこのアカウントを指定します。

vCenter Server インスタンスの Horizon 7 への追加

Horizon 7 環境内の vCenter Server インスタンスに接続するように、Horizon 7 を構成する必要があります。Horizon 7 がデスクトップ プールで使用する仮想マシンは、vCenter Server が作成し、管理します。

vCenter Server インスタンスをリンク モード グループ内で実行する場合は、各 vCenter Server インスタンスを個別に Horizon 7 に追加する必要があります。

Horizon 7 は、安全なチャネル (SSL) を使用して vCenter Server インスタンスに接続します。

開始する前に

- 接続サーバの製品ライセンス キーをインストールします。
- Horizon 7 をサポートするのに必要な vCenter Server で、操作を実行する権限のある vCenter Server ユーザーを準備します。View Composer を使用するには、このユーザーに権限を追加する必要があります。

  Horizon 7 のための vCenter Server ユーザーの構成の詳細については、『Horizon 7 のインストール』ドキュメントを参照してください。
- TLS/SSL サーバ証明書が vCenter Server ホストにインストールされていることを確認します。本番環境で、信頼された証明機関 (CA) によって署名された有効な証明書をインストールします。

  テスト環境では、vCenter Server でインストールされたデフォルト証明書を使用できますが、vCenter Server を Horizon 7 に追加する際に証明書サムプリントを受け入れる必要があります。
- 複製されたグループ内のすべての接続サーバ インスタンスが、vCenter Server ホストにインストールされているサーバ証明書のルート CA 証明書を信頼していることを確認します。ルート CA 証明書が、接続サーバ ホスト上の Windows ローカル コンピュータの証明書ストア内の [信頼されたルート証明機関] - [証明書] フォルダにあるかどうか確認します。このフォルダにない場合、ルート CA 証明書を Windows ローカル コンピュータの証明書ストアにインポートします。

  『Horizon 7 のインストール』ドキュメントの「ルート証明書と中間証明書を Windows 証明書ストアにインポートする」を参照してください。
- vCenter Server インスタンスに ESXi ホストが含まれていることを確認します。vCenter Server インスタンスでホストが構成されていない場合、そのインスタンスを Horizon 7 に追加することはできません。
- vSphere 5.5 以降のリリースにアップグレードする場合、vCenter Server ユーザーとして使用するドメイン管理者アカウントが、vCenter Server のローカル ユーザーによって vCenter Server にログインするために明示的に指定された権限であったことを確認してください。
- Horizon 7 で FIPS モードを使用する予定の場合は、vCenter Server 6.0 以降および ESXi 6.0 以降のホストを使用していることを確認してください。

  詳細については、『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。
- vCenter Server と View Composer の操作数の上限を決定する設定について理解しておきます。「「vCenter Server と View Composer の同時操作の制限」および「リモート デスクトップ ログオン ストームをサポートするための同時電源操作レートの設定」」を参照してください。

手順

1 Horizon Administrator で、[View 構成] - [サーバ] を選択します。

2 [vCenter Servers] タブで、[追加] をクリックします。

3 [vCenter Server 設定] の [サーバ アドレス] テキスト ボックスに、vCenter Server インスタンスの完全修飾ドメイン名 (FQDN) を入力します。

FQDN にはホスト名とドメイン名が含まれます。たとえば、FQDN の **<myserverhost>.<companydomain>.com** で、 **<myserverhost>** はホスト名で、**<companydomain>.com** はドメインです。

注 DNS 名または URL を使用してサーバを入力すると、Horizon 7 は管理者が以前に IP アドレスを使用して Horizon 7 にこのサーバを追加したかどうかを確認する DNS 検索を実行しません。vCenter Server をその DNS 名と IP アドレスの両方で追加すると、競合が発生します。

4 vCenter Server ユーザーの名前を入力します。

例：**domain\user** または **user@domain.com**

5 vCenter Server ユーザーのパスワードを入力します。

6 (オプション) この vCenter Server インスタンスの説明を入力します。

7 TCP のポート番号を入力します。

デフォルトのポートは 443 です。

8 [詳細設定] で、vCenter Server と View Composer の同時操作の制限を設定します。

9 [次へ] をクリックして [View Composer 設定] ページを表示します。

次に進む前に

View Composer 設定を構成します。

- vCenter Server インスタンスが署名された SSL 証明書で構成されていて、接続サーバがルート証明書を信頼している場合、[vCenter Server を追加] ウィザードで [View Composer 設定] ページが表示されます。
- vCenter Server インスタンスがデフォルト証明書で構成されている場合、最初に既存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。「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 で複数の vCenter Server インスタンスを使用している場合、この手順を繰り返してその他の vCenter Server インスタンスを追加します。

View Composer 設定を構成する

View Composer を使用するには、Horizon 7 に VMware Horizon View Composer サービスへの接続を許可する設定を構成する必要があります。View Composer は個別のホストにインストールすることも、vCenter Server と同じホストにインストールすることもできます。

それぞれの VMware Horizon View Composer サービスと vCenter Server インスタンスが 1 対 1 で対応している必要があります。1 つの View Composer サービスは 1 つの vCenter Server インスタンスのみと一緒に作動できます。1 つの vCenter Server インスタンスは 1 つの VMware Horizon View Composer サービスにのみ関連付けることができます。

初期の Horizon 7 展開後に、Horizon 7 展開の規模拡大または変化に対応するために、VMware Horizon View Composer サービスを新しいホストに移行できます。初期の View Composer 設定は Horizon Administrator で編集できますが、確実に移行を成功させるためには追加の手順を実行する必要があります。「別のマシンへの View Composer の移行」を参照してください。

開始する前に

- リンク クローンを含む Active Directory ドメインに仮想マシンを追加したり、ドメインから仮想マシンを削除したりするための権限を付与されたユーザーが Active Directory に作成されていることを確認します。「View Composer AD 操作のユーザー アカウントの作成」を参照してください。
- vCenter Server に接続するように Horizon 7 を構成したことを確認します。そのためには、[vCenter Server を追加] ウィザードで [vCenter Server の情報] ページを完了する必要があります。「vCenter Server インスタンスの Horizon 7 への追加」を参照してください。
- この VMware Horizon View Composer サービスがまだ別の vCenter Server インスタンスに接続するように構成されていないことを確認します。

手順

1 Horizon Administrator で、[vCenter Server を追加] ウィザードで [vCenter Server の情報] ページを完了します。

   a [View 構成] - [サーバ] を選択します。

   b [vCenter Servers] タブで、[追加] をクリックして vCenter Server 設定を指定します。

2 [View Composer 設定] ページで、View Composer を使用していない場合、[View Composer を使用しない] を選択します。

   [View Composer を使用しない] を選択した場合、その他の View Composer 設定が非アクティブになります。[次へ] をクリックすると、[vCenter Server を追加] ウィザードで [ストレージ設定] ページが表示されます。[View Composer ドメイン] ページは表示されません。

3 View Composer を使用している場合、View Composer ホストの場所を選択します。

オプション	説明
View Composer が vCenter Server と同じホストにインストールされます。	a [View Composer を vCenter Server と一緒にインストール] を選択します。 b ポート番号が vCenter Server に VMware Horizon View Composer サービスをインストールしたときに指定したポートと同じであることを確認します。デフォルトのポート番号は 18443 です。
View Composer が個別のホストにインストールされます。	a [スタンドアロン View Composer Server] を選択します。 b View Composer Server アドレスのテキスト ボックスに、View Composer ホストの完全修飾ドメイン名 (FQDN) を入力します。 c View Composer ユーザーの名前を入力します。 例：**`domain.com\user`** または **`user@domain.com`** d View Composer ユーザーのパスワードを入力します。 e ポート番号が VMware Horizon View Composer サービスをインストールしたときに指定したポートと同じであることを確認します。デフォルトのポート番号は 18443 です。

4 [次へ] をクリックして [View Composer ドメイン] ページを表示します。

次に進む前に

View Composer ドメインを構成します。

- View Composer インスタンスが署名された TLS 証明書で構成されていて、接続サーバがルート証明書を信頼している場合、[vCenter Server を追加] ウィザードで [View Composer ドメイン] ページが表示されます。
- View Composer インスタンスがデフォルト証明書で構成されている場合、最初に既存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。「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。

View Composer ドメインを構成する

View Composer がリンク クローン デスクトップを展開する Active Directory ドメインを構成する必要があります。View Composer 用に複数のドメインを構成できます。最初に vCenter Server と View Composer の設定を View に追加した後で、Horizon Administrator で vCenter Server インスタンスを編集することでさらに View Composer ドメインを追加できます。

開始する前に

- Active Directory 管理者は、AD 操作に必要な View Composer ユーザーを作成する必要があります。このドメイン ユーザーには、リンク クローンを含んでいる Active Directory ドメインから仮想マシンを追加または削除する権限が必要です。このユーザーに必要な権限の詳細については、「View Composer AD 操作のユーザー アカウントの作成」 を参照してください。
- Horizon Administrator で、[vCenter Server を追加] ウィザードで [vCenter Server の情報] ページと [View Composer 設定] ページを完了していることを確認します。

手順

1 [View Composer ドメイン] ページで、[追加] をクリックして、AD 操作に必要な View Composer ユーザーのアカウント情報を追加します。

2 Active Directory ドメインのドメイン名を入力します。

例：**`domain.com`**

3 View Composer ユーザーの（ドメイン名を含む）ドメイン ユーザー名を入力します。

例：**`domain.com\admin`**

4 アカウントのパスワードを入力します。

5 [OK] をクリックします。

6 リンク クローン プールを展開する他の Active Directory ドメインでの権限を持つドメイン ユーザー アカウントを追加するには、前記の手順を繰り返します。

7 [次へ] をクリックして [ストレージ設定] ページを表示します。

次に進む前に

仮想マシンのディスク領域再利用を有効にして、Horizon 7 用に View Storage Accelerator を構成します。

vSphere でリンク クローン仮想マシンのディスク領域を再利用できるようにする

vSphere 5.1 以降では、Horizon 7 用にディスク容量再利用機能を有効にできます。vSphere 5.1 からは、Horizon 7 がリンク クローン仮想マシンを効率的なディスク形式で作成するようになりました。これにより、ESXi ホストはリンク クローン内で使用されていないディスク容量を再利用できるようになり、リンク クローンに必要なストレージ容量の合計を削減できます。

ユーザーがリンク クローン デスクトップを操作するたびに、クローンの OS ディスクが大きくなり、最終的には完全クローン デスクトップとほとんど同じディスク領域を使用する場合もあります。ディスク領域再利用により、リンク クローンを更新または再構成しなくても、OS ディスクのサイズを減らすことができます。仮想マシンがパワーオンされ、ユーザーがリモート デスクトップを操作している間に、領域を再利用することができます。

ディスク領域再利用は、ログオフ時の更新などのストレージ節約戦略を利用できない展開にとって特に便利です。たとえば、ユーザー アプリケーションを専用リモート デスクトップにインストールするナレッジ ワーカの場合、リモート デスクトップが更新または再構成されたときに、個人用アプリケーションが失われることがあります。Horizon 7 はディスク領域再利用により、最初にプロビジョニングされたときの小さなサイズとほぼ同じサイズにリンク クローンを保つことができます。

この機能には、効率的なディスク フォーマットとスペース再利用操作の 2 つのコンポーネントがあります。

vSphere 5.1 以降の環境では、親の仮想マシンが仮想ハードウェア バージョン 9 以降の場合、Horizon 7 は領域再利用操作が有効になっているかどうかにかかわらず、領域効率の高い OS ディスクでリンク クローンを作成します。

容量再利用操作を有効にするには、Horizon Administrator を使用して vCenter Server 用の容量再利用を有効にして、個別のデスクトップ プール用に仮想マシンのディスク容量を再利用する必要があります。vCenter Server 用の領域再利用設定には、vCenter Server インスタンスによって管理されるすべてのデスクトップ プールでこの機能を無効にするためのオプションがあります。vCenter Server 用にこの機能を無効にすると、デスクトップ プール レベルの設定が上書きされます。

以下のガイドラインは、領域再利用機能に適用されます。

- リンク クローン内の領域効率の高い OS ディスクでのみ使用できます。
- これは、View Composer 通常ディスクには影響しません。
- vSphere 5.1 以降、および仮想ハードウェア バージョン 9 以降の仮想マシンのみで機能します。
- 完全クローン デスクトップでは使用できません。
- SCSI コントローラを備えた仮想マシンで使用できます。IDE コントローラはサポートされていません。

ネイティブ NFS スナップショット テクノロジー（VAAI）は、領域効率の高いディスクが使用されている仮想マシンを含むプールでサポートされていません。

開始する前に

- vCenter Server および ESXi ホストについて、クラスタにすべての ESXi ホストが含まれ、ダウンロード パッチ ESXi510-201212001 以降を適用済みの ESXi 5.1 以降が搭載されたバージョン 5.1 であることを確認します。

手順

1 Horizon Administrator で、[ストレージ設定] ページの前に表示される [vCenter Server を追加] ウィザード ページを完了します。

   a [View 構成] - [サーバ] の順に選択します。

   b [vCenter Servers] タブで、[追加] をクリックします。

   c [vCenter Server の情報] ページ、[View Composer 設定] ページ、[View Composer ドメイン] ページを完了します。

2 [ストレージ設定] ページで、[領域再利用を有効にする] が選択されていることを確認します。

   Horizon 7 5.2 以降の新規インストールを実行している場合は、領域再利用がデフォルトで選択されています。You must select if you are upgrading to Horizon 7 5.1 以前のリリースから Horizon 7 5.2 以降にアップグレードしている場合は、[領域再利用を有効にする] を選択する必要があります。

次に進む前に

[ストレージ設定] ページで、View Storage Accelerator を構成します。

Horizon 7 でディスク領域再利用の構成を終了するには、デスクトップ プール用の領域再利用をセットアップします。

vCenter Server 用に View Storage Accelerator を構成する

vSphere 5.1 以降では、仮想マシンのディスク データをキャッシュするよう ESXi ホストを構成できます。この View Storage Accelerator と呼ばれている機能は、ESXi ホストで Content Based Read Cache（CBRC）機能を使用します。多くの仮想マシンが起動しているかウイルス対策スキャンが一度に実行される場合に I/O ストームが発生することがありますが、View Storage Accelerator により、I/O ストーム時の Horizon 7 のパフォーマンスが向上します。この機能は、管理者またはユーザーがアプリケーションまたはデータを頻繁にロードする場合にも役立ちます。ホストは、OS 全体またはアプリケーションをストレージ システムから何度も読み取るのではなく、共通のデータ ブロックをキャッシュから読み取ることができます。

ブート ストーム中の IOPS 数を減らすことにより、View Storage Accelerator によるストレージ アレイの要求が抑えられ、これにより Horizon 7 展開をサポートするためのストレージ I/O バンド幅が小さくなります。

この手順で説明しているように、Horizon Administrator の vCenter Server ウィザードで View Storage Accelerator 設定を選択することで、ESXi ホストでのキャッシュ機能を有効にします。

View Storage Accelerator がそれぞれのデスクトップ プール用にも構成されていることを確認します。デスクトップ プールで操作するには、View Storage Accelerator を vCenter Server とそれぞれのデスクトップ プールで有効にする必要があります。

View Storage Accelerator は、デフォルトでデスクトップ プール用に有効になっています。この機能は、プールを作成または編集するときに無効または有効に設定できます。デスクトップ プールを初めて作成するときにこの機能を有効にすることをお勧めします。既存のプールを編集してこの機能を有効にする場合は、リンク クローンをプロビジョニングする前に、新しいレプリカとそのダイジェスト ディスクが作成されていることを確認する必要があります。新しいレプリカは、プールを新しいスナップショットに再構成するか、プールを新しいデータストアに再分散することによって作成できます。ダイジェスト ファイルは、デスクトップ プール内の仮想マシンがパワーオフされているときにのみ構成できます。

リンク クローンを含むデスクトップ プールと、フル仮想マシンを含むプールで View Storage Accelerator を有効にすることができます。

ネイティブ NFS スナップショット テクノロジー (VAAI) は、View Storage Accelerator 用に有効にされているプールでサポートされていません。

View Storage Accelerator は、Horizon 7 レプリカ階層を使用する構成で機能するようになり、レプリカはリンク クローンでなく別のデータストアに保存されます。Horizon 7 レプリカ階層で View Storage Accelerator を使用するパフォーマンスの利点は実質的には大きくありませんが、特定の容量に関わる利点は別のデータストアにレプリカを保存することによって実現できる場合があります。したがって、この組み合わせがテストおよびサポートされます。

重要　この機能を使用する計画であり、いくつかの ESXi ホストを共有する複数の View ポッドを使用している場合は、共有 ESXi ホストのすべてのプールについて View Storage Accelerator 機能を有効にする必要があります。複数ポッドの設定に一貫性がない場合は、共有 ESXi ホストの仮想マシンが不安定になることがあります。

開始する前に

- vCenter Server ホストおよび ESXi ホストのバージョンが 5.1 以降であることを確認します。

  ESXi クラスタで、すべてのホストのバージョンが 5.1 以降であることを確認します。

- vCenter Server の **[ホスト] > [構成] > [詳細] 設定**の権限が vCenter Server ユーザに割り当てられていることを確認します。

  『Horizon 7 のインストール』ドキュメントで、vCenter Server ユーザーに必要な Horizon 7 および View Composer の権限について説明しているトピックを参照してください。

手順

1 Horizon Administrator で、[ストレージ設定] ページの前に表示される [vCenter Server を追加] ウィザード ページを完了します。

   a [View 構成] - [サーバ] の順に選択します。

   b [vCenter Servers] タブで、[追加] をクリックします。

   c [vCenter Server の情報] ページ、[View Composer 設定] ページ、[View Composer ドメイン] ページを完了します。

2 [ストレージ設定] ページで、[View Storage Accelerator を有効にする] 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。

   デフォルトでは、このチェック ボックスはオンになっています。

3 デフォルトのホスト キャッシュ サイズを指定します。

   デフォルトのキャッシュ サイズは、この vCenter Server インスタンスで管理されるすべての ESXi ホストに適用されます。

   デフォルト値は 1,024 MB です。キャッシュ サイズは、100 MB ～ 2,048 MB の範囲でなければなりません。

4 個別の ESXi ホスト向けに別のキャッシュ サイズを指定するには、ESXi ホストを選択して、[キャッシュ サイズの編集] をクリックします。

   a [ホスト キャッシュ] ダイアログ ボックスで、[デフォルトのホスト キャッシュ サイズを上書き] のチェックボックスをオンにします。

   b [ホスト キャッシュ サイズ] の値を 100 MB ～ 2,048 MB の範囲で入力し、[OK] をクリックします。

5 [ストレージ設定] ページで、[次へ] をクリックします。

6 [終了] をクリックして、vCenter Server、View Composer、ストレージ設定を Horizon 7 に追加します。

次に進む前に

クライアント セッションおよび接続用の設定を構成します。「クライアント セッションの構成」を参照してください。

Horizon 7 で View Storage Accelerator 設定を完了するには、デスクトップ プール用に View Storage Accelerator を構成します。『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントの「デスクトップ プール用に View Storage Accelerator を構成する」を参照してください。

vCenter Server と View Composer の同時操作の制限

vCenter Server を Horizon 7 に追加する場合、または vCenter Server 設定を編集する場合には、vCenter Server と View Composer で実行される同時操作の最大数を設定するオプションをいくつか構成できます。

これらのオプションは、[vCenter Server の情報] ページの [詳細設定] パネルで構成します。

表 2-1. vCenter Server と View Composer の同時操作の制限

設定	説明
[最大同時 vCenter プロビジョニング操作数]	接続サーバがこの vCenter Server インスタンスでフル仮想マシンのプロビジョニングと削除のために出すことができる同時要求の最大数を指定します。 デフォルト値は 20 です。 この設定はフル仮想マシンにのみ適用されます。
[最大同時電源操作数]	この vCenter Server インスタンス内の接続サーバによって管理されている仮想マシンで同時に実行できる電源操作（起動、シャットダウン、サスペンドなど）の最大数を決定します。 デフォルト値は 50 です。 この設定の値を計算するためのガイドラインについては、「リモート デスクトップ ログオン ストームをサポートするための同時電源操作レートの設定」を参照してください。 この設定は、フル仮想マシンとリンク クローンに適用されます。

表 2-1. vCenter Server と View Composer の同時操作の制限 (続き)

設定	説明
[最大同時 View Composer メンテナンス操作数]	この View Composer インスタンスによって管理されているリンク クローンで同時に実行できる、View Composer の更新、再構成、再分散などの操作の最大数を決定します。 デフォルト値は 12 です。 メンテナンス操作を開始する前に、アクティブなセッションが存在するリモート デスクトップからログオフする必要があります。メンテナンス操作の開始直後にユーザーを強制的にログオフさせた場合、ログオフが必要なリモート デスクトップ上の同時操作の最大数は、構成値の半分になります。たとえば、この設定を 24 に構成して、ユーザーを強制的にログオフさせた場合、ログオフが必要なリモート デスクトップ上の同時操作の最大数は 12 です。 この設定はリンク クローンにのみ適用されます。
[最大同時 View Composer プロビジョン操作数]	この View Composer インスタンスによって管理されているリンク クローンで同時に実行できる作成および削除操作の最大数を指定します。 デフォルト値は 8 です。 この設定はリンク クローンにのみ適用されます。

リモート デスクトップ ログオン ストームをサポートするための同時電源操作レートの設定

[最大同時電源操作数] 設定は、vCenter Server インスタンスのリモート デスクトップ仮想マシンで使用可能な同時電源操作の最大数を制御します。この最大数はデフォルトで 50 に設定されています。この値は、多くのユーザーが同時にデスクトップにログインするときのピーク時パワーオン率をサポートするように変更できます。

ベスト プラクティスとして、この設定の適切な値を判断するためにパイロット段階を実施できます。プラニングのガイドラインについては、『Horizon 7 アーキテクチャの計画』ドキュメントの「アーキテクチャ設計の要素と計画のガイドライン」を参照してください。

必要な同時電源操作の数は、デスクトップがパワーオンになるピーク率と、デスクトップがパワーオンになり、起動し、接続可能になるのに要する時間に基づきます。一般的に、推奨される電源操作の最大数は、デスクトップの開始に要した合計時間にピーク時パワーオン率を掛け合わせたものです。

たとえば、平均的なデスクトップは起動に 2 ～ 3 分要します。したがって、同時電源操作の最大数はピーク時パワーオン率の 3 倍にする必要があります。デフォルト設定の 50 は、毎分 16 台のデスクトップのピーク時パワーオン率をサポートできることを見込んでいます。

システムは、デスクトップが起動するまで最大 5 分待機します。起動にこれ以上の時間を要すると、他のエラーが発生する可能性があります。万一に備えて、同時電源操作の最大数をピーク時パワーオン率の 5 倍に設定できます。控えめに考えて、デフォルト設定の 50 は、毎分 10 台のデスクトップのピーク時パワーオン率をサポートします。

ログオン、つまりデスクトップのパワーオン操作は、通常、特定の時間範囲で正規分散されて行われます。時間範囲の中間にパワーオン操作が発生し、パワーオン操作の 40% が時間範囲の 6 分の 1 で発生すると仮定して、ピーク時パワーオン率を概算することができます。たとえば、ユーザーが午前 8:00 から午前 9:00 の間にログオンすると、時間範囲は 1 時間であり、ログオンの 40% は午前 8:25 から午前 8:35 までの 10 分間に発生します。ユーザーが 2,000 人いる場合、そのうち 20% がデスクトップをパワーオフしており、400 台のデスクトップのパワーオン操作の 40% がこの 10 分間に発生することになります。ピーク時パワーオン率は、毎分 16 台のデスクトップになります。

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 からの vCenter Server インスタンスの削除

Horizon 7 と vCenter Server インスタンス間の接続を削除できます。これを行うと、Horizon 7 は、vCenter Server インスタンスで作成された仮想マシンを管理しなくなります。

開始する前に

vCenter Server インスタンスに関連付けられているすべての仮想マシンを削除します。仮想マシンの削除の詳細については、『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントで「デスクトップ プールの削除」を参照してください。

手順

1 Horizon Administrator で、[View 構成] - [サーバ] の順にクリックします。

2 [vCenter Server] タブで、vCenter Server インスタンスを選択します。

3 [削除] をクリックします。

Horizon 7 がこの vCenter Server インスタンスによって管理される仮想マシンにアクセスできなくなることを警告するダイアログが表示されます。

4 [OK] をクリックします。

Horizon 7 は、vCenter Server インスタンスで作成された仮想マシンにアクセスできなくなります。

Horizon 7 からの View Composer の削除

vCenter Server インスタンスに関連付けられている VMware Horizon View Composer サービスと Horizon 7 との接続を削除できます。

View Composer への接続を無効にする前に、View Composer によって作成されたすべてのリンク クローン仮想マシンを Horizon 7 から削除する必要があります。Horizon 7 では、関連付けられたリンク クローンが残っている場合は、View Composer を削除できません。View Composer への接続を無効にすると、Horizon 7 で新しいリンク クローンをプロビジョニングまたは管理できなくなります。

手順

1 View Composer によって作成されたリンク クローン デスクトップ プールを削除します。

   a Horizon Administrator で、[カタログ] - [デスクトップ プール] の順に選択します。

   b リンク クローン デスクトップ プールを選択して、[削除] をクリックします。

   リンク クローン デスクトップ プールが Horizon 7 から完全に削除されることを警告するダイアログ ボックスが表示されます。リンク クローン仮想マシンがパーシステント ディスクを使用して構成されている場合、パーシステント ディスクを切断または削除できます。

   c [OK] をクリックします。

   仮想マシンが vCenter Server から削除されます。さらに、関連付けられた View Composer データベース エントリおよび View Composer によって作成されたレプリカも削除されます。

   d View Composer によって作成された各リンク クローン デスクトップ プールに対して、これらの手順を繰り返します。

2 [View 構成] - [サーバ] を選択します。

3 [vCenter Server] タブで、View Composer が関連付けられている vCenter Server インスタンスを選択します。

4 [編集] をクリックします。

5 [View Composer Server 設定] で [編集] をクリックし、[View Composer を使用しない] を選択して [OK] をクリックします。

この vCenter Server インスタンスでリンク クローン デスクトップ プールを作成することはできなくなりますが、vCenter Server インスタンスでフル仮想マシン デスクトップ プールの作成と管理を引き続き行うことができます。

次に進む前に

別のホストに View Composer をインストールし、Horizon 7 を再構成して新しい VMware Horizon View Composer サービスに接続する場合は、特定の追加手順を実行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」を参照してください。

競合している vCenter Server の一意の ID

環境内に複数の vCenter Server インスタンスが構成されている場合は、新しいインスタンスを追加しようとすると、一意の ID が競合しているために失敗することがあります。

問題

Horizon 7 に vCenter Server インスタンスを追加しようとしていますが、新しい vCenter Server インスタンスの一意の ID が既存のインスタンスと競合しています。

原因

2 つの vCenter Server インスタンスが同じ一意の ID を使用することはできません。vCenter Server の一意の ID は、デフォルトではランダムに生成されますが、編集できます。

解決方法

1 vSphere Client で、[管理] - [vCenter Server 設定] - [ランタイムの設定] をクリックします。

2 新しい一意の ID を入力し、[OK] をクリックします。

vCenter Server の一意の ID 値を編集する方法の詳細については、vSphere のドキュメントを参照してください。

Horizon 接続サーバのバックアップ

Horizon 接続サーバの初期構成が完了したら、Horizon 7 と View Composer の構成データの定期的なバックアップをスケジュール設定する必要があります。

Horizon 7 構成のバックアップと復元については、「Horizon 7 構成データのバックアップと復元」を参照してください。

クライアント セッションの構成

接続サーバ インスタンスまたは複製されたグループによって管理されるクライアント セッションおよび接続に影響を与えるグローバル設定を指定できます。セッション タイムアウトの長さを設定したり、ログイン前メッセージや警告メッセージを表示したり、セキュリティ関連のクライアント接続オプションを設定したりすることができます。

クライアント セッションおよび接続のオプションの設定

グローバル設定を構成して、クライアント セッションおよび接続の動作方法を決定します。

グローバル設定は、単一の接続サーバ インスタンスに固有ではありません。スタンドアローン接続サーバ インスタンスまたは複製されたインスタンスのグループによって管理されるすべてのクライアント セッションに影響します。

また、Horizon クライアントとリモート デスクトップの間でトンネリングされていない直接接続を使用するように接続サーバ インスタンスを構成することもできます。直接接続の構成方法については、「セキュアなトンネルと PCoIP Secure Gateway を構成する」を参照してください。

開始する前に

グローバル設定について理解しておきます。「クライアント セッションのグローバル設定」および「クライアント セッションおよび接続のグローバル セキュリティ設定」を参照してください。

手順

1 Horizon Administrator で、[View 構成] - [グローバル設定] の順に選択します。

2 全般設定またはセキュリティ設定のどちらを構成するかを選びます。

オプション	説明
全般的なグローバル設定	[全般] ペインで、[編集] をクリックします。
グローバル セキュリティ設定	[セキュリティ] ペインで、[編集] をクリックします。

3 グローバル設定を構成します。

4 [OK] をクリックします。

次に進む前に

インストール中に指定したデータ リカバリ パスワードを変更できます。「Data Recovery パスワードを変更する」を参照してください。

Data Recovery パスワードを変更する

接続サーバ バージョン 5.1 以降をインストールするときに、データ リカバリ パスワードを指定します。インストール後、このパスワードは View Administrator で変更できます。パスワードは、View LDAP 構成をバックアップから復元する場合に必要です。

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。安全なパスワードの生成に関する組織のベスト プラクティスに従ってください。

手順

1 Horizon Administrator で、[View 構成] - [グローバル設定] の順に選択します。

2 [セキュリティ] ペインで、[データ リカバリのパスワードを変更] をクリックします。

3 新しいパスワードを 2 回入力します。

4 (オプション) パスワードを忘れた場合のヒントを入力します。

注 データ リカバリのパスワードは、Horizon 7 構成データがバックアップされるようにスケジュールを設定する際にも変更できます。「Horizon 7 構成バックアップのスケジュール」を参照してください。

次に進む前に

`vdmimport` ユーティリティを使用してバックアップの Horizon 7 構成を復元する際には、この新しいパスワードを指定します。

クライアント セッションのグローバル設定

全般的なグローバル設定により、セッション タイムアウトの長さ、SSO の有効性およびタイムアウト制限、Horizon Administrator でのステータス更新、ログイン前メッセージと警告メッセージが表示されるかどうか、Horizon Administrator が Windows Server をリモート デスクトップ用にサポートされるオペレーティング システムとして扱うかどうか、およびその他の設定が決定されます。

以下の表の設定の変更はただちに有効になります。Horizon 7 接続サーバまたは Horizon Client の再起動は不要です。

表 2-2. クライアント セッションの全般的なグローバル設定

設定	説明
[View Administrator セッション タイムアウト]	セッションがタイムアウトする前にアイドル状態の Horizon Administrator セッションがどれだけ続くかを決定します。 重要 Horizon Administrator セッション タイムアウトを長い分数に設定すると、Horizon Administrator が不正に使用されるリスクが増します。アイドル状態のセッションを長時間許可する場合は用心してください。 デフォルトでは、Horizon Administrator セッション タイムアウトは 30 分です。セッション タイムアウトは 1 分から 4320 分（72 時間）の間で設定できます。
[ユーザーの強制切断]	ユーザーが Horizon 7 にログインしてから指定した時間（分）が経過すると、すべてのデスクトップとアプリケーションが切断されます。すべてのデスクトップとアプリケーションは、ユーザーがそれらをいつ開いたかにかかわらず同時に切断されます。 アプリケーションのリモート処理をサポートしないクライアントでは、この設定の値が [なし] または 1200 分よりも長い場合、最大タイムアウト値である 1200 分が適用されます。 デフォルトは、[600 分後] です。
[シングル サインオン (SSO)]	SSO が有効な場合、Horizon 7 にはユーザーの認証情報がキャッシュされるため、ユーザーは Windows リモート セッションにログインするための認証情報を指定せずにリモート デスクトップまたはアプリケーションを起動できます。デフォルトは [有効化] です Horizon 7 以降で導入されている True SSO 機能を使用する場合は、SSO を有効にする必要があります。True SSO では、ユーザーが Active Directory 認証情報以外の認証形式を使用してログインする場合、ユーザーが VMware Identity Manager にログインした後に、キャッシュされた認証情報ではなく短期間の証明書が True SSO 機能によって生成されます。 注 デスクトップが Horizon Client から起動し、セキュリティ ポリシーに基づきユーザーまたは Windows のいずれかによりロックされた場合、デスクトップで Horizon 7 Agent 6.0 以降または Horizon Agent 7.0 以降が実行されている場合は、Horizon 7 接続サーバはユーザーの SSO 認証情報を破棄します。ユーザーはログイン認証情報を指定して新しいデスクトップまたは新しいアプリケーションを起動するか、または切断されたデスクトップまたはアプリケーションに再接続する必要があります。SSO を再度有効にするには、Horizon 7 接続サーバから切断するか、または Horizon Client を終了し、Horizon 7 接続サーバに再接続する必要があります。ただし、デスクトップが Workspace ONE または VMware Identity Manager から起動してロックされている場合、SSO 認証情報は破棄されません。

表 2-2. クライアント セッションの全般的なグローバル設定 (続き)

設定	説明
[アプリケーションをサポートするクライアント。] [ユーザーがキーボードとマウスを使用しなくなった場合に、アプリケーションを切断し、SSO 認証情報を破棄する：]	クライアント デバイスで、キーボードやマウスが使用されなくなった場合にアプリケーション セッションを保護します。[経過時間...分] に設定した場合、指定された時間（分）ユーザーのアクティビティがないと、Horizon 7 により、すべてのアプリケーションが切断され、SSO 認証情報は破棄されます。デスクトップ セッションは切断されません。ユーザーは、再度ログインして切断されたアプリケーションに再接続するか、新しいデスクトップまたはアプリケーションを起動する必要があります。 この設定は True SSO 機能にも適用されます。SSO 認証情報が破棄されると、ユーザーは Active Directory 認証情報の入力を求められます。ユーザーが Active Directory 認証情報を使用せずに VMware Identity Manager にログイン済みで、入力すべき Active Directory 認証情報がわからない場合は、ログアウトしてから VMware Identity Manager にログインし直してリモート デスクトップとアプリケーションにアクセスできます。 重要　アプリケーションとデスクトップの両方が開いて、タイムアウトによりアプリケーションが切断されている場合でも、デスクトップは接続されたままになることを認識しておく必要があります。ユーザーはデスクトップの保護のためにこのタイムアウトに依存することがないようにしてください。 [なし] に設定すると、ユーザーのアクティビティがなくても、Horizon 7 によるアプリケーションの切断や SSO 認証情報の破棄は行われません。 デフォルトは [なし] です。
[その他のクライアント。] [SSO 認証情報の破棄：]	指定した時間（分）が経過すると、SSO 認証情報は破棄されます。この設定は、アプリケーションのリモート処理をサポートしていないクライアント用です。[経過時間...分] に設定した場合、クライアント デバイスでのユーザー アクティビティにかかわらず、Horizon 7 へログイン後指定時間（分）が経過したら、ユーザーはデスクトップへ再度ログインしてデスクトップに接続する必要があります。 [なし] に設定すると、ユーザーが Horizon Client を閉じるまで、または [ユーザーの強制切断] タイムアウトに達するまで、このどちらが先であっても、Horizon 7 は SSO 認証情報を保存します。 デフォルトは、[15 分後] です。
[ステータスの自動更新を有効にする]	ステータスの更新が、Horizon Administrator の左上隅にあるグローバル ステータス ペインに数分ごとに表示されるかどうかを指定します。また、Horizon Administrator のダッシュボード ページも数分ごとに更新されます。 デフォルトでは、この設定は有効になっていません。
[ログイン前メッセージを表示する]	Horizon Client ユーザーがログインしたときに免責事項または別のメッセージを表示します。 [グローバル設定] ダイアログ ボックスのテキスト ボックスに情報または指示を入力します。 メッセージを表示しない場合は、チェック ボックスをオフのままにします。
[強制的にログオフする前に警告を表示する]	スケジュール設定された更新や、デスクトップの更新操作などの即座の更新が開始されようとしているためにユーザーが強制的にログオフされる場合、警告メッセージを表示します。この設定では、警告を表示してからユーザーがログオフするまでの待機時間も指定します。 警告メッセージを表示するにはチェック ボックスをオンにします。 警告を表示してからユーザーがログオフするまでの待機時間を分単位で入力します。デフォルトは 5 分です。 警告メッセージを入力します。次のデフォルト メッセージを使用できます。 **お使いのデスクトップは、重要なアップデートがスケジュールされているため、5 分後にシャットダウンされます。保存していない作業を今すぐ保存してください。**

表 2-2. クライアント セッションの全般的なグローバル設定 (続き)

設定	説明
[Windows Server デスクトップを有効にする]	デスクトップとして使用できる Windows Server 2008 R2 および Windows Server 2012 R2 マシンを選択できるかどうかを指定します。この設定が有効な場合、Horizon Administrator では、Horizon 7 Server コンポーネントがインストールされているマシンを含む、使用可能なすべての Windows Server マシンが表示されます。 注 Horizon Agent ソフトウェアは、セキュリティ サーバ、Horizon 7 接続サーバ、Horizon 7 Composer を含む他の Horizon 7 Server ソフトウェア コンポーネントと同じ仮想マシンまたは物理マシンにインストールすることはできません。
[HTML Access のタブを閉じるときに認証情報をクリーンアップする]	リモート デスクトップやアプリケーションに接続するタブや、HTML Access クライアントのデスクトップとアプリケーションの選択ページに接続するタブをユーザーが閉じるときに、キャッシュからユーザーの認証情報を削除します。 この設定が有効である場合、Horizon 7 は、次の HTML Access クライアントのシナリオにおいても認証情報をキャッシュから削除します。 ■ ユーザーが、デスクトップおよびアプリケーションの選択ページやリモート セッション ページを更新する。 ■ サーバから自己署名証明書が提示されており、ユーザーがリモート デスクトップやアプリケーションを起動し、セキュリティの警告が表示されるときにユーザーがその証明書を受け入れる。 ■ リモート セッションが含まれるタブで URI コマンドをユーザーが実行する。 この設定が無効である場合、証明書はキャッシュに残ります。デフォルトでは、この機能は無効になっています。 注 この機能は、Horizon 7 バージョン 7.0.2 以降で利用できます。
[Mirage サーバの構成]	Miragemirage://**server-name<:>port<>** **または** mirages://**server-name<:>port<>** **という形式で** サーバの URL を指定できるようにします。(<server-name> は完全修飾ドメイン名)。ポート番号を指定しないと、デフォルトのポート番号 8000 が使用されます。 注 デスクトップ プール設定に Mirage サーバを指定することで、このグローバル設定をオーバーライドできます。 Mirage クライアントのインストール時に Mirage サーバを指定する代わりに、Horizon Administrator で Mirage サーバを指定することもできます。Horizon Administrator での Mirage サーバの指定をサポートしているのはどの Mirage バージョンかを確認するには、https://www.vmware.com/support/pubs/mirage_pubs.html で公開されている Mirage ドキュメントを参照してください。

表 2-2. クライアント セッションの全般的なグローバル設定 (続き)

設定	説明
[クライアントのユーザー インターフェイスでサーバ情報を非表示]	このセキュリティ設定を有効にして、Horizon Client 4.4 以降でサーバの URL 情報を非表示にします。
[クライアントのユーザー インターフェイスでドメイン リストを非表示]	このセキュリティ設定を有効にして、Horizon Client 4.4 以降で [ドメイン] ドロップダウン メニューを非表示にします。 [クライアントのユーザー インターフェイスでドメイン リストを非表示] グローバル設定が有効になっている接続サーバにユーザーがログインすると、ドメイン ドロップダウン メニューが Horizon Client で非表示になり、ユーザーはドメイン情報を Horizon Client の [ユーザー名] テキスト ボックスに指定する必要があります。たとえば、ユーザー名を `domain\username` または `username@domain` の形式で入力する必要があります。 重要 [クライアントのユーザー インターフェイスでサーバ情報を非表示] および [クライアントのユーザー インターフェイスでドメイン リストを非表示] 設定を有効にしており、接続サーバ インスタンスで 2 要素認証 (RSA SecureID または RADIUS) を選択している場合、Windows ユーザー名の一致を強制しないでください。Windows ユーザー名の一致を強制すると、ユーザーは、ユーザー名のテキスト ボックスにドメイン情報を入力できなくなり、ログインが常に失敗します。詳細については、『Horizon 7 の管理』の 2 要素認証についてのトピックを参照してください。

クライアント セッションおよび接続のグローバル セキュリティ設定

グローバル セキュリティ設定によって、割り込み後にクライアントを再認証するかどうか、メッセージ セキュリティ モードを有効にするかどうか、セキュリティ サーバ接続に IPSec を使用するかどうかが決定されます。

Horizon 7 に対するすべての Horizon Client 接続および Horizon Administrator 接続には、TLS が必要です。Horizon 7 の展開でロード バランサまたはその他のクライアントが接続する中間サーバが使用されている場合、TLS をそれらにオフロードしてから、それぞれの接続サーバ インスタンスおよびセキュリティ サーバで非 TLS 接続を構成できます。「TLS 接続の中間サーバへのオフロード」を参照してください。

表 2-3. クライアント セッションおよび接続のグローバル セキュリティ設定

設定	説明
[ネットワークへの割り込み後に安全なトンネル接続を再認証する]	Horizon Client がリモート デスクトップへの安全なトンネル接続を使用する場合、ネットワークへの割り込み後にユーザー認証情報を再認証する必要があるかどうかを指定します。 この設定を選択すると、安全なトンネル接続に割り込みが入った場合に、Horizon Client では再接続する前にユーザーの再認証が必要になります。 この設定により、セキュリティが強化されます。たとえば、ラップトップが盗まれて別のネットワークに移動された場合、認証情報を入力しなければ、ユーザーはリモート デスクトップに自動的にアクセスできません。 この設定を選択しない場合は、クライアントがリモート デスクトップに再接続するときに、ユーザーの再認証を要求しません。 安全なトンネルが使用されていない場合、この設定は効果がありません。
[メッセージ セキュリティ モード]	コンポーネント間で JMS メッセージを送信するために使用されるセキュリティ メカニズムを指定します。 ■ モードが [有効] に設定されている場合、Horizon 7 コンポーネント間で渡される JMS メッセージの署名と検証が行われます。 ■ モードが [拡張済み] に設定されている場合、相互認証された TLS でセキュリティが提供されます。JMS 接続とアクセスは JMS トピックで制御されます。 詳細については、「Horizon 7 コンポーネントのメッセージ セキュリティ モード」を参照してください。 新規インストールの場合、メッセージ セキュリティ モードはデフォルトで [拡張済み] に設定されています。前のバージョンからアップグレードする場合は、前のバージョンで使用されていた設定が維持されます。
[拡張セキュリティのステータス]（読み取り専用）	[メッセージ セキュリティ モード] が [有効] から [拡張済み] に変更された場合に表示される読み取り専用フィールド。変更は段階的に行われるため、このフィールドにはフェーズを通じた進捗が表示されます。 ■ [MessageBus の再起動待機中] が最初のフェーズです。この状態は、手動でポッド内のすべての接続サーバ インスタンスを再起動するか、ポッド内のすべての接続サーバ ホストの VMware Horizon Message Bus Component サービスを再起動するまで、表示されます。 ■ 次の段階は [拡張の保留] です。すべての Horizon Message Bus コンポーネント サービスが再起動されると、すべてのデスクトップ サーバおよびセキュリティ サーバに対して、システムはメッセージ セキュリティ モードを [拡張済み] に変更する処理を開始します。 ■ 最後の段階は [拡張済み] であり、すべてのコンポーネントが [拡張済み] メッセージ セキュリティ モードを使用するようになったことを示します。 `vdmutil` コマンド ライン ユーティリティを使用して進捗を監視することもできます。「vdmutil ユーティリティを使用した JMS メッセージ セキュリティ モードの構成」を参照してください。
[セキュリティ サーバの接続に IPSec を使用]	セキュリティ サーバと接続サーバ インスタンス間の接続に Internet Protocol Security (IPsec) を使用するかどうかを決定します。 デフォルトでは、セキュリティ サーバ接続に対して安全な接続（IPSec を使用）が有効になっています。

注　以前の Horizon 7 リリースから View 5.1 以降にアップグレードした場合は、グローバル設定 [クライアント接続に SSL が必要] が Horizon Administrator に表示されます。ただしアップグレード前に Horizon 7 構成でこの設定が無効になっている場合に限ります。TLS は Horizon 7 へのすべての Horizon Client 接続および Horizon Administrator 接続に必要であるため、この設定は Horizon 7 5.1 以降のバージョンの新規インストールには表示されません。またこの設定が以前の Horizon 7 構成で既に有効になっている場合は、アップグレード後にこの設定が表示されることはありません。

アップグレード後、[クライアント接続に SSL が必要] 設定を有効にしない場合、Horizon Client からの HTTPS 接続は失敗します。ただし HTTP を使用して前方接続を行うように構成された中間デバイスに接続する場合は、この限りではありません。「TLS 接続の中間サーバへのオフロード」を参照してください。

Horizon 7 コンポーネントのメッセージ セキュリティ モード

メッセージ セキュリティ モードを設定して、JMS メッセージが Horizon 7 コンポーネント間を通過するときに使用されるセキュリティ メカニズムを指定できます。

次の表に、メッセージ セキュリティ モードを構成する場合に選択できるオプションを示します。オプションを設定するには、グローバル設定ダイアログ ウィンドウの [メッセージ セキュリティ モード] リストから選択します。

表 2-4. メッセージ セキュリティ モードのオプション

オプション	説明
[無効]	メッセージ セキュリティ モードを無効にします。
[混在]	メッセージ セキュリティ モードは有効ですが、実行されません。 このモードを使用して、Horizon 7 環境内の Horizon 7 3.0 よりも前のコンポーネントを検出できます。接続サーバによって生成されるログ ファイルには、これらのコンポーネントへの参照が含まれています。この設定は推奨されません。アップグレードする必要のあるコンポーネントを検出する場合にのみ、この設定を使用してください。
[有効]	メッセージ署名と暗号化の組み合わせを使用して、メッセージ セキュリティ モードが有効になります。署名がないか無効な場合、あるいは署名された後でメッセージが変更された場合、JMS メッセージは拒否されます。 JMS メッセージの中には、認証情報などの機密情報を含むために暗号化されるものもあります。[有効] 設定を使用すると、IPsec を使用して、接続サーバ インスタンス間、および接続サーバ インスタンスとセキュリティ サーバ間のすべての JMS メッセージを暗号化することもできます。 注　Horizon 7 バージョン 3.0 よりも前のコンポーネントは、その他の Horizon 7 コンポーネントと通信することはできません。
[拡張済み]	すべての JMS 接続に SSL が使用されます。JMS アクセス制御も有効になっているため、デスクトップ、セキュリティ サーバ、および接続サーバ インスタンスは特定のトピックに関する JMS のみを送受信できます。 Horizon 6 バージョン 6.1 よりも前の Horizon 7 コンポーネントは、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。 注　このモードを使用するには、DMZ ベースのセキュリティ サーバと、それらとペアになっている接続サーバ インスタンスの間で TCP ポート 4002 が開かれている必要があります。

Horizon 7 をシステムに初めてインストールしたときのメッセージ セキュリティ モードは、[拡張済み] に設定されています。前のリリースから Horizon 7 をアップグレードしても、メッセージ セキュリティ モードは既存の設定のまま変更されません。

重要　アップグレードされた Horizon 7 環境を [有効] から [拡張済み] に変更する場合は、最初にすべての接続サーバ インスタンス、セキュリティ サーバ、および Horizon 7 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する必要があります。設定を [拡張済み] に変更した後、新しい設定が段階的に実行されます。

1　手動でポッド内のすべての接続サーバ ホストの VMware Horizon View Message Bus コンポーネント サービスを手動で再起動するか、接続サーバ インスタンスを再起動する必要があります。

2　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。

3　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。

または、**vdmutil** コマンド ライン ユーティリティを使用して進捗を監視することもできます。「vdmutil ユーティリティを使用した JMS メッセージ セキュリティ モードの構成」を参照してください。

Horizon 6 バージョン 6.1 よりも前の Horizon 7 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。

アクティブな Horizon 7 環境を [無効化] から [有効化] に変更する場合や、[有効化] から [無効化] に変更する場合は、しばらく [混在] モードにしてから、最終的なモードに変更します。たとえば、現在のモードが [無効化] の場合に、1 日だけ [混在] モードに変更してから、[有効化] に変更します。[混在] モードの場合は、メッセージに署名が添付されますが、検証されません。このため、メッセージ モードの変更を環境全体に伝達できます。

vdmutil ユーティリティを使用した JMS メッセージ セキュリティ モードの構成

vdmutil コマンドライン インターフェイスを使用し、JMS メッセージが Horizon 7 コンポーネント間で渡されるときに使用されるセキュリティ メカニズムを構成し、管理できます。

ユーティリティの構文と場所

vdmutil コマンドで、以前のバージョンの Horizon 7 に同梱されていた **lmvutil** コマンドと同じ処理を実行できます。また、**vdmutil** コマンドには、使用するメッセージ セキュリティ モードの決定やすべての Horizon 7 コンポーネントを拡張モードに変更する処理の進行状況の監視を行うオプションがあります。Windows コマンド プロンプトで、次の形式の **vdmutil** コマンドを使用します。

```
vdmutil <command_option> [<additional_option argument>] ...
```

使用できる追加のオプションは、コマンド オプションによって異なります。このトピックでは、メッセージ セキュリティ モードのオプションについて説明します。クラウド ポッド アーキテクチャに関係するその他のオプションについては、『Horizon 7 でのクラウド ポッド アーキテクチャの管理』ドキュメントを参照してください。

デフォルトの場合、**vdmutil** コマンドの実行可能ファイルのパスは **C:\Program Files\VMware\VMware View\Server\tools\bin** です。コマンド ラインにパスを入力するのを避けるには、PATH 環境変数にパスを追加します。

認証

管理者ロールを持つユーザーとしてコマンドを実行する必要があります。Horizon Administrator を使用して管理者ロールをユーザーに割り当てることができます。第 6 章「ロールベースの委任管理の構成」を参照してください。

vdmutil コマンドには、認証に使用するユーザー名、ドメイン、およびパスワードを指定するオプションがあります。

表 2-5. vdmutil コマンド認証オプション

オプション	説明
--authAs	Horizon 7 管理ユーザーの名前。<domain\username> またはユーザー プリンシパル名 (UPN) 形式を使用しないでください。
--authDomain	Horizon 7 オプションで指定された **--authAs** 管理者ユーザーの完全修飾ドメイン名。
--authPassword	Horizon 7 オプションで指定された **--authAs** 管理者ユーザーのパスワード。パスワードの代わりに **"*"** を入力すると、**vdmutil** コマンドでパスワードが要求され、機密性の高いパスワードはコマンド ラインのコマンド履歴に残りません。

認証オプションは、**--help** および **--verbose** を除くすべての **vdmutil** コマンド オプションを指定して使用する必要があります。

JMS メッセージ セキュリティ モード専用のオプション

次の表は、**vdmutil** の JMS メッセージ セキュリティ モードを表示、設定、または監視するコマンドライン オプションのみを一覧で示しています。特定のオプションで使用可能な引数のリストについては、**--help** コマンドライン オプションを使用してください。

vdmutil コマンドは、操作が成功すると 0 を返し、失敗すると操作の失敗に固有の 0 以外のコードを返します。**vdmutil** コマンドは標準エラー出力にエラー メッセージを書き込みます。操作で出力が生成されたり、**--verbose** オプションを使用して詳細なログ記録が有効になっていると、**vdmutil** コマンドは標準出力に米国英語で出力を書き込みます。

表 2-6. vdmutil コマンド オプション

オプション	説明
--activatePendingConnectionServerCertificates	ローカル ポッドの接続サーバ インスタンスの保留中セキュリティ証明書をアクティベーションします。
--countPendingMsgSecStatus	拡張モードへ、または拡張モードからの移行を阻んでいるマシンの数をカウントします。
--createPendingConnectionServerCertificates	ローカル ポッドの接続サーバ インスタンスの新しい保留中セキュリティ証明書を作成します。

表 2-6. vdmutil コマンド オプション (続き)

オプション	説明
`--getMsgSecLevel`	ローカル ポッドの拡張されたメッセージ セキュリティ ステータスを取得します。このステータスは Horizon 7 環境内のすべてのコンポーネントに対して、JMS メッセージ セキュリティ モードを [有効] から [拡張済み] に変更するプロセスに関連します。
`--getMsgSecMode`	ローカル ポッドのメッセージ セキュリティ モードを取得します。
`--help`	`vdmutil` コマンドのオプションを一覧表示します。`--help` を、`--setMsgSecMode --help` などの特定のコマンドで使用することもできます。
`--listMsgBusSecStatus`	ローカル ポッドの 全接続サーバのメッセージ バス セキュリティ ステータスを一覧表示します。
`--listPendingMsgSecStatus`	拡張モードへ、または拡張モードからの移行を阻んでいるマシンを一覧表示します。デフォルトでは、25 エントリに制限されます。
`--setMsgSecMode`	ローカル ポッドのメッセージ セキュリティ モードを設定します。
`--verbose`	詳細ログを有効にします。このオプションは、詳細なコマンド出力を取得する他のオプションに追加できます。`vdmutil` コマンドで、標準出力への書き込みが行われます。

セキュアなトンネルと PCoIP Secure Gateway を構成する

安全なトンネルが有効になっている場合は、ユーザーがリモート デスクトップに接続すると、Horizon Client は View 接続サーバまたはセキュリティ サーバ ホストへの 2 番目の HTTPS 接続を作成します。

PCoIP Secure Gateway が有効になっている場合は、ユーザーが PCoIP 表示プロトコルを使用してリモート デスクトップに接続すると、Horizon Client は接続サーバまたはセキュリティ サーバ ホストへのさらに安全な接続を作成します。

注　Horizon 6 バージョン 6.2 以降のリリースでは、Horizon 6 サーバおよびデスクトップへの安全な外部アクセスのために、セキュリティ サーバではなく Unified Access Gateway アプライアンスを使用できます。Unified Access Gateway アプライアンスを使用する場合、接続サーバ インスタンスで Secure Gateway を無効にして、これらのゲートウェイを Unified Access Gateway アプライアンスで有効に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。

セキュアなトンネルまたは PCoIP Secure Gateway が有効になっていない場合、セッションは、接続サーバまたはセキュリティ サーバ ホストをバイパスして、クライアント システムとリモート デスクトップ仮想マシンの間で直接確立されます。このタイプの接続を直接接続といいます。

重要　外部クライアントに安全な接続を提供する一般的なネットワーク構成には、セキュリティ サーバが含まれています。Horizon Administrator を使用してセキュリティ サーバ上でセキュアなトンネルや PCoIP Secure Gateway を有効または無効にするには、そのセキュリティ サーバと対になっている接続サーバ インスタンスを編集する必要があります。

外部クライアントが接続サーバ ホストに直接接続するネットワーク構成では、Horizon Administrator で接続サーバ インスタンスを編集して、安全なトンネルや PCoIP Secure Gateway を有効または無効にする必要があります。

開始する前に

- PCoIP Secure Gateway を有効にする場合は、接続サーバ インスタンスおよびペアのセキュリティ サーバが Horizon 7 4.6 以降であることを確認します。
- PCoIP Secure Gateway をすでに有効にしている接続サーバ インスタンスに対してセキュリティ サーバをペアにする場合は、セキュリティ サーバが Horizon 7 4.6 以降であることを確認します。

手順

1 Horizon Administrator で、[View 構成] - [サーバ] を選択します。

2 [接続サーバ] タブで、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。

3 安全なトンネルの使用を設定します。

オプション	説明
安全なトンネルを有効にする	[マシンへの安全なトンネル接続を使用する] を選択します。
安全なトンネルを無効にする	[マシンへの安全なトンネル接続を使用する] の選択を解除します。

デフォルトでは、安全なトンネルは有効になっています。

4 PCoIP Secure Gateway の使用を設定します。

オプション	説明
PCoIP Secure Gateway を有効にする	[マシンへの PCoIP 接続に PCoIP Secure Gateway を使用する] を選択します
PCoIP Secure Gateway を無効にする	[マシンへの PCoIP 接続に PCoIP Secure Gateway を使用する] の選択を解除します

デフォルトでは、PCoIP Secure Gateway は無効になっています。

5 [OK] をクリックして変更を保存します。

Blast Secure Gateway の構成

Horizon Administrator では、HTML Access、または VMware Blast 表示プロトコルを使用するクライアント接続を介してリモート デスクトップおよびアプリケーションに安全にアクセスできるように、Blast Secure Gateway の使用を構成できます。

Blast Secure Gateway には Blast Extreme Adaptive Transport (BEAT) ネットワークが含まれています。これは、速度の変化やパケット損失などのネットワーク状態に動的に適合します。

- Blast Secure Gateway は、Unified Access Gateway アプライアンスで実行されている場合にのみ、BEAT ネットワークをサポートします。
- Unified Access Gateway アプライアンス バージョン 3.3 以降に接続している場合、IPv4 を使用する Horizon Client と IPv6 を使用する Horizon Client を TCP ポート 8443 と UDP ポート 8443（BEAT 用）で同時に処理できます。
- 一般的なネットワーク状態では、Horizon Client を接続サーバ（BSG 無効）、セキュリティ サーバ（BSG 無効）またはバージョン 2.8 以降の Unified Access Gateway アプライアンスに接続する必要があります。一般的なネットワーク状態で Horizon Client を接続サーバ（BSG 有効）、セキュリティ サーバ（BSG 有効）またはバージョン 2.8 より前の Unified Access Gateway アプライアンスに接続すると、クライアントはネットワーク状態を自動的に感知し、TCP ネットワークに戻ります。

- ネットワーク状態が良好でない場合、Horizon Client はバージョン 2.9 以降の Unified Access Gateway アプライアンス（UDP トンネル サーバ有効）に接続する必要があります。ネットワーク状態が良好でないときに Horizon Client を接続サーバ（BSG 有効）、セキュリティ サーバ（BSG 有効）またはバージョン 2.8 より前の Unified Access Gateway アプライアンスに接続すると、クライアントはネットワーク状態を自動的に感知し、TCP ネットワークに戻ります。
- ネットワーク状態が良好でないときに、Horizon Client を接続サーバ（BSG 無効）、セキュリティ サーバ（BSG 無効）、バージョン 2.9 以降の Unified Access Gateway アプライアンス（UDP トンネル サーバ無効）またはバージョン 2.8 の Unified Access Gateway アプライアンスに接続すると、クライアントはネットワーク状態を自動的に感知し、一般的なネットワーク状態に戻ります。

詳細については、https://docs.vmware.com/jp/VMware-Horizon-Client/index.html にある Horizon Client のドキュメントを参照してください。

注　また、セキュリティ サーバではなく、Unified Access Gateway アプライアンスを使用して、Horizon 7 サーバおよびデスクトップに安全に外部アクセスすることもできます。Unified Access Gateway アプライアンスを使用する場合、接続サーバ インスタンスで Secure Gateway を無効にして、これらのゲートウェイを Unified Access Gateway アプライアンスで有効に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。

Blast Secure Gateway が有効になっていない場合、クライアント デバイスおよびクライアント Web ブラウザは、VMware Blast Extreme プロトコルを使用して、リモート デスクトップ仮想マシンおよびアプリケーションに直接接続することで、Blast Secure Gateway をバイパスします。

重要　外部ユーザーに安全な接続を提供する一般的なネットワーク構成には、セキュリティ サーバが含まれています。セキュリティ サーバで Blast Secure Gateway を有効または無効にするには、セキュリティ サーバとペアになっている接続サーバ インスタンスを編集する必要があります。外部ユーザーが接続サーバ ホストに直接接続する場合、その接続サーバ インスタンスを編集して Blast Secure Gateway を有効または無効にします。

開始する前に

ユーザーが VMware Identity Manager を使用してリモート デスクトップを選択する場合、VMware Identity Manager がインストールされ、接続サーバで使用するために構成されており、接続サーバが SAML 2.0 認証サーバとペアになっていることを確認します。

手順

1 Horizon Administrator で、[View 構成] - [サーバ] を選択します。

2 [接続サーバ] タブで、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。

3 Blast Secure Gateway の使用を構成します。

オプション	説明
Blast Secure Gateway を有効にする	[Blast Secure Gateway を使用してマシンに Blast 接続する] を選択します。
Blast secure Gateway を無効にする	[Blast Secure Gateway を使用してマシンに Blast 接続する] を選択解除します。

Blast Secure Gateway はデフォルトで有効になります。

4 [OK] をクリックして変更を保存します。

TLS 接続の中間サーバへのオフロード

Horizon Client は HTTPS を使用して Horizon 7 に接続する必要があります。Horizon Client が接続サーバ インスタンスまたはセキュリティ サーバにロード バランサなどの中間サーバを経由して接続する場合、TLS を中間サーバにオフロードすることができます。

TLS オフロード サーバの証明書を Horizon 7 サーバにインポートする

TLS 接続を中間サーバにオフロードする場合、中間サーバの証明書を接続サーバ インスタンスまたは中間サーバに接続するセキュリティ サーバにインポートする必要があります。同じ TLS サーバ証明書が、オフロードする中間サーバと、中間サーバに接続する、オフロードされる各 Horizon 7 Server の両方に存在している必要があります。

セキュリティ サーバを展開する場合、中間サーバおよびそれに接続するセキュリティ サーバに、同じ TLS 証明書が必要です。同じ TLS 証明書を、セキュリティ サーバとペアリングされて中間サーバに直接接続していない接続サーバ インスタンスにインストールする必要はありません。

セキュリティ サーバを展開しない場合、またはいくつかのセキュリティ サーバおよび外部に接続している接続サーバ インスタンスを含む混在ネットワーク環境の場合、中間サーバおよびそれに接続する接続サーバ インスタンスに同じ TLS 証明書が必要です。

中間サーバの証明書が接続サーバ インスタンスまたはセキュリティ サーバにインストールされていないと、クライアントは Horizon 7 への接続を検証できません。この場合、Horizon 7 Server によって送信された証明書のサムプリントが、Horizon Client が接続している中間サーバの証明書と一致しません。

ロード バランシングを TLS オフロードと混同しないようにしてください。この前提条件は、一部のタイプの負荷分散を含む、TLS オフロードを提供するように構成されたすべてのデバイスに適用されます。ただし、純粋な負荷分散には、デバイス間の証明書のコピーは必要ありません。

Horizon 7 Server への証明書のインポートの詳細については、『Horizon 7 のインストール』ドキュメントの「署名付きサーバ証明書を Windows Certificate Store にインポートする」を参照してください。

クライアントを TLS オフロード サーバにポイントするように Horizon 7 Server の外部 URL を設定する

TLS が中間サーバにオフロードされ、Horizon Client デバイスがセキュアなトンネルを使用して Horizon 7 に接続する場合は、セキュアなトンネルの外部 URL を、クライアントが中間サーバへのアクセスに使用できるアドレスに設定するようにします。

中間サーバに接続する接続サーバ インスタンスまたはセキュリティ サーバの外部 URL 設定を構成します。

セキュリティ サーバを展開する場合、それらのセキュリティ サーバに外部 URL が必要ですが、セキュリティ サーバとペアになる接続サーバ インスタンスには外部 URL は必要ありません。

セキュリティ サーバを展開しない場合や、セキュリティ サーバや外部向けの接続サーバ インスタンスがいくつか集まった混合ネットワーク環境を利用している場合には、中間サーバに接続する接続サーバ インスタンスに外部 URL が必要です。

注　PCoIP Secure Gateway (PSG) または Blast Secure Gateway から TLS 接続をオフロードすることはできません。PCoIP 外部 URL と Blast Secure Gateway 外部 URL は、PSG と Blast Secure Gateway をホストするコンピュータへの接続をクライアントに許可する必要があります。中間サーバと Horizon 7 Server 間に TLS 接続を要求する予定がない限り、中間サーバをポイントするように PCoIP 外部 URL と Blast 外部 URL をリセットすることは避けてください。

外部 URL の構成についての詳細は、『Horizon 7 のインストール』ドキュメントの「PCoIP Secure Gateway 接続およびトンネル接続用の外部 URL の構成」を参照してください。

中間サーバからの HTTP 接続を許可する

TLS が中間サーバにオフロードされる場合、接続サーバ インスタンスまたはセキュリティ サーバが、クライアントが接続する中間デバイスからの HTTP 接続を許可するように構成できます。中間デバイスは Horizon Client 接続の HTTPS を受け入れる必要があります。

Horizon 7 Server と中間デバイスとの HTTP 接続を許可するには、HTTP 接続が許可される各接続サーバ インスタンスおよびセキュリティ サーバに `locked.properties` ファイルを構成する必要があります。

Horizon 7 Server サーバと中間デバイスとの間の HTTP 接続が許可されたとしても、Horizon 7 での TLS を無効にすることはできません。Horizon 7 サーバは HTTP 接続と同様に HTTPS 接続を引き続き受け入れます。

注　Horizon クライアントがスマート カード認証を使用する場合、クライアントは接続サーバまたはセキュリティ サーバに対し直接 HTTPS 接続を行う必要があります。TLS オフロードはスマート カード認証ではサポートされていません。

手順

1 接続サーバ ホストまたはセキュリティ サーバ ホスト上で、TLS/SSL ゲートウェイ構成フォルダ内の `locked.properties` ファイルを作成または編集します。

例： `<install_directory>\VMware\VMware View\Server\SSLgateway\conf\locked.properties`

2 Horizon 7 Server のプロトコルを構成するには、`ServerProtocol` プロパティを追加して、`http` に設定します。

値 `http` は小文字で入力する必要があります。

3 (オプション) プロパティを追加して、デフォルト以外の HTTP リスニング ポートおよびネットワーク インターフェイスを Horizon 7 Server に構成します。

- HTTP リスニング ポートを 80 から変更するには、`serverPortNonTLS` を、中間デバイスの接続先に構成されている別のポート番号に設定します。

- Horizon 7 Server に複数のネットワーク インターフェイスがあり、サーバに 1 つのインターフェイスのみで HTTP 接続をリスンさせる場合、`serverHostNonTLS` をそのネットワーク インターフェイスの IP アドレスに設定します。

4 `locked.properties` ファイルを保存します。

5 変更を反映するため、接続サーバ サービスまたはセキュリティ サーバ サービスを再起動してください。

例: locked.properties ファイル

このファイルにより Horizon 7 Server への非 TLS HTTP 接続が許可されます。Horizon 7 Server のクライアント側のネットワーク インターフェイスの IP アドレスは 10.20.30.40 です。サーバは、デフォルトのポート 80 を使用して、HTTP 接続を待機します。その値 `http` は小文字である必要があります。

```
serverProtocol=http
serverHostNonTLS=10.20.30.40
```

Horizon 接続サーバまたはセキュリティ サーバ ホスト用のゲートウェイの場所の構成

デフォルトのゲートウェイの場所は、Horizon 接続サーバ インスタンスでは `Internal` に設定され、セキュリティ サーバでは `External` に設定されています。デフォルトのゲートウェイの場所を変更するには、`locked.properties` ファイルの `gatewayLocation` プロパティを設定します。

ゲートウェイの場所により、リモート デスクトップの `ViewClient_Broker_GatewayLocation` レジストリ キーの値が決定されます。この値をスマート ポリシーで使用すると、ユーザーが企業ネットワーク内から、または企業ネットワーク以外からリモート デスクトップに接続した場合にのみ有効になるポリシーを作成できます。詳細については、『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントの「スマート ポリシーの使用」を参照してください。

手順

1 Horizon 接続サーバ ホストまたはセキュリティ サーバ ホスト上で、TLS/SSL ゲートウェイ構成フォルダ内の `locked.properties` ファイルを作成または編集します。

例：`<install_directory>\VMware\VMware View\Server\sslgateway\conf\locked.properties`

`locked.properties` ファイルのプロパティは、大文字と小文字が区別されます。

2 次の行を `locked.properties` ファイルに追加します。

`gatewayLocation=<value>`

<value> は、`External` または `Internal` のいずれかになります。`External` は、企業ネットワークの外部のユーザーがゲートウェイを使用できることを示します。`Internal` は、企業ネットワークの内部のユーザーのみがゲートウェイを使用できることを示します。

例：`gatewayLocation=External`

3 `locked.properties` ファイルを保存します。

4 変更を反映するため、VMware Horizon 接続サーバ サービスまたは VMware Horizon セキュリティ サーバ サービスを再起動してください。

Horizon 接続サーバの無効化または有効化

接続サーバ インスタンスを無効にして、ユーザーが仮想または公開デスクトップやアプリケーションにログインできないようにすることができます。インスタンスを無効にした後、再度有効にすることができます。

接続サーバ インスタンスを無効にしても、現在デスクトップやアプリケーションにログインしているユーザーは影響を受けません。

インスタンスを無効にするとユーザーがどのような影響を受けるかは、Horizon 7 の展開によって決まります。

- 単一でスタンドアローンの接続サーバ インスタンスの場合、ユーザーはデスクトップまたはアプリケーションにログインできません。接続サーバに接続できません。
- これが複製された接続サーバ インスタンスの場合は、ユーザーを別の複製されたインスタンスにルーティングできるかどうかはネットワーク トポロジーによって決まります。別のインスタンスにアクセスできる場合、ユーザーはデスクトップやアプリケーションにログインできます。

手順

1 Horizon Administrator で、[View 構成] - [サーバ] を選択します。

2 [接続サーバ] タブで、接続サーバ インスタンスを選択します。

3 [無効化] をクリックします。

[有効化] をクリックすることによって、インスタンスを再び有効にすることができます。

外部 URL の編集

Horizon Administrator を使用して、接続サーバ インスタンスおよびセキュリティ サーバの外部 URL を編集できます。

デフォルトでは、接続サーバまたはセキュリティ サーバ ホストに接続できるクライアントは、同じネットワーク内に存在するトンネル クライアントだけです。ネットワークの外部で実行されているトンネル クライアントは、クライアントで解決できる URL を使用して接続サーバまたはセキュリティ サーバ ホストに接続する必要があります。

ユーザーが PCoIP 表示プロトコルを使用してリモート デスクトップに接続した場合には、Horizon Client はさらに接続サーバ ホストまたはセキュリティ サーバ ホスト上の PCoIP Secure Gateway に接続することができます。PCoIP Secure Gateway を使用するには、クライアント システムが接続サーバ ホストまたはセキュリティ サーバ ホストに到達するための IP アドレスにアクセスできる必要があります。この IP アドレスは PCoIP 外部 URL に指定します。

さらにもう 1 つは、Blast Secure Gateway 経由で安全な接続を行えるようにするための URL です。

安全なトンネルの外部 URL、PCoIP 外部 URL、および Blast 外部 URL は、このホストに到達するためにクライアント システムで使用されるアドレスでなければなりません。

注 接続サーバ 4.5 以降にアップグレードされていないセキュリティ サーバの外部 URL を編集することはできません。

手順

1 Horizon Administrator で、[View 構成] - [サーバ] を選択します。

オプション	アクション
View 接続サーバ インスタンス	[接続サーバ] タブで接続サーバ インスタンスを選択し、[編集] をクリックします。
セキュリティ サーバ	[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、[編集] をクリックします。

2 [外部 URL] テキスト ボックスに安全なトンネルの外部 URL を入力します。

URL には、プロトコル、クライアントで解決可能なホスト名、およびポート番号が含まれている必要があります。

例：https://view.example.com:443

注 ホスト名が解決できないときに接続サーバ インスタンスまたはセキュリティ サーバにアクセスする必要がある場合は、IP アドレスを使用できます。ただし、通信するホストは、接続サーバ インスタンスまたはセキュリティ サーバに対して構成された SSL 証明書に一致しないため、アクセスがブロックされたりアクセスのセキュリティが低下したりします。

3 [PCoIP 外部 URL] テキスト ボックスに、PCoIP Secure Gateway の外部 URL を入力します。

PCoIP 外部 URL は、IP アドレスとポート番号 4172 の組み合わせとして指定します。プロトコル名は含めないでください。

例： `10.20.30.40:4172`

URL には、クライアント システムがこのセキュリティ サーバまたは接続サーバ インスタンスに到達する際に使用できる IP アドレスとポート番号を含める必要があります。

4 [Blast 外部 URL] テキスト ボックスに Blast Secure Gateway の外部 URL を入力します。

URL には、HTTPS プロトコル、クライアントが解決可能なホスト名、およびポート番号が含まれている必要があります。

例：`https://myserver.example.com:8443`

デフォルトでは、URL には安全なトンネル外部 URL の FQDN およびデフォルトのポート番号 8443 が含まれます。URL には、このホストに到達するためにクライアント システムで使用できる FQDN とポート番号を含める必要があります。

5 このダイアログのすべてのアドレスでクライアント システムがこのホストに到達できることを確認します。

6 [OK] をクリックして変更を保存します。

外部 URL はすぐに更新されます。変更を反映するために接続サーバ サービスまたはセキュリティ サーバ サービスを再起動する必要はありません。

カスタマー エクスペリエンス プログラムに参加または参加を取り消す

接続サーバを新しい構成でインストールする場合は、カスタマー エクスペリエンス向上プログラムに参加することを選択できます。インストール後に参加に関する考えが変わったら、Horizon Administrator を使用して、プログラムに参加したり参加を取り消したりすることができます。

プログラムに参加すると、VMware は、ユーザー要件に対する対応を向上させるために、お客様の展開に関する匿名データを収集します。企業が特定できるような情報は収集されません。

匿名のフィールドを含め、データが収集されたフィールドのリストを確認するには、GUID-4FDD21B3-5F28-419F-AA16-4C7578996A54#GUID-4FDD21B3-5F28-419F-AA16-4C7578996A54 を参照してください。

手順

1 Horizon Administrator で、[View 構成] - [製品のライセンスと使用状況] の順に選択します。

2 [ユーザー使用環境改善プログラム] ペインで、[編集設定] をクリックします。

3 [VMware に匿名のデータを送信] チェックボックスをオンまたはオフにすることで、プログラムに参加するか参加を取り消すかを指定します。

4 (オプション) 参加する場合は、組織の地理的な位置、業種、従業員数を選択できます。

5 [OK] をクリックします。

View LDAP ディレクトリ

View LDAP は、Horizon 7 構成情報すべてのデータ リポジトリです。View LDAP は、接続サーバのインストールによって提供される、組み込み Lightweight Directory Access Protocol（LDAP）ディレクトリです。

View LDAP には、Horizon 7 で使用される標準 LDAP ディレクトリ コンポーネントが含まれます。

- Horizon 7 のスキーマ定義
- ディレクトリ情報ツリー（DIT）の定義
- アクセス制御リスト（ACL）

View LDAP には、Horizon 7 オブジェクトを表すディレクトリ エントリが含まれます。

- アクセス可能な各デスクトップを表すリモート デスクトップ エントリ。各エントリには、デスクトップの使用が許可されている、Active Directory 内の Windows ユーザーおよびグループの外部セキュリティ プリンシパル（FSP）エントリへの参照が含まれています。
- まとめて管理される複数のデスクトップを表すリモート デスクトップ プール エントリ。
- 各リモート デスクトップの vCenter Server 仮想マシンを表す仮想マシン エントリ。
- 設定を格納するための Horizon 7 コンポーネント エントリ。

View LDAP には、他の Horizon 7 コンポーネントに自動化と通知サービスを提供する、一連の Horizon 7 プラグイン DLL も含まれています。

注 セキュリティ サーバ インスタンスには、View LDAP ディレクトリは含まれていません。

LDAP レプリケーション

複製された接続サーバのインスタンスをインストールするときは、Horizon 7 が既存の接続サーバ インスタンスから View LDAP 構成データをコピーします。複製されたグループのすべての接続サーバ インスタンスで、同一の View LDAP 構成データが維持されます。1 つのインスタンスで構成が変更されると、更新された情報が他のインスタンスにコピーされます。

複製されたインスタンスで障害が発生した場合は、グループ内の他のインスタンスが動作を続行します。障害が発生したインスタンスが活動を再開した場合、停止中に発生した変更で構成が更新されます。Horizon 7 以降のリリースでは、レプリケーションのステータス チェックが 15 分ごとに実行され、各インスタンスが複製されたグループの他のサービスと通信できるかどうか、およびグループ内の他のサーバから LDAP の更新を取得できるかどうかが決まります。

Horizon Administrator のダッシュボードを使用して、レプリケーションのステータスを確認できます。ダッシュボードで接続サーバ インスタンスに赤色のアイコンがある場合は、アイコンをクリックするとレプリケーションのステータスが表示されます。次のいずれかの理由で、複製が失敗することがあります。

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

デフォルトでは、レプリケーションのチェックは 15 分ごとに実行されます。チェック間隔を変更するには、接続サーバ インスタンスで ADSI Edit を使用します。分数を設定するには、[DC=vdi,DC=vmware,DC=int] に接続して、[CN=Common,OU=Global,OU=Properties] オブジェクトの [pae-ReplicationStatusDataExpiryInMins] 属性を編集します。

[pae-ReplicationStatusDataExpiryInMins] 属性値は、10 ～ 1440 分（1 日）の範囲で設定する必要があります。属性が 10 分未満の値に設定されている場合、Horizon 7 では 10 分として扱われます。属性が 1440 分を超える値に設定されている場合、Horizon 7 では 1440 分として扱われます。

スマート カード認証の設定

3

セキュリティを強化するため、ユーザーと管理者がスマート カードを使用して認証できるように、接続サーバ インスタンスまたはセキュリティ サーバを構成できます。

スマート カードは、コンピュータ チップを搭載した小型のプラスチック カードです。ミニチュア コンピュータのようなこのチップは、秘密鍵および公開鍵の証明書など、データの安全なストレージを備えています。米国国防省が使用するスマート カードの 1 種には、Common Access Card （CAC）というカードがあります。

スマート カード認証では、クライアント コンピュータに接続されたスマート カード リーダにユーザーまたは管理者がスマート カードを差し込み、PIN を入力します。スマート カード認証は、個人が持っているもの（スマート カード）と個人が知っていること (PIN) の両方を検証することによって、2 要素認証を提供します。

スマート カード認証を実装するためのハードウェア要件およびソフトウェア要件については、『Horizon 7 のインストール』を参照してください。Microsoft TechNet の Web サイトでは、Windows システム用にスマート カード認証を計画して実装する方法についての詳細情報が提供されています。

スマート カードを使用するには、クライアント マシンにスマート カード ミドルウェアおよびスマート カード リーダが必要です。スマート カードに証明書をインストールするには、コンピュータを登録ステーションとして動作するように設定する必要があります。特定のタイプの Horizon Client がスマート カードをサポートするかどうかの詳細については、Horizon Client ドキュメント（https://docs.vmware.com/jp/VMware-Horizon-Client/index.html）を参照してください。

この章では次のトピックについて説明します。

スマート カードを使用したログイン

ユーザーまたは管理者がスマート カード リーダにスマート カードを差し込むと、クライアント オペレーティング システムが Windows の場合、スマート カードのユーザー証明書がクライアント システムのローカル証明書ストアにコピーされます。ローカル証明書ストアの証明書は、Horizon Client を含め、クライアント コンピュータ上で実行されているすべてのアプリケーションで利用可能です。

スマート カード認証が構成されている接続サーバ インスタンスまたはセキュリティ サーバへの接続をユーザーまたは管理者が開始すると、信頼された認証局 (CA) のリストがその接続サーバ インスタンスまたはセキュリティ サーバからクライアント システムに送信されます。クライアント システムは信頼された CA のリストを使用可能なユーザー証明書と照合し、適切な証明書を選択してから、ユーザーまたは管理者にスマート カード PIN の入力を要求します。有効なユーザー証明書が複数ある場合、クライアント システムはユーザーまたは管理者に証明書の選択を求めます。

そのユーザー証明書がクライアント システムから接続サーバ インスタンスまたはセキュリティ サーバに送信され、証明書の信頼および有効期間を確認することによって証明書が検証されます。一般に、ユーザー証明書が署名されていて有効であれば、ユーザーおよび管理者は正常に認証されます。証明書失効チェックが構成されている場合、失効した証明書を持つユーザーまたは管理者は認証ができません。

環境によっては、ユーザーのスマート カード証明書を複数の Active Directory ドメインのユーザー アカウントにマップできます。ユーザーは管理者権限のある複数のアカウントを持っている場合がありますが、その場合、スマート カードでログインするときの [ユーザー名のヒント] フィールドで使用するアカウントを指定する必要があります。Horizon Client のログイン ダイアログ ボックスで [ユーザー名のヒント] フィールドを表示させるには、管理者は、Horizon Administrator の接続サーバ インスタンスでスマート カード ユーザー名のヒント機能を有効にする必要があります。次に、スマート カード ユーザーは、スマート カードでログインするときに、[ユーザー名のヒント] フィールドにユーザー名または UPN を入力できます。

外部アクセスの安全を確保するために、お使いの環境で Unified Access Gateway アプライアンスを使用している場合、スマート カード ユーザー名のヒント機能をサポートするように、Unified Access Gateway アプライアンスを構成する必要があります。スマート カード ユーザー名のヒント機能は、Unified Access Gateway バージョン 2.7.2 以降でのみサポートされます。Access Point でスマート カード ユーザー名のヒント機能を有効にする方法については、『Unified Access Gateway の導入および設定』を参照してください。

Horizon Client でのスマート カード認証では、表示プロトコルの切り替えがサポートされていません。Horizon Client でのスマート カードによる認証後に、表示プロトコルを変更するには、ユーザーはログオフして、再度ログオンする必要があります。

Horizon 接続サーバでのスマート カード認証の構成

スマート カード認証を構成するには、ルート証明書を取得してサーバ信頼ストア ファイルに追加し、接続サーバの構成プロパティを変更して、スマートカード認証を設定する必要があります。使用する環境によっては、追加の手順が必要になることがあります。

手順

1 証明機関の証明書の取得

ユーザーまたは管理者が提示したスマート カード上のすべての信頼されたユーザー証明書について、該当するすべての CA（証明機関）の証明書を取得する必要があります。これらの証明書にはルート証明書が含まれ、ユーザーのスマート カード証明書が中間証明機関によって発行された場合には中間証明書が含まれる場合があります。

2 Windows からの CA 証明書の取得

CA が署名したユーザー証明書またはそれを含むスマート カードがあり、Windows でルート証明書が信頼される場合は、そのルート証明書を Windows からエクスポートできます。ユーザー証明書の発行元が中間証明機関である場合は、その証明書をエクスポートできます。

3 サーバ信頼ストア ファイルへの CA 証明書の追加

信頼するすべてのユーザーおよび管理者のサーバ信頼ストア ファイルに、ルート証明書と中間証明書のいずれかまたは両方を追加する必要があります。接続サーバ インスタンスおよびセキュリティ サーバは、この情報を使用してスマート カード ユーザーおよび管理者を認証します。

4 Horizon 接続サーバの構成プロパティの変更

スマート カード認証を有効にするには、接続サーバまたはセキュリティ サーバ ホストの接続サーバ構成プロパティを変更する必要があります。

5 Horizon Administrator でのスマート カード設定の構成

Horizon Administrator を使用して、スマート カード認証のさまざまなシナリオに対応する設定を指定できます。

証明機関の証明書の取得

ユーザーまたは管理者が提示したスマート カード上のすべての信頼されたユーザー証明書について、該当するすべての CA（証明機関）の証明書を取得する必要があります。これらの証明書にはルート証明書が含まれ、ユーザーのスマート カード証明書が中間証明機関によって発行された場合には中間証明書が含まれる場合があります。

ユーザーおよび管理者によって提示されたスマート カード上の証明書に署名した CA のルート証明書または中間証明書を持っていない場合、CA が署名したユーザー証明書またはそれを含むスマート カードから証明書をエクスポートできます。「Windows からの CA 証明書の取得」を参照してください。

手順

- CA の証明書は次のいずれかの発行元から取得します。
  - Microsoft Certificate Services を実行する Microsoft IIS サーバ。Microsoft IIS のインストール、証明書の発行、および組織内での証明書配布の詳細については、Microsoft TechNet の Web サイトを参照してください。
  - 信頼された CA の公開ルート証明書。これは、スマート カード インフラストラクチャがすでに使用されていて、スマート カードの配布および認証方法が標準化されている環境で最もよく利用されるルート証明書の発行元です。

次に進む前に

ルート証明書と中間証明書のいずれかまたは両方をサーバ信頼ストア ファイルに追加します。

Windows からの CA 証明書の取得

CA が署名したユーザー証明書またはそれを含むスマート カードがあり、Windows でルート証明書が信頼される場合は、そのルート証明書を Windows からエクスポートできます。ユーザー証明書の発行元が中間証明機関である場合は、その証明書をエクスポートできます。

手順

1 ユーザー証明書がスマート カード上にある場合は、そのスマート カードをリーダに挿入して、ユーザー証明書を個人用ストアに追加します。

ユーザー証明書が個人用ストアに表示されない場合は、リーダ ソフトウェアを使用してユーザー証明書をファイルにエクスポートします。このファイルは、この操作の手順 4 で使用されます。

2 Internet Explorer で [ツール] - [インターネット オプション] を選択します。

3 [コンテンツ] タブで [証明書] をクリックします。

4 [個人] タブで、使用する証明書を選択し、[表示] をクリックします。

ユーザー証明書がリストに表示されない場合は、[インポート] をクリックして手動でファイルからインポートします。証明書がインポートされると、その証明書をリストから選択できます。

5 [証明のパス] タブで、ツリーの最上位にある証明書を選択して [証明書を表示] をクリックします。

ユーザー証明書が信頼階層の一部として署名されている場合は、署名する証明書が別の上位の証明書によって署名されていることがあります。親証明書（ユーザー証明書に実際に署名した証明書）をルート証明書として選択してください。場合によっては発行元が中間 CA となります。

6 [詳細] タブで [ファイルにコピー] をクリックします。

[証明書のエクスポート ウィザード] が表示されます。

7 [次へ] - [次へ] をクリックし、エクスポートするファイルの名前と場所を入力します。

8 [次へ] をクリックして、指定した場所にファイルをルート証明書として保存します。

次に進む前に

CA 証明書をサーバ信頼ストア ファイルに追加します。

サーバ信頼ストア ファイルへの CA 証明書の追加

信頼するすべてのユーザーおよび管理者のサーバ信頼ストア ファイルに、ルート証明書と中間証明書のいずれかまたは両方を追加する必要があります。接続サーバ インスタンスおよびセキュリティ サーバは、この情報を使用してスマート カード ユーザーおよび管理者を認証します。

開始する前に

- ユーザーまたは管理者が提示したスマート カード上の証明書への署名に使用したルート証明書または中間証明書を取得します。「証明機関の証明書の取得」および「Windows からの CA 証明書の取得」を参照してください。

  重要　ユーザーのスマート カード証明書が中間証明機関によって発行された場合、これらの証明書には中間証明書が含まれることがあります。

- `keytool` ユーティリティが、接続サーバまたはセキュリティ サーバ ホストのシステム パスに追加されていることを確認します。詳細については、『Horizon 7 のインストール』ドキュメントを参照してください。

手順

1 接続サーバまたはセキュリティ サーバ ホストで、keytool ユーティリティを使用して、ルート証明書または中間証明書のいずれかまたは両方をサーバ信頼ストア ファイルにインポートします。

例：
keytool –import –alias <alias> –file <root_certificate> –keystore <truststorefile.key>

このコマンドでは、<alias> は信頼ストア ファイル内の新しいエントリの大文字と小文字を区別する一意の名前で、<root_certificate> は取得またはエクスポートしたルート証明書または中間証明書です。また、<truststorefile.key> はルート証明書の追加先の信頼ストア ファイルの名前です。ファイルが存在しない場合、現在のディレクトリに作成されます。

注 keytool ユーティリティによって、信頼ストア ファイルのパスワードの作成を求められる場合があります。後で信頼ストア ファイルにさらに証明書を追加する必要がある場合は、このパスワードの入力が求められます。

2 接続サーバまたはセキュリティ サーバ ホストの SSL ゲートウェイ構成フォルダに、信頼ストア ファイルをコピーします。

例：<install_directory>\VMware\VMware View\Server\sslgateway\conf\<truststorefile.key>

次に進む前に

接続サーバの構成プロパティを変更して、スマート カード認証を有効にします。

Horizon 接続サーバの構成プロパティの変更

スマート カード認証を有効にするには、接続サーバまたはセキュリティ サーバ ホストの接続サーバ構成プロパティを変更する必要があります。

開始する前に

信頼されたすべてのユーザー証明書の CA（認証局）証明書をサーバ信頼ストア ファイルに追加します。これらの証明書にはルート証明書が含まれ、ユーザーのスマート カード証明書が中間認証局によって発行された場合には中間証明書が含まれる場合があります。

手順

1 接続サーバ ホストまたはセキュリティ サーバ ホスト上で、TLS/SSL ゲートウェイ構成フォルダ内の locked.properties ファイルを作成または編集します。

例：<install_directory>\VMware\VMware View\Server\sslgateway\conf\locked.properties

2 `locked.properties` ファイルに `trustKeyfile`、`trustStoretype`、および `useCertAuth` プロパティを追加します。

   a `trustKeyfile` に信頼ストア ファイルの名前を設定します。

   b `trustStoretype` に **`jks`** を設定します。

   c `useCertAuth` に **`true`** を設定して、証明書認証を有効にします。

3 変更を反映するため、接続サーバ サービスまたはセキュリティ サーバ サービスを再起動してください。

例: locked.properties ファイル

例に示すファイルでは、すべての信頼されたユーザーのルート証明書がある場所としてファイル `lonqa.key` が指定され、信頼ストアのタイプが `jks` に設定され、証明書認証が有効になります。

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
```

次に進む前に

接続サーバ インスタンスでスマート カード認証を構成した場合は、Horizon Administrator でスマート カード認証の設定をします。セキュリティ サーバではスマート カード認証設定を構成する必要はありません。Horizon 接続サーバ インスタンスに構成された設定は、ペアになっているセキュリティ サーバにも適用されます。

Horizon Administrator でのスマート カード設定の構成

Horizon Administrator を使用して、スマート カード認証のさまざまなシナリオに対応する設定を指定できます。

これらの設定を接続サーバ インスタンスで構成すると、その設定はペアになっているセキュリティ サーバにも適用されます。

開始する前に

- 接続サーバ ホストの接続サーバ構成プロパティを変更します。
- Horizon Client が接続サーバまたはセキュリティ サーバのホストに対して HTTPS 接続を直接確立していることを確認します。TLS を中間デバイスにオフロードしている場合、スマート カード認証はサポートされません。

手順

1 Horizon Administrator で、[View 構成] - [サーバ] を選択します。

2 [接続サーバ] タブで、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。

3 リモート デスクトップ ユーザーおよびアプリケーション ユーザーのスマート カード認証を構成するには、次の手順を実行します。

a [認証] タブで、[View 認証] セクションの [ユーザー用スマート カード認証] ドロップダウン メニューから構成オプションを選択します。

オプション	アクション
不許可	接続サーバ インスタンスでのスマート カード認証が無効になります。
Optional	ユーザーはスマート カード認証またはパスワード認証を使用して接続サーバ インスタンスに接続できます。スマート カード認証が失敗した場合、ユーザーはパスワードを入力する必要があります。
Required	接続サーバ インスタンスに接続するときにユーザーはスマート カード認証を使用する必要があります。 スマート カード認証が必須の場合は、接続サーバ インスタンスに接続する際に [現在のユーザーとしてログイン] チェック ボックスをオンにしたユーザーの認証が失敗します。これらのユーザーは、接続サーバにログインする際にスマート カードと PIN を使用して再認証する必要があります。

オプション	アクション
	注　スマート カード認証を設定すると、Windows パスワード認証は利用できなくなりますが、他の認証は利用できます。SecurID が有効になっている場合は、ユーザーは SecurID とスマート カード認証の両方による認証を求められます。

b　スマート カード取り外しポリシーを構成します。

スマート カード認証が [不許可] に設定されている場合は、スマート カード取り外しポリシーを構成できません。

オプション	アクション
ユーザーがスマート カードを取り外したら、View 接続サーバにらユーザーを切断する。	[スマート カードを取り出すときはユーザー セッションを切断します] チェック ボックスをオンにします。
ユーザーがスマート カードを取り外しても View 接続サーバへの接続を維持して、再認証しなくても新しいデスクトップまたはアプリケーション セッションを開始できるようにする。	[スマート カードを取り出すときはユーザー セッションを切断します] チェック ボックスをオフにします。

ユーザーが [現在のユーザーとしてログイン] チェック ボックスをオンにして接続サーバ インスタンスに接続している場合は、スマート カードでクライアント システムにログインしている場合であっても、スマート カード取り外しポリシーは適用されません。

c　スマート カードのユーザー名のヒント機能を構成する。

スマート カード認証が [不許可] に設定されている場合は、スマート カードのユーザー名のヒント機能を構成できません。

オプション	アクション
ユーザーが 1 つのスマート カード証明書を使用して、複数のユーザー アカウントを認証できるようにする。	[スマート カード ユーザー名のヒントを許可します] チェック ボックスをオンにします。
ユーザーが 1 つのスマート カード証明書を使用して、複数のユーザー アカウントを認証できないようにする。	[スマート カード ユーザー名のヒントを許可します] チェック ボックスをオフにします。

4　Horizon Administrator にログインする管理者にスマート カード認証を構成するには、[認証] タブをクリックし、[View 管理認証] セクションで [管理者用スマート カード認証] ドロップダウン メニューから構成オプションを選択します。

オプション	アクション
不許可	接続サーバ インスタンスでのスマート カード認証が無効になります。
Optional	管理者はスマート カード認証またはパスワード認証を使用して Horizon Administrator にログインできます。スマート カード認証が失敗した場合、管理者はパスワードを入力する必要があります。
Required	管理者は Horizon Administrator にログインするときにスマート カード認証を使用する必要があります。

5　[OK] をクリックします。

6 接続サーバ サービスを再起動します。

スマート カードの設定に対する変更を反映するには、接続サーバ サービスを再起動する必要があります。1 つだけ例外があります。スマート カード認証の設定は、接続サーバ サービスを再起動せずに、[オプション] と [必須] の間で変更できます。

スマート カードの設定を変更しても、現在ログインしているユーザーおよび管理者に影響はありません。

次に進む前に

必要に応じて、スマート カード認証のために Active Directory を準備します。「スマート カード認証用の Active Directory を準備する」を参照してください。

スマート カード認証の構成を検証します。「スマート カード認証の構成の検証」を参照してください。

サードパーティ製ソリューションでのスマート カード認証の構成

ロード バランサやゲートウェイなどのサードパーティ製ソリューションは、スマート カードの X.590 証明書と暗号化された PIN が含まれる SAML アサーションを渡すことで、スマート カード認証を実行できます。

このトピックでは、証明書がパートナ デバイスによって検証された後に関連する X.590 証明書を接続サーバに提供するためのサードパーティ製ソリューションの設定に伴うタスクについて概説します。この機能では SAML 認証を使用するため、タスクの 1 つとして Horizon Administrator で SAML 認証子を作成します。

Unified Access Gateway でのスマート カード認証の構成については、『Unified Access Gateway の導入および設定』を参照してください。

手順

1 サードパーティ製ゲートウェイまたはロード バランサ用の SAML 認証子を作成します。

「Horizon Administrator での SAML 認証子の構成」を参照してください。

2 接続サーバのメタデータの有効期間を延長して、リモート セッションが 24 時間経過後に終了されないようにします。

「接続サーバでのサービス プロバイダ メタデータの有効期間の変更」を参照してください。

3 必要に応じて、接続サーバからサービス プロバイダのメタデータを使用するようにサードパーティ製デバイスを構成します。

サードパーティ製デバイスの製品ドキュメントを参照してください。

4 サードパーティ製デバイスでスマート カード設定を構成します。

サードパーティ製デバイスの製品ドキュメントを参照してください。

スマート カード認証用の Active Directory を準備する

スマート カード認証を実装するときは、Active Directory で特定のタスクを実行する必要があります。

- スマート カード ユーザーの UPN を追加する

  スマート カード ログインはユーザー プリンシパル名 (UPN) に依存するので、Horizon 7 での認証にスマート カードを使用するユーザーおよび管理者の Active Directory アカウントには有効な UPN が必要です。

- Enterprise NTAuth ストアにルート証明書を追加する

  CA を使用してスマート カード ログイン証明書またはドメイン コントローラ証明書を発行する場合は、Active Directory でルート証明書を Active Directory の Enterprise NTAuth ストアに追加する必要があります。Windows ドメイン コントローラがルート CA として機能する場合は、この手順を実行する必要はありません。

- 信頼されたルート証明機関へのルート証明書の追加

  証明機関（CA）を使用してスマート カード ログイン証明書またはドメイン コントローラ証明書を発行する場合は、Active Directory でルート証明書を信頼されたルート証明機関グループ ポリシーに追加する必要があります。Windows ドメイン コントローラがルート CA として機能する場合は、この手順を実行する必要はありません。

- 中間証明機関への中間証明書の追加

  中間証明機関（CA）を使用してスマート カード ログイン証明書またはドメイン コントローラ証明書を発行する場合は、Active Directory で中間証明書を中間証明機関グループ ポリシーに追加する必要があります。

スマート カード ユーザーの UPN を追加する

スマート カード ログインはユーザー プリンシパル名 (UPN) に依存するので、Horizon 7 での認証にスマート カードを使用するユーザーおよび管理者の Active Directory アカウントには有効な UPN が必要です。

スマート カード ユーザーが属しているドメインが、ルート証明書が発行されたドメインとは異なる場合は、ユーザーの UPN を、信頼された CA のルート証明書に含まれるサブジェクトの別名 (SAN) に設定する必要があります。ルート証明書がスマート カード ユーザーの現在のドメイン内のサーバから発行された場合は、ユーザーの UPN を変更する必要はありません。

注　証明書が同じドメインから発行された場合であっても、組み込み Active Directory アカウントの UPN を設定することが必要な場合があります。Administrator などの組み込みアカウントには、デフォルトでは UPN は設定されません。

開始する前に

- 証明書のプロパティを表示して、信頼された CA のルート証明書に含まれる SAN を取得します。
- Active Directory サーバに ADSI Edit ユーティリティがない場合は、Microsoft の Web サイトから適切な Windows Support Tools をダウンロードし、インストールします。

手順

1. Active Directory サーバで ADSI Edit ユーティリティを起動します。
2. 左ペインで、ユーザーがいるドメインを展開し、**CN=Users** をダブルクリックします。
3. 右ペインで、ユーザーを右クリックして [プロパティ] をクリックします。
4. **userPrincipalName** 属性をダブルクリックし、信頼された CA 証明書の SAN 値を入力します。
5. [OK] をクリックして属性の設定を保存します。

Enterprise NTAuth ストアにルート証明書を追加する

CA を使用してスマート カード ログイン証明書またはドメイン コントローラ証明書を発行する場合は、Active Directory でルート証明書を Active Directory の Enterprise NTAuth ストアに追加する必要があります。Windows ドメイン コントローラがルート CA として機能する場合は、この手順を実行する必要はありません。

手順

- Active Directory サーバで、**certutil** コマンドを使用して、証明書を Enterprise NTAuth ストアに発行します。

  例：**certutil –dspublish –f <ルート CA 証明書へのパス> NTAuthCA**

CA がこの種の証明書の発行元として信頼されるようになります。

信頼されたルート証明機関へのルート証明書の追加

証明機関（CA）を使用してスマート カード ログイン証明書またはドメイン コントローラ証明書を発行する場合は、Active Directory でルート証明書を信頼されたルート証明機関グループ ポリシーに追加する必要があります。Windows ドメイン コントローラがルート CA として機能する場合は、この手順を実行する必要はありません。

手順

1 Active Directory サーバで、Group Policy Management プラグインに移動します。

Active Directory のバージョン	ナビゲーション パス
Windows 2003	a [スタート] - [すべてのプログラム] - [管理ツール] - [Active Directory ユーザーとコンピュータ] の順に選択します。 b ドメインを右クリックして、[プロパティ] をクリックします。 c [グループ ポリシ] タブで、[開く] をクリックして Group Policy Management プラグインを開きます。 d [既定のドメイン ポリシー] を右クリックし、[編集] をクリックします。
Windows 2008	a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。
Windows 2012 R2	a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。
Windows 2016	a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。

2 [コンピュータの構成] セクションを展開し、[Windows 設定¥キュリティ設定¥開鍵] を開きます。

3 [信頼されたルート証明機関] を右クリックして、[インポート] を選択します。

4 ウィザードの指示に従ってルート証明書（**rootCA.cer** など）をインポートし、[OK] をクリックします。

5 [グループ ポリシー] ウィンドウを閉じます。

ドメイン内のすべてのシステムの信頼されたルート ストアに、ルート証明書がコピーされます。

次に進む前に

中間証明機関（CA）がスマート カードのログイン証明書またはドメイン コントローラ証明書を発行する場合は、Active Directory で中間証明機関のグループ ポリシーに中間証明書を追加します。「中間証明機関への中間証明書の追加」を参照してください。

中間証明機関への中間証明書の追加

中間証明機関（CA）を使用してスマート カード ログイン証明書またはドメイン コントローラ証明書を発行する場合は、Active Directory で中間証明書を中間証明機関グループ ポリシーに追加する必要があります。

手順

1 Active Directory サーバで、Group Policy Management プラグインに移動します。

Active Directory のバージョン	ナビゲーション パス
Windows 2003	a [スタート] - [すべてのプログラム] - [管理ツール] - [Active Directory ユーザーとコンピュータ] の順に選択します。 b ドメインを右クリックして、[プロパティ] をクリックします。 c [グループ ポリシ] タブで、[開く] をクリックして Group Policy Management プラグインを開きます。 d [既定のドメイン ポリシー] を右クリックし、[編集] をクリックします。
Windows 2008	a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。
Windows 2012 R2	a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。
Windows 2016	a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。

2 [コンピュータの構成] セクションを展開し、[Windows Settings\Security Settings\Public Key] のポリシーを開きます。

3 [中間証明機関] を右クリックして、[インポート] を選択します。

4 ウィザードの指示に従って中間証明書（`intermediateCA.cer` など）をインポートし、[OK] をクリックします。

5 [グループ ポリシー] ウィンドウを閉じます。

ドメイン内のすべてのシステムの中間証明機関ストアに、中間証明書がコピーされます。

スマート カード認証の構成の検証

スマート カード認証を初めて設定したとき、またはスマート カード認証が正しく動作しないときは、スマート カード認証の構成を検証する必要があります。

手順

- 各クライアント システムに、スマート カード ミドルウェア、スマート カードとその有効な証明書、およびスマート カード リーダがあることを確認します。エンド ユーザーについては、Horizon Client を所有しているかを確認します。

  スマート カードのソフトウェアとハードウェアの構成方法については、スマート カード ベンダから提供されているマニュアルを参照してください。

- 各クライアント システムで、[スタート] - [設定] - [コントロール パネル] - [インターネット オプション] - [コンテンツ] - [証明書] - [個人] を選択し、スマート カード認証に証明書が使用できることを確認します。

  ユーザーまたは管理者がスマート カード リーダにスマート カードを差し込むと、Windows によって証明書がスマート カードからユーザーのコンピュータにコピーされます。クライアント システム上のアプリケーション（Horizon Client を含む）は、これらの証明書を使用できます。

- 接続サーバまたはセキュリティ サーバ ホストの `locked.properties` ファイルで、`useCertAuth` プロパティが **`true`** に設定されていて、スペルが正しいことを確認します。

  `locked.properties` ファイルは `<install_directory>\VMware\VMware View\Server\sslgateway\conf` にあります。`useCertAuth` プロパティのスペルを `userCertAuth` と誤ることがよくあります。

- 接続サーバ インスタンスでスマート カード認証を構成した場合は、Horizon Administrator でスマート カード認証の設定を確認します。

  a [View 構成] - [サーバ] を選択します。

  b [接続サーバ] タブで、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。

  c ユーザーのスマート カード認証を構成した場合は、[認証] タブで、[ユーザー用スマート カード認証] が [オプション] または [必須] に設定されていることを確認します。

  d 管理者のスマート カード認証を構成した場合は、[認証] タブで、[管理者用スマート カード認証] が [オプション] または [必須] に設定されていることを確認します。

  スマート カードの設定に対する変更を反映するには、接続サーバ サービスを再起動する必要があります。

- スマート カード ユーザーが属しているドメインが、ルート証明書が発行されたドメインとは異なる場合は、ユーザーの UPN が、信頼された CA のルート証明書に含まれる SAN に設定されていることを確認します。

  a 証明書のプロパティを表示して、信頼された CA のルート証明書に含まれる SAN を調べます。

  b Active Directory サーバで、[スタート] - [管理ツール] - [Active Directory ユーザーおよびコンピュータ] を選択します。

  c [ユーザー] フォルダでユーザーを右クリックし、[プロパティ] を選択します。

  [アカウント] タブの [ユーザー ログオン名] テキスト ボックスに、UPN が表示されます。

- スマート カード ユーザーが PCoIP 表示プロトコルまたは VMware Blast 表示プロトコルを選択して、シングル セッション デスクトップに接続する場合は、Smartcard リダイレクトという名前の View Agent または Horizon Agent コンポーネントが単一ユーザー マシンにインストールされていることを確認します。スマート カード機能を使用すると、ユーザーはスマート カードを使用してシングルセッション デスクトップにログインできます。リモート デスクトップ サービス ロールがインストールされた RDS ホストでは、スマート カード機能が自動的にサポートされるため、この機能をインストールする必要はありません。
- 接続サーバまたはセキュリティ サーバ ホストの `<drive>:\Documents and Settings\All Users\Application Data\VMware\VDM\logs` にあるログ ファイルで、スマートカード認証が有効であることを示すメッセージを確認します。

スマート カードでの証明書失効チェックの使用

証明書失効チェックを構成すると、失効したユーザー証明書を持つユーザーがスマート カードを使用して認証されるのを回避できます。証明書は、ユーザーが組織を離れたとき、スマート カードを紛失したとき、別の部門に異動したときなどに失効します。

Horizon 7 は、証明書失効リスト (CRL) およびオンライン証明書状態プロトコル (OCSP) による証明書失効チェックをサポートします。CRL は、証明書を発行した CA によって公開される、失効した証明書のリストです。OCSP は、X.509 証明書の失効ステータスを取得するために使用される証明書検証プロトコルです。

証明書失効チェックは、接続サーバ インスタンスまたはセキュリティ サーバ上で構成できます。接続サーバ インスタンスがセキュリティ サーバと対になっている場合は、セキュリティ サーバ上で証明書失効チェックを構成します。認証局 (CA) は、接続サーバまたはセキュリティ サーバ ホストからアクセスできる必要があります。

同じ接続サーバ インスタンスまたはセキュリティ サーバ上で CRL と OCSP の両方を構成できます。両方のタイプの証明書失効チェックを構成すると、Horizon 7 は最初に OCSP の使用を試行し、OCSP に失敗すると CRL にフォール バックします。Horizon 7 は、CRL が失敗した場合、OCSP にフォール バックしません。

- CRL チェックを使用したログイン

  CRL チェックを構成すると、Horizon 7 によって CRL が構築されて読み取られ、ユーザー証明書の失効ステータスが判別されます。

- OCSP による証明書失効チェックを使用したログイン

  OCSP による証明書失効チェックを構成すると、特定のユーザー証明書の失効ステータスの判別を求める要求が Horizon 7 から OCSP レスポンダに送信されます。Horizon 7 では、OCSP 署名証明書を使用して、OCSP レスポンダから受信した応答が本物であることを確認します。

- CRL チェックの構成

  CRL チェックを構成すると、Horizon 7 によって CRL が読み取られ、スマート カードのユーザー証明書の失効ステータスが判別されます。

- OCSP による証明書失効チェックの構成

  OCSP による証明書失効チェックを構成すると、スマート カードにあるユーザー証明書の失効ステータスの判別を求める検証要求が Horizon 7 から OCSP レスポンダに送信されます。

- スマート カードでの証明書失効チェックのプロパティ

  `locked.properties` ファイル内の値を設定して、スマート カードでの証明書失効チェックを有効化および構成します。

CRL チェックを使用したログイン

CRL チェックを構成すると、Horizon 7 によって CRL が構築されて読み取られ、ユーザー証明書の失効ステータスが判別されます。

証明書が失効していて、スマート カード認証がオプションになっている場合は、**[Enter your user name and password (ユーザー名とパスワードを入力してください)]** ダイアログ ボックスが表示され、ユーザーは認証のためにパスワードを入力する必要があります。スマート カード認証が必須の場合は、エラー メッセージが表示され、ユーザーの認証が許可されません。Horizon 7 が CRL を読み取ることができない場合にも、同じイベントが発生します。

OCSP による証明書失効チェックを使用したログイン

OCSP による証明書失効チェックを構成すると、特定のユーザー証明書の失効ステータスの判別を求める要求が Horizon 7 から OCSP レスポンダに送信されます。Horizon 7 では、OCSP 署名証明書を使用して、OCSP レスポンダから受信した応答が本物であることを確認します。

ユーザー証明書が失効していて、スマート カード認証がオプションになっている場合は、**[Enter your user name and password（ユーザー名とパスワードを入力してください)]** ダイアログ ボックスが表示され、ユーザーは認証のためにパスワードを入力する必要があります。スマート カード認証が必須の場合は、エラー メッセージが表示され、ユーザーの認証が許可されません。

Horizon 7 は、OCSP レスポンダからの応答がない場合、または応答が無効な場合、CRL チェックにフォール バックします。

CRL チェックの構成

CRL チェックを構成すると、Horizon 7 によって CRL が読み取られ、スマート カードのユーザー証明書の失効ステータスが判別されます。

開始する前に

CRL チェックに使用される `locked.properties` ファイルのプロパティを理解しておきます。「スマート カードでの証明書失効チェックのプロパティ」を参照してください。

手順

1 接続サーバ ホストまたはセキュリティ サーバ ホスト上で、TLS/SSL ゲートウェイ構成フォルダ内の `locked.properties` ファイルを作成または編集します。

例：`<install_directory>\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2 `locked.properties` ファイルに `enableRevocationChecking` および `crlLocation` プロパティを追加します。

a `enableRevocationChecking` に **`true`** を設定して、スマート カードでの証明書失効チェックを有効にします。

b `crlLocation` に CRL の場所を設定します。この値には、URL またはファイル パスを指定できます。

3 変更を反映するため、接続サーバ サービスまたはセキュリティ サーバ サービスを再起動してください。

例: locked.properties ファイル

例に示すファイルでは、スマート カード認証とスマート カードでの証明書失効チェックが有効になり、CRL チェックが構成され、CRL の場所の URL が指定されます。

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
crlLocation=http://root.ocsp.net/certEnroll/ocsp-ROOT_CA.crl
```

OCSP による証明書失効チェックの構成

OCSP による証明書失効チェックを構成すると、スマート カードにあるユーザー証明書の失効ステータスの判別を求める検証要求が Horizon 7 から OCSP レスポンダに送信されます。

開始する前に

OCSP による証明書失効チェックに使用される `locked.properties` ファイルのプロパティを理解しておきます。「スマート カードでの証明書失効チェックのプロパティ」を参照してください。

手順

1 接続サーバ ホストまたはセキュリティ サーバ ホスト上で、TLS/SSL ゲートウェイ構成フォルダ内の `locked.properties` ファイルを作成または編集します。

   例：`<install_directory>\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2 `locked.properties` ファイルに `enableRevocationChecking`、`enableOCSP`、`ocspURL`、`ocspSigningCert` プロパティを追加します。

   a `enableRevocationChecking` に **`true`** を設定して、スマート カードでの証明書失効チェックを有効にします。

   b `enableOCSP` に **`true`** を設定して、OCSP による証明書失効チェックを有効にします。

   c `ocspURL` に OCSP レスポンダの URL を設定します。

   d `ocspSigningCert` に OCSP レスポンダの署名証明書を含むファイルの場所を設定します。

3 変更を反映するため、接続サーバ サービスまたはセキュリティ サーバ サービスを再起動してください。

例: locked.properties ファイル

例に示すファイルでは、スマート カード認証およびスマート カードでの証明書失効チェックが有効になり、CRL と OCSP の両方の証明書失効チェックが構成され、OCSP レスポンダの場所が指定され、OCSP 署名証明書を含むファイルが特定されます。

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
enableOCSP=true
allowCertCRLs=true
ocspSigningCert=te-ca.signing.cer
ocspURL=http://te-ca.lonqa.int/ocsp
```

スマート カードでの証明書失効チェックのプロパティ

`locked.properties` ファイル内の値を設定して、スマート カードでの証明書失効チェックを有効化および構成します。

表 3-1 は、証明書取り消し確認用の `locked.properties` のファイル プロパティをリストします。

表 3-1. スマート カードでの証明書失効チェックのプロパティ

プロパティ	説明
`enableRevocationChecking`	このプロパティを **`true`** に設定すると、証明書失効チェックが有効になります。 このプロパティを **`false`** に設定すると、証明書失効チェックが無効になり、他のすべての証明書失効チェック プロパティが無視されます。 デフォルト値は **`false`** です。
`crlLocation`	CRL の場所を指定します。URL またはファイル パスを指定できます。 URL を指定しない場合、または指定した URL が無効な場合に、`allowCertCRLs` が **`true`** に設定されているか、または指定されていないと、Horizon 7 はユーザー証明書の CRL のリストを使用します。 Horizon 7 が CRL にアクセスできない場合は、CRL チェックが失敗します。
`allowCertCRLs`	このプロパティを **`true`** に設定すると、Horizon 7 はユーザー証明書から CRL のリストを抽出します。 デフォルト値は **`true`** です。
`enableOCSP`	このプロパティを **`true`** に設定すると、OCSP による証明書失効チェックが有効になります。 デフォルト値は **`false`** です。
`ocspURL`	OCSP レスポンダの URL を指定します。
`ocspResponderCert`	OCSP レスポンダの署名証明書を含むファイルを指定します。Horizon 7 では、この証明書を使用して、OCSP レスポンダから受信した応答が本物であることを確認します。

表 3-1. スマート カードでの証明書失効チェックのプロパティ (続き)

プロパティ	説明
ocspSendNonce	このプロパティを **true** に設定すると、応答の繰り返しを回避するために OCSP 要求とともにノンスが送信されます。 デフォルト値は **false** です。
ocspCRLFailover	このプロパティを **true** に設定すると、Horizon 7 は OCSP 証明書失効チェックが失敗した場合に CRL チェックを使用します。 デフォルト値は **true** です。

4 他のタイプのユーザー認証の設定

Horizon 7 は、ユーザーおよび管理者を認証および管理するために既存の Active Directory インフラストラクチャを利用します。また、 スマート カードに加え、バイオメトリクス認証や、RSA SecurID、RADIUS など の 2 要素認証ソリューションなど他の形式の認証と Horizon 7 を統合して、リモート デスクトップおよびアプリケーション ユーザーを認証することもできます。

この章では次のトピックについて説明します。

2 要素認証の使用

ユーザーが RSA SecurID 認証または RADIUS (Remote Authentication Dial-In User Service) 認証を使用しなければならないように、Horizon 接続サーバ インスタンスを構成できます。

- RADIUS サポートは、さまざまな代替 2 要素トークン ベースの認証オプションを提供します。
- Horizon 7 は、オープン標準拡張インターフェイスも提供して、サードパーティ ソリューション プロバイダが詳細認証拡張を Horizon 7 に統合できるようにします。

RSA SecurID や RADIUS などの 2 要素認証ソリューションは、個別のサーバにインストールされた認証マネージャと連携するため、接続サーバ ホストにアクセスできるようにこれらのサーバを構成する必要があります。たとえば RSA SecurID を使用する場合、認証マネージャは RSA Authentication Manager になります。RADIUS を使用する場合、認証マネージャは RADIUS サーバになります。

2 要素認証を使用するには、認証マネージャに登録されている RSA SecurID トークンなどのトークンがユーザーごとに必要です。2 要素認証トークンは、一定の間隔で認証コードを生成するハードウェアまたはソフトウェアです。多くの場合、認証には PIN と認証コードの両方に関する知識が必要です。

接続サーバ インスタンスが複数ある場合は、一部のインスタンスで 2 要素認証を構成し、他のインスタンスでは別のユーザー認証方法を構成することができます。たとえば、インターネットを介して企業ネットワークの外からリモート デスクトップとアプリケーションにアクセスするユーザーのみに 2 要素認証を構成できます。

Horizon 7 は RSA SecurID Ready プログラムによって認定されており、新規 PIN モード、次のトークン コード モード、RSA Authentication Manager、負荷分散など、SecurID のあらゆる機能をサポートしています。

2 要素認証を用いたログイン

RSA SecurID 認証または RADIUS 認証が有効になっている View 接続サーバ インスタンスにユーザーが接続すると、Horizon Client に特別なログイン ダイアログ ボックスが表示されます。

ユーザーは、特別なログイン ダイアログ ボックスに RSA SecurID または RADIUS 認証ユーザー名とパスコードを入力します。通常、2 要素認証パスコードは PIN とそれに続くトークン コードで構成されます。

- RSA Authentication Manager で、ユーザーが RSA SecurID ユーザー名とパスコードを入力した後に、新しい RSA SecurID PIN の入力が必要な場合は、PIN ダイアログ ボックスが表示されます。新しい PIN を設定した後、ユーザーはログインする前に次のトークン コードを待つよう求められます。システムによって生成された PIN を使用するように RSA Authentication Manager が構成されている場合は、PIN を確認するためのダイアログ ボックスが表示されます。
- Horizon 7 にログインしているときは、RADIUS 認証は RSA SecurID とほとんど同じ働きをします。RADIUS サーバがアクセス チャレンジを発行すると、Horizon Client は次のトークン コードに対し RSA SecurID プロンプトに似たダイアログ ボックスを表示します。RADIUS チャレンジの現在のサポートは、テキスト入力に対するプロンプトの表示に限られます。RADIUS サーバから送信された、いかなるチャレンジ テキストも表示されません。複数の選択肢や画像の選択など、より複雑な形式のチャレンジは、現在サポートされていません。

  ユーザーが認証情報を Horizon Client に入力すると、RADIUS サーバは SMS テキスト メッセージまたは電子メール、あるいは他のアウトオブバンド機能を使用してテキストを、コードと共にユーザーの携帯電話に送信できます。ユーザーはこのテキストおよびコードを Horizon Client に入力して、認証を完了することができます。
- RADIUS ベンダーによっては Active Directory からユーザーをインポートする機能が提供されるので、エンドユーザーは、RADIUS 認証ユーザー名およびパスコードを要求される前に、Active Directory 認証情報の入力を最初に要求される場合があります。

Horizon Administrator で 2 要素認証を有効にする

Horizon Administrator で接続サーバの設定を変更して、接続サーバ インスタンスで RSA SecurID 認証または RADIUS 認証を有効にします。

開始する前に

RSA SecurID ソフトウェアや RADIUS ソフトウェアなどの 2 要素認証ソフトウェアを、認証マネージャのサーバにインストールして構成します。

- RSA SecurID 認証の場合、`sdconf.rec` ファイルを RSA Authentication Manager から接続サーバ インスタンスにエクスポートします。RSA Authentication Manager のドキュメントを参照してください。
- RADIUS 認証の場合、ベンダーの構成に関するドキュメントに従ってください。RADIUS サーバのホスト名または IP アドレス、RADIUS 認証をリスンしているポート番号（通常は 1812）、認証タイプ（PAP、CHAP、MS-CHAPv1 または MS-CHAPv2）、および共有シークレットを書き留めておきます。これらの値を Horizon Administrator に入力します。値をプライマリおよびセカンダリ RADIUS 認証子に入力できます。

手順

1 Horizon Administrator で、[View 構成] - [サーバ] を選択します。

2 [接続サーバ] タブでサーバを選択し、[編集] をクリックします。

3 [認証] タブで、[高度な認証] セクションの [2 要素認証] ドロップダウン リストから、[RSA SecureID] または [RADIUS] を選択します。

4 RSA SecurID ユーザー名または RADIUS ユーザー名を Active Directory 内のユーザー名と強制的に一致させるには、[SecurID と Windows のユーザー名を強制的に一致させる] または [2 要素認証と Windows ユーザー名の一致の確認を強制します] を選択します。

   このオプションを選択した場合、ユーザーは Active Directory 認証にも同じ RSA SecurID ユーザー名または RADIUS ユーザー名を使用する必要があります。このオプションを選択しない場合は、名前が異なってもかまいません。

5 RSA SecurID の場合、[ファイルのアップロード] をクリックして `sdconf.rec` ファイルの場所を入力するか、[参照] をクリックしてファイルを検索します。

6 RADIUS 認証の場合、残りのフィールドを入力します。

a 最初の RADIUS 認証が、トークン コードのアウトオブバンド伝送をトリガする Windows 認証を使用し、このトークン コードが RADIUS のチャレンジの一部として使用される場合、[RADIUS と Windows 認証には同じユーザー名とパスワードを使用します] を選択します。

このチェックボックスを選択すると、RADIUS 認証で Windows のユーザー名およびパスワードを使用している場合、RADIUS 認証後にユーザーは Windows 認証情報の入力を求められません。ユーザーは RADIUS 認証後、Windows ユーザー名およびパスワードを再入力する必要はありません。

b [認証子] ドロップダウン リストから、[新しい認証子の作成] を選択し、ページのすべての項目に入力します。

- RADIUS アカウンティングを有効にする必要がない限り、[アカウンティング ポート] は [0] に設定します。RADIUS サーバがアカウンティング データの収集をサポートする場合に限り、このポートをゼロ以外の数字に設定します。RADIUS サーバがアカウンティング メッセージをサポートせず、このポートをゼロ以外の数字に設定すると、メッセージが送信されて無視され、何度も再試行された結果、認証が遅延します。

  アカウンティング データは、利用時間およびデータに基づいた、ユーザーへの請求に使用できます。アカウンティング データは、統計目的および一般的なネットワーク監視にも使用することができます。

- レルムのプリフィックス文字列を指定すると、RADIUS サーバに送られるときに、その文字列がユーザー名の先頭に配置されます。たとえば、Horizon Client に入力されたユーザー名が **jdoe** で、レルムのプリフィックス **DOMAIN-A** が指定された場合、ユーザー名 **DOMAIN-A\jdoe** が RADIUS サーバに送信されます。同様に、レルムのサフィックスまたはポストフィックスに文字列 **@mycorp.com** を使用する場合、ユーザー名 **jdoe@mycorp.com** が RADIUS サーバに送信されます。

7 [OK] をクリックして変更を保存します。

接続サーバ サービスの再起動は不要です。必要な構成ファイルが自動的に配布され、構成の設定がすぐに有効になります。

ユーザーが Horizon Client を開き、接続サーバへ認証する場合、2 要素認証が求められます。RADIUS 認証の場合、ログイン ダイアログ ボックスに、指定したトークンのラベルを含むテキスト プロンプトが表示されます。

RADIUS 認証設定への変更は、構成が変更された後で開始されるリモート デスクトップおよびアプリケーション セッションに影響を及ぼします。RADIUS 認証設定を変更しても、現在のセッションには影響ありません。

次に進む前に

接続サーバ インスタンスの複製されたグループがあり、そこでも RADIUS 認証を設定する場合、既存の RADIUS 認証子の構成を再利用することができます。

RSA SecurID アクセス拒否のトラブルシューティング

Horizon Client が RSA SecurID 認証で接続すると、アクセスが拒否されます。

問題

RSA SecurID を使用した Horizon Client 接続で「**アクセスが拒否されました**」が表示され、RSA Authentication Manager Log Monitor にエラー「**ノードの検証に失敗しました**」が表示されます。

原因

RSA Agent ホスト ノードの秘密をリセットする必要があります。

解決方法

1 Horizon Administrator で、[View 構成] - [サーバ] を選択します。

2 [接続サーバ] タブで、接続サーバを選択して [編集] をクリックします。

3 [認証] タブで [ノード シークレットをクリア] を選択します。

4 [OK] をクリックしてノードの秘密をクリアします。

5 RSA Authentication Manager を実行しているコンピュータで、[スタート] - [RSA プログラム] - [RSA Security] - [RSA Authentication Manager ホスト モード] の順に選択します。

6 [エージェント ホスト] - [エージェント ホストの編集] の順に選択します。

7 リストから [View 接続サーバ]を選択し、[作成されたノードの秘密] チェック ボックスの選択を解除します。

編集するときは、毎回デフォルトで [作成されたノードの秘密] が選択されます。

8 [OK] をクリックします。

RADIUS アクセス拒否のトラブルシューティング

Horizon Client が RADIUS 2 要素認証で接続すると、アクセスが拒否されます。

問題

RADIUS 2 要素認証を使用して Horizon Client 接続を行うと、「**アクセスが拒否されました**」と表示されます。

原因

RADIUS は RADIUS サーバから応答を受け取ることができず、Horizon 7 がタイムアウトします。

解決方法

次に、この状況を引き起こしやすい一般的な構成エラーを示します。

- View 接続サーバ インスタンスを RADIUS クライアントとして受け入れるように RADIUS サーバが構成されていない。RADIUS を使用する各 View 接続サーバ インスタンスは、RADIUS サーバでクライアントとして設定する必要があります。詳細は、RADIUS 2 要素認証製品のドキュメントを参照してください。
- View 接続サーバ インスタンス上と RADIUS サーバ上の共有シークレット値が一致していない。

SAML 認証の使用

Security Assertion Markup Language (SAML) は、さまざまなセキュリティ ドメイン間で認証情報および権限情報を記述および交換するための XML ベースの標準です。SAML は、ID プロバイダとサービス プロバイダ間において、SAML アサーションと呼ばれる XML ドキュメントでユーザーに関する情報の受け渡しを行います。

SAML 認証を使用して、Horizon 7 を VMware Workspace ONE、VMware Identity Manager、または認定のサードパーティ製ロード バランサ/ゲートウェイと統合できます。サードパーティ製デバイスの SAML を設定する場合は、ベンダーのドキュメントを参照して、Horizon 7 の設定方法を確認してください。SSO が有効になっている場合、VMware Identity Manager またはサードパーティ製のデバイスにログインしたユーザーは、第 2 のログイン手順を介さずにリモート デスクトップやアプリケーションを起動できます。SAML 認証を使用して、VMware Access Point またはサードパーティ製のデバイスにスマート カード認証を実装することもできます。

Workspace ONE、VMware Identity Manager、またはサードパーティ製のデバイスに認証の責任を委任するには、Horizon 7 で SAML 認証子を作成する必要があります。SAML 認証子には、Horizon 7 と Workspace ONE、VMware Identity Manager、またはサードパーティ製のデバイス間での信頼とメタデータの交換が含まれます。SAML 認証子を接続サーバ インスタンスと関連付けます。

VMware Identity Manager 統合用の SAML 認証の使用

Horizon 7 と VMware Identity Manager（旧称 Workspace ONE）の統合では、SAML 2.0 標準を使用して、シングル サインオン (SSO) 機能に不可欠な相互信頼を確立します。SSO が有効になっている場合、Active Directory 認証情報を使用して VMware Identity Manager または Workspace ONE にログインしたユーザーは、第 2 のログイン手順を経ずにリモート デスクトップやアプリケーションを起動できます。

VMware Identity Manager と Horizon 7 が統合されている場合、ユーザーが VMware Identity Manager にログインしてデスクトップまたはアプリケーション アイコンをクリックするたびに、VMware Identity Manager は一意の SAML アーティファクトを生成します。VMware Identity Manager はこの SAML アーティファクトを使用して、Universal Resource Identifier (URI) を作成します。URI には、デスクトップ プールまたはアプリケーション プールが置かれている接続サーバ インスタンス、起動するデスクトップまたはアプリケーション、および SAML アーティファクトについての情報が含まれます。

VMware Identity Manager は SAML アーティファクトを Horizon Client に送信し、その後、接続サーバ インスタンスにアーティファクトを送信します。接続サーバ インスタンスは SAML アーティファクトを使用して、VMware Identity Manager から SAML アサーションを取得します。

接続サーバ インスタンスは SAML アサーションを受け取った後、アサーションを検証し、ユーザーのパスワードを復号化し、復号化されたパスワードを使用してデスクトップまたはアプリケーションを起動します。

VMware Identity Manager と Horizon 7 の統合の設定には、Horizon 7 の情報での VMware Identity Manager の構成、および VMware Identity Manager への認証責任を委任するための Horizon 7 の構成が含まれます。

VMware Identity Manager への認証責任を委任するには、Horizon 7 で SAML 認証を作成する必要があります。SAML 認証子には、Horizon 7 と VMware Identity Manager 間での信頼とメタデータの交換が含まれます。SAML 認証子を接続サーバ インスタンスと関連付けます。

注　VMware Identity Manager からデスクトップとアプリケーションへのアクセスを提供しようとしている場合、Horizon Administrator のルート アクセス グループで Administrators ロールを持つユーザーとしてデスクトップ プールとアプリケーション プールを作成していることを確認します。ルート アクセス グループ以外で Administrators ロールをユーザーに付与すると、VMware Identity Manager は、Horizon 7 で構成する SAML 認証システムを認識せず、VMware Identity Manager でプールを構成できません。

Horizon Administrator での SAML 認証子の構成

リモート デスクトップおよびアプリケーションを VMware Identity Manager から起動するか、サードパーティ製ロード バランサまたはゲートウェイを通じてリモート デスクトップおよびアプリケーションを接続するには、Horizon Administrator で SAML 認証子を作成する必要があります。SAML 認証子には、Horizon 7 とクライアントが接続するデバイス間での信頼とメタデータの交換が含まれます。

SAML 認証子を接続サーバ インスタンスと関連付けます。導入環境に複数の接続サーバ インスタンスが含まれる場合は、各インスタンスに SAML 認証子を関連付ける必要があります。

1 つの静的認証子と複数の動的認証子を一度にライブにすることができます。vIDM（動的）および Unified Access Gateway（静的）の認証子を構成して、これらをアクティブ状態に保持できます。これらの認証子のいずれかを通じて接続を行うことができます。

接続サーバに複数の SAML 認証子を構成して、すべての認証子を同時にアクティブにできます。ただし、接続サーバで構成される各 SAML 認証子のエンティティ ID は異なっている必要があります。

SAML 認証子は本質的に静的な事前定義済みメタデータであるため、ダッシュボードでのステータスは常に緑色です。ステータスが赤色と緑色の間で切り替わるのは、動的認証子のみです。

VMware Unified Access Gateway アプライアンスの SAML 認証子の構成については、『Unified Access Gateway の導入および設定』を参照してください。

開始する前に

- Workspace ONE、VMware Identity Manager またはサードパーティ製のゲートウェイまたはロード バランサがインストールされて構成されていることを確認します。該当製品のインストール ガイドを参照してください。
- 接続サーバ ホストに、SAML サーバ証明書用の CA が署名したルート証明書がインストールされていることを確認します。VMware では、自己署名の証明書を使用するように SAML 認証子を構成することは推奨されません。証明書認証の詳細については、『Horizon 7 のインストール』ドキュメントを参照してください。
- Workspace ONE サーバ、VMware Identity Manager サーバ、または外部に接しているロード バランサの FQDN または IP アドレスを書き留めます。
- (オプション) Workspace ONE または VMware Identity Manager を使用している場合、コネクタ Web インターフェイスの URL を書き留めます。
- SAML メタデータを生成して静的認証子を作成する必要のある Unified Access Gateway またはサードパーティ製アプライアンスの認証子を作成する場合、デバイスで SAML メタデータを生成する手順を実行し、そのメタデータをコピーします。

手順

1 Horizon Administrator で、[構成 > サーバ] の順に選択します。

2 [接続サーバ] タブで、SAML 認証子を関連付けるサーバ インスタンスを選択して [編集] をクリックします。

3 [認証] タブで、[VMware Horizon (SAML 2.0 認証子) への認証の委任] ドロップダウン メニューの設定を選択して、SAML 認証子を有効または無効にします。

オプション	説明
無効	SAML 認証が無効です。リモート デスクトップとアプリケーションは、Horizon Client からのみ起動できます。
許可	SAML 認証が有効です。リモート デスクトップとアプリケーションは、Horizon Client と VMware Identity Manager の両方またはサードパーティ製デバイスから起動できます。
Required	SAML 認証が有効です。リモート デスクトップとアプリケーションは、VMware Identity Manager またはサードパーティ製デバイスからのみ起動できます。デスクトップまたはアプリケーションを、Horizon Client から手動で起動できません。

要件に応じて、展開内の各接続サーバ インスタンスを異なる SAML 認証設定で構成できます。

4 [SAML 認証子の管理] をクリックし、[追加] をクリックします。

5 [SAML 2.0 認証子を追加] ダイアログ ボックスで SAML 認証子を構成します。

オプション	説明
Type	Unified Access Gateway またはサードパーティ製デバイスの場合、[静的] を選択します。VMware Identity Manager の場合、[動的] を選択します。動的認証子の場合、メタデータ URL および管理 URL を指定できます。静的認証子の場合、Unified Access Gateway またはサードパーティ製デバイスでメタデータを生成し、メタデータをコピーして [SAML メタデータ] テキスト ボックスに貼り付けます。
ラベル	SAML 認証子を識別する一意の名前。
説明	SAML 認証子の簡単な説明。この値はオプションです。
メタデータ URL	(動的認証子の場合) SAML ID プロバイダと接続サーバ インスタンス間で SAML 情報を交換するために必要な情報すべてを取得するための URL。URL `https://<Horizon Server 名>/SAAS/API/1.0/GET/metadata/idp.xml` で、[<Horizon Server 名>] をクリックして VMware Identity Manager サーバまたは外部接続ロード バランサ (サードパーティ製デバイス) の FQDN または IP アドレスに置換します。
管理 URL	(動的認証子の場合) SAML ID プロバイダの管理コンソールにアクセスするための URL。VMware Identity Manager の場合、この URL は VMware Identity Manager コネクタ Web インターフェイスを参照している必要があります。この値はオプションです。
SAML メタデータ	(静的認証子の場合) Unified Access Gateway またはサードパーティ製デバイスから生成およびコピーしたメタデータ テキスト。
接続サーバに有効	認証子を有効にするには、このチェック ボックスをオンにします。複数の認証子を有効にできます。有効になっている認証子のみがリストに表示されます。

6 [OK] をクリックして SAML 認証子の構成を保存します。

有効な情報を指定した場合、自己署名の証明書を受け入れるか (推奨されません)、Horizon 7 および VMware Identity Manager またはサードパーティ製デバイスの信頼できる証明書を使用する必要があります。

[SAML 認証子の管理] ダイアログ ボックスには、新しく作成された認証子が表示されます。

7 Horizon Administrator ダッシュボードの [システムの健全性] セクションで、[その他のコンポーネント] - [SAML 2.0 認証子] を選択し、追加した SAML 認証子を選択して詳細を確認します。

構成に成功した場合、認証子の健全性は緑色です。証明書が信頼されていない場合、VMware Identity Manager を利用できない場合、またはメタデータ URL が無効な場合、認証子の健全性が赤色で表示されることがあります。証明書が信頼されていない場合は、[検証] をクリックして証明書を検証してから受け入れることができます。

次に進む前に

接続サーバのメタデータの有効期間を延長して、リモート セッションが 24 時間経過後に終了されないようにします。「接続サーバでのサービス プロバイダ メタデータの有効期間の変更」を参照してください。

VMware Identity Manager でのプロキシ サポートの設定

Horizon 7 は、VMware Identity Manager (vIDM) サーバのプロキシのサポートを提供します。ホスト名やポート番号などのプロキシの詳細は ADAM データベースで設定できます。HTTP 要求はプロキシ経由で経路指定されます。

この機能は、オンプレミスの Horizon 7 環境がクラウド内の vIDM サーバと通信できるハイブリッド環境をサポートします。

開始する前に

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 ADAM ADSI ツリーで、オブジェクト パス `cd=vdi,dc=vmware,dc=int,ou=Properties,ou=Global,cn=Common Attributes` を展開します。

3 [アクション] - [プロパティ] の順に選択し、[pae-NameValuePair] 属性で、新しいエントリ **`pae-SAMLProxyName`** と **`pae-SAMLProxyPort`** を追加します。

接続サーバでのサービス プロバイダ メタデータの有効期間の変更

有効期間を変更しないと、接続サーバは 24 時間後に Unified Access Gateway や他社の ID プロバイダなどの SAML 認証子から SAML アサーションを受け入れるのを停止し、メタデータの交換を繰り返す必要があります。

この手順を使用して、接続サーバが ID プロバイダから SAML アサーションを受け入れるのを停止するまでの日数を指定します。この日数は、現在の有効期間が切れるときに使用されます。たとえば、現在の有効期間が 1 日の場合に 90 日を指定すると、1 日経過後に接続サーバは有効期間が 90 日間のメタデータを生成します。

開始する前に

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-NameValuePair] 属性を編集して次の値を追加します。

```
cs-samlencryptionkeyvaliditydays=<number-of-days>
cs-samlsigningkeyvaliditydays=<number-of-days>
```

この例で、<number-of-days> はリモート接続サーバが SAML アサーションを受け入れるのを停止するまでに経過できる日数です。この期間を過ぎると、SAML メタデータを交換するプロセスを繰り返す必要があります。

接続サーバをサービス プロバイダとして使用可能にするための SAML メタデータの生成

使用する ID プロバイダに SAML 認証子を作成して有効にすると、接続サーバ メタデータの生成が必要になる場合があります。このメタデータは、ID プロバイダである Unified Access Gateway アプライアンスまたはサードパーティ製ロード バランサでサービス プロバイダを作成するために使用します。

開始する前に

Unified Access Gateway またはサードパーティ製ロード バランサ/ゲートウェイ ID プロバイダの SAML 認証子を作成済みであることを確認します。Horizon Administrator ダッシュボードの [システムの健全性] セクションで、[その他のコンポーネント] - [SAML 2.0 認証子] を選択し、追加した SAML 認証子を選択して詳細を確認します。

手順

1 新規のブラウザ タブを開き、接続サーバの SAML メタデータを取得するための URL を入力します。

https://<connection-server.example.com>/SAML/metadata/sp.xml

この例で、<connection-server.example.com> は接続サーバ ホストの完全修飾ドメイン名です。

このページには、接続サーバからの SAML メタデータが表示されます。

2 [別名で保存] コマンドを使用して Web ページを XML ファイルに保存します。

たとえば、ページを **connection-server-metadata.xml** という名前のファイルに保存することもできます。このファイルの内容は次のテキストで始まります。

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...
```

次に進む前に

ID プロバイダで適切な手順を使用して、接続サーバ SAML メタデータ内にコピーします。Unified Access Gateway またはサードパーティ製ロード バランサ/ゲートウェイのドキュメントを参照してください。

複数の動的 SAML 認証子の応答時間に関する注意事項

接続サーバ インスタンスで SAML 2.0 認証をオプションまたは必須として設定し、複数の動的 SAML 認証子を接続サーバ インスタンスに関連付けている場合に、動的 SAML 認証子のいずれかに到達できなくなると、他の動的 SAML 認証子からリモート デスクトップを起動するための応答時間が長くなります。

他の動的 SAML 認証子でリモート デスクトップを起動するための応答時間を短縮するには、Horizon Administrator を使用して、到達できない動的 SAML 認証子を無効にします。SAML 認証子を無効にする方法については、「Horizon Administrator での SAML 認証子の構成」を参照してください。

Horizon Administrator での Workspace ONE アクセス ポリシーの設定

Workspace ONE または VMware Identity Manager (vIDM) の管理者は、Horizon 7 で資格のあるデスクトップおよびアプリケーションへのアクセスを制限するアクセス ポリシーを設定できます。vIDM で作成したポリシーを適用するには、Horizon Client がユーザーを Workspace ONE クライアントにプッシュして資格を開始できるように、Horizon Client を Workspace ONE モードに切り替える必要があります。Horizon Client にログインすると、アクセス ポリシーにより、Workspace ONE 経由で公開デスクトップおよびアプリケーションにアクセスできます。

開始する前に

- Workspace ONE でアプリケーションのアクセス ポリシーを設定します。アクセス ポリシーの設定の詳細については、『VMware Identity Manager 管理ガイド』を参照してください。
- Horizon Administrator で公開デスクトップおよびアプリケーションの資格をユーザーに付与します。

手順

1. Horizon Administrator で、[構成 > サーバ] の順に選択します。
2. [接続サーバ] タブで、SAML 認証子に関連するサーバ インスタンスを選択して [編集] をクリックします。
3. [認証] タブで、[VMware Horizon (SAML 2.0 認証子) への認証の委任] オプションを [必須] に設定します。

   [必須] オプションにより、SAML 認証が有効になります。エンドユーザーが Horizon Server に接続するには、vIDM またはサードパーティの ID プロバイダによって提供される SAML トークンを使用する必要があります。デスクトップまたはアプリケーションを、Horizon Client から手動で起動することはできません。
4. [Workspace ONE モードを有効にする] を選択します。
5. [Workspace ONE サーバ ホスト名] テキスト ボックスに Workspace ONE ホスト名の FQDN 値を入力します。
6. (オプション) [Workspace ONE モードをサポートしていないクライアントからの接続をブロックする] を選択して、Workspace ONE モードをサポートする Horizon Client からアプリケーションへのアクセスを制限します。

   バージョン 4.5 より前の Horizon Client では、Workspace ONE モード機能がサポートされていません。このオプションを選択した場合、バージョン 4.5 より前の Horizon Client は Workspace ONE でアプリケーションにアクセスできません。Workspace ONE のバージョンがバージョン 2.9.1 よりも古い場合、Horizon 7 7.2 よりも新しいバージョンで Workspace ONE モード機能が有効になりません。

バイオメトリクス認証の構成

バイオメトリクス認証は、LDAP データベースで **pae-ClientConfig** 属性を編集することで構成できます。

開始する前に

お使いのバージョンの Windows サーバでの 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 [接続設定] ダイアログ ボックスで、[DC=vdi,DC=vmware,DC=int] を選択するか接続します。

3 [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.mydomain.com:389**

4 オブジェクトの [CN=Common, OU=Global, OU=Properties] で、[pae-ClientConfig] 属性を編集して値 [BioMetricsTimeout=<integer>] を追加します。

次の **BioMetricsTimeout** 値が有効です。

BioMetricsTimeout 値	説明
0	バイオメトリクス認証はサポートされません。これはデフォルトです。
-1	バイオメトリクス認証は時間制限なしでサポートされます。
任意の正の整数	バイオメトリクス認証はサポートされ、指定した分数の間、使用することができます。

新しい設定はただちに有効になります。接続サーバ サービスまたはクライアント デバイスを再起動する必要はありません。

5 認証情報を必要としないユーザー認証

ユーザーは、クライアント デバイスまたは VMware Identity Manager にログインすれば、Active Directory 認証情報を求められることなく公開アプリケーションまたはデスクトップに接続できます。

管理者は、ユーザー要件に基づいて構成を設定できます。

- ユーザーに、公開アプリケーションへの非認証アクセスを提供できます。管理者は、ユーザーが Active Directory 認証情報を入力して Horizon Client にログインする必要がないようにセットアップを構成できます。
- Windows ベースのクライアントに現在のユーザーとしてログインを使用できます。Windows ベースのクライアントの場合、管理者は、ユーザーが Active Directory 認証情報を使用して Windows ベースのクライアントにログインすれば、追加の認証情報を入力せずに Horizon Server にログインできるようにセットアップを構成できます。
- モバイルおよび Mac に認証情報を保存できます。モバイルおよび Mac クライアントの場合、管理者は、認証情報を保存するように Horizon Server を構成できます。この機能を使用すると、ユーザーはモバイルまたは Mac クライアントに SSO（シングル サインオン）の Active Directory 認証情報を一度入力すれば、この認証情報を記憶しておく必要がなくなります。
- VMware Identity Manager に True SSO を設定します。VMware Identity Manager の場合、管理者は、Active Directory 認証以外の方法を使用して認証を受けたユーザーが、Active Directory の認証情報を求められることなく公開デスクトップまたはアプリケーションにログインできるように True SSO を構成できます。

この章では次のトピックについて説明します。

公開アプリケーションでの非認証アクセスの提供

管理者は、非認証ユーザーが Active Directory 認証情報を使用せずに Horizon Client から公開アプリケーションにアクセスできるように設定できます。ユーザーが自身のセキュリティ管理とユーザー管理を行うアプリケーションにシームレスにアクセスする必要がある場合には、非認証アクセスの設定を考慮してください。

ユーザーが非認証アクセスを設定した公開アプリケーションを起動すると、RDS ホストが必要に応じてローカル ユーザー セッションを作成し、ユーザーにセッションを割り当てます。

この機能には、Horizon Client のバージョン 4.4 以降が必要です。HTML Access クライアントの場合は、バージョン 4.5 以降が必要です。

非認証ユーザーの構成ワークフロー

1 非認証アクセス ユーザーを作成します。「非認証アクセス ユーザーの作成」を参照してください。

2 ユーザーに非認証アクセスの資格を付与し、デフォルトの非認証ユーザーを設定します。「ユーザーの非認証アクセスの有効化」を参照してください。

3 公開アプリケーションに対する資格を非認証アクセス ユーザーに付与します。「公開アプリケーションに対する非認証アクセス ユーザーへの資格付与」を参照してください。

4 Horizon Client からの非認証アクセスを有効にします。「Horizon Client からの非認証アクセス」を参照してください。

非認証ユーザーの構成ルールとガイドライン

- RSA や RADIUS などの 2 要素認証およびスマート カード認証では、非認証のアクセスには対応していません。
- スマート カード認証と非認証アクセスは同時に使用できません。接続サーバでスマート カード認証が [必須] に設定された場合、非認証アクセスがそれ以前は有効であっても無効になります。
- VMware Identity Manager および VMware App Volumes では、非認証のアクセスには対応していません。
- この機能は、PCoIP および VMware Blast 表示プロトコルをサポートしています。
- 非認証アクセス機能は、RDS ホストのライセンス情報を確認しません。管理者がデバイスのライセンスを構成し、使用する必要があります。
- 非認証アクセス機能は、ユーザー固有のデータを保持しません。ユーザーは、アプリケーションのデータ ストレージの要件を確認できます。
- 非認証のアプリケーション セッションに再接続することはできません。ユーザーがクライアントから切断されると、RDS ホストはローカルのユーザー セッションから自動的にログオフします。
- 非認証アクセスは、公開アプリケーションでのみサポートされます。
- セキュリティ サーバまたは Unified Access Gateway アプライアンスでは、非認証アクセスはサポートされません。
- 非認証ユーザーのユーザー設定は保存されません。
- 非認証ユーザーに対しては仮想デスクトップはサポートされません。
- 接続サーバが CA 署名の証明書で構成され、非認証アクセスが有効になっていても、デフォルトの非認証ユーザーが構成されていないと、Horizon Administrator で接続サーバのステータスが赤色で表示されます。
- RDS ホストにインストールされた Horizon Agent の **AllowSingleSignon** グループ ポリシー設定が無効になっていると、非認証アクセスは機能しません。また、管理者は、非認証アクセスの有効、無効の管理を **UnAuthenticatedAccessEnabled** Horizon Agent グループ ポリシーの設定を使用して行うこともできます。Horizon Agent グループ ポリシー設定は、**Vdm_agent.admx** テンプレート ファイルに含まれています。このポリシーを有効にするには、RDS ホストを再起動する必要があります。

非認証アクセス ユーザーの作成

管理者は、公開アプリケーションに非認証でアクセスするユーザーを作成できます。管理者が非認証アクセスのユーザーを設定すると、ユーザーは Horizon Client から非認証アクセスでのみ接続サーバ インスタンスにログインできます。

開始する前に

- 非認証アクセスを設定する Active Directory (AD) ユーザーに有効な UPN があることを確認します。非認証アクセス ユーザーに設定できるのは Active Directory ユーザーだけです。

注　管理者が作成できるユーザーは、Active Directory アカウントごとに 1 つだけです。管理者は、非認証のユーザー グループを作成できません。非認証アクセス ユーザーを作成するときに、この Active Directory ユーザーに対する既存のクライアント セッションがある場合には、変更を反映するためにクライアント セッションを再起動する必要があります。

手順

1. Horizon Administrator で、[ユーザーとグループ] を選択します。
2. [非認証アクセス] タブで [追加] をクリックします。
3. **[認証されていないユーザーの追加]** ウィザードで、1 つ以上の検索条件を選択します。[検索] をクリックして、検索条件に基づいてユーザーを検索します。

   ユーザーには有効な UPN が必要です。
4. ユーザーを選択し、[次へ] をクリックします。

   複数のユーザーを追加するには、この手順を繰り返します。
5. (オプション) ユーザー エイリアスを入力します。

   デフォルトのユーザー エイリアスは、Active Directory アカウントに設定されたユーザー名です。エンド ユーザーは、ユーザー エイリアスを使用して Horizon Client から接続サーバ インスタンスにログインできます。
6. (オプション) ユーザーの詳細を確認して、コメントを追加します。
7. [終了] をクリックします。

接続サーバが非認証アクセス ユーザーを作成し、ユーザー エイリアス、ユーザー名、氏名、ソース ポッドの数、アプリケーションの資格、セッションなどのユーザーの詳細を表示します。[ソース ポッド] 列の数字をクリックすると、ポッドの情報が表示されます。

次に進む前に

接続サーバでのユーザーの非認証アクセスを有効にします。「ユーザーの非認証アクセスの有効化」を参照してください。

ユーザーの非認証アクセスの有効化

非認証アクセスのユーザーの作成後、接続サーバで非認証アクセスを有効にして、公開アプリケーションにユーザーがアクセスできるようにする必要があります。

手順

1 Horizon Administrator で、[View 構成] - [サーバ] を選択します。

2 [接続サーバ] タブをクリックします。

3 接続サーバ インスタンスを選択し、[編集] をクリックします。

4 [認証] タブをクリックします。

5 [非認証アクセス] を [有効] に変更します。

6 [デフォルトの非認証アクセス ユーザー] ドロップダウン メニューで、デフォルトにするユーザーを選択します。

デフォルト ユーザーは、クラウド ポッド アーキテクチャ 環境のローカル ポッドに配置される必要があります。異なるポッドからデフォルト ユーザーを選択すると、ユーザーをデフォルト ユーザーに設定する前に、接続サーバがローカル ポッドにユーザーを作成します。

7 (オプション) ユーザーのデフォルト セッション タイムアウトを入力します。

デフォルトのセッション タイムアウトは、アイドル状態になってから 10 分です。

8 [OK] をクリックします。

次に進む前に

公開アプリケーションに対する資格を非認証アクセス ユーザーに付与します。「公開アプリケーションに対する非認証アクセス ユーザーへの資格付与」を参照してください。

公開アプリケーションに対する非認証アクセス ユーザーへの資格付与

非認証アクセス ユーザーの作成後、公開アプリケーションにアクセスする資格をユーザーに付与する必要があります。

開始する前に

- RDS ホストのグループに基づいてファームを作成します。『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』 ドキュメントの「ファームの作成」を参照してください。
- RDS ホストのファームで実行される公開アプリケーションのアプリケーション プールを作成します。『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』 ドキュメントの「アプリケーション プールの作成」を参照してください。

手順

1 Horizon Administrator で、[カタログ] - [アプリケーション プール] の順に選択し、アプリケーション プールの名前をクリックします。

2 [資格] ドロップダウン メニューから [資格を追加] を選択します。

3 [追加] をクリックして、1 つ以上の検索条件を選択します。[検索] をクリックして [非認証ユーザー] チェックボックスをオンにし、検索条件に基づいて非認証アクセス ユーザーを検索します。

4 プールのアプリケーションに対する資格を付与するユーザーを選択して、[OK] をクリックします。

5 [OK] をクリックして変更を保存します。

資格付与プロセスが完了すると、非認証アクセス ユーザーの横に非認証アクセスのアイコンが表示されます。

次に進む前に

非認証アクセス ユーザーを使用して、Horizon Client にログインします。「Horizon Client からの非認証アクセス」を参照してください。

非認証アクセス セッションの検索

Horizon Administrator を使用して、ユーザーが非認証アクセスで接続しているアプリケーション セッションのリストを作成したり、検索したりできます。非認証アクセス ユーザーが接続しているセッションの横に、非認証アクセス ユーザーのアイコンが表示されます。

手順

1 Horizon Administrator で、[監視] - [セッション] の順に選択します。

2 [アプリケーション] をクリックして、アプリケーション セッションを検索します。

3 検索条件を選択し、検索を開始します。

検索結果には、ユーザー、セッションのタイプ（デスクトップまたはアプリケーション）、マシン、プールまたはファーム、DNS 名、クライアント ID、セキュリティ ゲートウェイが表示されます。セッション開始時刻、所要時間、状態、前回のセッションも検索結果に表示されます。

非認証アクセス ユーザーの削除

非認証アクセス ユーザーを削除する場合には、アプリケーション プールに対するユーザーの資格も削除する必要があります。非認証アクセス ユーザーがデフォルト ユーザーの場合、このユーザーは削除できません。

注 非認証アクセス ユーザーを削除するときに、この Active Directory ユーザーに対する既存のクライアント セッションがある場合には、変更を反映するためにクライアント セッションを再起動する必要があります。

手順

1 Horizon Administrator で、[ユーザーとグループ] を選択します。

2 [非認証アクセス] タブで [削除] をクリックします。

3 [OK] をクリックします。

次に進む前に

アプリケーションに対するユーザーの資格を削除します。『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』ドキュメントの「デスクトップまたはアプリケーション プールからの資格の削除」を参照してください。

Horizon Client からの非認証アクセス

非認証アクセスで Horizon Client にログインして、公開アプリケーションを起動します。

セキュリティを強化するため、非認証アクセス ユーザーには、Horizon Client へのログインに使用できるユーザー エイリアスが存在します。ユーザー エイリアスを選択する場合、ユーザーの Active Directory 認証情報または UPN を入力する必要はありません。Horizon Client にログインすると、公開アプリケーションをクリックして、アプリケーションを起動できます。Horizon Client のインストールと設定の詳細については、VMware Horizon Client ドキュメント Web ページにある Horizon Client のドキュメントを参照してください。

開始する前に

- Horizon 7 バージョン 7.1 の接続サーバで非認証アクセスが構成されていることを確認します。
- Horizon Administrator で、非認証アクセス ユーザーが作成されていることを確認します。デフォルトの非認証ユーザーが唯一の非認証アクセス ユーザーである場合、Horizon Client はデフォルトのユーザーで接続サーバ インスタンスに接続します。

手順

1. Horizon Client を開始します。
2. Horizon Client で、[認証されていないアクセスを使用して匿名ログイン] を選択します。
3. 接続サーバ インスタンスに接続します。
4. ドロップダウン メニューからユーザー エイリアスを選択して、[ログイン] をクリックします。

   デフォルト ユーザーには "default" というサフィックスが付いています。
5. 公開アプリケーションをダブルクリックして、アプリケーションを起動します。

公開アプリケーションに対する非認証アクセスのログイン遅延の設定

非認証アクセスを使用する場合、ユーザーは認証情報を入力しないため、RDS ホストで公開アプリケーションへの要求が処理できなくなる可能性があります。ログイン遅延を使用すると、この問題が緩和されます。遅延レベルを調整できます。遅延サポートしていないクライアントをブロックすることもできます。

開始する前に

- ユーザーの非認証アクセスが有効になっていることを確認します。
- Horizon Client バージョン 4.9 以降であることを確認します。Horizon Client バージョン 4.8 を使用している場合、ユーザーが非認証アクセスを使用して Horizon 7 バージョン 7.6 に匿名でログインすると、エラーが発生し、ログインの再試行が必要になる場合があります。

手順

1. Horizon Administrator で、[View 構成] - [サーバ] の順に選択します。
2. [接続サーバ] タブをクリックします。
3. [認証] タブをクリックします。

4 [ログイン遅延レベル] ドロップダウン メニューから、非認証アクセス ログイン遅延レベルを選択します。

オプション	説明
低	非認証アクセス ログインの遅延レベルを「低」に設定します。Microsoft Internet Explorer、Microsoft Edge などの Web ブラウザの場合、遅延レベルを低に設定することを推奨します。
中	非認証アクセス ログインの遅延レベルを「中」に設定します。デフォルトの設定です。Horizon Client バージョン 4.8 を使用している場合は、この設定を変更しないでください。
高	非認証アクセス ログインの遅延レベルを「高」に設定します。遅延レベルを「高」に設定すると、ログインまでの時間が長くなり、エンド ユーザー エクスペリエンスに影響を及ぼす可能性があります。

5 (オプション) ログイン遅延をサポートしないクライアントが非認証アクセスで Horizon 7 に接続しないようにするには、[非遵守のクライアントをブロック] を選択します。

バージョン 4.8 より前の Horizon Client は非準拠です。

6 [OK] をクリックします。

次に進む前に

非認証アクセスで Horizon Client にログインして、公開アプリケーションを起動します。「Horizon Client からの非認証アクセス」を参照してください。

Windows ベースの Horizon Client で使用できる現在のユーザーとしてログイン機能を使用

Windows の Horizon Client ユーザーが [現在のユーザーとしてログイン] チェックボックスを選択すると、クライアント システムへのログイン時に入力した認証情報が、Horizon 接続サーバ インスタンスおよびリモート デスクトップへの認証に使用されます。追加のユーザー認証は必要ありません。

この機能をサポートするため、ユーザー認証情報は接続サーバ インスタンスとクライアント システムの両方に格納されます。

- 接続サーバ インスタンスで、ユーザー認証情報は、ユーザー名、ドメイン、オプションの UPN とともにユーザー セッションに暗号化されて保存されます。認証情報は、認証が行われると追加され、セッション オブジェクトが破棄されると削除されます。セッション オブジェクトは、ユーザーがログアウトするか、セッションがタイムアウトになるか、認証が失敗した場合に破棄されます。セッション オブジェクトは揮発性メモリに保存され、Horizon LDAP またはディスク ファイルには保存されません。
- クライアント システムで、ユーザー認証情報は暗号化され、Horizon Client のコンポーネントである Authentication Package のテーブルに保存されます。認証情報は、ユーザーのログイン時にテーブルに追加され、ユーザーのログアウト時にテーブルから削除されます。テーブルは揮発性メモリに存在します。

管理者は、Horizon Client のグループ ポリシー設定を使用して、[現在のユーザーとしてログイン] チェック ボックスを使用可能にするかどうかを制御し、そのデフォルト値を設定することができます。さらに、管理者はグループ ポリシーを使用して、ユーザーが Horizon Client の [現在のユーザーとしてログイン] チェック ボックスをオンにした場合に渡されるユーザー ID と認証情報を受け入れる接続サーバ インスタンスを指定することもできます。

現在のユーザーとしてログイン機能を使用して接続サーバにログインすると、再帰的なロック解除機能が有効になります。再帰的なロック解除機能を使用すると、クライアント マシンのロックが解除された後で、すべてのリモート セッションのロックを解除できます。管理者は、Horizon Client の [クライアント マシンのロックを解除するときにリモート セッションのロックを解除します] グローバル ポリシー設定で再帰的なロック解除機能を制御できます。Horizon Client のグローバル ポリシー設定の詳細については、VMware Horizon Client ドキュメント Web ページにある Horizon Client ドキュメントを参照してください。

「現在のユーザーとしてログイン」機能には次の制限と要件があります。

- 接続サーバ インスタンスでスマート カード認証が [必須] に設定されている場合、接続サーバ インスタンスに接続する際に [現在のユーザーとしてログイン] チェック ボックスを選択したユーザーの認証が失敗します。これらのユーザーは、接続サーバにログインする際にスマート カードと PIN を使用して再認証する必要があります。
- クライアントがログインするシステムの時間と、接続サーバ ホストの時間が同期している必要があります。
- クライアント システムで、デフォルトの [ネットワーク経由でコンピュータへアクセス] ユーザー権限割り当てを変更する場合は、VMware ナレッジベース（KB）の記事 1025691 の説明に従って変更する必要があります。
- クライアント マシンは、会社の Active Directory サーバと通信できる必要があり、キャッシュされた認証情報は認証に使用されません。たとえば、ユーザーが社外のネットワークからクライアント マシンにログインすると、キャッシュされた認証情報が認証に使用されます。その後ユーザーが最初に VPN 接続を確立しないでセキュリティ サーバや接続サーバ インスタンスに接続しようとすると、認証情報の入力が求められ、現在のユーザーとしてログイン機能は機能しません。

モバイルおよび Mac 版 Horizon Client での認証情報の保存

管理者は、接続サーバを構成して、モバイルおよび Mac 版 Horizon Client を有効にして、ユーザーのユーザー名、パスワードおよびドメイン情報を記憶させることができます。

モバイルのデバイスの Horizon Client については、この機能により [パスワード保存] チェック ボックスがログイン ダイアログ ボックスに表示されます。Horizon Client for Mac の場合、この機能により [このパスワードを記憶する] チェック ボックスがログイン ダイアログ ボックスに表示されます。

ユーザーが認証情報の保存を選択すると、以後の接続時に Horizon Client のログイン フィールドに認証情報が追加されます。

この機能を有効にするには、View LDAP に値を設定して、クライアントの認証情報の保存時間を示す必要があります。Horizon Client for Mac のバージョン 4.1 以降でのみ、この機能はサポートされます。

注　Windows ベースの Horizon クライアントでは、現在のユーザーとしてログインする機能により、ユーザーに認証情報の入力を複数回求めることを回避できます。

Horizon Client の認証情報を保存するようにタイムアウト制限を構成

View LDAP の値を設定することにより、モバイル デバイスや Mac クライアント システムで、Horizon Client の認証情報の保存時間を示すタイムアウト制限を設定します。タイムアウト制限は分単位で設定します。接続サーバ インスタンス上で View LDAP を変更すると、複製されたすべての接続サーバ インスタンスに変更内容が伝わります。

開始する前に

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 [接続設定] ダイアログ ボックスで、[DC=vdi,DC=vmware,DC=int] を選択するか接続します。

3 [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.mydomain.com:389`**

4 オブジェクト [CN=Common, OU=Global, OU=Properties] で、[clientCredentialCacheTimeout] 属性の値を編集します。

   `clientCredentialCacheTimeout` が設定されていない場合、または **`0`** に設定されている場合、この機能は無効です。この機能を有効にするには、認証情報を保持する時間（分）を設定するか、値 [-1] を設定します。これは、タイムアウトがないことを示します。

接続サーバで、新しい設定がただちに有効になります。接続サーバ サービスまたはクライアント コンピュータを再起動する必要はありません。

True SSO の設定

True SSO（シングル サインオン）機能を使用すると、ユーザーは、スマート カード認証や RSA SecurID または RADIUS 認証を使用して VMware Identity Manager にログインした後、仮想デスクトップ、公開デスクトップまたはアプリケーションを使用するために、さらに Active Directory の認証情報を入力する必要がなくなります。

ユーザーが Active Directory 認証情報を使用して認証する場合は、True SSO 機能は必要ありませんが、この場合にも True SSO が使用されるように構成して、ユーザーが入力する Active Directory 認証情報が無視され、True SSO が使用されるようにできます。

仮想デスクトップまたは公開アプリケーションに接続する場合、ユーザーはネイティブ Horizon Client または HTML Access の使用を選択できます。

この機能には次の制限があります。

- この機能は、View Agent Direct Connection プラグインを使用して提供される仮想デスクトップでは動作しません。
- この機能は IPv4 環境でのみサポートされます。

以下は、True SSO の環境を設定するために実行する必要があるタスクの一覧です。

1 「True SSO のアーキテクチャの特定」

2 「エンタープライズ認証局の設定」

3 「True SSO とともに使用する証明書テンプレートの作成」

4 「登録サーバのインストールおよび設定」

5 「登録サービス クライアント証明書のエクスポート」

6 「True SSO と連携するための SAML 認証の構成」

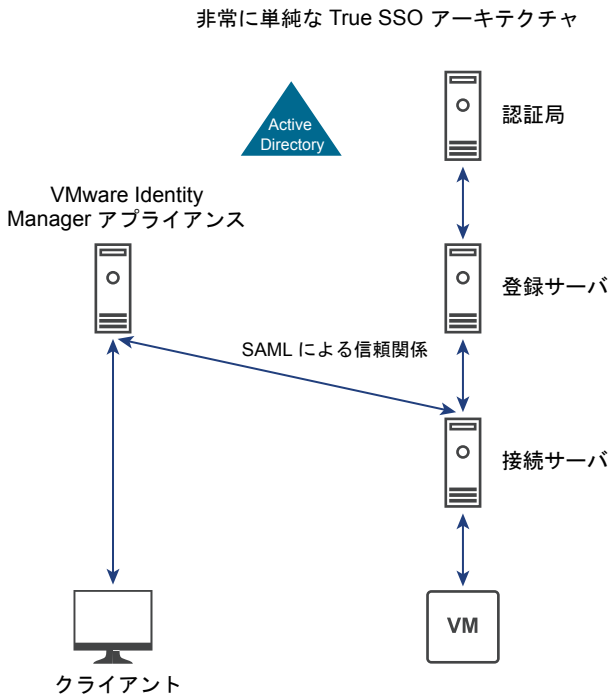
7 「True SSO のための Horizon 接続サーバの構成」

True SSO のアーキテクチャの特定

True SSO を使用するには、既存の認証局を使用するか認証局を追加して登録サーバを作成する必要があります。この 2 台のサーバの通信によって、パスワード不要の Windows ログオンを可能にする一時的な Horizon 仮想証明書が作成されます。True SSO は、1 つのドメイン、1 つのフォレストと複数ドメイン、および複数フォレストと複数ドメインのセットアップで使用できます。

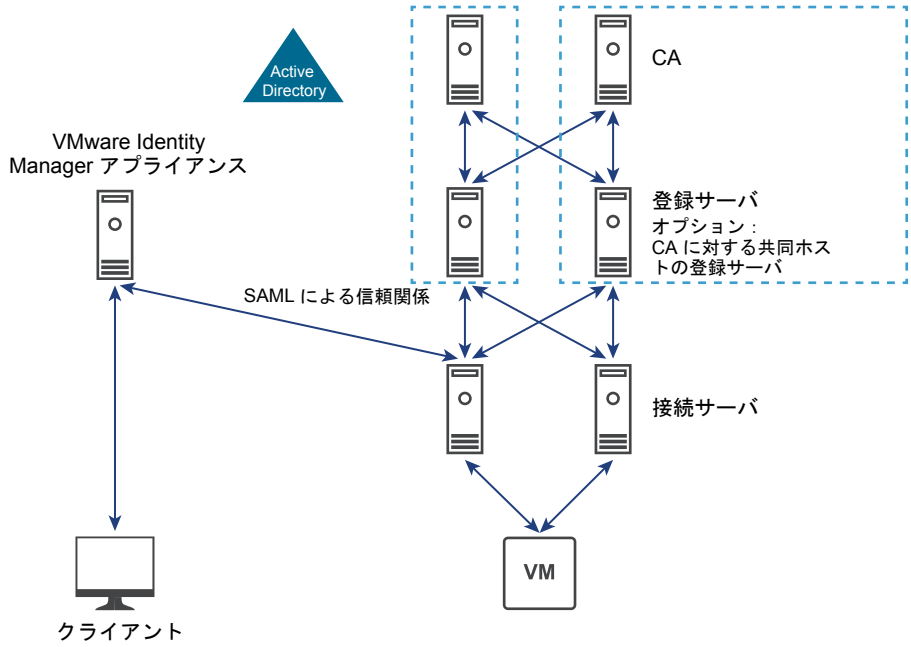
認証局 (CA) を 2 つ、登録サーバ (ES) を 2 台導入して、True SSO を使用することをお勧めします。次の例は、異なるアーキテクチャでの True SSO を示しています。

次の図は、単純な True SSO アーキテクチャを示しています。



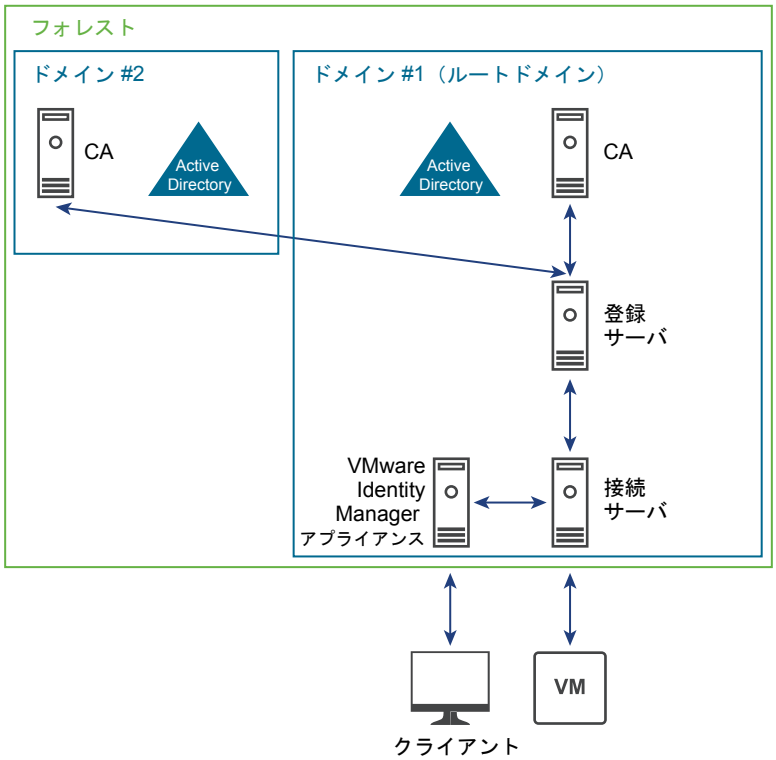
次の図は、単一ドメイン アーキテクチャでの True SSO を示しています。

HA、True SSO の典型的アーキテクチャ（単一ドメイン）

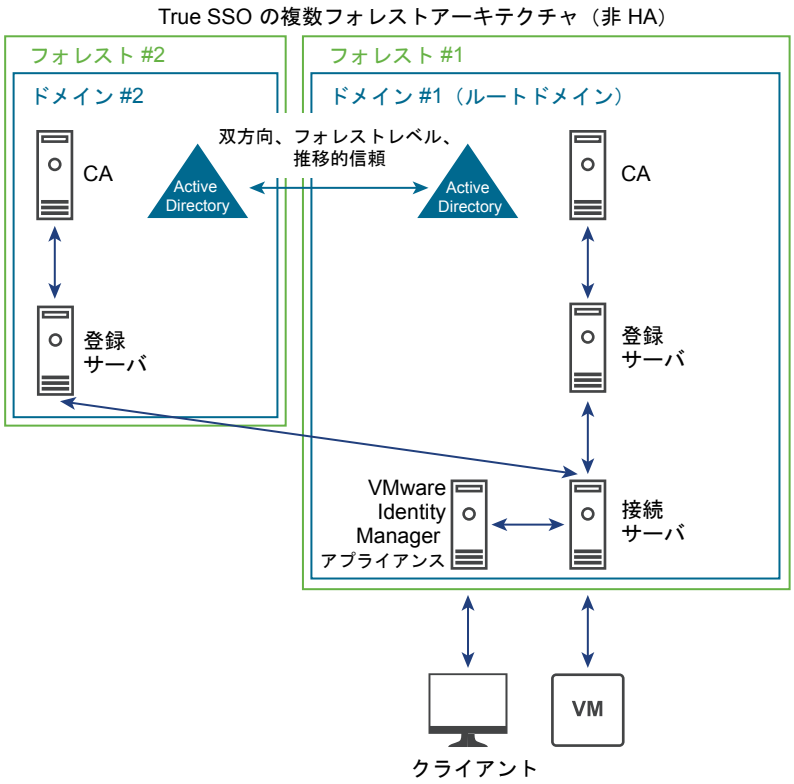


次の図は、複数ドメイン アーキテクチャを含む単一フォレストでの True SSO を示しています。

True SSO、単一フォレスト、複数ドメインのアーキテクチャ（非 HA）



次の図は、複数フォレストのアーキテクチャでの True SSO を示しています。



エンタープライズ認証局の設定

認証局をまだ設定していない場合、Active Directory Certificate Services (AD CS) ロールを Windows Server に追加し、Windows Server がエンタープライズ CA になるように構成する必要があります。

エンタープライズ CA をまだ設定していない場合、この手順に示される設定を使用していることを確認します。

エンタープライズ CA は少なくとも 1 つ必要です。VMware では、フェイルオーバーと負荷分散のために 2 つ用意することを推奨しています。True SSO 用に作成する登録サーバはエンタープライズ CA と通信します。複数のエンタープライズ CA を使用するように登録サーバを構成する場合、登録サーバは使用可能なエンタープライズ CA を交互に使用します。エンタープライズ CA をホストするマシンに登録サーバをインストールする場合、ローカル CA を優先して使用するように登録サーバを構成できます。最高のパフォーマンスを得るには、この構成をお勧めします。

この手順の一部には、読み取り専用証明書の処理の有効化が含まれます。デフォルトで、証明書の処理には、それぞれの証明書要求および発行される証明書のレコードの CA データベースへの格納が含まれています。大量の要求が継続すると、CA データベースの増加率が上昇し、ディスク容量を監視していない場合、使用可能なすべてのディスク容量が消費される可能性があります。読み取り専用証明書の処理を有効にすると、CA データベースの増加率およびデータベース管理タスクを行う頻度を削減することができます。

開始する前に

- Windows Server 2008 R2 または Windows Server 2012 R2 の仮想マシンを作成します。
- 仮想マシンが Horizon 7 のデプロイのための Active Directory ドメインの一部であることを確認します。

- IPv4 環境を使用していることを確認します。この機能は、IPv6 環境では現在サポートされていません。
- システムに固定 IP アドレスがあることを確認します。

手順

1 仮想マシン オペレーティング システムに管理者としてログインし、Server Manager を開始します。

2 ロールを追加するための設定を選択します。

オペレーティング システム	選択
Windows Server 2012 R2	a [ロールと機能を追加] を選択します。 b [インストール タイプを選択] ページで、[ロールベースまたは機能ベースのインストール] を選択します。 c [ターゲット サーバを選択] ページで、サーバを選択します。
Windows Server 2008 R2	a ナビゲーション ツリーで [ロール] を選択します。 b [ロールを追加] をクリックして**[ロールを追加]**ウィザードを起動します。

3 [サーバーの役割の選択] ページで、[Active Directory 証明書サービス] を選択します。

4 [役割と機能の追加] ウィザードで、[機能の追加] をクリックし、[管理ツールを含める] チェック ボックスを選択されたままにします。

5 [機能を選択] ページで、デフォルトを受け入れます。

6 [役割サービスの選択] ページで、[証明機関] を選択します。

7 指示に従ってインストールを終了します。

8 インストールが完了したら、[インストールの進行状況] ページで [対象サーバーに Active Directory 証明書サービスを構成する] リンクをクリックし、[AD CS の構成] ウィザードを開きます。

9 [資格情報] ページで [次へ] をクリックし、次の表に示されているとおりに [AD CS の構成] ウィザードのページに入力します。

オプション	アクション
役割サービス	[証明機関] を選択し、[構成] ではなく [次へ] をクリックします。
セットアップの種類	[エンタープライズ CA] を選択します。
CA の種類	[ルート CA] または [下位 CA] を選択します。一部の企業では 2 階層 PKI 導入が好まれます。詳細については、http://social.technet.microsoft.com/wiki/contents/articles/15037.ad-cs-step-by-step-guide-two-tier-pki-hierarchy-deployment.aspx を参照してください。
秘密キー	[新しい秘密キーを作成する] を選択します。
CA の暗号化	ハッシュ アルゴリズムには、[SHA1]、[SHA256]、[SHA384]、または [SHA512] を選択できます。キーの長さには、[1024]、[2048]、[3072]、または [4096] を選択できます。 少なくとも、SHA256、キーの長さ 2048 を使用することをお勧めします。
CA 名	デフォルトを受け入れるか名前を変更します。
有効期間	デフォルトの 5 年間を受け入れます。
証明書データベース	デフォルトを受け入れます。

10 [確認] ページで [構成] をクリックし、ウィザードで構成の成功が報告されたら、ウィザードを閉じます。

11 コマンド プロンプトを開き、次のコマンドを入力して、読み取り専用証明書の処理で使用する CA を構成します。

```
certutil –setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS
```

12 次のコマンドを入力して、CA のオフライン CRL（証明書失効リスト）のエラーを無視します。

```
certutil –setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE
```

True SSO が使用するルート証明書は通常オフラインであり、そのため失効チェックが失敗することが予想されるため、このフラグは必要です。

13 次のコマンドを入力してサービスを再起動します。

```
sc stop certsvc
sc start certsvc
```

次に進む前に

証明書テンプレートを作成します。「True SSO とともに使用する証明書テンプレートの作成」を参照してください。

True SSO とともに使用する証明書テンプレートの作成

一時的な証明書の発行に使用する証明書テンプレートを作成し、このタイプの証明書を要求できるドメイン内のコンピュータを指定する必要があります。

証明書テンプレートは複数作成することができます。設定できるテンプレートは各ドメインに 1 個のみですが、複数のドメイン間でテンプレートを共有することができます。たとえば、Active Directory フォレストにドメインが 3 個あり、すべてのドメインに True SSO を使用する場合、テンプレートは 1 個、2 個、または 3 個選択できます。すべてのドメインで同じテンプレートを共有することも、各ドメインごとに異なるテンプレートを設定することもできます。

開始する前に

- この手順で説明するテンプレートの作成に使用するエンタープライズ CA があることを確認します。「エンタープライズ認証局の設定」を参照してください。
- スマート カード認証用に Active Directory を準備していることを確認します。詳細については、『Horizon 7 のインストール』を参照してください。
- 登録サーバのドメインおよびフォレストにセキュリティ グループを作成し、そのグループに登録サーバのコンピュータ アカウントを追加します。

手順

1 True SSO を設定するには、認証局に使用しているマシンで、管理者としてオペレーティング システムにログインし、[管理ツール] - [証明機関] に移動します。

   a 左ペインのツリーを展開し、[証明書テンプレート] を右クリックし、[管理] を選択します。

   b [スマートカードによるログオン] テンプレートを右クリックし、[複製] を選択します。

c 以下のタブで次のように変更を加えます。

タブ	アクション
互換性タブ	■ [認証局] には、[Windows Server 2008 R2] を選択します。 ■ [証明書の受信者] には、[Windows 7/Windows Server 2008 R2] を選択します。
全般タブ	■ テンプレートの表示名を **True SSO** に変更します。 ■ 有効期間の長さを、一般的な営業日での時間、つまりユーザーのシステムへのログイン時間と想定される時間に変更します。 ユーザーがログオン中にネットワーク リソースへのアクセスを失わないように、有効期間をユーザー ドメインの Kerberos TGT 更新時間よりも長くする必要があります。 (チケットのデフォルトの最長有効期間は 10 時間です。デフォルトのドメイン ポリシーを検索するには、[コンピュータの構成] - [ポリシー] - [Windows の設定] - [セキュリティ設定] - [アカウント ポリシー] - [Kerberos ポリシー: チケットの最長有効期間] に移動します。) ■ 更新期間を有効期間の 50% ～ 75% に変更します。
要求処理タブ	■ [目的] には、[署名とスマート カード ログオン] を選択します。 ■ [スマート カードの自動…] を選択します。
暗号化タブ	■ [プロバイダーのカテゴリ] には、[キー格納プロバイダー] を選択します。 ■ [アルゴリズム名] には、[RSA] を選択します。
サーバ タブ	[CA データベース内に証明書および要求を保存しない] を選択します。 重要 [発行される証明書に失効情報を含めない] を必ず選択解除してください（このボックスは 1 番目のボックスを選択すると選択されるため、選択解除（クリア）する必要があります)。
発行の要件タブ	■ [次の数の認証署名] を選択し、このボックスに **1** と入力します。 ■ [ポリシーの種類] には、[アプリケーション ポリシー] を選択し、ポリシーを [証明書の要求エージェント] に設定します。 ■ [次の項目を再登録の要件とする] には、[既存の有効な証明書] を選択します。
セキュリティ タブ	登録サーバのコンピュータ アカウント用に作成したセキュリティ グループには、前提条件で説明したように、読み取り、登録の権限を指定します。 1 [追加] をクリックします。 2 証明書を登録できるコンピュータを指定します。 3 これらのコンピュータについて、該当するチェック ボックスを選択し、各コンピュータに読み取り、登録の権限を指定します。

d [新しいテンプレートのプロパティ] ダイアログ ボックスで、[OK] をクリックします。

e [証明書テンプレート コンソール] ウィンドウを閉じます。

f [証明書テンプレート] を右クリックし、[新規作成] - [発行する証明書テンプレート] を選択します。

注 この手順は、このテンプレートに基づいて証明書を発行するすべての認証局に必要です。

g [証明書テンプレートの選択] ウィンドウで、作成したテンプレート（[True SSO テンプレート] など）を選択し、[OK] をクリックします。

2 登録エージェント（コンピュータ）を設定するには、認証局に使用しているマシンで、管理者としてオペレーティング システムにログインし、[管理ツール] - [証明機関] に移動します。

a 左ペインのツリーを展開し、[証明書テンプレート] を右クリックし、[管理] を選択します。

b 登録エージェント（コンピュータ）テンプレートを選択して開き、[セキュリティ] タブで次の変更を加えます。

登録サーバのコンピュータ アカウント用に作成したセキュリティ グループには、前提条件で説明したように、読み取り、登録の権限を指定します。

1 [追加] をクリックします。

2 証明書を登録できるコンピュータを指定します。

3 これらのコンピュータについて、該当するチェック ボックスを選択し、各コンピュータに読み取り、登録の権限を指定します。

c [証明書テンプレート] を右クリックし、[新規作成] - [発行する証明書テンプレート] を選択します。

注 この手順は、このテンプレートに基づいて証明書を発行するすべての認証局に必要です。

d [証明書テンプレートの選択] ウィンドウで、[登録エージェント (コンピュータ)] を選択し、[OK] をクリックします。

次に進む前に

登録サービスを作成します。「登録サーバのインストールおよび設定」を参照してください。

登録サーバのインストールおよび設定

接続サーバ 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、登録サーバをインストールします。登録サーバは、指定したユーザーの代わりに一時的な証明書を要求します。これらの一時的な証明書は、ユーザーに Active Directory 認証情報を求めないようにするために True SSO で認証に使用されるメカニズムです。

少なくとも 1 台の登録サーバをインストールして設定する必要があります。登録サーバは、View 接続サーバと同じホストにインストールできません。フェイルオーバーと負荷分散のために、2 台の登録サーバを用意することを推奨します。2 台の登録サーバがある場合、デフォルトで一方が優先され、もう一方がフェイルオーバーに使用されます。ただし、このデフォルトを変更して、証明書要求が接続サーバから両方の登録サーバに交互に送信されるようにすることができます。

エンタープライズ CA をホストするマシンに登録サーバをインストールする場合、ローカル CA を優先して使用するように登録サーバを構成できます。最高のパフォーマンスを得るために、ローカル CA を優先して使用する構成と、登録サーバの負荷分散を行う構成を組み合わせることを推奨します。このようにすると、証明書要求が到着したときに、接続サーバは代替登録サーバを使用し、各登録サーバはローカル CA を使用して要求に対応します。使用する設定については、「登録サーバの設定」および「接続サーバの設定」を参照してください。

開始する前に

- メモリが 4 GB 以上ある Windows Server 2008 R2、Windows Server 2012 R2 または Windows Server 2016 の仮想マシンを作成するか、エンタープライズ CA をホストする仮想マシンを使用します。ドメイン コントローラになっているマシンは使用しないでください。

- View 接続サーバ、View Composer、セキュリティ サーバ、Horizon Client、View Agent、Horizon Agent などのその他の View コンポーネントが仮想マシンにインストールされていないことを確認します。
- 仮想マシンが Horizon 7 のデプロイのための Active Directory ドメインの一部であることを確認します。
- IPv4 環境を使用していることを確認します。現在、この機能は IPv6 環境ではサポートされません。
- システムに固定 IP アドレスを設定することを強く推奨します。
- 管理者権限のあるドメイン ユーザーとしてオペレーティング システムにログインできることを確認できます。インストーラを実行するには、管理者としてログインする必要があります。

手順

1 登録サーバに使用するマシンで、証明書スナップインを MMC に追加します。

   a MMC コンソールを開き、[ファイル] - [スナップインの追加と削除] を選択します。

   b [利用できるスナップイン] で [証明書] を選択し、[追加] をクリックします。

   c [証明書スナップイン] ウィンドウで、[コンピュータ アカウント] を選択し、[次へ] をクリックして [完了] をクリックします。

   d [スナップインの追加と削除] ウィンドウで、[OK] をクリックします。

2 登録エージェント証明書を発行します。

   a 証明書コンソールで、コンソールのルート ツリーを展開し、[個人] フォルダを右クリックして [すべてのタスク] - [新しい証明書の要求] を選択します。

   b [証明書の登録] ウィザードで、[証明書の要求] ページが表示されるまでデフォルトを受け入れます。

   c [証明書の要求] ページで、[登録エージェント (コンピュータ)] チェック ボックスをオンにして、[登録] をクリックします。

   d 他のウィザード ページでデフォルトを受け入れ、最後のページで [完了] をクリックします。

   MMC コンソールで、[個人] フォルダを展開し、左ペインで [証明書] を選択すると、新しい証明書が右ペインに表示されます。

3 登録サーバをインストールします。

   a VMware ダウンロード ページ (https://my.vmware.com/web/vmware/downloads) から、View 接続サーバ インストーラ ファイルをダウンロードします。

   [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 View 接続サーバ ファイルが含まれます。

   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。

   b インストーラ ファイルをダブルクリックしてウィザードを開始し、[インストール オプション] ページが表示されるまでプロンプトに従って進みます。

c [インストール オプション] ページで、[Horizon 7 登録サーバ]を選択し、登録サーバ インスタンスの認証モードを選択して [[次へ]] をクリックします。

オプション	説明
Horizon 7	Horizon 7 環境の認証モードを構成します。
Horizon Cloud	Horizon Cloud 環境の認証モードを構成します。

d プロンプトに従って、インストールを完了します。

登録サーバが機能するには、ポート 32111 (TCP) で外部からの接続を有効にする必要があります。インストール中に、インストーラはデフォルトでポートを開きます。

次に進む前に

- エンタープライズ CA をホストするマシンに登録サーバをインストールした場合、ローカル CA を優先して使用するように登録サーバを構成します。「登録サーバの設定」を参照してください。複数の登録サーバをインストールして設定する場合は、オプションで、接続サーバを設定して登録サーバ間での負荷分散を行えるようにします。「接続サーバの設定」を参照してください。
- 接続サーバと登録サーバをペアにします。「登録サービス クライアント証明書のエクスポート」を参照してください。

登録サービス クライアント証明書のエクスポート

ペアリングを実行するため、MMC 証明書スナップインを使用して、クラスタ内の 1 台の接続サーバから自動生成された自己署名登録サービス クライアント証明書をエクスポートできます。接続サーバは登録サーバによって提供される登録サービスのクライアントであるため、この証明書はクライアント証明書と呼ばれます。

登録サービスは、Active Directory ユーザー向けの一時的な証明書の発行を登録サーバに求めるときに、VMware Horizon 接続サーバを信頼する必要があります。このため、VMware Horizon 接続サーバ クラスタまたはポッドは登録サーバとペアになっている必要があります。

登録サービス クライアント証明書は、Horizon 7 以降の接続サーバがインストールされて VMware Horizon 接続サーバ サービスが開始されたときに、自動的に作成されます。証明書は View LDAP を介して、後でクラスタに追加される他の Horizon 7 接続サーバに配布されます。配布された証明書はコンピュータにある Windows 証明書ストアのカスタム コンテナ (`VMware Horizon View Certificates\Certificates`) に格納されます。

開始する前に

Horizon 7 以降の接続サーバがあることを確認します。インストール手順については、Horizon 7 のインストールを参照してください。アップグレード手順については、Horizon 7 のアップグレードを参照してください。

重要 接続サーバで作成された自己生成証明書を使用する代わりに、独自の証明書を使用してペアリングを実行できます。そのためには、優先する証明書（および関連付けられたプライベート キー）を接続サーバ マシンにある Windows 証明書ストアのカスタム コンテナ (`VMware Horizon View Certificates\Certificates`) に配置します。次に、証明書のわかりやすい名前を **`vdm.ec.new`** に設定し、サーバを再起動する必要があります。クラスタ内の他のサーバは、LDAP からこの証明書を取得します。その後この手順を実行できます。

手順

1 クラスタ内のいずれかの接続サーバ マシンで、証明書スナップインを MMC に追加します。

   a MMC コンソールを開き、[ファイル] - [スナップインの追加と削除] を選択します。

   b [利用できるスナップイン] で [証明書] を選択し、[追加] をクリックします。

   c [証明書スナップイン] ウィンドウで、[コンピュータ アカウント] を選択し、[次へ] をクリックして [完了] をクリックします。

   d [スナップインの追加と削除] ウィンドウで、[OK] をクリックします。

2 MMC コンソールの左ペインで、[VMware Horizon View Certificates] フォルダを展開し、[Certificates] フォルダを選択します。

3 右ペインで、わかりやすい名前の [vdm.ec] 証明書ファイルを右クリックし、[すべてのタスク] - [エクスポート] を選択します。

4 証明書のエクスポート ウィザードでデフォルト設定（[いいえ、秘密キーをエクスポートしません] ラジオ ボタンは選択されたまま）を適用します。

5 ファイルに名前を付けるように求められたら、登録サービス クライアント証明書用の **EnrollClient** などのファイル名を入力し、プロンプトに従って証明書のエクスポートを完了します。

次に進む前に

証明書を登録サーバにインポートします。「登録サーバでの登録サービス クライアント証明書のインポート」を参照してください。

登録サーバでの登録サービス クライアント証明書のインポート

ペアリング プロセスを完了するには、MMC の証明書スナップインを使用して、登録サービス クライアント証明書を登録サーバにインポートします。この手順は、各登録サーバで実行する必要があります。

開始する前に

- Horizon 7 以降の登録サーバがあることを確認します。「登録サーバのインストールおよび設定」を参照してください。
- インポートする証明書が正しいことを確認します。独自の証明書を使用することも、クラスタ内の 1 台の接続サーバで自動生成される自己署名の登録サービス クライアント証明書を使用することもできます。詳細については、「登録サービス クライアント証明書のエクスポート」を参照してください。

  重要 独自の証明書を使用してペアリングを行うには、優先される証明書（および関連付けられたプライベート キー）を接続サーバ マシンの Windows 証明書ストアのカスタム コンテナ (**VMware Horizon View Certificates\Certificates**) に配置します。次に、証明書のわかりやすい名前を **vdm.ec.new** に設定し、サーバを再起動する必要があります。クラスタ内の他のサーバは、LDAP からこの証明書を取得します。その後この手順を実行できます。

  独自のクライアント証明書がある場合、登録サーバにコピーする証明書は、クライアント証明書を生成するために使用したルート証明書です。

手順

1 適切な証明書ファイルを登録サーバ マシンにコピーします。

自動生成される証明書を使用するには、接続サーバの登録サービス クライアント証明書をコピーします。独自の証明書を使用するには、クライアント証明書を生成するために使用されたルート証明書をコピーします。

2 登録サーバで、証明書スナップインを MMC に追加します。

a MMC コンソールを開き、[ファイル] - [スナップインの追加と削除] を選択します。

b [利用できるスナップイン] で [証明書] を選択し、[追加] をクリックします。

c [証明書スナップイン] ウィンドウで、[コンピュータ アカウント] を選択し、[次へ] をクリックして [完了] をクリックします。

d [スナップインの追加と削除] ウィンドウで、[OK] をクリックします。

3 MMC コンソールの左ペインで、[VMware Horizon View 登録サーバの信頼されたルート] フォルダを右クリックし、[すべてのタスク] - [インポート] を選択します。

4 証明書のインポート ウィザードで、プロンプトに従って [EnrollClient] 証明書ファイルを参照して開きます。

5 プロンプトに従ってデフォルトを受け入れ、証明書のインポートを終了します。

6 インポートされた証明書を右クリックし、**vdm.ec**（登録クライアント証明書）などのわかりやすい名前を追加します。

Horizon 7 クラスタを識別するわかりやすい名前を使用することを推奨しますが、クライアント証明書を簡単に識別できる任意の名前を使用できます。

次に進む前に

認証を VMware Identity Manager に委任するために使用される SAML 認証子を構成します。「True SSO と連携するための SAML 認証の構成」を参照してください。

True SSO と連携するための SAML 認証の構成

Horizon 7 で導入された True SSO 機能により、ユーザーはスマート カード、RADIUS、または RSA SecurID 認証を使用して VMware Identity Manager 2.6 以降のリリースにログインできます。また、ユーザーがリモート デスクトップまたはアプリケーションを初めて起動するときでも、Active Directory 認証情報を求められなくなりました。

以前のリリースでは、SSO（シングル サインオン）は、以前に Active Directory 認証情報で認証されていないユーザーが最初にリモート デスクトップを起動したとき、またはアプリケーションを公開したときに Active Directory 認証情報をユーザーに求めることで機能していました。この認証情報がキャッシュされ、これによりユーザーは認証情報を再度入力せずに、以降の起動を行うことができました。True SSO では、一時的な証明書が作成され、Active Directory 認証情報の代わりに使用されます。

VMware Identity Manager の SAML 認証を構成するプロセスは変わっていませんが、True SSO では 1 つの手順が追加されています。パスワードのポップアップが表示されないように VMware Identity Manager を構成する必要があります。

注　導入環境に複数の接続サーバ インスタンスが含まれる場合は、各インスタンスに SAML 認証子を関連付ける必要があります。

開始する前に

- シングル サインオンがグローバル設定として有効になっていることを確認します。Horizon Administrator で、[構成 > グローバル設定] を選択し、[Single Sign On (SSO)] が [有効] に設定されていることを確認します。
- VMware Identity Manager がインストールされ、構成されていることを確認します。https://docs.vmware.com/jp/VMware-Identity-Manager/index.html にある VMware Identity Manager のドキュメントを参照してください。
- 接続サーバ ホストに、SAML サーバ証明書用の認証局 (CA) が署名したルート証明書がインストールされていることを確認します。VMware では、自己署名の証明書を使用するように SAML 認証子を構成することは推奨されません。『Horizon 7 のインストール』ドキュメントにある「Horizon 7 Server 用の SSL 証明書の構成」の章のトピック「ルート証明書と中間証明書を Windows 証明書ストアにインポートする」を参照してください。
- VMware Identity Manager サーバ インスタンスの FQDN を書き留めます。

手順

1. Horizon Administrator で、[構成 > サーバ] の順に選択します。
2. [接続サーバ] タブで、SAML 認証子を関連付けるサーバ インスタンスを選択して [編集] をクリックします。
3. [認証] タブで、[VMware Horizon (SAML 2.0 認証子) への認証の委任] ドロップダウン メニューから、[許可] または [必須] を選択します。

   要件に応じて、環境内の各接続サーバ インスタンスを異なる SAML 認証設定で構成できます。
4. [SAML 認証子の管理] をクリックし、[追加] をクリックします。
5. [SAML 2.0 認証子を追加] ダイアログ ボックスで SAML 認証子を構成します。

オプション	説明
ラベル	VMware Identity Manager サーバ インスタンスの FQDN を使用できます。
説明	（オプション）VMware Identity Manager サーバ インスタンスの FQDN を使用できます。
メタデータ URL	SAML ID プロバイダと Horizon 接続サーバ インスタンス間で SAML 情報を交換するために必要な情報すべてを取得するための URL。URL `https://<YOUR HORIZON SERVER NAME>/SAAS/API/1.0/GET/metadata/idp.xml` で、[<YOUR HORIZON SERVER NAME>] をクリックして VMware Identity Manager サーバ インスタンスの FQDN に置換します。
管理 URL	SAML ID プロバイダ（VMware Identity Manager インスタンス）の管理コンソールにアクセスするための URL。この URL の形式は、`https://<Identity-Manager-FQDN>:8443.` です。

6 [OK] をクリックして SAML 認証子の構成を保存します。

有効な情報を指定した場合、自己署名の証明書を受け入れるか（推奨されません）、Horizon 7 および VMware Identity Manager の信頼できる証明書を使用する必要があります。

[SAML 2.0 認証子] ドロップダウン メニューに、新規に作成された認証子が表示され、選択した認証子として設定されます。

7 Horizon Administrator ダッシュボードの [システムの健全性] セクションで、[その他のコンポーネント] - [SAML 2.0 認証子] を選択し、追加した SAML 認証子を選択して詳細を確認します。

構成に成功した場合、認証子の健全性は緑色です。証明書が信頼されていない場合、VMware Identity Manager サービスを利用できない場合、またはメタデータ URL が使用不可の場合、認証子の健全性が赤色で表示されることがあります。証明書が信頼されていない場合は、[検証] をクリックして証明書を検証してから受け入れることができます。

8 VMware Identity Manager 管理コンソールにログインし、[View プール] ページに移動して、[パスワードのポップアップを非表示にする] チェック ボックスをオンにします。

次に進む前に

- 接続サーバのメタデータの有効期間を延長して、リモート セッションが 24 時間経過後に終了されないようにします。「接続サーバでのサービス プロバイダ メタデータの有効期間の変更」を参照してください。
- `vdmutil` コマンドライン インターフェイスを使用して、接続サーバの True SSO を構成します。「True SSO のための Horizon 接続サーバの構成」を参照してください。

SAML 認証の仕組みの詳細については、「SAML 認証の使用」を参照してください。

True SSO のための Horizon 接続サーバの構成

`vdmutil` コマンドライン インターフェイスを使用して、True SSO の構成や有効化/無効化を行うことができます。

この手順は、クラスタ内の 1 つの接続サーバでのみ実行する必要があります。

重要　この手順では、True SSO を有効にするために必要なコマンドのみを使用します。True SSO 構成の管理に使用できるすべての構成オプションとその説明のリストについては、「True SSO 構成のコマンドライン リファレンス」を参照してください。

開始する前に

- 管理者ロールを持つユーザーとしてコマンドを実行できることを確認します。Horizon Administrator を使用して管理者ロールをユーザーに割り当てることができます。第 6 章「ロールベースの委任管理の構成」を参照してください。
- 次のサーバの完全修飾ドメイン名 (FQDN) があることを確認します。
  - 接続サーバ
  - 登録サーバ

    詳細については、「登録サーバのインストールおよび設定」を参照してください。

- エンタープライズ認証局

  詳細については、「エンタープライズ認証局の設定」を参照してください。

- ドメインの Netbios 名または FQDN を把握していることを確認します。
- 証明書テンプレートが作成されていることを確認します。「True SSO とともに使用する証明書テンプレートの作成」を参照してください。
- 認証を VMware Identity Manager に委任するための SAML 認証子が作成されていることを確認します。「True SSO と連携するための SAML 認証の構成」を参照してください。

手順

1 クラスタ内の接続サーバで、コマンド プロンプトを開き、登録サーバを追加するためのコマンドを入力します。

```
vdmUtil --authAs <admin-role-user> --authDomain <domain-name> --authPassword <admin-user-password> --truesso --environment --add --enrollmentServer <enroll-server-fqdn>
```

登録サーバがグローバル リストに追加されます。

2 登録サーバの情報をリストするコマンドを入力します。

```
vdmUtil --authAs <admin-role-user> --authDomain <domain-name> --authPassword <admin-user-password> --truesso --environment --list --enrollmentServer <enroll-server-fqdn> --domain <domain-fqdn>
```

出力には、フォレスト名、登録サーバの証明書が有効かどうか、使用できる証明書テンプレートの名前と詳細、認証局の共通名が表示されます。登録サーバが接続できるドメインを構成するには、登録サーバの Windows レジストリ設定を使用します。デフォルトでは、すべての信頼する側のドメインに接続されます。

重要　次の手順で認証局の共通名を指定する必要があります。

---

3 構成情報を保持する True SSO コネクタを作成して有効化するコマンドを入力します。

```
vdmUtil --authAs <admin-role-user> --authDomain <domain-name> --authPassword <admin-user-password> --truesso --create --connector --domain <domain-fqdn> --template <TrueSSO-template-name> --primaryEnrollmentServer <enroll-server-fqdn> --certificateServer <ca-common-name> --mode enabled
```

このコマンドの <TrueSSO-template-name> は、前の手順の出力に表示されていたテンプレートの名前で、<ca-common-name> は、その出力に表示されていたエンタープライズ認証局の共通名です。

True SSO コネクタは、指定されたドメインのプールまたはクラスタで有効になります。プール レベルで True SSO を無効にするには、`vdmUtil --certsso --edit --connector <domain> --mode disabled` を実行します。個別の仮想マシンで True SSO を無効にするには、GPO (vdm_agent.adm) を使用できます。

4 使用可能な SAML 認証子を検出するコマンドを入力します。

```
vdmUtil --authAs <admin-role-user> --authDomain <domain-name> --authPassword <admin-user-password> --truesso --list --authenticator
```

Horizon Administrator を使用して、VMware Identity Manager と接続サーバ間の SAML 認証を構成すると、認証子が作成されます。

出力には、認証子の名前や True SSO が有効になっているかどうかが表示されます。

重要 次の手順で認証子の名前を指定する必要があります。

5 認証子で True SSO モードを使用できるようにするコマンドを入力します。

```
vdmUtil --authAs <admin-role-user> --authDomain <domain-name> --authPassword <admin-user-password> --truesso --authenticator --edit --name <authenticator-fqdn> --truessoMode {ENABLED|ALWAYS}
```

ユーザーが VMware Identity Manager にログインしたときにパスワードを入力しなかった場合にのみ True SSO を使用するには、`--truessoMode` に `ENABLED` を使用します。この場合、パスワードが使用されていてキャッシュされていれば、そのパスワードが使用されます。ユーザーが VMware Identity Manager にログインしたときにパスワードを入力した場合でも True SSO を使用するには、`--truessoMode` を `ALWAYS` に設定します。

次に進む前に

Horizon Administrator で、True SSO 構成の健全性ステータスを確認します。詳細については、「システム健全性ダッシュボードを使用した True SSO に関する問題のトラブルシューティング」を参照してください。

詳細設定オプションを構成するには、適切なシステムの Windows の詳細設定を使用します。「True SSO の詳細設定」を参照してください。

True SSO 構成のコマンドライン リファレンス

True SSO 機能の構成と管理には vdmutil コマンドライン インターフェイスを使用できます。

ユーティリティの場所

デフォルトの場合、`vdmutil` コマンドの実行可能ファイルのパスは `C:\Program Files\VMware\VMware View\Server\tools\bin` です。コマンド ラインにパスを入力するのを避けるには、PATH 環境変数にパスを追加します。

構文と認証

Windows コマンド プロンプトで、次の形式の `vdmutil` コマンドを使用します。

```
vdmutil <authentication options> --truesso <additional options and arguments>
```

使用できる追加のオプションは、コマンド オプションによって異なります。このトピックでは、True SSO (--truesso) を構成するためのオプションについて説明します。次の例は、True SSO に構成されている接続を一覧表示するコマンドを示しています。

```
vdmUtil --authAs <admin-role-user> --authDomain <domain-name> --authPassword <admin-user-password> --truesso --list --connector
```

vdmutil コマンドには、認証に使用するユーザー名、ドメイン、およびパスワードを指定する認証オプションがあります。

表 5-1. vdmutil コマンド認証オプション

オプション	説明
--authAs	Horizon 7 管理ユーザーの名前。<domain\username> またはユーザー プリンシパル名 (UPN) 形式を使用しないでください。
--authDomain	--authAs オプションで指定された Horizon 7 管理者ユーザーのドメインの完全修飾ドメイン名または NETBIOS 名。
--authPassword	Horizon 7 オプションで指定された --authAs 管理者ユーザーのパスワード。パスワードの代わりに "*" を入力すると、vdmutil コマンドでパスワードが要求され、機密性の高いパスワードはコマンド ラインのコマンド履歴に残りません。

認証オプションは、--help および --verbose を除くすべての vdmutil コマンド オプションを指定して使用する必要があります。

コマンド出力

vdmutil コマンドは、操作が成功すると 0 を返し、失敗すると操作の失敗に固有の 0 以外のコードを返します。vdmutil コマンドは標準エラー出力にエラー メッセージを書き込みます。操作で出力が生成されたり、--verbose オプションを使用して詳細なログ記録が有効になっていると、vdmutil コマンドは標準出力に米国英語で出力を書き込みます。

登録サーバの管理のためのコマンド

ドメインごとに登録サーバを 1 台追加する必要があります。また、2 番目の登録サーバを追加し、サーバがバックアップとして使用されるように後で指定することもできます。

読みやすさを考慮し、次の表に示すオプションはユーザーが入力する完全なコマンドになっていません。特定のタスクに固有のオプションのみを記載しています。たとえば、ある行は --environment --list --enrollmentServers オプションを示しますが、実際に入力する vdmUtil コマンドには、次のように認証用のオプションや、True SSO を構成することを指定するためのオプションも含まれます。

```
vdmUtil --authAs <admin-role-user> --authDomain <netbios-name> --authPassword <admin-user-password> --truesso --environment --list --enrollmentServers
```

認証オプションの詳細については、「True SSO 構成のコマンドライン リファレンス」を参照してください。

表 5-2. 登録サーバの管理のための vdmutil truesso コマンド オプション

コマンドとオプション	説明
`--environment --add --enrollmentServer` <enroll-server-fqdn>	指定された登録サーバを環境に追加します。<enroll-server-fqdn> は登録サーバの FQDN です。登録サーバがすでに追加されている場合は、このコマンドを実行しても何も起こりません。
`--environment --remove --enrollmentServer` <enroll-server-fqdn>	指定した登録サーバを環境から削除します。<enroll-server-fqdn> は登録サーバの FQDN です。登録サーバがすでに削除されている場合は、このコマンドを実行しても何も起こりません。
`--environment --list --enrollmentServers`	環境にあるすべての登録サーバの FQDN を一覧表示します。
`--environment --list --enrollmentServer` <enroll-server-fqdn>	登録サーバが属するドメインおよびフォレストによって信頼されているドメインおよびフォレストの FQDN と、登録証明書の状態（VALID または INVALID）を一覧表示します。VALID は、登録サーバに Enrollment Agent 証明書がインストールされていることを意味します。この状態は以下のいくつかの理由で INVALID になる可能性があります。 ■ 証明書がインストールされていない。 ■ 証明書がまだ有効ではないか、期限切れである。 ■ 信頼できるエンタープライズ CA によって証明書が発行されていない。 ■ プライベート キーが使用できない。 ■ 証明書が破損している。 登録サーバのログ ファイルには INVALID 状態の理由を表示できます。
`--environment --list --enrollmentServer` <enroll-server-fqdn> `--domain` <domain-fqdn>	指定されたドメインの登録サーバについて、使用できる認証局の CN（共通名）を一覧表示し、True SSO に使用できる各証明書テンプレートに関する次の情報を表示します：名前、最小キー長、およびハッシュ アルゴリズム。

コネクタの管理のためのコマンド

ドメインごとにコネクタを 1 つ作成します。コネクタは True SSO に使用されるパラメータを定義します。

読みやすさを考慮し、次の表に示すオプションはユーザーが入力する完全なコマンドになっていません。特定のタスクに固有のオプションのみを記載しています。たとえば、ある行は `--list --connector` オプションを示しますが、実際に入力する `vdmUtil` コマンドには、次のように認証用のオプションや、True SSO を構成することを指定するためのオプションも含まれます。

```
vdmUtil --authAs <admin-role-user> --authDomain <netbios-name> --authPassword <admin-user-password> --truesso --list --connector
```

認証オプションの詳細については、「True SSO 構成のコマンドライン リファレンス」を参照してください。

表 5-3. コネクタの管理のための vdmutil truesso コマンド オプション

オプション	説明
`--create --connector --domain` <domain-fqdn> `--template` <template-name> `--primaryEnrollmentServer` <enroll-server1-fqdn> [`--secondaryEnrollmentServer` <enroll-server2-fqdn>] `--certificateServer` <CA-common-name> `--mode {enabled |disabled}`	指定したドメインのコネクタを作成し、次の設定を使用するようにコネクタを構成します。 ■ <template-name> は使用する証明書テンプレートの名前です。 ■ <enroll-server1-fqdn> は使用するプライマリ登録サーバの FQDN です。 ■ <enroll-server2-fqdn> は使用するセカンダリ登録サーバの FQDN です。この設定はオプションです。 ■ <CA-common-name> は使用する認証局の共通名です。これには、カンマで区切った CA のリストを指定できます。 特定の登録サーバで使用できる証明書テンプレートと認証局を確認するには、`--truesso --environment --list --enrollmentServer` <enroll-server-fqdn> `--domain` <domain-fqdn> オプションを指定して `vdmutil` コマンドを実行します。
`--list --connector`	コネクタがすでに作成されているドメインの FQDN を一覧表示します。
`--list --connector --verbose`	コネクタを持つすべてのドメインを一覧表示し、コネクタごとに次の情報を表示します。 ■ プライマリ登録サーバ ■ セカンダリ登録サーバ（1 台存在する場合） ■ 証明書テンプレートの名前 ■ コネクタが有効か無効か ■ 認証局サーバの共通名（複数ある場合）
`--edit --connector` <domain-fqdn> [`--template` <template-name>] [`--mode {enabled |disabled}`] [`--primaryEnrollmentServer` <enroll-server1-fqdn>] [`--secondaryEnrollmentServer` <enroll-server2-fqdn>] [`--certificateServer` <CA-common-name>]	<domain-fqdn> で指定したドメインに作成されるコネクタの場合、次のいずれかの設定を変更できます。 ■ <template-name> は使用する証明書テンプレートの名前です。 ■ モードは `enabled` または `disabled` のいずれかになります。 ■ <enroll-server1-fqdn> は使用するプライマリ登録サーバの FQDN です。 ■ <enroll-server2-fqdn> は使用するセカンダリ登録サーバの FQDN です。この設定はオプションです。 ■ <CA-common-name> は使用する認証局の共通名です。これには、カンマで区切った CA のリストを指定できます。
`--delete --connector` <domain-fqdn>	<domain-fqdn> で指定されたドメインに作成されたコネクタを削除します。

認証子の管理のためのコマンド

認証子は、VMware Identity Manager Horizon 7 と接続サーバの間の SAML 認証を構成すると作成されます。管理タスクは、認証子の True SSO を有効または無効にすることに限られます。

読みやすさを考慮し、次の表に示すオプションはユーザーが入力する完全なコマンドになっていません。特定のタスクに固有のオプションのみを記載しています。たとえば、ある行は `--list --authenticator` オプションを示しますが、実際に入力する `vdmUtil` コマンドには、次のように認証用のオプションや、True SSO を構成することを指定するためのオプションも含まれます。

```
vdmUtil --authAs <admin-role-user> --authDomain <netbios-name> --authPassword <admin-user-password> --truesso --list --authenticator
```

認証オプションの詳細については、「True SSO 構成のコマンドライン リファレンス」を参照してください。

表 5-4. 認証子の管理のための vdmutil truesso コマンド オプション

コマンドとオプション	説明
`--list --authenticator [--verbose]`	ドメイン内にあるすべての SAML 認証子の完全修飾ドメイン名 (FQDN) を一覧表示します。True SSO を有効にするかどうかを個々に指定します。`--verbose` オプションを使用した場合は、関連付けられた接続サーバの FQDN も一覧に表示されます。
`--list --authenticator --name` <label>	指定された認証子について、True SSO が有効かどうかと、関連付けられた接続サーバの FQDN も一覧表示します。<label> には、`--authenticator` オプションを使用して `--name` オプションを使用しない場合に一覧表示されるいずれかの名前を使用してください。
`--edit --authenticator --name` <label> `--truessoMode` <mode-value>	指定された認証子について、True SSO モードに、指定された値を設定します。<mode-value> には次のいずれかの値を指定できます。 ■ `ENABLED`。True SSO は、ユーザーの Active Directory 認証情報を使用できないときにのみ使用されます。 ■ `ALWAYS`。True SSO は、vIDM が ユーザーの Active Directory 認証情報を使用している場合でも常に使用されます。 ■ `DISABLED`。True SSO は無効になっています。 <label> には、`--authenticator` オプションを使用して `--name` オプションを使用しない場合に一覧表示されるいずれかの名前を使用してください。

True SSO の詳細設定

True SSO の詳細設定を管理するには、Horizon Agent マシンの GPO テンプレート、登録サーバのレジストリ設定、接続サーバの LDAP エントリを使用します。これらの設定には、デフォルトのタイムアウト、負荷分散の構成、含めるドメインの指定などが含まれます。

Horizon Agent の設定

エージェント OS で GPO テンプレートを使用してプール レベルで True SSO をオフにしたり、キーのサイズや数などの証明書設定および再接続試行の設定のデフォルトを変更したりできます。

注　次の表は、個々の仮想マシンでエージェントを構成するために使用する設定を示していますが、Horizon Agent の構成テンプレート ファイルを使用することもできます。ADMX テンプレート ファイルの名前は (`vdm_agent.admx`)。テンプレート ファイルを使用して、デスクトップまたはアプリケーション プールのすべての仮想マシンにこれらのポリシー設定を適用します。ポリシーが設定されている場合、レジストリ設定よりもポリシーが優先されます。

ADMX ファイルは、`VMware-Horizon-Extras-Bundle-<x.x.x>-<yyyyyyy>.zip` に含まれています。このファイルは、VMware ダウンロード サイト (https://my.vmware.com/web/vmware/downloads) 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。

表 5-5. Horizon Agent で True SSO を構成するためのキー

キー	最小～最大	説明
`Disable True SSO`	該当なし	エージェントで機能を無効にするには、このキーを **`true`** に設定します。グループ ポリシーでこの設定を使用すると、プール レベルで True SSO が無効になります。デフォルトは **`false`** です。
`Certificate wait timeout`	10 ～ 120	エージェントに到着する証明書のタイムアウト期間（秒）を指定します。デフォルトは **`40`** です。
`Minimum key size`	1024 ～ 8192	許可されるキーの最小サイズ。デフォルトは **`1024`** です。このデフォルト値は、キー サイズが 1024 未満の場合はキーを使用できないことを意味します。
`All key sizes`	該当なし	使用できるキー サイズのカンマ区切りのリスト。最大 5 個のサイズを指定できます（**`1024,2048,3072,4096`** など）。デフォルトは **`2048`** です。
`Number of keys to pre-create`	1 ～ 100	リモート デスクトップとホスト型 Windows アプリケーションを提供する RDS サーバで事前作成するキーの数。デフォルトは **`5`** です。
`Minimum validity period required for a certificate`	該当なし	ユーザーの再接続に証明書が再利用されるときに必要な最小有効期間（分）。デフォルトは **`5`** です。

登録サーバの設定

登録サーバ OS で Windows レジストリ設定を使用して、接続するドメイン、さまざまなタイムアウト期間、ポーリング期間、再試行回数、および同じローカル サーバにインストールされている認証局を使用するかどうかを構成できます（推奨）。

詳細な設定を変更するには、登録サーバ マシンで Windows レジストリ エディタ (`regedit.exe`) を開き、次のレジストリ キーに移動します。

```
HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Enrollment Service
```

表 5-6. 登録サーバで True SSO を構成するためのレジストリ キー

レジストリ キー	最小～最大	Type	説明
`ConnectToDomains`	該当なし	REG_MULTI_SZ	登録サーバが自動的に接続を試みるドメインのリストこの複数文字列のレジストリ タイプでは、各ドメインの DNS 完全修飾ドメイン名 (FQDN) が個別の行で表示されます。 デフォルトでは、すべてのドメインを信頼します。
`ExcludeDomains`	該当なし	REG_MULTI_SZ	登録サーバが自動的に接続しないドメインのリストドメインを含む設定が接続サーバによって提供されると、登録サーバはそのドメインへの接続を試みます。この複数文字列のレジストリ タイプでは、各ドメインの DNS FQDN が個別の行で表示されます。 デフォルトでは、除外されるドメインはありません。

表 5-6. 登録サーバで True SSO を構成するためのレジストリ キー (続き)

レジストリ キー	最小～最大	Type	説明
ConnectToDomainsInForest	該当なし	REG_SZ	登録サーバがメンバーになっているフォレスト内のすべてのドメインに接続して使用するかどうかを指定します。デフォルトは TRUE です。 次のいずれかの値を使用します。 ■ **0**：false を意味します。使用されているフォレストのドメインに接続しません。 ■ **! =0**：true を意味します。
ConnectToTrustingDomains	該当なし	REG_SZ	明示的に信頼/受信するドメインに接続するかどうかを指定します。デフォルトは TRUE です。 次のいずれかの値を使用します。 ■ **0**：false を意味します。明示的に信頼/受信するドメインに接続しません。 ■ **!=0**：true を意味します。
PreferLocalCa	該当なし	REG_SZ	パフォーマンス上の利点を得るため、ローカルにインストールされた CA が存在する場合に使用するかどうかを指定します。TRUE に設定されている場合、登録サーバはローカル CA に要求を送信します。ローカル CA への接続に失敗すると、登録サーバは別の CA への証明書要求の送信を試みます。デフォルトは FALSE です。 次のいずれかの値を使用します。 ■ **0**：false を意味します。 ■ **!=0**：true を意味します。
MaxSubmitRetryTime	9,500 ～ 59,000	DWORD	証明書署名要求の送信を再試行する前に待機する時間（ミリ秒）。デフォルトは **25000** です。
SubmitLatencyWarningTime	500 ～ 5000	DWORD	インターフェイスが「低下」とマークされている場合の送信遅延警告時間（ミリ秒）。デフォルトは **1500** です。 登録サーバはこの設定を使用して、CA が低下状態と見なされるべきかどうかを判断します。最後の 3 回の証明書要求の完了にかかった時間が、この設定で指定されたミリ秒数より長い場合、CA は低下状態と見なされます。このステータスは、Horizon Administrator の健全性ステータス ダッシュボードに表示されます。 一般的に CA は 20 ミリ秒以内に証明書を発行しますが、CA が数時間アイドル状態だった場合は、最初の要求の完了にかかる時間が長くなることがあります。この設定によって、CA を低速とマークする必要なしに、管理者は CA が低速であることを確認できます。この設定は、CA を低速とマークするしきい値を構成するために使用します。
WarnForLonglivedCert	該当なし	REG_SZ	長期間の True SSO 証明書 (テンプレート) の警告を無効にします。デフォルトは **true** です。 証明書の有効期間が 14 日間以上に設定されると、登録サーバは True SSO テンプレートの低下状態または最適でない状態を報告し、Horizon Administrator の健全性ステータス ダッシュ ボードに警告ステータスを表示します。登録サーバは、この設定を使用して警告を無効にします。 この設定を反映させるには、登録サーバを再起動する必要があります。

接続サーバの設定

接続サーバで View LDAP を編集し、証明書生成のタイムアウトと、登録サーバ間の証明書要求のロード バランシングを有効にする（推奨）かどうかを構成できます。

詳細設定を変更するには、接続サーバ ホストで ADSI Edit を使用する必要があります。接続するには、接続ポイントとして識別名 **DC=vdi, DC=vmware, DC=int** を入力し、コンピュータのサーバ名とポート (**localhost:389**) を入力します。[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。

[pae-NameValuePair] 属性を編集して、次の表に表示されている 1 つまたは複数の値を追加します。値の追加時に構文 <name>=<value> を使用する必要があります。

表 5-7. 接続サーバ用の True SSO の詳細設定

レジストリ キー	説明
`cs-view-certsso-enable-es-loadbalance=[true|false]`	2 台の登録サーバ間の CSR 要求の負荷分散を有効化するかどうかを指定します。デフォルトは false です。 たとえば、証明書要求の受信時に接続サーバが代替登録サーバを使用するように負荷分散を有効化するには、`cs-view-certsso-enable-es-loadbalance=true` を追加します。登録サーバと CA が同じホストにある場合、各登録サーバはローカル CA を使用して要求を提供できます。
`cs-view-certsso-certgen-timeout-sec=`<number>	CSR 受信後に証明書を生成するまでの待機時間（秒単位）。デフォルトは **35** です。

Active Directory UPN がない Active Directory ユーザーの識別

Active Directory の UPN がない Active Directory ユーザーを接続サーバで識別できるように、LDAP URL フィルタを設定できます。

接続サーバ ホストで ADAM ADSI Edit を使用する必要があります。識別名 **DC=vdi, DC=vmware, DC=int** を入力して接続できます。[OU=Properties] を展開して、[OU=Authenticator] を選択します。

[pae-LDAPURLList] 属性を編集して、LDAP URL フィルタを追加できます。

たとえば、次のフィルタを追加します。

```
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified=ldap:///???
(telephoneNumber=$NAMEID)
```

接続サーバは、次のデフォルトの LDAP URL フィルタを使用します。

```
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified=ldap:///???
(&(objectCategory=user)(objectclass=user)(sAMAccountName=$NAMEID))
ldap:///???(&(objectCategory=group)(objectclass=group)(sAMAccountName=
$NAMEID))
```

```
urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified=ldap:///???
(&(objectCategory=user)(objectclass=user)(sAMAccountName=$NAMEID))
ldap:///???(&(objectCategory=group)(objectclass=group)(sAMAccountName=
$NAMEID))
```

LDAP URL フィルタを設定すると、接続サーバはこの LDAP URL フィルタを使用してユーザーを識別します。デフォルトの LDAP URL フィルタは使用されません。

Active Directory UPN がない Active Directory ユーザーの SAML 認証に使用できる識別子の例：

- `"cn"`
- `"mail"`
- `"description"`
- `"givenName"`
- `"sn"`
- `"canonicalName"`
- `"sAMAccountName"`
- `"member"`
- `"memberOf"`
- `"distinguishedName"`
- `"telephoneNumber"`
- `"primaryGroupID"`

システム健全性ダッシュボードを使用した True SSO に関する問題のトラブルシューティング

Horizon Administrator のシステム健全性ダッシュボードを使用すると、True SSO 機能の動作に影響を及ぼす可能性のある問題を素早く調べることができます。

システムがリモート デスクトップまたはアプリケーションへのエンド ユーザーのログインを試行したときに True SSO の動作が停止すると、エンド ユーザーに「**ユーザー名またはパスワードが正しくありません**」というメッセージが表示されます。ユーザーが [OK] をクリックすると、ログイン画面が表示されます。Windows ログイン画面で、[VMware SSO ユーザー] という追加タイトルが表示されます。資格のあるユーザー用の Active Directory 認証情報を持っているユーザーは、Active Directory 認証情報を使用してログインできます。

Horizon Administrator の表示の左上にあるシステム健全性ダッシュボードには、True SSO に関連する項目がいくつかあります。

注　True SSO 機能は、毎分 1 回のみダッシュボードに情報を提供します。右上隅にある更新アイコンをクリックすると、情報が直ちに更新されます。

- [View コンポーネント] - [True SSO] をクリックして展開すると、True SSO を使用しているドメインのリストが表示されます。

  ドメイン名をクリックすると、そのドメインに構成された登録サーバのリスト、エンタープライズ認証局のリスト、使用されている証明書テンプレートの名前、およびステータスが表示されます。問題がある場合は、[ステータス] フィールドにその内容が表示されます。

  [True SSO ドメイン詳細] ダイアログ ボックスに表示される設定を変更するには、`vdmutil` コマンドライン インターフェイスを使用して True SSO コネクタを編集します。詳細については、「コネクタの管理のためのコマンド」を参照してください。

- [その他のコンポーネント] - [SAML 2.0 認証子] をクリックして展開すると、VMware Identity Manager インスタンスに認証を委任するために作成された SAML 認証子のリストが表示されます。認証子名をクリックしてその詳細とステータスを調べることができます。

注　True SSO を使用するには、SSO のグローバル設定が有効になっている必要があります。Horizon Administrator で、[構成 > グローバル設定] を選択し、[Single Sign On (SSO)] が [有効] に設定されていることを確認します。

表 5-8. 接続サーバと登録サーバの接続ステータス

ステータス テキスト	説明
True SSO の健全性情報の取得に失敗しました。	ダッシュボードが接続サーバ インスタンスから健全性情報を取得できません。
<FQDN> 登録サーバは、True SSO 構成サービスと通信できません。	ポッド内で、ポッドによって使用されるすべての登録サーバに構成情報を送信する 1 つの接続サーバ インスタンスが選択されます。この接続サーバ インスタンスは登録サーバ構成を毎分 1 回更新します。このメッセージは、構成タスクで登録サーバを更新できなかった場合に表示されます。詳細については、「登録サーバ接続」の表を参照してください。
<FQDN> 登録サーバは、この接続サーバと通信してサーバ上のセッションを管理できません。	現在の接続サーバ インスタンスが登録サーバに接続できません。このステータスは、ブラウザが参照している接続サーバ インスタンスについてのみ表示されます。ポッドに複数の接続サーバ インスタンスがある場合は、このステータスを確認するために他の接続サーバ インスタンスを参照するようにブラウザを変更する必要があります。詳細については、「登録サーバ接続」の表を参照してください。

表 5-9. 登録サーバ接続

ステータス テキスト	説明
このドメイン <Domain Name> は、<FQDN> 登録サーバに存在しません。	True SSO コネクタはこのドメインのこの登録サーバを使用するように構成されていますが、登録サーバはまだこのドメインに接続するように構成されていません。この状態が 1 分以上続く場合は、現在登録構成の更新を行っている接続サーバの状態を確認する必要があります。
ドメイン <Domain Name> への <FQDN> 登録サーバの接続は現在も確立中です。	登録サーバがこのドメインのドメイン コントローラに接続できていません。この状態が 1 分以上続く場合は、登録サーバからドメインへの名前解決が正しいことの確認、および登録サーバとドメイン間のネットワーク接続の確認が必要な可能性があります。

表 5-9. 登録サーバ接続 (続き)

ステータス テキスト	説明
ドメイン <Domain Name> への <FQDN> 登録サーバの接続は、停止中か問題のある状態になっています。	登録サーバはドメインのドメイン コントローラに接続済みですが、ドメイン コントローラから PKI 情報を読み取ることができません。この状態が発生する場合は、実際のドメイン コントローラに問題がある可能性があります。DNS が正しく構成されていない場合にもこの問題が発生する可能性があります。登録サーバのログ ファイルで、登録サーバが使用しようとしているドメイン コントローラを特定し、そのドメイン コントローラが完全に動作していることを確認します。
<FQDN> 登録サーバは、ドメイン コントローラから登録プロパティを読み取っていません。	この状態は一時的であり、登録サーバの起動中、または環境に新しいドメインが追加されたときにのみ表示されます。通常、この状態は 1 分以内に変更されます。この状態が 1 分以上続く場合は、ネットワークが極端に低速であるか、ドメイン コントローラにアクセスできない問題があります。
<FQDN> 登録サーバは、少なくとも 1 回登録プロパティを読み取っていますが、しばらくの間ドメイン コントローラに接続できていません。	登録サーバがドメイン コントローラから PKI 構成を読み取っている間は、変更のポーリングが 2 分に 1 回行われます。この状態は、しばらくの間ドメイン コントローラ (DC) に接続できていない場合に設定されます。通常、この DC への接続不能は登録サーバが PKI 構成の変更を検出できないことを意味します。登録サーバがドメイン コントローラにアクセス可能である限り、継続して証明書を発行できます。
<FQDN> 登録サーバは、少なくとも 1 回登録プロパティを読み取っていますが、長時間ドメイン コントローラに接続できていないか、別の問題が発生しています。	登録サーバが長時間ドメインのドメイン コントローラに接続できない場合、この状態が表示されます。この場合、登録サーバはこのドメインの別のドメイン コントローラの検出を試みます。証明書サーバがドメイン コントローラにアクセスできる場合、証明書は引き続き発行可能ですが、この状態が 1 分以上続く場合は登録サーバがそのドメインのすべてのドメイン コントローラにアクセスできなくなっているため、おそらく証明書は発行できません。

表 5-10. 登録証明書のステータス

ステータス テキスト	説明
ドメインの <domain name> フォレストの有効な登録証明書が <FQDN> 登録サーバにインストールされていないか、または有効期限が切れています。	このドメインの登録証明書がインストールされていないか、証明書が無効または有効期限が切れています。登録証明書は、このドメインがメンバーになっているフォレストで信頼されるエンタープライズ CA によって発行される必要があります。『Horizon 7 の管理』ドキュメントに記載されている、登録サーバでの登録証明書のインストール方法についての手順を実行していることを確認します。MMC、証明書管理スナップインを開いて、ローカル コンピュータ ストアを開くこともできます。個人証明書コンテナを開き、証明書がインストールされていて有効であることを確認します。登録サーバ ログ ファイルを開くこともできます。登録サーバは、検出した証明書の状態に関する追加情報をログに記録します。

表 5-11. 証明書テンプレートのステータス

ステータス テキスト	説明
テンプレート <name> が、<FQDN> 登録サーバ ドメインに存在しません。	正しいテンプレート名が指定されていることを確認します。
このテンプレートで生成された証明書は、Windows へのログオンには使用できません。	このテンプレートではスマート カードの使用が無効になっており、データの署名が有効になっています。正しいテンプレート名が指定されていることを確認します。「True SSO とともに使用する証明書テンプレートの作成」に記載されている手順を実行していることを確認します。
テンプレート <name> ではスマートカードによるログオンが有効になっていますが、使用できません。	このテンプレートはスマート カード ログオンに対して有効になっていますが、True SSO では使用できません。正しいテンプレート名が指定されていることを確認し、「True SSO とともに使用する証明書テンプレートの作成」に記載されている手順を実行していることを確認します。テンプレートのどの設定によって True SSO が使用できなくなっているかがログに記録されるため、登録サーバのログ ファイルを確認することもできます。

表 5-12. 証明書サーバ構成のステータス

ステータス テキスト	説明
証明書サーバ <CN of CA> がドメインに存在しません。	CA の正しい名前が指定されていることを確認します。共通名 (CN) を指定する必要があります。
証明書は、NTAuth（エンタープライズ）ストアにありません。	この CA はエンタープライズ CA でないか、CA 証明書が NTAUTH ストアに追加されていません。この CA がフォレストのメンバーでない場合は、このフォレストの NTAUTH ストアに CA 証明書を手動で追加する必要があります。

表 5-13. 証明書サーバ接続のステータス

ステータス テキスト	説明
<FQDN> 登録サーバは、証明書サーバ <CN of CA> に接続していません。	登録サーバが証明書サーバに接続されていません。登録サーバの起動直後の場合、または CA が最近 True SSO コネクタに追加された場合、この状態は一時的な可能性があります。この状態が 1 分以上続く場合は、登録サーバが CA に接続できません。名前解決が正常に機能していること、CA へのネットワーク接続があること、および登録サーバのシステム アカウントに CA へのアクセス権があることを確認します。
<FQDN> 登録サーバが証明書サーバ <CN of CA> に接続しましたが、この証明書サーバはデグレードされている状態です。	この状態は、CA の証明書の発行が低速の場合に表示されます。CA がこの状態のままの場合は、CA または CA によって使用されるドメイン コントローラの負荷を確認します。 注 CA が低速とマークされている場合は、少なくとも 1 つの証明書要求が正常に完了し、その証明書が通常の期間内に発行されるまで、この状態が続きます。
<FQDN> 登録サーバは、証明書サーバ <CN of CA> に接続できますが、サービスが利用できません。	この状態は、登録サーバが CA に接続されているにも関わらず証明書を発行できない場合に発生します。通常、この状態は一時的です。CA がすぐに使用可能にならない場合、この状態は「切断」に変わります。

ロールベースの委任管理の構成

6

Horizon 7 環境の重要な管理タスクは、Horizon Administrator を使用できるユーザーとそれらのユーザーが実行可能なタスクを決定することです。ロールベースの委任管理を使用すると、特定の Active Directory ユーザーおよびグループに管理者ロールを割り当てることによって、選択的に管理者権限を割り当てることができます。

この章では次のトピックについて説明します。

ロールと権限の概要

Horizon Administrator でタスクを実行できるかどうかは、管理者ロールおよび権限から構成されるアクセス制御システムで管理します。このシステムは vCenter Server アクセス制御システムに似ています。

管理者ロールは権限の集まりです。権限は、ユーザーにデスクトップ プールに対する資格を付与するなど、特定のアクションを実行できるようにするものです。さらに、権限は、管理者が Horizon Administrator で表示できるものも制御します。たとえば、管理者がグローバル ポリシーの表示または変更権限を持たない場合は、その管理者が Horizon Administrator にログインしてもナビゲーション パネルに [グローバル ポリシー] 設定は表示されません。

管理者権限はグローバルか、またはオブジェクト固有です。グローバル権限は、グローバル設定の表示や変更などシステム全体の操作を制御します。オブジェクト固有の権限は、特定のタイプのオブジェクトの操作を制御します。

管理者ロールは、一般に、上位レベルの管理タスクを実行するために必要な個別の権限をすべて組み合わせたものです。Horizon Administrator には、一般的な管理タスクの実行に必要な権限を含む定義済みのロールが用意されています。これらの定義済みのロールを管理者ユーザーおよびグループに割り当てることも、選択した権限を組み合わせて独自のロールを作成することもできます。定義済みのロールを変更することはできません。

管理者を作成するには、Active Directory ユーザーおよびグループからユーザーとグループを選択し、管理者ロールを割り当てます。管理者は、ロールの割り当てによって権限を取得します。権限を管理者に直接割り当てることはできません。複数のロールが割り当てられた管理者は、それらのロールに含まれるすべての権限を合わせたものを取得します。

アクセス グループを使用したプールおよびファーム管理の委任

デフォルトでは、自動デスクトップ プール、手動デスクトップ プールおよびファームは、Horizon Administrator に / または Root (/) で表示されるルート アクセス グループ内に作成されます。公開デスクトップ プールおよびアプリケーション プールでは、そのファームのアクセス グループが継承されます。ルート アクセス グループの下にアクセス グループを作成し、別の管理者に特定のプールやファームの管理を委任することができます。

注　公開デスクトップ プールまたはアプリケーション プールのアクセス グループを直接変更することはできません。公開デスクトップ プールまたはアプリケーション プールが属するファームのアクセス グループを変更する必要があります。

仮想または物理マシンでは、そのデスクトップ プールからアクセス グループが継承されます。接続された通常ディスクでは、そのマシンからアクセス グループが継承されます。ルート アクセス グループを含む最大 100 のアクセス グループを保持できます。

アクセス グループの管理者にロールを割り当てることにより、そのアクセス グループのリソースへの管理者アクセスを構成することができます。管理者は、ロールを割り当てられているアクセス グループのみに存在するリソースにアクセスできます。管理者が持つアクセス グループに対するロールによって、そのアクセス グループのリソースに対するアクセス レベルが決定されます。

ロールは、ルート アクセス グループから継承されるため、ルート アクセス グループに対するロールを持つ管理者は、すべてのアクセス グループに対してそのロールを持つことになります。ルート アクセス グループに対する管理者ロールを持つ管理者は、システムのすべてのオブジェクトに対するフル アクセス権を持つため、スーパー管理者になります。

ロールには、アクセス グループに適用する少なくとも 1 つのオブジェクト固有権限が含まれている必要があります。グローバル権限のみを含むロールはアクセス グループに適用できません。

Horizon Administrator を使用してアクセス グループを作成し、既存のデスクトップ プールをアクセス グループに移動することができます。自動デスクトップ プール、手動プールまたはファームを作成する場合、デフォルトのルート アクセス グループを受け入れるか、または別のアクセス グループを選択できます。

注　VMware Identity Manager からデスクトップとアプリケーションへのアクセスを提供しようとしている場合、Horizon Administrator のルート アクセス グループで Administrators ロールを持つユーザーとしてデスクトップ プールとアプリケーション プールを作成していることを確認します。ルート アクセス グループ以外で Administrators ロールをユーザーに付与すると、VMware Identity Manager は、Horizon 7 で構成する SAML 認証システムを認識せず、VMware Identity Manager でプールを構成できません。

- 異なるアクセス グループの異なる管理者

  構成内の各アクセス グループを管理する異なる管理者を作成できます。

- 同じアクセス グループの異なる管理者

  同じアクセス グループを管理する複数の異なる管理者を作成できます。

異なるアクセス グループの異なる管理者

構成内の各アクセス グループを管理する異なる管理者を作成できます。

たとえば、会社のデスクトップ プールが 1 つのアクセス グループ内にあり、ソフトウェア開発者用のデスクトップ プールが別のアクセス グループ内にある場合、複数の管理者を作成してアクセス グループごとにリソースを管理することができます。

表 6-1 に、このタイプの構成の例を示します。

表 6-1. 異なるアクセス グループの異なる管理者

管理者	ロール	アクセス グループ
view-domain.com\Admin1	インベントリ管理者	/CorporateDesktops
view-domain.com\Admin2	インベントリ管理者	/DeveloperDesktops

この例では、Admin1 という管理者が CorporateDesktops というアクセス グループのインベントリ管理者ロールを持ち、Admin2 という管理者が DeveloperDesktops というアクセス グループのインベントリ管理者ロールを持ちます。

同じアクセス グループの異なる管理者

同じアクセス グループを管理する複数の異なる管理者を作成できます。

たとえば、会社のデスクトップ プールが 1 つのアクセス グループ内にある場合、それらのプールを表示および変更できる管理者と、それらの表示のみが可能な別の管理者を作成することができます。

表 6-2 に、このタイプの構成の例を示します。

表 6-2. 同じアクセス グループの異なる管理者

管理者	ロール	アクセス グループ
view-domain.com\Admin1	インベントリ管理者	/CorporateDesktops
view-domain.com\Admin2	インベントリ管理者（読み取り専用）	/CorporateDesktops

この例では、Admin1 という管理者が CorporateDesktops というアクセス グループのインベントリ管理者ロールを持ち、Admin2 という管理者が同じアクセス グループのインベントリ管理者（読み取り専用）ロールを持ちます。

権限の概要

Horizon Administrator は、ロールの組み合わせ、管理者ユーザーまたはグループ、およびアクセス グループを権限として提供しています。ロールは実行できるアクションを定義し、ユーザーまたはグループはアクションを実行できる者を示し、アクセス グループはアクションの対象となるオブジェクトを格納します。

管理者ユーザーまたはグループ、アクセス グループ、ロールのどれを選択したかによって、Horizon Administrator での権限の表示が異なります。

次の表に、管理者ユーザーまたはグループを選択した場合に Horizon Administrator で権限がどのように表示されるかを示します。管理者ユーザーは Admin 1 という名前で、2 つの権限を持ちます。

表 6-3. Admin 1 の Administrators and Groups（管理者とグループ） タブでの権限

ロール	アクセス グループ
インベントリ管理者	MarketingDesktops
管理者（読み取り専用）	/

最初の権限は Admin 1 が MarketingDesktops というアクセス グループに対してインベントリ管理者ロールを持つことを示しています。2 番目の権限は、Admin 1 がルート アクセス グループに対して管理者（読み取り専用）ロールを持つことを示しています。

次の表に、MarketingDesktops アクセス グループを選択した場合に Horizon Administrator で同じ権限がどのように表示されるかを示します。

表 6-4. MarketingDesktops の Folders（フォルダ） タブの権限

Admin	ロール	継承
view-domain.com\Admin1	インベントリ管理者	
view-domain.com\Admin1	管理者（読み取り専用）	はい

最初の権限は、表 6-3 に示す最初の権限と同じです。2 番目の権限は、表 6-3 に示す 2 番目の権限から継承されています。アクセス グループはルート アクセス グループから権限を継承するため、Admin1 は MarketingDesktops アクセス グループに対する管理者（読み取り専用）ロールを持ちます。権限が継承された場合、継承された列に Yes（はい） が表示されます。

次の表に、インベントリ管理者ロールを選択した場合に 表 6-3 の最初の権限が Horizon Administrator でどのように表示されるかを示します。

表 6-5. インベントリ管理者の [ロール] タブの権限

Administrator	アクセス グループ
view-domain.com\Admin1	/MarketingDesktops

管理者の管理

Administrators（管理者）ロールを持つユーザーは、Horizon Administrator を使用して、管理者ユーザーおよびグループを追加および削除できます。

Administrators（管理者）ロールは、Horizon Administrator で最も強力なロールです。最初に、Administrator アカウントのメンバーに、Administrators（管理者）ロールが付与されます。接続サーバをインストールするときに、Administrator アカウントを指定します。管理者アカウントとしては、接続サーバ コンピュータ上のローカル Administrators グループ (BUILTIN\Administrators)、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。

注　デフォルトでは、Domain Admins グループはローカル Administrators グループのメンバーです。ローカル Administrators グループとして Administrator アカウントを指定した場合に、インベントリ オブジェクトおよび Horizon 7 設定に対するフル アクセス権限をドメイン管理者に与えたくないときは、ローカル Administrators グループから Domain Admins グループを削除する必要があります。

- 管理者の作成

  管理者を作成するには、Horizon Administrator で Active Directory ユーザーおよびグループからユーザーまたはグループを選択し、管理者ロールを割り当てます。

- 管理者の削除

  管理者ユーザーまたはグループを削除できます。システム内の最後のスーパー管理者は削除できません。スーパー管理者は、ルート アクセス グループに対する管理者ロールを持つ管理者です。

管理者の作成

管理者を作成するには、Horizon Administrator で Active Directory ユーザーおよびグループからユーザーまたはグループを選択し、管理者ロールを割り当てます。

開始する前に

- 定義済みの管理者ロールについて理解しておきます。「定義済みのロールと権限」を参照してください。
- 管理者ユーザーおよびグループを作成するためのベスト プラクティスについて理解しておきます。「管理者ユーザーおよびグループに関するベスト プラクティス」を参照してください。
- 管理者にカスタム ロールを割り当てるには、カスタム ロールを作成します。「カスタム ロールの追加」を参照してください。
- 特定のデスクトップ プールを管理できる管理者を作成するには、アクセス グループを作成し、デスクトップ プールをそのアクセス グループに移動します。「アクセス グループの管理と確認」を参照してください。

手順

1. Horizon Administrator で、[View 構成] - [管理者] の順に選択します。
2. [管理者とグループ] タブで [ユーザーまたはグループの追加] をクリックします。
3. [追加] をクリックして、1 つ以上の検索条件を選択し、[検索] をクリックして検索条件に基づいて Active Directory ユーザーまたはグループをフィルタ処理します。
4. 管理者ユーザーまたはグループにする Active Directory ユーザーまたはグループを選択して、[OK] をクリックし、[次へ] をクリックします。

   Ctrl + Shift キーを押すと、複数のユーザーやグループを選択できます。

5 管理者ユーザーまたはグループに割り当てるロールを選択します。

[アクセス グループに適用] 列は、ロールをアクセス グループに適用するかどうかを示します。アクセス グループに適用されるのは、オブジェクト固有の権限を含むロールのみです。グローバル権限のみを含むロールはアクセス グループに適用されません。

オプション	アクション
選択したロールがアクセス グループに適用される	1 つ以上のアクセス グループを選択して [次へ] をクリックします。
すべてのアクセス グループにロールを適用する	ルート アクセス グループを選択して [次へ] をクリックします。

6 [終了] をクリックして、管理者ユーザーまたはグループを作成します。

[管理者とグループ] タブの左ペインに新しい管理者ユーザーまたはグループが表示され、右ペインに選択したロールとアクセス グループが表示されます。

管理者の削除

管理者ユーザーまたはグループを削除できます。システム内の最後のスーパー管理者は削除できません。スーパー管理者は、ルート アクセス グループに対する管理者ロールを持つ管理者です。

手順

1 View Administrator で、[View 構成] - [管理者] を選択します。

2 [管理者とグループ] タブで、管理者ユーザーまたはグループを選択し、[ユーザーまたはグループの削除] をクリックして、[OK] をクリックします。

[管理者とグループ] タブに管理者ユーザーまたはグループが表示されなくなります。

権限の管理と確認

Horizon Administrator を使用して、特定の管理者ユーザーおよびグループ、特定のロール、特定のアクセス グループの権限を追加、削除、確認できます。

- 権限の追加

  特定の管理者ユーザーまたはグループ、特定のロール、または特定のアクセス グループを含む権限を追加できます。

- 権限の削除

  特定の管理者ユーザーまたはグループ、特定のロール、または特定のアクセス グループを含む権限を削除できます。

- 権限の確認

  特定の管理者またはグループ、特定のロール、または特定のアクセス グループを含む権限を確認できます。

権限の追加

特定の管理者ユーザーまたはグループ、特定のロール、または特定のアクセス グループを含む権限を追加できます。

手順

1 Horizon Administrator で、[View 構成] - [管理者] の順に選択します。

2 権限を作成します。

オプション	操作
特定の管理者ユーザーまたはグループを含む権限を作成する	a [管理者とグループ] タブで、管理者またはグループを選択し、[権限を追加] をクリックします。 b ロールを選択します。 c ロールをアクセス グループに適用しない場合、[終了] をクリックします。 d ロールをアクセス グループに適用する場合は、[次へ] をクリックし、1 つ以上のアクセス グループを選択して [終了] をクリックします。ロールには、アクセス グループに適用する少なくとも 1 つのオブジェクト固有権限が含まれている必要があります。
特定のロールを含む権限を作成する	a [ロール] タブでロールを選択し、[権限] をクリックし、[権限を追加] をクリックします。 b [追加] をクリックして、1 つ以上の検索条件を選択し、[検索] をクリックして検索条件に一致する管理者ユーザーまたはグループを検索します。 c 権限に含める管理者ユーザーまたはグループを選択して [OK] をクリックします。<Ctrl> + <Shift> キーを押すと、複数のユーザーやグループを選択できます。 d ロールをアクセス グループに適用しない場合、[終了] をクリックします。 e ロールをアクセス グループに適用する場合は、[次へ] をクリックし、1 つ以上のアクセス グループを選択して [終了] をクリックします。ロールには、アクセス グループに適用する少なくとも 1 つのオブジェクト固有権限が含まれている必要があります。
特定のアクセス グループを含む権限を作成する	a [アクセス グループ] タブで、アクセス グループを選択し、[権限を追加] をクリックします。 b [追加] をクリックして、1 つ以上の検索条件を選択し、[検索] をクリックして検索条件に一致する管理者ユーザーまたはグループを検索します。 c 権限に含める管理者ユーザーまたはグループを選択して [OK] をクリックします。<Ctrl> + <Shift> キーを押すと、複数のユーザーやグループを選択できます。 d [次へ] をクリックし、ロールを選択して [終了] をクリックします。ロールには、アクセス グループに適用する少なくとも 1 つのオブジェクト固有権限が含まれている必要があります。

権限の削除

特定の管理者ユーザーまたはグループ、特定のロール、または特定のアクセス グループを含む権限を削除できます。

管理者ユーザーまたはグループの最後の権限を削除すると、その管理者ユーザーまたはグループも削除されます。少なくとも 1 人の管理者がルート アクセス グループの Administrators （管理者）ロールを持つ必要があるため、その管理者が削除されるような権限の削除を行うことはできません。継承された権限は削除できません。

手順

1 Horizon Administrator で、[View 構成] - [管理者] の順に選択します。

2 削除する権限を選択します。

オプション	アクション
特定の管理者またはグループに適用される権限を削除する	[管理者とグループ] タブで管理者またはグループを選択します。
特定のロールに適用される権限を削除する	[ロール] タブでロールを選択します。
特定のアクセス グループに適用される権限を削除する	[アクセス グループ] タブでフォルダを選択します。

3 権限を選択し、[権限の削除] をクリックします。

権限の確認

特定の管理者またはグループ、特定のロール、または特定のアクセス グループを含む権限を確認できます。

手順

1 [View 構成] - [管理者] を選択します。

2 権限を確認します。

オプション	操作
特定の管理者またはグループを含む権限を確認する	[管理者とグループ] タブで管理者またはグループを選択します。
特定のロールを含む権限を確認する	[ロール] タブでロールを選択して、[アクセス権限] をクリックします。
特定のアクセス グループを含む権限を確認する	[アクセス グループ] タブでフォルダを選択します。

アクセス グループの管理と確認

Horizon Administrator を使用して、アクセス グループを追加または削除したり、特定のアクセス グループ内のデスクトップ プールとマシンを確認したりできます。

- アクセス グループの追加

  アクセス グループを作成することにより、特定のマシン、デスクトップ プールまたはファームの管理を委任できます。デフォルトでは、デスクトップ プール、アプリケーション プールおよびファームは、ルート アクセス プールにあります。

- 別のアクセス グループへのデスクトップ プールまたはファームの移動

  アクセス グループの作成後、自動デスクトップ プール、手動プールまたはファームを新しいアクセス グループに移動できます。

- アクセス グループの削除

  オブジェクトが含まれていないアクセス グループは削除できます。ルート アクセス グループは削除できません。

- アクセス グループ内のデスクトップ プール、アプリケーション プール、またはファームの確認

  特定のアクセス グループ内のデスクトップ プール、アプリケーション プール、またはファームは Horizon Administrator で確認できます。

- アクセス グループ内の vCenter Server 仮想マシンの確認

  Horizon Administrator で特定のアクセス グループ内の vCenter Server 仮想マシンを表示できます。vCenter 仮想マシンは、そのプールからアクセス グループを継承します。

アクセス グループの追加

アクセス グループを作成することにより、特定のマシン、デスクトップ プールまたはファームの管理を委任できます。デフォルトでは、デスクトップ プール、アプリケーション プールおよびファームは、ルート アクセス プールにあります。

ルート アクセス グループを含む最大 100 のアクセス グループを保持できます。

手順

1 Horizon Administrator で、[アクセス グループを追加] ダイアログ ボックスへ移動します。

オプション	アクション
カタログから	■ [カタログ] - [デスクトップ プール] の順に選択します。 ■ トップ ウィンドウ ペインの [アクセス グループ] ドロップダウン メニューから、[新しいアクセス グループ] を選択します。
リソースから	■ [リソース] - [ファーム] の順に選択します。 ■ トップ ウィンドウ ペインの [アクセス グループ] ドロップダウン メニューから、[新しいアクセス グループ] を選択します。
View 構成から	■ [View 構成] - [管理者] の順に選択します。 ■ [アクセス グループ] タブから、[アクセス グループを追加] を選択します。

2 アクセス グループの名前と説明を入力し、[OK] をクリックします。

説明はオプションです。

次に進む前に

1 つ以上のオブジェクトをアクセス グループに移動します。

別のアクセス グループへのデスクトップ プールまたはファームの移動

アクセス グループの作成後、自動デスクトップ プール、手動プールまたはファームを新しいアクセス グループに移動できます。

手順

1 Horizon Administrator で、[カタログ] - [デスクトップ プール] の順に選択するか、[リソース] - [ファーム] の順に選択します。

2 プールまたはファームを選択します。

3 上部ウィンドウ ペインにある [アクセス グループ] のドロップダウン メニューから [アクセス グループを変更] を選択します。

4 アクセス グループを選択し、[OK] をクリックします。

Horizon Administrator はプールを選択したアクセス グループに移動します。

アクセス グループの削除

オブジェクトが含まれていないアクセス グループは削除できます。ルート アクセス グループは削除できません。

開始する前に

アクセス グループにオブジェクトが含まれている場合は、オブジェクトを別のアクセス グループまたはルート アクセス グループに移動します。「別のアクセス グループへのデスクトップ プールまたはファームの移動」を参照してください。

手順

1 Horizon Administrator で、[View 構成] - [管理者] の順に選択します。

2 [アクセス グループ] タブでアクセス グループを選択して、[アクセス グループを削除] をクリックします。

3 [OK] をクリックしてアクセス グループを削除します。

アクセス グループ内のデスクトップ プール、アプリケーション プール、またはファームの確認

特定のアクセス グループ内のデスクトップ プール、アプリケーション プール、またはファームは Horizon Administrator で確認できます。

手順

1 Horizon Administrator で、オブジェクトのメイン ページに移動します。

オブジェクト	アクション
デスクトップ プール	[カタログ] - [デスクトップ プール] の順に選択します。
アプリケーション プール	[カタログ] - [アプリケーション プール] の順に選択します。
ファーム	[リソース] - [ファーム] の順に選択します。

デフォルトでは、すべてのアクセス グループ内のオブジェクトが表示されます。

2 メイン ウィンドウ ペインの [アクセス グループ] ドロップダウン メニューから、アクセス グループを選択します。

選択したアクセス グループ内のオブジェクトが表示されます。

アクセス グループ内の vCenter Server 仮想マシンの確認

Horizon Administrator で特定のアクセス グループ内の vCenter Server 仮想マシンを表示できます。vCenter 仮想マシンは、そのプールからアクセス グループを継承します。

手順

1 Horizon Administrator で、[リソース] - [マシン] の順に選択します。

2 [vCenter 仮想マシン] タブを選択します。

デフォルトでは、すべてのアクセス グループ内の vCenter 仮想マシンが表示されます。

3 [アクセス グループ] ドロップダウン メニューからアクセス グループを選択します。

選択したアクセス グループ内の vCenter 仮想マシンが表示されます。

カスタム ロールの管理

Horizon Administrator を使用して、カスタム ロールを追加、変更、および削除できます。

- カスタム ロールの追加

  定義済みの管理者ロールがニーズを満たしていない場合、Horizon Administrator で特定の権限を組み合わせて独自のロールを作成できます。

- カスタム ロールの権限の変更

  カスタム ロール内の権限を変更できます。定義済みの管理者ロールを変更することはできません。

- カスタム ロールの削除

  権限に含まれていない場合は、カスタム ロールを削除できます。定義済みの管理者ロールを削除することはできません。

カスタム ロールの追加

定義済みの管理者ロールがニーズを満たしていない場合、Horizon Administrator で特定の権限を組み合わせて独自のロールを作成できます。

開始する前に

カスタム ロールの作成に使用できる管理者権限について理解しておきます。「定義済みのロールと権限」を参照してください。

注 カスタム管理者ロールを作成するときに、カスタム管理者ユーザーにグローバル権限を付与できません。クラウド ポッド アーキテクチャ 環境でグローバル資格を管理できるグローバル権限があるのは、事前定義の管理者ロールだけです。

手順

1 Horizon Administrator で、[View 構成] - [管理者] の順に選択します。

2 [ロール] タブで [ロールを追加] をクリックします。

3 新しいロールの名前と説明を入力し、1 つ以上の権限を選択して、[OK] をクリックします。

左ペインに新しいロールが表示されます。

カスタム ロールの権限の変更

カスタム ロール内の権限を変更できます。定義済みの管理者ロールを変更することはできません。

開始する前に

カスタム ロールの作成に使用できる管理者権限について理解しておきます。「定義済みのロールと権限」を参照してください。

手順

1 Horizon Administrator で、[View 構成] - [管理者] の順に選択します。

2 [ロール] タブでロールを選択します。

3 [権限] をクリックしてロール内の権限を表示し、[編集] をクリックします。

4 権限を選択または選択解除します。

5 [OK] をクリックして変更を保存します。

カスタム ロールの削除

権限に含まれていない場合は、カスタム ロールを削除できます。定義済みの管理者ロールを削除することはできません。

開始する前に

ロールが権限に含まれる場合は、権限を削除します。「権限の削除」を参照してください。

手順

1 Horizon Administrator で、[View 構成] - [管理者] の順に選択します。

2 [ロール] タブで、ロールを選択し、[ロールを削除] をクリックします。

[ロールを削除] ボタンは、定義済みロールや、権限に含まれるカスタム ロールに対しては使用できません。

3 [OK] をクリックしてロールを削除します。

定義済みのロールと権限

Horizon Administrator には、管理者ユーザーおよびグループに割り当てることができる定義済みのロールがあります。選択した権限を組み合わせて独自の管理者ロールを作成することもできます。

- 定義済みの管理者ロール

  定義済みの管理者ロールは、一般的な管理タスクの実行に必要な個別の権限をすべて組み合わせたものです。定義済みのロールを変更することはできません。

- グローバル権限

  グローバル権限は、グローバル設定の表示や変更などシステム全体の操作を制御します。グローバル権限のみを含むロールはアクセス グループに適用できません。

- オブジェクト固有の権限

  オブジェクト固有権限は、特定のタイプのインベントリ オブジェクトの操作を制御します。オブジェクト固有の権限を含むロールは、アクセス グループに適用することができます。

- 内部権限

  一部の定義済みの管理者ロールには、内部権限が含まれています。カスタム ロールを作成するときに内部権限を選択することはできません。

定義済みの管理者ロール

定義済みの管理者ロールは、一般的な管理タスクの実行に必要な個別の権限をすべて組み合わせたものです。定義済みのロールを変更することはできません。

注　事前定義ロールまたはカスタム ロールの組み合わせをユーザーに割り当てると、個々の事前定義ロールまたはカスタム ロールで実行できない操作が可能になります。

次の表で定義済みロールについて説明し、ロールをアクセス グループに適用できるかどうかを示します。

表 6-6. Horizon Administrator の定義済みロール

ロール	ユーザーが可能な操作	アクセス グループに適用
管理者	すべての管理者の操作を実行する（追加の管理者ユーザーおよびグループの作成を含む）。クラウド ポッド アーキテクチャ環境では、このロールを持つ管理者は、ポッド フェデレーションの構成と管理およびリモート ポッド セッションの管理を行うことができます。 ルート アクセス グループに対する管理者ロールを持つ管理者は、システムのすべてのインベントリ オブジェクトに対するフル アクセス権を持つことから、スーパー ユーザーと呼ばれます。Administrators（管理者）ロールにはすべての権限が含まれるため、限られたユーザーに割り当てるようにしてください。最初に、接続サーバ ホスト上のローカル管理者グループのメンバーに、ルート アクセス グループに対するこのロールが付与されます。 重要　次のタスクを実行するためには、管理者がルート アクセス グループに対する管理者ロールを備えている必要があります。 ■ アクセス グループを追加および削除する。 ■ Horizon Administrator で ThinApp アプリケーションおよび設定を管理する。 ■ `vdmadmin`、`vdmimport` および `lmvutil` コマンドを使用する。	はい
管理者（読み取り専用）	■ グローバル設定とインベントリ オブジェクトを表示する（変更はできない）。 ■ ThinApp アプリケーションおよび設定を表示する（変更はできない）。 ■ すべての PowerShell コマンドやコマンド ライン ユーティリティ（`vdmexport` など。`vdmadmin`、`vdmimport` および `lmvutil` は除く）を実行する。 クラウド ポッド アーキテクチャ環境では、このロールを持つ管理者は、グローバル データ レイヤでインベントリ オブジェクトと設定を表示できます。 管理者がアクセス グループに対してこのロールを持つ場合、そのアクセス グループ内のインベントリ オブジェクトのみを表示できます。	はい
エージェント登録管理者	物理システム、スタンドアロン仮想マシン、RDS ホストなどの管理対象外のマシンを登録する。	いいえ
グローバル構成およびポリシー管理者	グローバル ポリシーと設定（管理者ロールと権限を除く）および ThinApp アプリケーションと設定を表示し、変更する。	いいえ
グローバル構成およびポリシー管理者（読み取り専用）	グローバル ポリシーと設定（管理者ロールと権限を除く）および ThinApp アプリケーションと設定を表示する（変更はできない）。	いいえ

表 6-6. Horizon Administrator の定義済みロール (続き)

ロール	ユーザーが可能な操作	アクセス グループに適用
ヘルプデスク管理者	シャットダウン、リセット、再起動など、デスクトップやアプリケーションで操作を実行したり、ユーザーのデスクトップまたはアプリケーションのプロセス終了など、リモート アシスタントの操作を実行します。Horizon Help Desk Tool にアクセスするには、管理者にルート アクセス グループの権限が必要です。 ■ Horizon Help Desk Tool に対する読み取り専用アクセス。 ■ グローバル セッションを管理します。 ■ Horizon Administrator にログインできます。 ■ すべてのマシンおよびセッション関連のコマンドを実行します。 ■ リモートのプロセスとアプリケーションを管理します。 ■ 仮想デスクトップまたは公開デスクトップのリモート アシスタント。	いいえ
ヘルプデスク管理者 (読み取り専用)	ユーザーとセッションの情報を表示し、ドリルダウンでセッションの詳細情報を表示します。Horizon Help Desk Tool にアクセスするには、管理者にルート アクセス グループの権限が必要です。 ■ Horizon Help Desk Tool に対する読み取り専用アクセス。 ■ Horizon Administrator にログインできます。	いいえ
インベントリ管理者	■ すべてのマシン、セッション、およびプール関連の操作を実行する。 ■ 通常ディスクを管理します。 ■ リンク クローン プールを再同期、更新、再分散し、デフォルトのプール イメージを変更する。 管理者がアクセス グループに対してこのロールを持つ場合、そのアクセス グループ内のインベントリ オブジェクトに対してのみこれらの操作を実行できます。	はい
インベントリ管理者（読み取り専用）	インベントリ オブジェクトを表示する（変更はできない）。 管理者がアクセス グループに対してこのロールを持つ場合、そのアクセス グループ内のインベントリ オブジェクトのみを表示できます。	はい
ローカル管理者	すべてのローカル管理者操作を実行する（追加の管理者ユーザーおよびグループの作成を除く）。クラウド ポッド アーキテクチャ環境では、このロールを持つ管理者は、グローバル データ レイヤで操作を実行したり、リモート ポッドでセッションを管理することはできません。 注 ローカル管理者ロールを持つ管理者は、Horizon Help Desk Tool にアクセスできません。CPA 以外の環境の管理者にグローバル セッションの管理権限はありません。Horizon Help Desk Tool でタスクを実行するには、この権限が必要です。	はい
ローカル管理者（読み取り専用）	管理者（読み取り専用）ロールと同じ（グローバル データ レイヤでのインベントリ オブジェクトおよび設定の表示を除く）。このロールを持つ管理者は、ローカル ポッドでのみ読み取り専用の権限を持ちます。 注 ローカル管理者（読み取り専用）ロールを持つ管理者は、Horizon Help Desk Tool にアクセスできません。CPA 以外の環境の管理者にグローバル セッションの管理権限はありません。Horizon Help Desk Tool でタスクを実行するには、この権限が必要です。	はい

グローバル権限

グローバル権限は、グローバル設定の表示や変更などシステム全体の操作を制御します。グローバル権限のみを含むロールはアクセス グループに適用できません。

次の表で、グローバル権限について説明し、各権限を含む定義済みのロールを示します。

表 6-7. グローバル権限

権限	ユーザーが可能な操作	定義済みロール
コンソール操作	Horizon Administrator にログインし使用する。	管理者 管理者（読み取り専用） インベントリ管理者 インベントリ管理者（読み取り専用） グローバル構成およびポリシー管理者 グローバル構成およびポリシー管理者（読み取り専用） ヘルプデスク管理者 ヘルプデスク管理者（読み取り専用） ローカル管理者 ローカル管理者（読み取り専用）
直接操作	すべての PowerShell コマンドやコマンド ライン ユーティリティ（`vdmadmin` および `vdmimport` 以外）を実行する。 `vdmadmin`、`vdmimport`、および `lmvutil` コマンドを使用する管理者には、ルート アクセス グループに対する管理者ロールが必要です。	管理者 管理者（読み取り専用）
グローバル構成とポリシーを管理	グローバル ポリシーおよび設定（管理者ロールおよび権限を除く）を表示し、変更する。	管理者 グローバル構成およびポリシー管理者
グローバル セッションを管理	グローバル セッションはクラウド ポッド アーキテクチャ環境で管理します。	管理者
ロールと権限を管理	管理者ロールおよび権限を作成、変更、削除する。	管理者
エージェントを登録	物理システム、スタンドアロン仮想マシン、RDS ホストなどの管理対象外のマシンに Horizon Agent をインストールする。 Horizon Agent のインストール時に、管理者ログイン認証情報を指定し、接続サーバ インスタンスに管理対象外のマシンを登録する必要があります。	管理者 エージェント登録管理者

オブジェクト固有の権限

オブジェクト固有権限は、特定のタイプのインベントリ オブジェクトの操作を制御します。オブジェクト固有の権限を含むロールは、アクセス グループに適用することができます。

次の表に、オブジェクト固有の権限を示します。定義済みのロール Administrators（管理者）および Inventory Administrators（インベントリ管理者）にはこれらのすべての権限が含まれます。

表 6-8. オブジェクト固有の権限

権限	ユーザーが可能な操作	オブジェクト
ファームおよびデスクトップ プールを有効にする	デスクトップ プールを有効または無効にする。	デスクトップ プール、ファーム
デスクトップおよびアプリケーション プールに資格を割り当てる	ユーザーの資格を追加または削除する。	デスクトップ プール、アプリケーション プール

表 6-8. オブジェクト固有の権限 (続き)

権限	ユーザーが可能な操作	オブジェクト
Composer デスクトップ プール イメージを管理	リンク クローン プールを再同期、更新、再調整し、デフォルトのプール イメージを変更する。	デスクトップ プール
マシンを管理	すべてのマシンおよびセッション関連の操作を実行します。	マシン
通常ディスクを管理	View Composer の通常ディスクの操作を実行する（通常ディスクの接続、切断、インポートなど）。	通常ディスク
ファーム、デスクトップおよびアプリケーション プールを管理	ファームを追加、変更、削除します。デスクトップおよびアプリケーション プールの追加、変更、削除、資格割り当てを行います。マシンを追加および削除します。	デスクトップ プール、アプリケーション プール、ファーム
セッションを管理	セッションを切断してログオフし、ユーザーにメッセージを送信します。	セッション
再起動操作を管理	仮想マシンをリセットしたり、仮想デスクトップを再起動したりします。	マシン

内部権限

一部の定義済みの管理者ロールには、内部権限が含まれています。カスタム ロールを作成するときに内部権限を選択することはできません。

次の表で、内部権限について説明し、各権限を含む定義済みのロールを示します。

表 6-9. 内部権限

権限	説明	定義済みロール
フル（読み取り専用）	すべての設定への読み取り専用アクセス権を付与します。	管理者（読み取り専用）
Manage Inventory (Read only)（インベントリの管理（読み取り専用））	インベントリ オブジェクトへの読み取り専用アクセス権を付与します。	インベントリ管理者（読み取り専用）
Manage Global Configuration and Policies (Read only)（グローバル構成とポリシーの管理（読み取り専用））	設定およびグローバル ポリシー（管理者とロールを除く）への読み取り専用アクセス権を付与します。	グローバル構成およびポリシー管理者（読み取り専用）

一般的なタスクに必要な権限

多くの一般的な管理者タスクには、調整された一連の権限が必要です。一部の操作では、操作対象のオブジェクトへのアクセスに加えて、ルート アクセス グループでの権限が必要です。

プール管理のための権限

管理者が Horizon Administrator でプールを管理するためには、特定の権限が必要です。

次の表に、一般的なプール管理タスクの一覧と、各タスクを実行するために必要となる権限を示します。

表 6-10. プール管理タスクと権限

タスク	必要な権限
デスクトップ プールを有効または無効にする	**ファームおよびデスクトップ プールを有効にする**
プールに対する資格をユーザーに付与する、または資格を取り消す	**デスクトップおよびアプリケーション プールに資格を割り当てる**
プールを追加する	**ファーム、デスクトップおよびアプリケーション プールを管理**
プールを変更または削除する	**ファーム、デスクトップおよびアプリケーション プールを管理**
プールにデスクトップを追加またはプールからデスクトップを削除する	**ファーム、デスクトップおよびアプリケーション プールを管理**
デフォルトの View Composer イメージを更新、再構成、再分散、または変更する	**Composer デスクトップ プール イメージを管理**
アクセス グループを変更	ソースおよびターゲット アクセス グループでの [ファーム、デスクトップおよびアプリケーション プールを管理]。

マシン管理のための権限

管理者が Horizon Administrator でマシンを管理するためには、特定の権限が必要です。

次の表に、一般的なマシン管理タスクの一覧と、各タスクを実行するために必要な権限を示します。

表 6-11. マシン管理タスクと権限

タスク	必要な権限
仮想マシンを削除する	**マシンを管理**
仮想マシンをリセットする	**再起動操作を管理**
仮想デスクトップを再起動する	**再起動操作を管理**
ユーザー所有権を割り当てる、または削除する	**マシンを管理**
メンテナンス モードに切り替える、またはメンテナンス モードを終了する	**マシンを管理**
セッションから切断またはログオフする	**セッションを管理**

通常ディスク管理のための権限

管理者が Horizon Administrator で通常ディスクを管理するためには、特定の権限が必要です。

次の表に、一般的なパーシステント ディスクの管理タスクの一覧と、各タスクを実行するために必要な権限を示します。これらのタスクは Horizon Administrator の [通常ディスク] ページで実行します。

表 6-12. 通常ディスク管理タスクと権限

タスク	必要な権限
ディスクを切断する	ディスクに対する**通常ディスクを管理**、およびプールに対する**ファーム、デスクトップおよびアプリケーション プールを管理**。
ディスクの接続	マシンに対する**通常ディスクを管理**、およびマシンに対する**ファーム、デスクトップおよびアプリケーション プールを管理**。
ディスクの編集	ディスクに対する**通常ディスクを管理**、および選択したプールに対する**ファーム、デスクトップおよびアプリケーション プールを管理**。

表 6-12. 通常ディスク管理タスクと権限 (続き)

タスク	必要な権限
アクセス グループを変更	ソースおよびターゲットのアクセス グループに対する**通常ディスクを管理**。
デスクトップを再作成する	ディスクに対する**通常ディスクを管理**、最後のプールに対する**ファーム、デスクトップおよびアプリケーション プールを管理**。
vCenter からインポートする	フォルダに対する**通常ディスクを管理**、およびプールに対する**プールの管理**。
ディスクを削除する	ディスクに対する**通常ディスクを管理**。

ユーザーと管理者の管理のための権限

管理者が Horizon Administrator でユーザーと管理者を管理するためには、特定の権限が必要です。

次の表に、一般的なユーザーと管理者の管理タスクの一覧と、各タスクの実行に必要な権限を示します。ユーザーの管理は Horizon Administrator の [ユーザーとグループ] ページで行います。管理者の管理は Horizon Administrator の [グローバル管理者ビュー] ページで行います。

表 6-13. ユーザーと管理者の管理タスクと権限

タスク	必要な権限
一般的なユーザー情報を更新する	**グローバル構成とポリシーを管理**
ユーザーにメッセージを送信する	マシン上の**リモート セッションの管理**。
管理者ユーザーまたはグループを追加する	**ロールと権限を管理**
管理者の権限を追加、変更、または削除する	**ロールと権限を管理**
管理者ロールを追加、修正、または削除する	**ロールと権限を管理**

Horizon Help Desk Tool タスクの権限

Horizon Help Desk Tool の管理者には、Horizon Administrator でトラブルシューティング タスクを実行するため、特定の権限が必要です。

次の表に、Horizon Help Desk Tool の管理者が実行できる一般的なタスクと、各タスクの実行に必要な権限を示します。

表 6-14. Horizon Help Desk Tool タスクと権限

タスク	必要な権限
Horizon Help Desk Tool に対する読み取り専用アクセス。	[ヘルプデスクを管理（読み取り専用）]
グローバル セッションを管理します。	[グローバル セッションを管理]
Horizon Administrator にログインできます。	[コンソール操作]
すべてのマシンおよびセッション関連のコマンドを実行します。	[マシンを管理]
マシンをリセットまたは再起動します。	[再起動操作を管理]
セッションから切断してログオフします。	[セッションを管理]
リモートのプロセスとアプリケーションを管理します。	[リモートのプロセスとアプリケーションを管理]
仮想デスクトップまたは公開デスクトップのリモート アシスタンス。	[リモート アシスタンス]

表 6-14. Horizon Help Desk Tool タスクと権限 (続き)

タスク	必要な権限
グローバル セッションの切断、ログアウト、リセット、再起動操作。	[ヘルプデスクを管理（読み取り専用）]、[グローバル セッションを管理]
ローカル セッションのリセットと再起動操作。	[ヘルプデスクを管理（読み取り専用）]、[再起動操作を管理]
リモート アシスタンス操作。	[ヘルプデスクを管理（読み取り専用）]、[リモート アシスタンス]
リモートのプロセスとアプリケーションを終了します。	[ヘルプデスクを管理（読み取り専用）]、[リモートのプロセスとアプリケーションを管理]
Horizon Help Desk Tool で、すべてのタスクを実行します。	[ヘルプデスクを管理（読み取り専用）]、[グローバル セッションを管理]、[再起動操作を管理]、[リモート アシスタンス]、[リモートのプロセスとアプリケーションを管理]
リモート アシスタンス操作とリモートのプロセスとアプリケーションの終了。	[ヘルプデスクを管理（読み取り専用）]、[リモート アシスタンス]、[リモートのプロセスとアプリケーションを管理]
ローカル セッションの切断とログアウト操作。	[ヘルプデスクを管理（読み取り専用）]、[セッションを管理]

一般的な管理タスクと管理コマンドのための権限

管理者が一般的な管理タスクを実行したりコマンド ライン ユーティリティを実行したりするには、特定の権限が必要です。

次の表に、一般的な管理タスクやコマンド ライン ユーティリティを実行するために必要な権限を示します。

表 6-15. 一般的な管理タスクと管理コマンドのための権限

タスク	必要な権限
アクセス グループを追加または削除する	ルート アクセス グループに対する管理者ロールが必要。
Horizon Administrator で ThinApp アプリケーションおよび設定を管理する	ルート アクセス グループに対する管理者ロールが必要。
物理システム、スタンドアロン仮想マシン、RDS ホストなどの管理対象外のマシンに Horizon Agent をインストールする	**エージェントを登録**
Horizon Administrator で設定（管理者向けを除く）を表示または修正する	**グローバル構成とポリシーを管理**
すべての PowerShell コマンドやコマンド ライン ユーティリティ（`vdmadmin` および `vdmimport` 以外）を実行する。	**直接操作**
`vdmadmin` および `vdmimport` コマンドを使用する	ルート アクセス グループに対する管理者ロールが必要。
`vdmexport` コマンドを使用する	ルート アクセス グループに対する管理者ロールまたは管理者（読み取り専用）ロールが必要。

管理者ユーザーおよびグループに関するベスト プラクティス

Horizon 7 環境のセキュリティと管理性を高めるために、管理者ユーザーおよびグループを管理するときのベスト プラクティスに従うようにしてください。

- Active Directory に新しいユーザー グループを作成して、作成したグループに管理者ロールを割り当てます。Horizon 7 権限を持つ必要のない、または持つべきではないユーザーが含まれる可能性があるため、Windows のビルトイン グループやその他の既存グループは使用しないようにします。

- Horizon 7 管理権限を持つユーザーの数は最小限にします。
- 管理者ロールにはすべての権限が含まれるため、日常的な管理に管理者ロールを使用しないでください。
- 目につきやすく推測が容易なため、管理者ユーザーおよびグループを作成するときは Administrator という名前の使用を避けます。
- アクセス グループを作成して、機密情報を扱うデスクトップとファームを分離します。それらのアクセス グループの管理を限られたユーザーに委任します。
- グローバル ポリシーと Horizon 7 設定を変更できる管理者を別途作成します。

Horizon Administrator および Active Directory のポリシーの構成

7

Horizon Administrator を使用して、クライアント セッションのポリシーを設定できます。View 接続サーバ、PCoIP 表示プロトコル、および Horizon 7 のログの動作、およびパフォーマンス アラームを制御する Active Directory グループ ポリシー設定を構成できます。

Horizon Agent、Horizon Client for Windows、Horizon Persona Management、および特定の機能の動作を制御する Active Directory グループ ポリシー設定をすることもできます。これらのポリシー設定については、『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントを参照してください。

この章では次のトピックについて説明します。

- Horizon Administrator でのポリシーの設定
- 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 Administrator でのポリシーの設定

Horizon Administrator を使用して、クライアント セッションのポリシーを設定できます。

これらのポリシーを設定して、特定のユーザー、特定のデスクトップ プール、またはすべてのクライアント セッション ユーザーに適用できます。特定のユーザーとデスクトップ プールに適用するポリシーは、ユーザー レベルのポリシーおよびデスクトップ プール レベルのポリシーと呼ばれます。すべてのセッションとユーザーに適用するポリシーはグローバル ポリシーと呼ばれます。

ユーザー レベルのポリシーでは、対応するデスクトップ プール レベルのポリシー設定から設定が継承されます。同様に、デスクトップ プール レベルのポリシーでは、対応するグローバル ポリシー設定から設定が継承されます。デスクトップ プール レベルのポリシー設定は、対応するグローバル ポリシー設定より優先されます。ユーザー レベルのポリシー設定は、対応するグローバル ポリシー設定およびデスクトップ プール レベルのポリシー設定より優先されます。

低いレベルのポリシー設定は、対応する高いレベルの設定より、制限を厳しくすることも緩くすることもできます。たとえば、グローバル ポリシーを [拒否] に設定し、対応するデスクトップ プール レベルのポリシーを [許可] に設定することも、この逆に設定することもできます。

注　公開デスクトップおよびアプリケーション プールでは、グローバル ポリシーのみを使用できます。公開デスクトップおよびアプリケーション プールに対して、ユーザー レベル ポリシーまたはプール レベル ポリシーを設定することはできません。

- グローバル ポリシー設定の構成

  すべてのクライアント セッション ユーザーの動作を制御するグローバル ポリシーを構成できます。

- デスクトップ プールのポリシーの構成

  特定のデスクトップ プールに影響を与えるデスクトップ レベルのポリシーを構成できます。デスクトップ レベルのポリシー設定は、対応するグローバル ポリシー設定より優先されます。

- ユーザーのポリシーの構成

  特定のユーザーに影響を与えるユーザー レベルのポリシーを構成できます。ユーザー レベルのポリシー設定は、常に、対応するグローバルおよびデスクトップ プール レベルのポリシー設定より優先されます。

- Horizon 7 ポリシー

  すべてのクライアント セッションに影響を与えるように Horizon 7 ポリシーを構成することも、特定のデスクトップ プールまたはユーザーに影響を与えるように View ポリシーを適用することもできます。

グローバル ポリシー設定の構成

すべてのクライアント セッション ユーザーの動作を制御するグローバル ポリシーを構成できます。

開始する前に

ポリシーの説明を理解しておきます。「Horizon 7 ポリシー」を参照してください。

手順

1 Horizon Administrator で、[ポリシー] - [グローバル ポリシー] の順に選択します。

2 [View ポリシー] ペインで [ポリシーを編集] をクリックします。

3 [OK] をクリックして変更を保存します。

デスクトップ プールのポリシーの構成

特定のデスクトップ プールに影響を与えるデスクトップ レベルのポリシーを構成できます。デスクトップ レベルのポリシー設定は、対応するグローバル ポリシー設定より優先されます。

開始する前に

ポリシーの説明を理解しておきます。「Horizon 7 ポリシー」を参照してください。

手順

1 Horizon Administrator で、[カタログ] - [デスクトップ プール] の順に選択します。

2 デスクトップ プールの ID をダブルクリックし、[ポリシー] タブをクリックします。

  [ポリシー] タブには、現在のポリシー設定が表示されます。設定が対応するグローバル ポリシーから継承されている場合は、[デスクトップ プール ポリシー] 列に [継承] と表示されます。

3 [View ポリシー] ペインで [ポリシーを編集] をクリックします。

4 [OK] をクリックして変更を保存します。

ユーザーのポリシーの構成

特定のユーザーに影響を与えるユーザー レベルのポリシーを構成できます。ユーザー レベルのポリシー設定は、常に、対応するグローバルおよびデスクトップ プール レベルのポリシー設定より優先されます。

開始する前に

ポリシーの説明を理解しておきます。「Horizon 7 ポリシー」を参照してください。

手順

1 Horizon Administrator で、[カタログ] - [デスクトップ プール] の順に選択します。

2 デスクトップ プールの ID をダブルクリックし、[ポリシー] タブをクリックします。

[ポリシー] タブには、現在のポリシー設定が表示されます。設定が対応するグローバル ポリシーから継承されている場合は、[デスクトップ プール ポリシー] 列に [継承] と表示されます。

3 [ユーザーによる上書き] をクリックし、[ユーザーの追加] をクリックします。

4 ユーザーを見つけるには、[追加] をクリックし、ユーザーの名前または説明を入力して、[検索] をクリックします。

5 リストから 1 名以上のユーザーを選択し、[OK] をクリックし、[次へ] をクリックします。

Add Individual Policy（個別のポリシーの追加） ダイアログ ボックスが表示されます。

6 Horizon ポリシーを構成し、[終了] をクリックして変更を保存します。

Horizon 7 ポリシー

すべてのクライアント セッションに影響を与えるように Horizon 7 ポリシーを構成することも、特定のデスクトップ プールまたはユーザーに影響を与えるように View ポリシーを適用することもできます。

次の表では、Horizon 7 グループ ポリシー設定を説明します。

表 7-1. Horizon ポリシー

ポリシー	説明
マルチメディア リダイレクト (MMR)	クライアント システムで MMR を有効にするかどうかを指定します。 MMR は Windows Media Foundation のフィルタであり、マルチメディア データをリモート デスクトップ上の特定のコーデックから TCP ソケット経由で直接クライアント システムに転送します。その後、データはクライアント システム上で直接デコードされ、そこで再生されます。 デフォルト値は [拒否] です。 クライアント システムにローカル マルチメディアのデコードを処理する十分なリソースがない場合、設定を [拒否] のままにします。 マルチメディア リダイレクト (MMR) データは、アプリケーション ベースの暗号化なしでネットワークを介して送信され、リダイレクトされる内容によっては機密データが含まれる場合があります。このデータがネットワークで盗まれないようにするには、安全なネットワークで MMR だけを使用してください。
USB Access（USB アクセス）	リモート デスクトップがクライアント システムに接続されている USB デバイスを使用できるかどうかを指定します。 デフォルト値は [許可] です。セキュリティ上の理由のため、外部デバイスを使用できないようにするには、設定を [拒否] に変更します。
PCoIP ハードウェアのアクセラレーション	PCoIP 表示プロトコルのハードウェアのアクセラレーションを有効にするかどうか、および PCoIP ユーザー セッションに割り当てられるアクセラレーションの優先度を指定します。 この設定は、リモート デスクトップをホストする物理コンピュータ上に PCoIP ハードウェアのアクセラレーション デバイスが存在する場合にのみ有効です。 デフォルト値は [許可] で、優先度が [中] です。

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。

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。

Horizon 7 ADMX テンプレート ファイル

Horizon 7 ADMX テンプレート ファイルでは、Horizon 7 コンポーネントを制御および最適化できるグループ ポリシー設定が提供されます。

表 7-2. Horizon ADMX テンプレート ファイル

テンプレート名	テンプレート ファイル	説明
VMware View Agent の構成	vdm_agent.admx	Horizon Agent の認証および環境コンポーネントに関するポリシー設定が含まれています。 『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントを参照してください。
VMware Horizon Client の設定	vdm_client.admx	Horizon Client for Windows に関するポリシー設定が含まれています。 接続サーバ ホスト ドメインの外部から接続するクライアントは、Horizon Client に適用されるポリシーの影響を受けません。 『VMware Horizon Client for Windows のインストールとセットアップ ガイド』ドキュメントを参照してください。
VMware Horizon URL リダイレクト	urlRedirection.admx	URL コンテンツ リダイレクト機能に関するポリシー設定が含まれています。このテンプレートをリモート デスクトップ プールまたはアプリケーション プールの GPO に追加すると、リモート デスクトップまたはアプリケーション内でクリックされた特定の URL リンクを Windows ベースのクライアントにリダイレクトし、クライアント側のブラウザで開くことができます。 このテンプレートをクライアント側の GPO に追加すると、ユーザーが Windows ベースのクライアント システムで特定の URL リンクをクリックしたときに、リモート デスクトップまたはアプリケーションで URL を開くことができます。 『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントおよび『VMware Horizon Client for Windows のインストールとセットアップ ガイド』ドキュメントを参照してください。
VMware View Server の構成	vdm_server.admx	接続サーバに関するポリシー設定が含まれています。
VMware View の一般的な設定	vdm_common.admx	すべての Horizon コンポーネントに共通のポリシー設定が含まれています。
PCoIP セッション変数	pcoip.admx	PCoIP 表示プロトコルに関するポリシー設定が含まれています。 『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントを参照してください。
PCoIP クライアントのセッション変数	pcoip.client.admx	Horizon Client for Windows に影響を与える PCoIP 表示プロトコルに関するポリシー設定が含まれています。 『VMware Horizon Client for Windows のインストールとセットアップ ガイド』ドキュメントを参照してください。

表 7-2. Horizon ADMX テンプレート ファイル (続き)

テンプレート名	テンプレート ファイル	説明
個人設定管理	`ViewPM.admx`	Horizon Persona Management に関するポリシー設定が含まれています。 『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。
リモート デスクトップ サービス	`vmware_rdsh_server.admx`	リモート デスクトップ サービスに関するポリシー設定が含まれています。 『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントを参照してください。
View の RTAV 構成	`vdm_agent_rtav.admx`	リアルタイム オーディオ ビデオ機能で使用される Web カメラに関するポリシー設定が含まれています。 『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントを参照してください。
スキャナ リダイレクト	`vdm_agent_scanner.admx`	公開されたデスクトップおよびアプリケーションで使用するためにリダイレクトされるスキャン デバイスに関するポリシー設定が含まれています。 『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントを参照してください。
シリアル COM	`vdm_agent_serialport.admx`	仮想デスクトップで使用するためにリダイレクトされるシリアル（COM）ポートに関するポリシー設定が含まれています。 『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントを参照してください。
VMware Horizon プリンタ リダイレクト	`vdm_agent_printing.admx`	リダイレクトされたプリンタのフィルタリングに関するポリシー設定が含まれます。 『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントを参照してください。
View Agent Direct-Connection	`view_agent_direct_connection.admx`	View Agent Direct-Connection プラグインに関連するポリシー設定が含まれます。『View Agent Direct Connection プラグイン管理』ドキュメントを参照してください。

Horizon 接続サーバの構成 ADMX テンプレートの設定

View Server の構成 ADMX (`vdm_server.admx`) テンプレート ファイルには、すべての Horizon 接続サーバに関連するポリシー設定が含まれます。

次の表に、接続サーバの構成 ADMX テンプレート ファイルの各ポリシー設定を示します。このテンプレートには、コンピュータの設定のみが含まれます。グループ ポリシー管理エディタで [コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [VMware View Server の構成] の順に移動すると、これらの設定を確認できます。

表 7-3. Horizon Server の構成テンプレート設定

設定	プロパティ
Enumerate Forest Trust Child Domains	サーバが含まれるドメインによって信頼されるドメインをすべて列挙するかどうかを指定します。完全な信頼チェーンを確立するために、信頼される側の各ドメインによって信頼されるドメインも列挙され、信頼されるすべてのドメインが検索されるまでプロセスが再帰的に続行します。クライアントがログイン時に信頼されるすべてのドメインを使用できるように、この情報は接続サーバに渡されます。 デフォルトでは、このプロパティは有効になっています。無効にすると、直接信頼されるドメインのみが列挙され、リモート ドメイン コントローラには接続されません。 注 ドメイン関係が複雑な環境（フォレスト内のドメイン間で信頼を持つ複数のフォレスト構造を使用する環境など）では、このプロセスが完了するまでに数分かかる場合があります。
Recursive Enumeration of Trusted Domains	サーバが存在するドメインによって信頼されるドメインをすべて列挙するかどうかを指定します。完全な信頼チェーンを確立するために、信頼される側の各ドメインによって信頼されるドメインも列挙され、信頼されるすべてのドメインが検索されるまでプロセスが再帰的に続行します。クライアントがログイン時に信頼されるすべてのドメインを使用できるように、この情報は View 接続サーバに渡されます。 デフォルトでは、この設定は有効になっています。無効にすると、直接信頼されるドメインのみが列挙され、リモート ドメイン コントローラには接続されません。 ドメイン関係が複雑な環境（フォレスト内のドメイン間で信頼を持つ複数のフォレスト構造を使用する環境など）では、このプロセスが完了するまでに数分かかる場合があります。
Windows Password Authentication Mode	Windows パスワード認証のモードを選択します。 ■ KerberosOnly。Kerberos で認証を行います。 ■ KerberosWithFallbackToNTLM。Kerberos で認証を行いますが、失敗した場合には NTLM にフォールバックします。 ■ Legacy。NTLM で認証を行いますが、失敗した場合には Kerberos にフォールバックします。レガシー NT ドメイン コントローラのサポートに使用されます。 デフォルトは、KerberosOnly です。

Horizon 7 Common の構成 ADMX テンプレート設定

Horizon 7 Common の構成 ADMX (vdm_common.admx) テンプレート ファイルには、すべての Horizon コンポーネントに共通のポリシー設定が含まれます。これらのテンプレートには、コンピュータの設定のみが含まれます。

ログ設定

次の表に、Horizon Common の構成 ADMX テンプレート ファイル内のログ設定ポリシーを示します。グループ ポリシー管理エディタで [コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [VMware View Common の構成] - [ログ設定] の順に移動すると、これらの設定を確認できます。

表 7-4. View Common の構成テンプレート：ログ設定

設定	プロパティ
Number of days to keep production logs	ログ ファイルをシステムに保持する日数を指定します。値が設定されていない場合、デフォルト値が適用され、ログ ファイルは 7 日間保持されます。
Maximum number of debug logs	システムで保持するデバッグ ログ ファイルの最大数を指定します。ログ ファイルが最大サイズに達すると、新しいエントリは追加されず、新しいログ ファイルが作成されます。以前のログ ファイル数がこの値に達すると、最も古いログ ファイルが削除されます。
Maximum debug log size in Megabytes	デバッグ ログの最大サイズをメガバイト単位で指定します。このサイズに達すると、デバッグ ログ ファイルが閉じられ、新しいログ ファイルが作成されます。
Log Directory	ログ ファイルのディレクトリの完全パスを指定します。この場所が書き込み可能でない場合、デフォルトの場所が使用されます。クライアント ログ ファイルの場合は、クライアント名で追加のディレクトリが作成されます。
Send logs to a Syslog server	View Server のログを、VMware vCenter Log Insight などの Syslog サーバに送信できます。ログは、この GPO が構成されている OU またはドメイン内のすべての View Server から送信されます。 デスクトップを含む OU にリンクされている GPO でこの設定を有効にすることで、Horizon Agent のログを Syslog サーバに送信できます。 Syslog サーバにログ データを送信するには、この設定を有効にして、ログ レベルおよびサーバの完全修飾ドメイン名 (FQDN) または ID アドレスを指定します。デフォルトのポート 514 を使用しない場合は代替ポートを指定できます。縦棒 (¦) で仕様内の各要素を区切ります。次の構文を使用します: `Log Level|Server FQDN or IP [|Port number(514 default)]` 例：`Debug|192.0.2.2` 重要 Syslog データは、ソフトウェアベースの暗号化なしにネットワーク経由で送信されます。View Server のログには機密データが含まれていることがあるため、Syslog データを安全でないネットワーク上で送信しないようにします。可能であれば、IPsec などのリンク レイヤ セキュリティを使用して、こうしたデータがネットワーク上で監視されることを防ぎます。

パフォーマンス アラーム設定

表 7-5 で、Horizon Common の構成 ADMX テンプレート ファイル内のパフォーマンス アラーム設定について説明します。グループ ポリシー管理エディタで [コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [VMware View Common の構成] - [パフォーマンス アラーム] の順に移動すると、これらの設定を確認できます。

表 7-5. View Common の構成テンプレート：パフォーマンス アラーム設定

設定	プロパティ
CPU and Memory Sampling Interval in Seconds	CPU およびメモリのポーリング間隔を指定します。サンプリング間隔を小さくすると、ログへの出力レベルが高くなる可能性があります。
Overall CPU usage percentage to issue log info	システムの CPU 合計使用率をログに記録するしきい値を指定します。複数のプロセッサを使用できる場合、このパーセンテージは組み合わされた使用率を表します。
Overall memory usage percentage to issue log info	コミットされたシステム メモリの合計使用率をログに記録するしきい値を指定します。コミットされたシステム メモリは、プロセッサによって割り当てられ、オペレーティング システムが物理メモリまたはページファイルのページ スロットをコミットしたメモリです。

表 7-5. View Common の構成テンプレート：パフォーマンス アラーム設定 (続き)

設定	プロパティ
Process CPU usage percentage to issue log info	各プロセスの CPU 使用率がログに記録されるしきい値を指定します。
Process memory usage percentage to issue log info	各プロセスのメモリ使用率がログに記録されるしきい値を指定します。
Process to check, comma separated name list allowing wild cards and exclusion	調査する 1 つ以上のプロセス名に対応する、クエリーのカンマ区切りのリストを指定します。各クエリー内でワイルドカードを使用して、リストをフィルタ処理できます。 ■ アスタリスク（*）は 0 文字以上に一致します。 ■ 疑問符（?）は 1 文字に一致します。 ■ クエリーの先頭の感嘆符（!）は、そのクエリーによって生成されるすべての結果を除外します。 たとえば、次のクエリーは **ws** で始まるすべてのプロセスを選択し、**sys** で終わるすべてのプロセスを除外します。 **'! *sys,ws*'**

注　パフォーマンス アラーム設定は、Horizon 接続サーバと Horizon Agent システムにのみ適用されます。Horizon Client システムには適用されません。

セキュリティ設定

表 7-6 で、Horizon Common の構成 ADMX テンプレート ファイル内のセキュリティ設定について説明します。グループ ポリシー管理エディタで [コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [VMware View Common の構成] - [セキュリティ設定] の順に移動すると、これらの設定を確認できます。

表 7-6. View Common の構成テンプレート：セキュリティ設定

設定	プロパティ
Only use cached revocation URLS	証明書の失効チェックは、キャッシュ内の URL にのみアクセスします。 未設定の場合、デフォルトは false になります。
Revocation URL check timeout milliseconds	すべての失効 URL ワイヤ取得の累積的なタイムアウト（ミリ秒）。 未設定または値が 0 に設定されている場合、Microsoft のデフォルト処理が使用されます。
Type of certificate revocation check	実行する証明書失効チェックのタイプを選択します。 ■ なし ■ EndCertificateOnly ■ WholeChain ■ WholeChain デフォルトは WholeChainButRoot です。

全般設定

表 7-7 で、Horizon Common の構成 ADMX テンプレート ファイル内の全般設定について説明します。グループ ポリシー管理エディタで [コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [VMware View Common の構成] の順に移動すると、これらの設定を確認できます。

表 7-7. View Common の構成テンプレート：全般設定

設定	プロパティ
Disk threshold for log and events in Megabytes	ログおよびイベント用のディスク空き領域の最小しきい値を指定します。値を指定しない場合、デフォルトは 200 です。指定した値に達すると、イベント ログの作成が停止します。
Enable extended logging	トレースおよびデバッグのイベントをログ ファイルに記録するかどうかを指定します。
Override the default View Windows event generation	次の値がサポートされています。 ■ 0 = View イベントに対してのみイベント ログ エントリが生成されます（ログ メッセージのイベント ログ エントリは生成されません）。 ■ 1 = イベント ログ エントリが 4.5 以前の互換モードで生成されます。標準の View イベントにイベント ログ エントリは生成されません。イベント ログ エントリは、ログ ファイルのテキストにのみ基づいて生成されます。 ■ 2 = イベント ログ エントリが 4.5 以前の互換モードで生成されますが、View イベントも追加されます。

Horizon 7 コンポーネントのメンテナンス

8

Horizon 7 コンポーネントが常に使用でき、実行し続けるように、さまざまなメンテナンス タスクを実行できます。

この章では次のトピックについて説明します。

Horizon 7 構成データのバックアップと復元

Horizon Administrator で自動バックアップをスケジュール設定するか実行して、Horizon 7 と View Composer の構成データをバックアップできます。Horizon 7 構成を復元するには、バックアップした View LDAP ファイルと View Composer データベース ファイルを手動でインポートします。

バックアップと復元機能を使用して、Horizon 7 構成データを保持および移行できます。

Horizon 接続サーバと View Composer のデータのバックアップ

接続サーバの初期構成が完了したら、Horizon 7 と View Composer の構成データの定期的なバックアップをスケジューリングする必要があります。Horizon Administrator を使用して、Horizon 7 と View Composer のデータを保持できます。

Horizon 7 は、接続サーバの構成データを View LDAP リポジトリに保存します。View Composer はリンク クローン デスクトップの構成データを View Composer データベースに保存します。

Horizon Administrator を使用してバックアップを実行すると、Horizon 7 が View LDAP 構成データと View Composer データベースをバックアップします。両方のバックアップ ファイル セットは同じ場所に保存されます。View LDAP データは暗号化された LDAP データ交換形式（LDIF）でエクスポートされます。View LDAP については、「View LDAP ディレクトリ」を参照してください。

バックアップは複数の方法で実行できます。

- Horizon 7 構成バックアップ機能を使用して自動バックアップをスケジュール設定します。
- Horizon Administrator の [今すぐバックアップ] 機能を使用してすぐにバックアップを開始します。
- `vdmexport` ユーティリティを使用して、手動で View LDAP データをエクスポートします。このユーティリティは、接続サーバの各インスタンスで提供されます。

  `vdmexport` ユーティリティは、View LDAP データを暗号化された LDIF データ、プレーン テキスト、パスワードなどの秘密データが削除されたプレーン テキストとしてエクスポートできます。

  注 `vdmexport` ツールは View LDAP データのみをバックアップします。このツールは View Composer データベース情報はバックアップしません。

  `vdmexport` の詳細については、「Horizon 接続サーバからの構成データのエクスポート」を参照してください。

次のガイドラインは、Horizon 7 構成データのバックアップに適用されます。

- Horizon 7 は任意の接続サーバ インスタンスから構成データをエクスポートできます。
- 複製されたグループに複数の接続サーバ インスタンスがある場合は、1 つのインスタンスのデータをエクスポートするだけで済みます。複製されたすべてのインスタンスに同じ構成データが含まれています。
- 接続サーバの複製されたインスタンスを使用しているからといって、バックアップ メカニズムが機能していると考えないでください。Horizon 7 が接続サーバの複製されたインスタンスのデータの同期を実行するとき、1 つのインスタンスで何らかのデータが失われていると、グループのすべてのメンバーでそのデータが失われる可能性があります。
- 接続サーバが複数の Composer サービスで複数の vCenter Server インスタンスを使用する場合、Horizon 7 は vCenter Server インスタンスに関連付けられているすべての View Composer データベースをバックアップします。

Horizon 7 構成バックアップのスケジュール

Horizon 7 構成データを定期的にバックアップするようにスケジュールを設定できます。Horizon 7 は、接続サーバ インスタンスが構成データを格納する View LDAP リポジトリの内容をバックアップします。

構成をすぐにバックアップするには、接続サーバ インスタンスを選択し、[今すぐバックアップ] をクリックします。

開始する前に

バックアップ設定について理解しておきます。「Horizon 7 構成バックアップ設定」を参照してください。

手順

1 Horizon Administrator で、[View 構成] - [サーバ] を選択します。

2 [接続サーバ] タブで、バックアップ対象の接続サーバ インスタンスを選択して [編集] をクリックします。

3 [バックアップ] タブで、Horizon 7 構成バックアップ設定を指定して、バックアップの頻度、バックアップの最大数、バックアップ ファイルのフォルダの場所を設定します。

4 (オプション) データ リカバリのパスワードを変更します。

   a [データ リカバリのパスワードを変更] をクリックします。

   b 新しいパスワードを 2 回入力します。

   c (オプション) パスワードを忘れた場合のヒントを入力します。

   d [OK] をクリックします。

5 [OK] をクリックします。

Horizon 7 構成バックアップ設定

Horizon 7 では、接続サーバと View Composer の構成データを定期的にバックアップできます。Horizon Administrator で、バックアップ処理の頻度とその他の側面を設定できます。

表 8-1. Horizon 7 構成バックアップ設定

設定	説明
Automatic backup frequency（自動バックアップの頻度）	Every Hour（1 時間ごと）：1 時間ごとにバックアップを行います。 Every 6 Hours（6 時間ごと）：午前 0 時、午前 6 時、午後 0 時、午後 6 時にバックアップを行います。 Every 12 Hours（12 時間ごと）：午前 0 時と午後 0 時にバックアップを行います。 Every Day（毎日）：毎日午前 0 時にバックアップを行います。 Every 2 Days（2 日ごと）：土曜日、月曜日、水曜日、金曜日の午前 0 時にバックアップを行います。 Every Week（毎週）：毎週、土曜日の午前 0 時にバックアップを行います。 Every 2 Weeks（2 週ごと）：隔週の土曜日の午前 0 時にバックアップを行います。 Never（バックアップしない）：自動バックアップを行いません。
Max number of backups（バックアップの最大数）	接続サーバ インスタンスに格納できるバックアップ ファイル数です。この数には、0 より大きい整数を指定する必要があります。 最大数に達すると、Horizon 7 は最も古いバックアップ ファイルを削除します。 この設定は、[今すぐバックアップ] を使用した場合に作成されるバックアップ ファイルにも適用されます。
フォルダの場所	接続サーバが実行されているコンピュータでバックアップ ファイルが保存されるデフォルトの場所： `C:\Programdata\VMware\VDM\backups` [今すぐバックアップ] を使用した場合も、Horizon 7 ではこの場所にバックアップ ファイルを保存します。

Horizon 接続サーバからの構成データのエクスポート

View LDAP リポジトリの内容をエクスポートして、Horizon 接続サーバ インスタンスの構成データをバックアップできます。

`vdmexport` コマンドを使用して、View LDAP 構成データを暗号化された LDIF ファイルにエクスポートします。`vdmexport -v`（逐語的）オプションを使用してデータをプレーン テキスト LDIF ファイルにエクスポートすることも、`vdmexport -c`（クレンジング）オプションを使用してデータをパスワードなどの秘密データが削除されたプレーン テキストとしてエクスポートすることもできます。

任意の接続サーバ インスタンスで vdmexport コマンドを実行できます。複製されたグループに複数の接続サーバ インスタンスがある場合は、1 つのインスタンスのデータをエクスポートするだけで済みます。複製されたすべてのインスタンスに同じ構成データが含まれています。

注 vdmexport.exe コマンドは View LDAP データのみをバックアップします。このコマンドでは、View Composer データベース情報はバックアップされません。

開始する前に

- 接続サーバとともにインストールされている vdmexport.exe コマンドの実行可能ファイルを次のデフォルト パスで見つけます。

  C:\Program Files\VMware\VMware View\Server\tools\bin

- Administrators（管理者）または Administrators (Read Only)（管理者（読み取り専用））ロールのユーザーとして接続サーバ インスタンスにログインします。

手順

1 [スタート] - [コマンド プロンプト] を選択します。

2 コマンド プロンプトで vdmexport コマンドを入力し、出力をファイルにリダイレクトします。例：

```
vdmexport > Myexport.LDF
```

デフォルトでは、エクスポートされるデータは暗号化されています。

出力ファイル名を –f オプションの引数として指定できます。例：

```
vdmexport –f Myexport.LDF
```

–v オプションを使用することで、データをプレーン テキスト形式（逐語的）でエクスポートできます。例：

```
vdmexport –f Myexport.LDF –v
```

–c オプションを使用することで、データをパスワードなどの秘密データが削除されたプレーン テキスト形式（クレンジング データ）でエクスポートできます。例：

```
vdmexport –f Myexport.LDF –c
```

注 View LDAP 構成を復元するためにクレンジング バックアップ データの使用は検討しないでください。クレンジング構成データでは、パスワードなどの重要な情報が欠落しています。

vdmexport コマンドの詳細については、『Horizon 7 の統合』を参照してください。

次に進む前に

vdmimport コマンドを使用して、接続サーバの構成情報を復元または転送できます。

LDIF ファイルのインポートの詳細については、「Horizon 接続サーバと View Composer の構成データの復元」を参照してください。

Horizon 接続サーバと View Composer の構成データの復元

Horizon 7 によってバックアップされた接続サーバ LDAP 構成ファイルおよび View Composer データベース ファイルを手動で復元できます。

個別のユーティリティを手動で実行して、接続サーバと View Composer の構成データを復元します。

構成データを復元する前に、Horizon Administrator で構成データをバックアップしたことを確認します。「Horizon 接続サーバと View Composer のデータのバックアップ」を参照してください。

vdmimport ユーティリティを使用して、接続サーバ データを LDIF バックアップ ファイルから接続サーバ インスタンス内の View LDAP リポジトリにインポートします。

SviConfig ユーティリティを使用すると、View Composer データを **.svi** バックアップ ファイルから View Composer SQL データベースにインポートできます。

注　場合によっては、接続サーバ インスタンスの現在のバージョンをインストールし、接続サーバの LDAP 構成ファイルをインポートして既存の Horizon 7 構成を復元しなければならないことがあります。既存の Horizon 7 構成で 2 番目のデータセンターをセットアップするときなどは、ビジネス継続性とディザスタ リカバリ (BC/DR) 計画の一環としてこの手順が必要になる場合があります。詳細については、『Horizon 7 のインストール』を参照してください。

Horizon 接続サーバへの構成データのインポート

LDIF ファイルに格納されているデータのバックアップ コピーをインポートして、接続サーバ インスタンスの構成データを復元できます。

vdmimport コマンドを使用して、LDIF ファイルのデータを接続サーバ インスタンス内の View LDAP リポジトリにインポートします。

Horizon Administrator またはデフォルトの **vdmexport** コマンドを使用して View LDAP 構成をバックアップした場合、エクスポートされた LDIF ファイルは暗号化されています。LDIF ファイルの暗号化を解除してからでないと、インポートできません。

エクスポートされた LDIF ファイルがプレーン テキスト形式の場合、ファイルの暗号化を解除する必要はありません。

注　クレンジング形式の LDIF ファイルをインポートしないでください。この形式では、パスワードなどの秘密データが削除されたプレーン テキストになっています。インポートすると、復元された View LDAP リポジトリから重要な構成情報が失われます。

View LDAP リポジトリのバックアップの詳細については、「Horizon 接続サーバと View Composer のデータのバックアップ」を参照してください。

開始する前に

- 接続サーバとともにインストールされている vdmimport コマンドの実行可能ファイルを次のデフォルト パス配下で探します。

  C:\Program Files\VMware\VMware View\Server\tools\bin

- 管理者ロールのユーザーとして接続サーバ インスタンスにログインします。
- データ リカバリ パスワードを知っていることを確認します。パスワード リマインダが構成されていた場合、パスワード オプションを付けずに vdmimport コマンドを実行することでリマインダを表示できます。

手順

1 View Composer が動作しているサーバで Windows サービスの VMware Horizon View Composer を停止して、View Composer のすべてのインスタンスを停止します。

2 すべてのセキュリティ サーバで Windows サービスの VMware Horizon セキュリティ サーバを停止して、すべてのセキュリティ サーバ インスタンスを停止します。

3 Horizon 接続サーバのすべてのインスタンスをアンインストールします。

  VMware Horizon 接続サーバと AD LDS Instance VMwareVDMDS の両方をアンインストールします。

4 1 つの接続サーバ インスタンスをインストールします。

5 Windows サービスの VMware Horizon 接続サーバを停止して、接続サーバ インスタンスを停止します。

6 [スタート] - [コマンド プロンプト] の順にクリックします。

7 LDIF ファイルの暗号化を解除します。

  コマンド プロンプトで、vdmimport コマンドを入力します。–d オプション、–p オプションとデータ リカバリ パスワード、–f オプションと既存の暗号化された LDIF ファイルを指定し、次に暗号化を解除された LDIF ファイルの名前を指定します。例：

```
vdmimport –d –p <mypassword>
–f MyEncryptedexport.LDF > MyDecryptedexport.LDF
```

  データ リカバリ パスワードを覚えていない場合は、–p オプションを使用せずにコマンドを入力します。ユーティリティでパスワード リマインダが表示され、パスワードを入力するように要求されます。

8 暗号化が解除された LDIF ファイルをインポートし、View LDAP 構成を復元します。

  –f オプションと暗号化を解除された LDIF ファイルを指定します。例：

```
vdmimport –f MyDecryptedexport.LDF
```

9 接続サーバをアンインストールします。

  VMware Horizon 接続サーバ パッケージのみをアンインストールします。

10 接続サーバを再インストールします。

11 Horizon Administrator にログインして、構成が正しいかどうかを検証します。

12 View Composer インスタンスを開始します。

13 レプリカ サーバ インスタンスを再インストールします。

14 セキュリティ サーバ インスタンスを開始します。

セキュリティ サーバの構成に不整合があるというリスクが存在する場合は、セキュリティ サーバを停止するのではなくアンインストールしてからプロセスの最後に再インストールする必要があります。

`vdmimport` コマンドは、接続サーバ内の View LDAP リポジトリを LDIF ファイルの構成データで更新します。`vdmimport` コマンドの詳細については、『Horizon 7 のインストール』を参照してください。

注　復元される構成が、vCenter Server および View Composer（使用されている場合）に認識される仮想マシンと一致することを確認します。必要に応じて、View Composer の構成をバックアップから復元します。「View Composer データベースの復元」を参照してください。View Composer 構成のバックアップによって vCenter Server 内の仮想マシンが変更された場合は、View Composer 構成を復元した後に不整合を手動で解決する必要があります。

View Composer データベースの復元

View Composer 構成のバックアップ ファイルを、リンククローン情報が格納された View Composer データベースにインポートできます。

`SviConfig restoredata` コマンドを使用して、システムの障害の発生後に View Composer データベース データを復元したり、View Composer 構成を以前の状態に戻したりすることができます。

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。

開始する前に

View Composer データベース バックアップ ファイルの場所を確認します。デフォルトでは、Horizon 7 はバックアップ ファイルを接続サーバ コンピュータの `C:` ドライブ（`C:\Programdata\VMWare\VDM\backups`）に格納します。

View Composer バックアップ ファイルは日付スタンプと `.svi` サフィックスが付く命名規則を使用します。

`Backup-<YearMonthDayCount>-<vCenter Server Name_Domain Name>.svi`

例：`Backup-20090304000010-foobar_test_org.svi`

`SviConfig restoredata` パラメータについて理解しておく必要があります。

- `DsnName` - データベースに接続するために使用される DSN。`DsnName` パラメータは必須で、空の文字列にすることはできません。
- `Username` - データベースに接続するために使用されるユーザー名。このパラメータを指定しない場合、Windows 認証が使用されます。
- `Password` - データベースに接続するために使用されるパスワード。このパラメータが指定されておらず、Windows 認証が使用されない場合、後でパスワードの入力を求められます。

- **BackupFilePath** - View Composer バックアップ ファイルへのパス。

DsnName および **BackupFilePath** パラメータは必須で、空の文字列にすることはできません。**Username** および **Password** パラメータはオプションです。

手順

1 View Composer バックアップ ファイルを、接続サーバ コンピュータから、VMware Horizon View Composer サービスがインストールされているコンピュータからアクセス可能な場所にコピーします。

2 View Composer がインストールされているコンピュータで、VMware Horizon View Composer サービスを停止します。

3 Windows のコマンド プロンプトを開き、**SviConfig** 実行可能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 (x86)\VMware\VMware View Composer\sviconfig.exe** です。

4 **SviConfig restoredata** コマンドを実行します。

```
sviconfig –operation=restoredata
          –DsnName=<target_database_source_name_(DSN)>
          –Username=<database_administrator_username>
          –Password=<database_administrator_password>
          –BackupFilePath=<path_to_View_Composer_backup_file>
```

例：

```
sviconfig –operation=restoredata –dsnname=LinkedClone
–username=Admin –password=Pass
–backupfilepath="C:\Program Files (x86)\VMware\VMware View
Composer\Backup–20090304000010–foobar_test_org.SVI"
```

5 VMware Horizon View Composer サービスを開始します。

次に進む前に

SviConfig restoredata コマンドの出力結果コードについては、「View Composer データベースの復元の結果コード」を参照してください。

View Composer データベースの復元の結果コード

View Composer データベースを復元すると、**SviConfig restoredata** コマンドで結果コードが表示されます。

表 8-2. restoredata 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。

表 8-2. restoredata の結果コード (続き)

コード	説明
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 VMware Horizon 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、サービスを終了してください。
15	復元処理中に問題が発生しました。詳細は画面ログ出力として提供されます。

View Composer データベースのデータをエクスポート

View Composer データベースからデータをファイルにエクスポートできます。

重要　熟練した View Composer 管理者である場合に限って **SviConfig** ユーティリティを使用してください。

開始する前に

デフォルトでは、Horizon 7 はバックアップ ファイルを View 接続サーバ コンピュータの **C:** ドライブ (**C:\Programdata\VMware\VDM\backups**) に格納します。

SviConfig exportdata パラメータについて理解しておきます。

- **DsnName** - データベースに接続するために使用される DSN。指定しなければ、DSN 名、ユーザー名、およびパスワードは、サーバの構成ファイルから取得されません。
- **Username** - データベースに接続するために使用されるユーザー名。このパラメータを指定しなければ、Windows 認証が使用されます。
- **Password** - データベースに接続するために使用されるパスワード。このパラメータを指定せず、Windows 認証を使用しなければ、後でパスワードを入力するように求められます。
- **OutputFilePath** - 出力ファイルへのパス。

手順

1 View Composer がインストールされているコンピュータで、VMware Horizon View Composer サービスを停止します。

2 Windows のコマンド プロンプトを開き、**SviConfig** 実行可能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。

<View-Composer-installation-directory>\sviconfig.exe

3 `SviConfig exportdata` コマンドを実行します。

```
sviconfig –operation=exportdata
          –DsnName=<target_database_source_name_(DSN)>
          –Username=<database_administrator_username>
          –Password=<database_administrator_password>
          –OutputFilePath=<path_to_View_Composer_output_file>
```

例：

```
sviconfig –operation=exportdata –dsnname=LinkedClone
–username=Admin –password=Pass
–outputfilepath="C:\Program Files\VMware\VMware View
Composer\Export–20090304000010–foobar_test_org.SVI"
```

次に進む前に

`SviConfig exportdata` コマンドのエクスポート結果コードについては、「View Composer データベースのエクスポートの結果コード」を参照してください。

View Composer データベースのエクスポートの結果コード

View Composer データベースをエクスポートすると、`SviConfig exportdata` コマンドで終了コードが表示されます。

表 8-3. Exportdata ExitStatus コード

コード	説明
0	データのエクスポートが問題なく終了しました。
1	指定された DSN 名が見つかりません。
2	指定した証明書は無効です。
3	サポートされないドライバがデータベースに提供されました。
4	予期しない問題が発生しました。
18	データベース サーバに接続できません。
24	出力ファイルを開くことができません。

Horizon 7 コンポーネントの監視

Horizon Administrator のダッシュボードを使用して、Horizon 7 導入環境内の Horizon 7 および vSphere コンポーネントのステータスを素早く調査できます。

Horizon Administrator には、接続サーバ インスタンス、イベント データベース、セキュリティ サーバ、View Composer サービス、データストア、vCenter Server インスタンス、およびドメインに関する監視情報が表示されます。

注 Horizon 7 は、Kerberos ドメインに関するステータス情報を特定できません。ドメインが構成され、機能している場合でも、Horizon Administrator には Kerberos ドメインのステータスが不明として表示されます。

手順

1 Horizon Administrator で、[ダッシュボード] をクリックします。

2 システムの健全性ペインで、[View コンポーネント]、[vSphere コンポーネント]、または [その他のコンポーネント] を展開します。

- 緑色の上向き矢印は、コンポーネントに問題がないことを示します。
- 赤色の下向き矢印は、コンポーネントが使用できないか、または機能していないことを示します。
- 黄色の二重矢印は、コンポーネントが警告状態にあることを示します。
- 疑問符は、コンポーネントのステータスが不明であることを示します。

3 コンポーネント名をクリックします。

ダイアログに名前、バージョン、ステータス、その他のコンポーネント情報が表示されます。

次に進む前に

vCenter Server を使用して、vSAN データストアに参加する vSAN クラスタとディスクを監視します。vSphere 5.5 Update 1 での vSAN の監視の詳細については、『vSphere ストレージ マニュアル』と『vSphere 監視とパフォーマンス マニュアル』を参照してください。vSphere 6 以降の vSAN のモニタリングの詳細については、『VMware vSAN の管理』を参照してください。

マシンのステータスの監視

Horizon Administrator のダッシュボードを使用して、Horizon 7 環境内のマシンのステータスを素早く調査できます。たとえば、切断されたすべてのマシンやメンテナンス モードのマシンを表示できます。

開始する前に

仮想マシンのステータス値について理解しておきます。仮想マシンのステータスの詳細については、『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントの「vCenter Server 仮想マシンのステータス」を参照してください。

手順

1 Horizon Administrator で、[ダッシュボード] をクリックします。

2 [マシンのステータス] ペインで、ステータス フォルダを展開します。

オプション	説明
準備中	マシンがプロビジョニング中、削除中、またはメンテナンス モードにある場合の状態を表示します。
問題のあるマシン	エラー状態を表示します。
準備完了	マシンが使用できるようになったときの状態を表示します。

3 マシンのステータスを見つけて、その横のハイパーリンクされた番号をクリックします。

[マシン] ページに選択したステータスのすべてのマシンが表示されます。

次に進む前に

マシン名をクリックしてマシンの詳細を表示できます。また、Horizon Administrator の戻る矢印をクリックしてダッシュボード ページに戻ることができます。

Horizon 7 サービスの概要

接続サーバ インスタンスおよびセキュリティ サーバの動作は、システムで実行しているいくつかのサービスに依存しています。これらのシステムは、自動で起動および停止されますが、これらのサービスの動作を手動で調整する必要がある場合があります。

Microsoft Windows サービス ツールを使用して、Horizon 7 サービスを停止または開始します。接続サーバ ホストまたはセキュリティ サーバ上の Horizon 7 サービスを停止した場合は、そのサービスを再起動するまで、エンド ユーザーはリモート デスクトップまたはアプリケーションに接続できません。さらに、サービスの実行が停止した場合またはそのサービスが制御する Horizon 7 機能が応答していないように見える場合も、サービスを再起動する必要がある可能性があります。

Horizon 7 サービスの停止と開始

接続サーバ インスタンスおよびセキュリティ サーバの動作は、システムで実行しているいくつかのサービスに依存しています。Horizon 7 の動作に関する問題をトラブルシューティングするときに、これらのサービスを手動で停止したり開始したりすることが必要になる場合があります。

Horizon 7 サービスを停止すると、エンド ユーザーはリモート デスクトップおよびアプリケーションに接続できなくなります。このような操作はシステム メンテナンスのためにすでにスケジュール設定されている時間に実行するか、またはデスクトップおよびアプリケーションが一時的に使用できくなることをエンド ユーザーに警告する必要があります。

注　接続サーバ ホストの VMware Horizon View 接続サーバ サービスまたはセキュリティ サーバの VMware Horizon View セキュリティ サーバ サービスのみを停止します。他のコンポーネント サービスは停止しないでください。

開始する前に

接続サーバ ホストおよびセキュリティ サーバで実行するサービスについて、「接続サーバ ホスト上のサービス」および「セキュリティ サーバ上のサービス」を参照してください。

手順

1　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。

2　接続サーバ ホストの VMware Horizon View 接続サーバ サービスまたはセキュリティ サーバの VMware Horizon View セキュリティ サーバ サービスを選択して、必要に応じて [停止]、[再起動] または [開始] をクリックします。

3　一覧表示されたサービスのステータスが期待どおりに変更されたことを確認します。

接続サーバ ホスト上のサービス

Horizon 7 の処理は、接続サーバ ホストで実行しているいくつかのサービスに依存しています。

表 8-4. Horizon 接続サーバ ホスト サービス

サービス名	スタートアップの種類	説明
VMware Horizon View Blast Secure Gateway	自動	安全な HTML Access サービスと Blast Extreme サービスを提供します。クライアントが Blast Secure Gateway を介して接続サーバに接続する場合には、このサービスを実行する必要があります。
VMware Horizon View 接続サーバ	自動	コネクション ブローカー サービスを提供します。このサービスは常に実行する必要があります。このサービスを開始または停止すると、Framework、Message Bus、Security Gateway、および Web サービスも開始または停止されます。このサービスでは、VMwareVDMDS サービスまたは VMware Horizon View スクリプト ホスト サービスは開始または停止されません。
VMware Horizon View Framework コンポーネント	Manual	イベント ログ、セキュリティ、および COM+ Framework サービスを提供します。このサービスは常に実行する必要があります。
VMware Horizon View Message Bus コンポーネント	Manual	Horizon 7 コンポーネント間のメッセージング サービスを提供します。このサービスは常に実行する必要があります。
VMware Horizon View PCoIP Secure Gateway	Manual	PCoIP Secure Gateway サービスを提供します。クライアントが PCoIP Secure Gateway を介して接続サーバに接続する場合には、このサービスを実行する必要があります。
VMware Horizon View スクリプト ホスト	無効	仮想マシンを削除する場合に実行するサードパーティ スクリプトをサポートします。デフォルトでは、このサービスは無効になっています。スクリプトを実行する場合、このサービスを有効にする必要があります。
VMware Horizon View Security Gateway コンポーネント	Manual	一般的なゲートウェイ サービスを提供します。このサービスは常に実行する必要があります。
VMware Horizon View Web コンポーネント	Manual	Web サービスを提供します。このサービスは常に実行する必要があります。
VMwareVDMDS	自動	LDAP ディレクトリ サービスを提供します。このサービスは常に実行する必要があります。Horizon 7 のアップグレード中、このサービスにより既存のデータが正しく移行されます。

セキュリティ サーバ上のサービス

Horizon 7 の動作は、セキュリティ サーバで実行するいくつかのサービスに依存しています。

表 8-5. セキュリティ サーバ サービス

サービス名	スタートアップの種類	説明
VMware Horizon View Blast Secure Gateway	自動	安全な HTML Access サービスと Blast Extreme サービスを提供します。クライアントが Blast Secure Gateway を介してこのセキュリティ サーバに接続する場合には、このサービスを実行する必要があります。
VMware Horizon View セキュリティ サーバ	自動	セキュリティ サーバ サービスを提供します。このサービスは常に実行する必要があります。このサービスを開始または停止すると、Framework および Security Gateway サービスも開始または停止されます。

表 8-5. セキュリティ サーバ サービス (続き)

サービス名	スタートアップの種類	説明
VMware Horizon View Framework コンポーネント	手動	イベント ログ、セキュリティ、および COM+ Framework サービスを提供します。このサービスは常に実行する必要があります。
VMware Horizon View PCoIP Secure Gateway	手動	PCoIP Secure Gateway サービスを提供します。クライアントが PCoIP Secure Gateway を介してこのセキュリティ サーバに接続する場合には、このサービスを実行する必要があります。
VMware Horizon View Security Gateway コンポーネント	手動	一般的なゲートウェイ サービスを提供します。このサービスは常に実行する必要があります。

製品のライセンス キーの変更

システムに対する現在のライセンスの有効期限が切れるか、または現在ライセンスされていない Horizon 7 機能にアクセスする必要がある場合は、Horizon Administrator を使用して製品のライセンス キーを変更できます。

Horizon 7 の実行中に Horizon 7 にライセンスを追加できます。システムを再起動する必要はなく、デスクトップおよびアプリケーションへのアクセスは中断されません。

開始する前に

Horizon 7 と、View Composer や公開アプリケーションなどのアドオン機能の正しい動作のために、有効な製品のライセンス キーを入手してください。

手順

1 Horizon Administrator で、[View 構成] - [製品のライセンスと使用状況] の順に選択します。

現在のライセンス キーの最初と最後の 5 文字は、[ライセンス] パネルに表示されます。

2 [ライセンスを編集] をクリックします。

3 ライセンス シリアル番号を入力し、[OK] をクリックします。

[製品ライセンス] ウィンドウに更新されたライセンス情報が表示されます。

4 ライセンスの有効期限の日付を確認します。

5 お持ちの製品のライセンスによって使用資格が付与されている VMware Horizon 7 のエディションに基づいて、デスクトップ、アプリケーションのリモート処理、および View Composer ライセンスが有効または無効になっていることを確認します。

エディションによっては、VMware Horizon 7 の一部の機能を使用できません。各エディションの機能セットの比較については、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。

6 ライセンスの使用状況モデルが製品ライセンスで使用しているモデルと一致することを確認します。

使用状況は、製品ライセンスのエディションおよび使用状況の取り決めによって、指定ユーザーまたは同時ユーザーの数でカウントされます。

製品ライセンスの使用状況の監視

Horizon 7 Administrator では、Horizon に同時接続しているアクティブなユーザーの監視ができます。[製品のライセンスと使用状況] ページには、履歴使用数の現在値および最大値が表示されます。これらの数値を使用して、製品ライセンスの使用状況を追跡できます。履歴使用状況データをリセットして、現在のデータで始めからやり直すこともできます。

Horizon では、指定ユーザーのライセンス使用モデルと、同時ユーザーのライセンス使用モデルの 2 つを使用できます。Horizon は、製品ライセンスのエディションや使用モデルの契約にかかわらず、環境内の指定ユーザーと同時ユーザーをカウントします。

指定ユーザーの場合、Horizon は、Horizon 環境にアクセスした固有ユーザーの数をカウントします。指定ユーザーが複数の単一ユーザー デスクトップ、公開デスクトップおよび公開アプリケーションを実行すると、このユーザーは 1 回だけカウントされます。

指定ユーザーの場合、[製品のライセンスと使用状況] ページの [現在] 列には、Horizon のデプロイを最初に構成した以降のユーザー数、または [指定ユーザー数] を最後にリセットした以降のユーザー数が表示されます。[最高] 列は、指定ユーザーには該当しません。

同時ユーザーの場合、Horizon は、セッションあたりの単一ユーザー デスクトップ接続数をカウントします。同時ユーザーが複数の単一ユーザー デスクトップを実行している場合、接続された各デスクトップ セッションは個別にカウントされます。

同時ユーザーの場合、公開デスクトップとアプリケーションの接続はユーザーごとにカウントされます。同時ユーザーが複数の公開デスクトップ セッションおよびアプリケーションを実行すると、このユーザーは 1 回だけカウントされます。各公開デスクトップやアプリケーションが別々の RDS ホストでホストされている場合であってもユーザーがカウントされるのは 1 回です。同時ユーザーが 1 台の単一ユーザー デスクトップの他に、さらに公開デスクトップとアプリケーションを実行していても、このユーザーがカウントされるのは 1 回だけです。

同時ユーザーの場合、[製品のライセンスと使用状況] ページの [最大] 列には、並列デスクトップ セッションの最大数および公開デスクトップとアプリケーションのユーザー数が表示されます。カウントは Horizon を最初に構成した時点、または [最大数] を最後にリセットした時点からのカウント数になります。

共同作業セッション数、およびセッションに接続していた共同作業ユーザー数を監視できます。

- アクティブ - 共同作業セッション：セッション オーナーが複数のユーザーにセッションへの参加を招待した場合のセッション数です。例：John が 2 人のユーザーを自分のセッションに招待し、Mary が 1 人のユーザーを自分のセッションに招待しました。この行の値は 2 になります。招待されたユーザーがセッションに参加したかどうかは関係ありません。

- アクティブ - 共同作業者の合計：共同作業セッションに接続したユーザーの合計数です。セッション オーナーおよびすべての共同作業ユーザーが含まれます。例：John は 2 人のユーザーを招待し、1 人だけがセッションに参加しました。Mary は 1 人のユーザーを招待しましたが、このユーザーはセッションには参加しませんでした。この行の値は 3 になります。John の共同作業セッションにはオーナーが 1 人と参加者が 1 人いました。Mary の共同作業セッションにはオーナーが 1 人で参加者はいませんでした。セッション オーナーがカウントされるため、共同作業者の合計数は、常に共同作業セッションの合計数と同等またはそれ以上になります。

製品ライセンスの使用状況データのリセット

Horizon Administrator で、製品使用状況データ履歴をリセットして、現在のデータで始めからやり直すこともできます。

グローバル構成とポリシーを管理 権限を備えた管理者は、[最大数をリセット] 設定と [指定ユーザー数をリセット] 設定を選択できます。これらの設定へのアクセスを制限するには、指定した管理者にのみこの権限を付与してください。

開始する前に

製品ライセンスの使用状況について理解しておきます。「製品ライセンスの使用状況の監視」を参照してください。

手順

1 Horizon Administrator で、[View 構成] - [製品のライセンスと使用状況] の順に選択します。

2 (オプション) [用途] ペインで [最大数をリセット] を選択します。

履歴同時接続数の最高値が、現在の数値にリセットされます。

3 (オプション) [用途] ペインで [指定ユーザー数をリセット] を選択します。

指定ユーザーの最大履歴数が 0 にリセットされます。

> 注 [ユーザーとグループ] ページで [全般的なユーザー情報を更新する] を選択した場合も、指定ユーザーの最大履歴数が 0 にリセットされます。

Active Directory からの一般的なユーザー情報の更新

Horizon 7 を Active Directory に格納されている現在のユーザー情報で更新できます。この機能によって、Horizon 7 ユーザーの名前、電話、電子メール、ユーザー名、デフォルトの Windows ドメインを更新します。信頼された外部ドメインも更新されます。

この機能は、Active Directory の信頼される外部ドメインのリストを変更する場合、特にドメイン間の信頼関係の変更が Horizon 7 のユーザー権限に影響する場合に使用します。

この機能は Active Directory で最新のユーザー情報をスキャンし、Horizon 7 の構成を更新します。

全般的なユーザー情報を更新した場合も、指定ユーザーの数が 0 にリセットされます。この数は、Horizon Administrator の [製品のライセンスと使用状況] ページに表示されます。「製品ライセンスの使用状況データのリセット」を参照してください。

また、`vdmadmin` コマンドを使用して、ユーザーやドメインの情報を更新することもできます。「-F オプションを使用した外部セキュリティ プリンシパルの更新」を参照してください。

開始する前に

グローバル構成とポリシーを管理権限を持つ管理者として Horizon Administrator にログインできることを確認します。

手順

1 Horizon Administrator で、[ユーザーとグループ] をクリックします。

2 すべてのユーザーの情報を更新するか、個別のユーザーの情報を更新するかを選択します。

オプション	アクション
すべてのユーザーの場合	[全般的なユーザー情報を更新する] をクリックします。 すべてのユーザーとグループの更新には長い時間がかかることがあります。
個別のユーザーの場合	a 更新するユーザー名をクリックします。 b [全般的なユーザー情報を更新する] をクリックします。

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。

- 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。

開始する前に

- 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。「「View Composer 設定を構成する」」および 「「View Composer ドメインを構成する」」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. (オプション) RSA 鍵コンテナを新しいマシンに移行します。

5 VMware Horizon View Composer サービスを新しいマシンにインストールします。

インストール中、元の VMware Horizon View Composer サービスで使用されていたデータベースの DSN を指定します。また、そのデータベースに対して、ODBC データ ソース用に提供されたドメイン管理者のユーザー名とパスワードを指定します。

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

6 新しいマシンで View Composer 用の SSL サーバ証明書を構成します。

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

7 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。

開始する前に

- 『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 からの View Composer の削除」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 デスクトップ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。「「View Composer 設定を構成する」および「View Composer ドメインを構成する」」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。

開始する前に

.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。

次に進む前に

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。

開始する前に

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\v2.0<xxxxx>` 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\v2.0<xxxxx>` 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。

次に進む前に

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。

接続サーバ インスタンス、セキュリティ サーバ、または View Composer で証明書を更新する

更新済みのサーバ TLS 証明書または中間証明書を受信した場合は、それらの証明書を、各接続サーバ、セキュリティ サーバ、または View Composer ホストの Windows ローカル コンピュータ証明書ストアにインポートします。

通常、サーバ証明書の有効期限は 12 カ月です。ルート証明書および中間証明書の有効期限は 5 年または 10 年です。

サーバ証明書と中間証明書のインポートに関する詳細については、『Horizon 7 のインストール』の「新しい TLS 証明書を使用するように Horizon 接続サーバ、セキュリティ サーバ、View Composer を構成する」を参照してください。

開始する前に

- 現在有効な証明書の有効期限が切れる前に、更新済みのサーバ証明書および中間証明書を CA から入手します。
- 接続サーバ インスタンス、セキュリティ サーバ、または VMware Horizon View Composer サービスがインストールされた Windows Server の MMC に、証明書スナップインが追加されていることを確認します。

手順

1 Windows Server ホストの Windows ローカル コンピュータ証明書ストアに、署名された TLS サーバ証明書をインポートします。

   a 証明書スナップインで、サーバ証明書を [証明書（ローカル コンピュータ）] - [個人] - [証明書] フォルダにインポートします。

   b [この鍵をエクスポート可能にマークする] を選択します。

   c [次へ] をクリックして [終了] をクリックします。

2 接続サーバまたはセキュリティ サーバの場合は、Horizon 7 Server に発行された古い証明書から証明書のフレンドリ名 [vdm] を削除します。

   a 古い証明書を右クリックし、[プロパティ] をクリックします。

   b [一般] タブで、フレンドリ名テキスト [vdm] を削除します。

3 接続サーバまたはセキュリティ サーバの場合は、証明書のフレンドリ名 [vdm] を、古い証明書と置き換える新しい証明書に追加します。

   a 新しい証明書を右クリックし、[プロパティ] をクリックします。

   b [一般] タブのフレンドリ名フィールドに、[vdm] を入力します。

   c [適用]、[OK] の順にクリックします。

4 View Composer に発行されたサーバ証明書の場合は、`SviConfig ReplaceCertificate` ユーティリティを実行し、View Composer が使用するポートに新しい証明書をバインドします。

   このユーティリティにより、古い証明書のバインドが新しい証明書のバインドに置き換えられます。

   a VMware Horizon View Composer サービスを停止します。

   b Windows のコマンド プロンプトを開き、`SviConfig` 実行可能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 (x86)\VMware\VMware View Composer\sviconfig.exe` です。

   c `SviConfig ReplaceCertificate` コマンドを入力します。例：

```
sviconfig –operation=ReplaceCertificate
          –delete=false
```

      このユーティリティでは、Windows ローカル コンピュータ証明書ストアで使用可能な TLS 証明書の番号付きリストが表示されます。

   d 証明書を選択するには、証明書の番号を入力し、Enter キーを押します。

5 接続サーバ、セキュリティ サーバ、または View Composer ホストに中間証明書が発行された場合は、Windows 証明書ストアの [証明書（ローカル コンピュータ）] - [中間証明機関] - [証明書] フォルダに、更新された最新の中間証明書をインポートします。

6 変更を反映するため、VMware Horizon View 接続サーバ サービス、VMware Horizon View セキュリティ サーバ サービス、VMware Horizon View Composer サービスを再起動します。

カスタマ エクスペリエンス改善プログラム

この製品は、VMware のカスタマ エクスペリエンス改善プログラム (CEIP) の対象です。この製品の CEIP に参加することも、参加を取り消すこともできます。

CEIP を通して収集されるデータおよび VMware のその使用目的に関する詳細は、信頼と確実性センター (http://www.vmware.com/trustvmware/ceip.html) に記載されています。

手順

1 Horizon Administrator で、[View 構成] - [製品のライセンスと使用状況] の順に選択します。

2 [[ユーザー使用環境改善プログラム]] パネルで、[編集設定] をクリックします。

3 CEIP に参加するには、[VMware カスタマ エクスペリエンス改善プログラムに参加する] を選択します。

このオプションを選択しないと、CEIP に参加できません。

4 [OK] をクリックします。

Horizon Administrator での ThinApp アプリケーションの管理

9

Horizon Administrator を使用して、VMware ThinApp にパッケージ化されたアプリケーションを配布したり、管理したりすることができます。Horizon Administrator での ThinApp アプリケーションの管理には、アプリケーション パッケージのキャプチャと格納、Horizon Administrator への ThinApp アプリケーションの追加、マシンやデスクトップ プールへの ThinApp アプリケーションの割り当てなどが含まれます。

Horizon Administrator で ThinApp 管理機能を使用するためのライセンスを持っている必要があります。

重要　マシンおよびデスクトップ プールに指定して ThinApps を配布する代わりに、ThinApps を Active Directory ユーザーおよびグループに指定する場合、VMware Identity Manager を使用できます。

この章では次のトピックについて説明します。

ThinApp アプリケーションに対する Horizon 7 の要件

Horizon Administrator で、リモート デスクトップに配布される ThinApp アプリケーションをキャプチャして格納する場合は、いくつかの要件を満たす必要があります。

- アプリケーションは Microsoft Installation（MSI）パッケージとしてパッケージ化する必要があります。
- ThinApp バージョン 4.6 以降を使用して、MSI パッケージを作成または再パッケージ化する必要があります。
- 接続サーバ ホストとリモート デスクトップにアクセス可能な Active Directory ドメイン内に存在する Windows ネットワーク共有上に MSI パッケージを格納する必要があります。ファイル サーバは、コンピュータ アカウントに基づく認証およびファイル アクセス権をサポートする必要があります。
- MSI パッケージをホストするネットワーク共有に対するファイルおよび共有権限を構成して、ビルトイン Active Directory グループ ドメイン コンピュータに読み取りアクセス権を与える必要があります。ThinApp アプリケーションをドメイン コントローラに配布する予定がある場合は、ビルトイン Active Directory グループ ドメイン コントローラにも読み取りアクセス権を与える必要があります。

- ストリーミングされた ThinApp アプリケーション パッケージへのアクセスをユーザーに許可するには、その ThinApp パッケージをホストするネットワーク共有のユーザー用の NTFS 権限を **Read&Execute** に設定する必要があります。
- 不整合な名前空間によって、ドメイン メンバーのコンピュータが MSI パッケージをホストするネットワーク共有へのアクセスを妨げられないことを確認します。不整合な名前空間は、Active Directory ドメイン名がそのドメイン内のマシンで使われる DNS 名前空間の名前と異なる場合に発生します。詳細については、VMware ナレッジベース（KB）の記事 1023309 を参照してください。
- リモート デスクトップ上でストリーミングされた ThinApp アプリケーションを実行するには、MSI パッケージをホストするネットワーク共有にユーザーがアクセスできる必要があります。

アプリケーション パッケージのキャプチャと格納

ThinApp は基盤のオペレーティング システムとそのライブラリおよびフレームワークからアプリケーションを切り離し、アプリケーションをアプリケーション パッケージと呼ばれる 1 つの実行可能ファイルにバンドルすることによって、アプリケーションの仮想化を実現します。

Horizon Administrator で ThinApp アプリケーションを管理するには、ThinApp **[セットアップ キャプチャ]** ウィザードを使用してアプリケーションをキャプチャして MSI 形式でパッケージ化し、MSI パッケージをアプリケーション リポジトリに格納する必要があります。

アプリケーション リポジトリは Windows ネットワーク共有です。ネットワーク共有をアプリケーション リポジトリとして登録するには、Horizon Administrator を使用します。複数のアプリケーション リポジトリを登録できます。

注　複数のアプリケーション リポジトリがある場合は、サードパーティ ソリューションを使用して、ロード バランシングと可用性を管理できます。Horizon 7 には、ロード バランシングまたは可用性ソリューションが含まれていません。

ThinApp の機能の詳細および ThinApp **[セットアップ キャプチャ]** ウィザードの使用方法については、『Introduction to VMware ThinApp（VMware ThinApp 入門）』および『ThinApp ユーザーズ ガイド』を参照してください。

1 アプリケーションのパッケージ化

   アプリケーションをキャプチャしてパッケージ化するには、ThinApp **[セットアップ キャプチャ]** ウィザードを使用します。

2 Windows ネットワーク共有の作成

   リモート デスクトップやプールに配布される MSI パッケージをホストするには、Horizon Administrator で Windows ネットワーク共有を作成する必要があります。

3 アプリケーション リポジトリの登録

   Horizon Administrator で、MSI パッケージをホストする Windows ネットワーク共有をアプリケーション リポジトリとして登録する必要があります。

4 Horizon Administrator への ThinApp アプリケーションの追加

   ThinApp アプリケーションを Horizon Administrator に追加するには、アプリケーション リポジトリをスキャンし、ThinApp アプリケーションを選択します。ThinApp アプリケーションを Horizon Administrator に追加した後、その ThinApp アプリケーションをマシンやデスクトップ プールに割り当てることができます。

5 ThinApp テンプレートの作成

Horizon Administrator でテンプレートを作成して、ThinApp アプリケーションのグループを指定できます。テンプレートを使用して、アプリケーションを機能、ベンダー、または組織に適したその他の論理グループでグループ化することができます。

アプリケーションのパッケージ化

アプリケーションをキャプチャしてパッケージ化するには、ThinApp **[セットアップ キャプチャ]** ウィザードを使用します。

開始する前に

- http://www.vmware.com/products/thinapp から ThinApp ソフトウェアをダウンロードし、それをクリーンなコンピュータにインストールします。View は ThinApp バージョン 4.6 以降をサポートしています。
- 『ThinApp ユーザーズ ガイド』で ThinApp のソフトウェア要件とアプリケーションのパッケージ化手順を理解しておきます。

手順

1 ThinApp **[セットアップ キャプチャ]** ウィザードを起動し、ウィザードの指示に従います。

2 ThinApp **[セットアップ キャプチャ]** ウィザードでプロジェクトの場所の入力を求められたら、[MSI パッケージの構築] を選択します。

3 アプリケーションをリモート デスクトップにストリーミングする予定がある場合は、`package.ini` ファイルで MSIStreaming プロパティを 1 に設定します。

```
MSIStreaming=1
```

ThinApp **[セットアップ キャプチャ]** ウィザードによって、そのアプリケーション、つまりアプリケーションの実行に必要なすべてのコンポーネントとアプリケーション自体が MSI パッケージにカプセル化されます。

次に進む前に

MSI パッケージを格納するための Windows ネットワーク共有を作成します。

Windows ネットワーク共有の作成

リモート デスクトップやプールに配布される MSI パッケージをホストするには、Horizon Administrator で Windows ネットワーク共有を作成する必要があります。

開始する前に

- ThinApp **[セットアップ キャプチャ]** ウィザードを使用して、アプリケーションをパッケージ化します。
- ネットワーク共有が、ThinApp アプリケーションを格納するための Horizon 7 要件を満たしていることを確認します。詳細については、「ThinApp アプリケーションに対する Horizon 7 の要件」を参照してください。

手順

1 接続サーバ ホストとリモート デスクトップの両方にアクセス可能な、Active Directory ドメイン内のコンピュータに共有フォルダを作成します。

2 その共有フォルダに対するファイルおよび共有権限を構成して、ビルトイン Active Directory グループ ドメイン コンピュータに読み取りアクセス権を与えます。

3 ThinApp アプリケーションをドメイン コントローラに割り当てる予定がある場合は、ビルトイン Active Directory グループ ドメイン コントローラに読み取りアクセス権を与えます。

4 ストリーミングされた ThinApp アプリケーション パッケージを使用する予定がある場合は、ThinApp パッケージをホストするネットワーク共有の NTFS 権限をユーザーに対して `Read&Execute` に設定します。

5 MSI パッケージを共有フォルダにコピーします。

次に進む前に

Horizon Administrator で、Windows ネットワーク共有をアプリケーション リポジトリとして登録します。

アプリケーション リポジトリの登録

Horizon Administrator で、MSI パッケージをホストする Windows ネットワーク共有をアプリケーション リポジトリとして登録する必要があります。

複数のアプリケーション リポジトリを登録できます。

開始する前に

Windows ネットワーク共有を作成します。

手順

1 Horizon Administrator で、[View 構成] - [ThinApp 構成] の順に選択し、[リポジトリの追加] をクリックします。

2 [表示名] テキスト ボックスに、アプリケーション リポジトリの表示名を入力します。

3 [共有パス] テキスト ボックスに、アプリケーション パッケージをホストする Windows ネットワーク共有へのパスを入力します。

   ネットワーク共有パスは、¥¥<ServerComputerName>¥<ShareName> の形式である必要があります。<ServerComputerName> はサーバ コンピュータの DNS 名です。IP アドレスを指定しないでください。

   例：`¥¥server.domain.com¥MSIPackages`

4 [保存] をクリックして、Horizon Administrator にアプリケーション リポジトリを登録します。

Horizon Administrator への ThinApp アプリケーションの追加

ThinApp アプリケーションを Horizon Administrator に追加するには、アプリケーション リポジトリをスキャンし、ThinApp アプリケーションを選択します。ThinApp アプリケーションを Horizon Administrator に追加した後、その ThinApp アプリケーションをマシンやデスクトップ プールに割り当てることができます。

開始する前に

Horizon Administrator にアプリケーション リポジトリを登録します。

手順

1 Horizon Administrator で、[カタログ] - [ThinApps] の順に選択します。

2 [サマリ] タブで、[新しい ThinApp をスキャン] をクリックします。

3 スキャンするアプリケーション リポジトリとフォルダを選択し、[次へ] をクリックします。

アプリケーション リポジトリにサブフォルダが含まれている場合は、ルート フォルダを展開してサブフォルダを選択できます。

4 Horizon Administrator に追加する ThinApp アプリケーションを選択します。

Ctrl キーまたは Shift キーを押しながらクリックして、複数の ThinApp アプリケーションを選択できます。

5 [スキャン] をクリックして、選択した MSI パッケージのスキャンを開始します。

スキャンを停止する必要がある場合は、[スキャンを停止] をクリックできます。

Horizon Administrator は、各スキャン操作のステータスと、Horizon Administrator に追加された ThinApp アプリケーションの数を報告します。すでに Horizon Administrator に存在するアプリケーションを選択しても、そのアプリケーションが再び追加されることはありません。

6 [終了] をクリックします。

新しい ThinApp アプリケーションが [サマリ] タブに表示されます。

次に進む前に

（オプション）ThinApp テンプレートを作成します。

ThinApp テンプレートの作成

Horizon Administrator でテンプレートを作成して、ThinApp アプリケーションのグループを指定できます。テンプレートを使用して、アプリケーションを機能、ベンダー、または組織に適したその他の論理グループでグループ化することができます。

ThinApp テンプレートを使用すると、複数のアプリケーションの配布を効率化できます。ThinApp テンプレートをマシンまたはデスクトップ プールに割り当てると、Horizon Administrator は、現在そのテンプレートに含まれているすべてのアプリケーションをインストールします。

ThinApp テンプレートの作成はオプションです。

注 ThinApp テンプレートをマシンまたはデスクトップ プールに割り当てた後にそのテンプレートにアプリケーションを追加した場合、Horizon Administrator はその新しいアプリケーションをマシンまたはデスクトップ プールに自動的には割り当てません。以前にマシンまたはデスクトップ プールに割り当てられた ThinApp テンプレートからアプリケーションを削除した場合、そのアプリケーションはマシンまたはデスクトップ プールに割り当てられたままになります。

開始する前に

選択した ThinApp アプリケーションを Horizon Administrator に追加します。

手順

1 Horizon Administrator で、[カタログ] - [ThinApp] の順に選択し、[新規テンプレート] をクリックします。

2 テンプレートの名前を入力し、[追加] をクリックします。

使用可能なすべての ThinApp アプリケーションが表に表示されます。

3 特定の ThinApp アプリケーションを見つけるには、[検索] テキスト ボックスにアプリケーションの名前を入力し、[検索] をクリックします。

4 テンプレートに含める ThinApp アプリケーションを選択し、[追加] をクリックします。

Ctrl キーまたは Shift キーを押しながらクリックして、複数のアプリケーションを選択できます。

5 [OK] をクリックしてテンプレートを保存します。

マシンまたはデスクトップ プールへの ThinApp アプリケーションの割り当て

リモート デスクトップに ThinApp アプリケーションをインストールするには、Horizon Administrator を使用して ThinApp アプリケーションをマシンまたはデスクトップ プールに割り当てます。

ThinApp アプリケーションをマシンに割り当てると、Horizon Administrator は数分後に仮想マシンへのアプリケーションのインストールを開始します。ThinApp アプリケーションをデスクトップ プールに割り当てると、ユーザーがそのプール内のリモート デスクトップに初めてログインしたときに、Horizon Administrator がアプリケーションのインストールを開始します。

ストリーミング	Horizon Administrator は、リモート デスクトップに ThinApp アプリケーションへのショートカットをインストールします。このショートカットは、リポジトリをホストするネットワーク共有上の ThinApp アプリケーションを参照します。ストリーミングされた ThinApp アプリケーションを実行するには、ユーザーがそのネットワーク共有にアクセスできる必要があります。
フル	Horizon Administrator は、ローカル ファイル システムに完全な ThinApp アプリケーションをインストールします。

ThinApp アプリケーションのインストールにかかる時間は、そのアプリケーションのサイズによって異なります。

重要 ThinApp アプリケーションは、仮想マシンベースのデスクトップおよび vCenter Server 仮想マシンを含む自動デスクトップ プールまたは手動プールに割り当てることができます。ThinApp アプリケーションを公開デスクトップまたは従来の PC に割り当てることはできません。

- ThinApp アプリケーションを割り当てるためのベスト プラクティス

  ThinApp アプリケーションをマシンやデスクトップ プールに割り当てるときは、ベスト プラクティスに従ってください。

- 複数のマシンへの ThinApp アプリケーションの割り当て

  特定の ThinApp を 1 つ以上のマシンに割り当てることができます。

- マシンに複数の ThinApp アプリケーションを割り当てる

  1 つ以上の ThinApp アプリケーションを特定のマシンに割り当てることができます。

- 複数のデスクトップ プールへの ThinApp アプリケーションの割り当て

  特定の ThinApp アプリケーションを 1 つ以上のデスクトップ プールに割り当てることができます。

- デスクトップ プールへの複数の ThinApp アプリケーションの割り当て

  1 つ以上の ThinApp アプリケーションを特定のデスクトップ プールに割り当てることができます。

- マシンまたはデスクトップ プールへの ThinApp テンプレートの割り当て

  ThinApp テンプレートをマシンまたはデスクトップ プールに割り当てることによって、複数の ThinApp アプリケーションの配布を効率化できます。

- ThinApp アプリケーション割り当ての確認

  特定の ThinApp アプリケーションが現在割り当てられているすべてのマシンとデスクトップ プールを確認できます。また、特定のマシンまたはデスクトップ プールに割り当てられているすべての ThinApp アプリケーションを確認することもできます。

- MSI パッケージ情報の表示

  ThinApp アプリケーションを Horizon Administrator に追加した後、そのアプリケーションの MSI パッケージに関する情報を表示できます。

ThinApp アプリケーションを割り当てるためのベスト プラクティス

ThinApp アプリケーションをマシンやデスクトップ プールに割り当てるときは、ベスト プラクティスに従ってください。

- ThinApp アプリケーションを特定のリモート デスクトップにインストールするには、そのデスクトップをホストする仮想マシンにアプリケーションを割り当てます。マシンに共通する命名規則を使用すると、マシン割り当てを使用して、その命名規則を使用するすべてのマシンにアプリケーションを素早く配布することができます。
- ThinApp アプリケーションをデスクトップ プール内のすべてのマシンにインストールするには、そのデスクトップ プールにアプリケーションを割り当てます。デスクトップ プールを部門またはユーザーの種類ごとに構成すると、デスクトップ プール割り当てを使用して、特定の部門またはユーザーにアプリケーションを素早く配布することができます。たとえば、会計部門のユーザー用のデスクトップ プールがある場合は、アプリケーションをアカウンティング プールに割り当てることによって、同じアプリケーションをアカウンティング部門内のすべてのユーザーに配布できます。
- 複数の ThinApp アプリケーションの配布を効率化するには、それらのアプリケーションを ThinApp テンプレート内に含めます。ThinApp テンプレートをマシンまたはデスクトップ プールに割り当てると、Horizon Administrator は、現在そのテンプレートに含まれているすべてのアプリケーションをインストールします。

- ThinApp テンプレートに、マシンまたはデスクトップ プールにすでに割り当てられている ThinApp アプリケーションが含まれている場合は、テンプレートをそのマシンまたはデスクトップ プールに割り当てないでください。また、別のインストール タイプを使用して同じマシンまたはデスクトップ プールに複数回 ThinApp テンプレートを割り当てることは避けてください。このどちらの場合も、Horizon Administrator は ThinApp 割り当てエラーを返します。

複数のマシンへの ThinApp アプリケーションの割り当て

特定の ThinApp を 1 つ以上のマシンに割り当てることができます。

開始する前に

アプリケーション リポジトリをスキャンし、選択した ThinApp アプリケーションを Horizon Administrator に追加します。「Horizon Administrator への ThinApp アプリケーションの追加」を参照してください。

手順

1 Horizon Administrator で、[カタログ] - [ThinApps] の順に選択し、ThinApp アプリケーションを選択します。

2 [割り当てを追加] ドロップダウン メニューから [マシンを割り当てる] を選択します。

その ThinApp アプリケーションがまだ割り当てられていないマシンが表に表示されます。

オプション	アクション
特定のマシンを検索する	[検索] テキスト ボックスにマシンの名前を入力し、[検索] をクリックします。
同じ命名規則に従うすべてのマシンを検索する	[検索] テキスト ボックスにマシン名の一部を入力し、[検索] をクリックします。

3 ThinApp アプリケーションを割り当てるマシンを選択し、[追加] をクリックします。

Ctrl キーまたは Shift キーを押しながらクリックして、複数のマシンを選択できます。

4 インストール タイプを選択し、[OK] をクリックします。

オプション	アクション
ストリーミング	マシンにアプリケーションへのショートカットをインストールします。このショートカットは、リポジトリをホストするネットワーク共有上のアプリケーションを参照します。アプリケーションを実行するには、ユーザーがそのネットワーク共有にアクセスできる必要があります。
フル	マシンのローカル ファイル システムにアプリケーション全体をインストールします。

両方のインストール タイプをサポートしていない ThinApp アプリケーションもあります。アプリケーション パッケージがどのように作成されたかによって、どのインストール タイプを使用できるかが決まります。

Horizon Administrator は数分後に ThinApp アプリケーションのインストールを開始します。インストールが終了すると、仮想マシンによりホストされたデスクトップのすべてのユーザーがそのアプリケーションを使用できるようになります。

マシンに複数の ThinApp アプリケーションを割り当てる

1 つ以上の ThinApp アプリケーションを特定のマシンに割り当てることができます。

開始する前に

アプリケーション リポジトリをスキャンし、選択した ThinApp アプリケーションを Horizon Administrator に追加します。「Horizon Administrator への ThinApp アプリケーションの追加」を参照してください。

手順

1 Horizon Administrator で、[リソース] - [マシン] の順に選択し、[マシン] 列のマシン名をダブルクリックします。

2 [サマリ] タブで、ThinApp ペインの [割り当てを追加] をクリックします。

マシンにまだ割り当てられていない ThinApp アプリケーションが表に表示されます。

3 特定のアプリケーションを見つけるには、[検索] テキスト ボックスにアプリケーションの名前を入力し、[検索] をクリックします。

4 マシンに割り当てる ThinApp アプリケーションを選択し、[追加] をクリックします。

複数のアプリケーションを追加するには、この手順を繰り返します。

5 インストール タイプを選択し、[OK] をクリックします。

オプション	アクション
ストリーミング	マシンにアプリケーションへのショートカットをインストールします。このショートカットは、リポジトリをホストするネットワーク共有上のアプリケーションを参照します。アプリケーションを実行するには、ユーザーがそのネットワーク共有にアクセスできる必要があります。
フル	マシンのローカル ファイル システムにアプリケーション全体をインストールします。

両方のインストール タイプをサポートしていない ThinApp アプリケーションもあります。アプリケーション パッケージがどのように作成されたかによって、どのインストール タイプを使用できるかが決まります。

Horizon Administrator は数分後に ThinApp アプリケーションのインストールを開始します。インストールが終了すると、仮想マシンでホストされているデスクトップのすべてのユーザーがアプリケーションを使用できるようになります。

複数のデスクトップ プールへの ThinApp アプリケーションの割り当て

特定の ThinApp アプリケーションを 1 つ以上のデスクトップ プールに割り当てることができます。

ThinApp アプリケーションをリンク クローン プールに割り当て、後でそのプールを更新、再構成、または再調整すると、Horizon Administrator によってそのアプリケーションが自動的に再インストールされます。アプリケーションを手動で再インストールする必要はありません。

開始する前に

アプリケーション リポジトリをスキャンし、選択した ThinApp アプリケーションを Horizon Administrator に追加します。「Horizon Administrator への ThinApp アプリケーションの追加」を参照してください。

手順

1 Horizon Administrator で、[カタログ] - [ThinApps] の順に選択し、ThinApp アプリケーションを選択します。

2 [割り当てを追加] ドロップダウン メニューから [デスクトップ プールを割り当てる] を選択します。

ThinApp アプリケーションがまだ割り当てられていないデスクトップ プールが表に表示されます。

オプション	アクション
特定のデスクトップ プールを検索する	[検索] テキスト ボックスにデスクトップ プールの名前を入力し、[検索] をクリックします。
同じ命名規則に従うすべてのデスクトップ プールを検索する	[検索] テキスト ボックスにデスクトップ プール名の一部を入力し、[検索] をクリックします。

3 ThinApp アプリケーションを割り当てるデスクトップ プールを選択し、[追加] をクリックします。

Ctrl キーまたは Shift キーを押しながらクリックして、複数のデスクトップ プールを選択できます。

4 インストール タイプを選択し、[OK] をクリックします。

オプション	アクション
ストリーミング	マシンにアプリケーションへのショートカットをインストールします。このショートカットは、リポジトリをホストするネットワーク共有上のアプリケーションを参照します。アプリケーションを実行するには、ユーザーがそのネットワーク共有にアクセスできる必要があります。
フル	マシンのローカル ファイル システムにアプリケーション全体をインストールします。

両方のインストール タイプをサポートしていない ThinApp アプリケーションもあります。アプリケーション パッケージがどのように作成されたかによって、どのインストール タイプを使用できるかが決まります。

ユーザーがそのプール内のデスクトップに初めてログインしたときに、Horizon Administrator は ThinApp アプリケーションのインストールを開始します。インストールが終了すると、デスクトップ プールのすべてのユーザーがそのアプリケーションを使用できるようになります。

デスクトップ プールへの複数の ThinApp アプリケーションの割り当て

1 つ以上の ThinApp アプリケーションを特定のデスクトップ プールに割り当てることができます。

ThinApp アプリケーションをリンク クローン プールに割り当て、後でそのプールを更新、再構成、または再調整すると、Horizon Administrator によってそのアプリケーションが自動的に再インストールされます。アプリケーションを手動で再インストールする必要はありません。

開始する前に

アプリケーション リポジトリをスキャンし、選択した ThinApp アプリケーションを Horizon Administrator に追加します。「Horizon Administrator への ThinApp アプリケーションの追加」を参照してください。

手順

1 Horizon Administrator で、[カタログ] - [デスクトップ プール] を選択し、プール ID をダブルクリックします。

2 [インベントリ] タブで、[ThinApp] をクリックし、[割り当てを追加] をクリックします。

プールにまだ割り当てられていない ThinApp アプリケーションが表に表示されます。

3 特定のアプリケーションを見つけるには、[検索] テキスト ボックスに ThinApp アプリケーションの名前を入力し、[検索] をクリックします。

4 プールに割り当てる ThinApp アプリケーションを選択し、[追加] をクリックします。

複数のアプリケーションを選択するには、この手順を繰り返します。

5 インストール タイプを選択し、[OK] をクリックします。

オプション	アクション
ストリーミング	マシンにアプリケーションへのショートカットをインストールします。このショートカットは、リポジトリをホストするネットワーク共有上のアプリケーションを参照します。アプリケーションを実行するには、ユーザーがそのネットワーク共有にアクセスできる必要があります。
フル	マシンのローカル ファイル システムにアプリケーション全体をインストールします。

両方のインストール タイプをサポートしていない ThinApp アプリケーションもあります。アプリケーション パッケージがどのように作成されたかによって、どのインストール タイプを使用できるかが決まります。

ユーザーがそのプール内のデスクトップに初めてログインしたときに、Horizon Administrator は ThinApp アプリケーションのインストールを開始します。インストールが終了すると、デスクトップ プールのすべてのユーザーがそれらのアプリケーションを使用できるようになります。

マシンまたはデスクトップ プールへの ThinApp テンプレートの割り当て

ThinApp テンプレートをマシンまたはデスクトップ プールに割り当てることによって、複数の ThinApp アプリケーションの配布を効率化できます。

ThinApp テンプレートをマシンまたはデスクトップ プールに割り当てると、Horizon Administrator で、現在そのテンプレートに含まれている ThinApp アプリケーションがインストールされます。

開始する前に

ThinApp テンプレートを作成します。「ThinApp テンプレートの作成」を参照してください。

手順

1 Horizon Administrator で、[カタログ] - [ThinApps] の順に選択します。

2 ThinApp テンプレートを選択します。

3 [割り当てを追加] ドロップダウン メニューから [マシンを割り当てる] または [デスクトップ プールを割り当てる] を選択します。

すべてのマシンまたはデスクトップ プールが表に表示されます。

オプション	アクション
特定のマシンまたはデスクトップ プールを検索する	[検索] テキスト ボックスにマシンまたはデスクトップ プールの名前を入力し、[検索] をクリックします。
同じ命名規則に従うすべてのマシンまたはデスクトップ プールを検索する	[検索] テキスト ボックスにマシン名またはデスクトップ プール名の一部を入力し、[検索] をクリックします。

4 ThinApp テンプレートを割り当てるマシンまたはデスクトップ プールを選択し、[追加] をクリックします。

複数のマシンまたはデスクトップ プールを選択するには、この手順を繰り返します。

5 インストール タイプを選択し、[OK] をクリックします。

オプション	アクション
ストリーミング	マシンにアプリケーションへのショートカットをインストールします。このショートカットは、リポジトリをホストするネットワーク共有上のアプリケーションを参照します。アプリケーションを実行するには、ユーザーがそのネットワーク共有にアクセスできる必要があります。
フル	マシンのローカル ファイル システムにアプリケーション全体をインストールします。

両方のインストール タイプをサポートしていない ThinApp アプリケーションもあります。アプリケーション パッケージがどのように作成されたかによって、どのインストール タイプを使用できるかが決まります。

ThinApp テンプレートをマシンに割り当てると、Horizon Administrator で、数分後にテンプレート内のアプリケーションのインストールが開始されます。ThinApp テンプレートをデスクトップ プールに割り当てると、ユーザーがそのデスクトップ プール内のリモート デスクトップに初めてログインしたときに、Horizon Administrator で、テンプレート内のアプリケーションのインストールが開始されます。インストールが終了すると、マシンまたはデスクトップ プールのすべてのユーザーがそれらのアプリケーションを使用できるようになります。

ThinApp テンプレートに、マシンまたはデスクトップ プールにすでに割り当てられているアプリケーションが含まれている場合、Horizon Administrator はアプリケーション割り当てエラーを返します。

ThinApp アプリケーション割り当ての確認

特定の ThinApp アプリケーションが現在割り当てられているすべてのマシンとデスクトップ プールを確認できます。また、特定のマシンまたはデスクトップ プールに割り当てられているすべての ThinApp アプリケーションを確認することもできます。

開始する前に

「ThinApp アプリケーションのインストール ステータス値」で ThinApp インストール ステータス値について理解しておきます。

手順

- 確認する ThinApp アプリケーション割り当てを選択します。

オプション	操作
特定の ThinApp アプリケーションが割り当てられているすべてのマシンとデスクトップ プールを確認する	[カタログ] - [ThinApp] を選択し、ThinApp アプリケーションの名前をダブルクリックします。 [割り当て] タブに、そのアプリケーションが現在割り当てられているマシンとデスクトップ プール、およびインストール タイプが表示されます。 [マシン] タブに、そのアプリケーションに現在関連付けられているマシン、およびインストール ステータス情報が表示されます。 注 ThinApp アプリケーションをプールに割り当てた場合、そのプール内のマシンは、アプリケーションのインストール後に [マシン] タブに表示されます。
特定のマシンに割り当てられているすべての ThinApp アプリケーションを確認する	[リソース] - [マシン] を選択し、[マシン] 列のマシン名をダブルクリックします。 [サマリ] タブの [ThinApp] ペインに、そのマシンに現在割り当てられている各アプリケーション、およびインストール ステータスが表示されます。
特定のデスクトップ プールに割り当てられているすべての ThinApp アプリケーションを確認する	[カタログ] - [デスクトップ プール] を選択し、プール ID をダブルクリックします。次に、[インベントリ] タブを選択し、[ThinApp] をクリックします。 [ThinApp 割り当て] ペインに、そのデスクトップ プールに現在割り当てられている各アプリケーションが表示されます。

ThinApp アプリケーションのインストール ステータス値

ThinApp アプリケーションをマシンまたはプールに割り当てると、Horizon Administrator にインストールのステータスが表示されます。

次の表で、各ステータス値を説明します。

表 9-1. ThinApp アプリケーションのインストール ステータス

ステータス	説明
割り当て済み	ThinApp アプリケーションはマシンに割り当てられています。
インストール エラー	Horizon Administrator が ThinApp アプリケーションをインストールしようとしたときにエラーが発生しました。
アンインストール エラー	Horizon Administrator が ThinApp アプリケーションをアンインストールしようとしたときにエラーが発生しました。
インストール済み	ThinApp アプリケーションはインストールされています。
インストールの保留中	Horizon Administrator は ThinApp アプリケーションをインストールしようとしています。 このステータスのアプリケーションを割り当て解除することはできません。 注 この値は、デスクトップ プール内のマシンには表示されません。
アンインストールの保留中	Horizon Administrator は ThinApp アプリケーションをアンインストールしようとしています。

MSI パッケージ情報の表示

ThinApp アプリケーションを Horizon Administrator に追加した後、そのアプリケーションの MSI パッケージに関する情報を表示できます。

手順

1 Horizon Administrator で、[カタログ] - [ThinApps] の順に選択します。

[サマリ] タブに、現在使用可能なアプリケーションが一覧表示され、完全割り当てとストリーミング割り当ての数が表示されます。

2 ThinApp 列のアプリケーションの名前をダブルクリックします。

3 MSI パッケージに関する一般的な情報を表示するには、[サマリ] タブを選択します。

4 MSI パッケージに関する詳細情報を表示するには、[パッケージ情報] をクリックします。

Horizon Administrator での ThinApp アプリケーションのメンテナンス

Horizon Administrator での ThinApp アプリケーションのメンテナンスには、ThinApp アプリケーション割り当ての削除、ThinApp アプリケーションおよびアプリケーション リポジトリの削除、ThinApp テンプレートの変更や削除などのタスクが含まれます。

注 ThinApp アプリケーションをアップグレードするには、アプリケーションの古いバージョンを割り当て解除して削除し、新しいバージョンを追加して割り当てる必要があります。

- 複数のマシンからの ThinApp アプリケーション割り当ての削除

  特定の ThinApp アプリケーションへの割り当てを 1 つ以上のマシンから削除できます。

- マシンからの複数の ThinApp アプリケーション割り当ての削除

  1 つ以上の ThinApp アプリケーションへの割り当てを特定のマシンから削除できます。

- 複数のデスクトップ プールからの ThinApp アプリケーション割り当ての削除

  1 つ以上のデスクトップ プールから、特定の ThinApp アプリケーションへの割り当てを削除できます。

- デスクトップ プールからの複数の ThinApp アプリケーション割り当ての削除

  1 つ以上の ThinApp アプリケーション割り当てを特定のデスクトップ プールから削除できます。

- Horizon Administrator からの ThinApp アプリケーションの削除

  ThinApp アプリケーションを Horizon Administrator から削除すると、そのアプリケーションをマシンやデスクトップ プールに割り当てることができなくなります。

- ThinApp テンプレートの変更または削除

  アプリケーションを ThinApp テンプレートに追加したり、ThinApp テンプレートから削除したりできます。また、ThinApp テンプレートを削除することもできます。

- アプリケーション リポジトリの削除

  アプリケーション リポジトリを Horizon Administrator から削除できます。

複数のマシンからの ThinApp アプリケーション割り当ての削除

特定の ThinApp アプリケーションへの割り当てを 1 つ以上のマシンから削除できます。

開始する前に

マシンにホストされているリモート デスクトップのユーザーに、アプリケーションを削除しようとしていることを通知します。

手順

1 Horizon Administrator で、[カタログ] - [ThinApp] の順に選択して、ThinApp アプリケーションの名前をダブルクリックします。

2 [割り当て] タブで、マシンを選択し、[割り当ての削除] をクリックします。

Ctrl キーまたは Shift キーを押しながらクリックして、複数のマシンを選択できます。

Horizon Administrator は数分後に ThinApp アプリケーションをアンインストールします。

重要 Horizon Administrator が ThinApp アプリケーションをアンインストールしようとした時点でエンド ユーザーがそのアプリケーションを使用している場合、アンインストールは失敗し、アプリケーションのステータスが「Uninstall Error（アンインストール エラー）」に変わります。このエラーが発生した場合は、まず ThinApp アプリケーション ファイルをマシンから手動でアンインストールし、次に Horizon Administrator で [デスクトップのアプリ ステータスを削除] をクリックする必要があります。

マシンからの複数の ThinApp アプリケーション割り当ての削除

1 つ以上の ThinApp アプリケーションへの割り当てを特定のマシンから削除できます。

開始する前に

マシンでホストされているリモート デスクトップのユーザーに、アプリケーションを削除しようとしていることを通知します。

手順

1 Horizon Administrator で、[リソース] - [マシン] の順に選択し、[マシン] 列のマシン名をダブルクリックします。

2 [サマリ] タブで、ThinApp アプリケーションを選択し、ThinApp ペインの [割り当ての削除] をクリックします。

別のアプリケーション割り当てを削除するには、この手順を繰り返します。

Horizon Administrator は数分後に ThinApp アプリケーションをアンインストールします。

重要 Horizon Administrator が ThinApp アプリケーションをアンインストールしようとした時点でエンド ユーザーがそのアプリケーションを使用している場合、アンインストールは失敗し、アプリケーションのステータスが Uninstall Error（アンインストール エラー）に変わります。このエラーが発生した場合は、まず ThinApp アプリケーション ファイルをマシンから手動でアンインストールし、次に Horizon Administrator で [デスクトップのアプリ ステータスを削除] をクリックする必要があります。

複数のデスクトップ プールからの ThinApp アプリケーション割り当ての削除

1 つ以上のデスクトップ プールから、特定の ThinApp アプリケーションへの割り当てを削除できます。

開始する前に

プール内のリモート デスクトップのユーザーに、アプリケーションを削除しようとしていることを通知します。

手順

1 Horizon Administrator で、[カタログ] - [ThinApp] の順に選択して、ThinApp アプリケーションの名前をダブルクリックします。

2 [割り当て] タブで、デスクトップ プールを選択し、[割り当てを削除] をクリックします。

Ctrl キーまたは Shift キーを押しながらクリックして、複数のデスクトップ プールを選択できます。

ユーザーがそのプール内のリモート デスクトップに初めてログインした際に、Horizon Administrator は ThinApp アプリケーションをアンインストールします。

デスクトップ プールからの複数の ThinApp アプリケーション割り当ての削除

1 つ以上の ThinApp アプリケーション割り当てを特定のデスクトップ プールから削除できます。

開始する前に

プール内のリモート デスクトップのユーザーに、アプリケーションを削除しようとしていることを通知します。

手順

1 Horizon Administrator で、[カタログ] - [デスクトップ プール] を選択し、プール ID をダブルクリックします。

2 [インベントリ] タブで、[ThinApp] をクリックし、ThinApp アプリケーションを選択して、[割り当ての削除] をクリックします。

複数のアプリケーションを削除するには、この手順を繰り返します。

ユーザーがそのプール内のリモート デスクトップに初めてログインした際に、Horizon Administrator は ThinApp アプリケーションをアンインストールします。

Horizon Administrator からの ThinApp アプリケーションの削除

ThinApp アプリケーションを Horizon Administrator から削除すると、そのアプリケーションをマシンやデスクトップ プールに割り当てることができなくなります。

組織で ThinApp アプリケーションを別のベンダーのアプリケーションに置き換えることを決定した場合は、その ThinApp アプリケーションの削除が必要になることがあります。

注 ThinApp アプリケーションがマシンまたはデスクトップ プールにすでに割り当てられている場合や、アンインストールの保留中状態にある場合は、その ThinApp アプリケーションを削除できません。

開始する前に

現在、ThinApp アプリケーションがマシンまたはデスクトップ プールに割り当てられている場合は、そのマシンまたはデスクトップ プールから割り当てを削除します。

手順

1 Horizon Administrator で、[カタログ] - [ThinApps] の順に選択し、ThinApp アプリケーションを選択します。

2 [ThinApp の削除] をクリックします。

3 [OK] をクリックします。

ThinApp テンプレートの変更または削除

アプリケーションを ThinApp テンプレートに追加したり、ThinApp テンプレートから削除したりできます。また、ThinApp テンプレートを削除することもできます。

ThinApp テンプレートをマシンまたはデスクトップ プールに割り当てた後にそのテンプレートにアプリケーションを追加した場合、Horizon Administrator はその新しいアプリケーションをマシンまたはデスクトップ プールに自動的には割り当てません。以前にマシンまたはデスクトップ プールに割り当てられた ThinApp テンプレートからアプリケーションを削除した場合、そのアプリケーションはマシンまたはデスクトップ プールに割り当てられたままになります。

手順

- Horizon Administrator で、[カタログ] - [ThinApps] の順に選択し、ThinApp テンプレートを選択します。

オプション	アクション
ThinApp アプリケーションをテンプレートに追加するか、またはテンプレートから削除する	[テンプレートの編集] をクリックします。
テンプレートを削除する	[テンプレートを削除] をクリックします。

アプリケーション リポジトリの削除

アプリケーション リポジトリを Horizon Administrator から削除できます。

アプリケーション リポジトリに格納されている MSI パッケージが必要なくなった場合や、MSI パッケージを別のネットワーク共有に移動する必要がある場合は、アプリケーション リポジトリの削除が必要になることがあります。Horizon Administrator で、アプリケーション リポジトリの共有パスを編集することはできません。

手順

1 Horizon Administrator で、[View 構成] - [ThinApp 構成] の順に選択し、アプリケーション リポジトリを選択します。

2 [リポジトリを削除] をクリックします。

Horizon Administrator での ThinApp アプリケーションの監視とトラブルシューティング

Horizon Administrator は、ThinApp アプリケーションの管理に関連したイベントをイベントおよびレポート データベースに記録します。これらのイベントは、Horizon Administrator の [イベント] ページで表示できます。

次の状況が発生した場合に、[イベント] ページにイベントが表示されます。

- ThinApp アプリケーションが割り当てられたか、またはアプリケーション割り当てが削除された

- ThinApp アプリケーションがマシンにインストールされたか、またはアンインストールされた
- ThinApp アプリケーションをインストールまたはアンインストールできない
- Horizon Administrator で ThinApp アプリケーション リポジトリが登録、変更、または削除された
- ThinApp アプリケーションが Horizon Administrator に追加された

ThinApp アプリケーションの管理に関する一般的な問題についてのトラブルシューティングのヒントを参照できます。

アプリケーション リポジトリを登録できない

Horizon Administrator にアプリケーション リポジトリを登録できません。

問題

Horizon Administrator でアプリケーション リポジトリを登録しようとすると、エラー メッセージが表示されます。

原因

接続サーバ ホストが、アプリケーション リポジトリをホストするネットワーク共有にアクセスできません。[共有パス] テキスト ボックスに入力したネットワーク共有パスが正しくない可能性があるか、アプリケーション リポジトリをホストするネットワーク共有が接続サーバ ホストからアクセスできないドメイン内にあるか、またはネットワーク共有の権限が正しく設定されていません。

解決方法

- ネットワーク共有パスが正しくない場合は、正しいネットワーク共有パスを入力します。IP アドレスを含むネットワーク共有パスはサポートされていません。
- ネットワーク共有がアクセス可能なドメイン内にない場合、接続サーバ ホストからアクセス可能なドメイン内のネットワーク共有にアプリケーション パッケージをコピーします。
- 共有フォルダに対するファイルおよび共有権限によって、ビルトイン Active Directory グループ ドメイン コンピュータに読み取りアクセス権が与えられていることを確認します。ThinApp をドメイン コントローラに割り当てる予定がある場合は、ファイルおよび共有権限によって、ビルトイン Active Directory グループ ドメイン コントローラにも読み取りアクセス権が与えられていることを確認します。権限を設定または変更すると、ネットワーク共有がアクセスできるようになるまで最大 20 分かかることがあります。

ThinApp アプリケーションを Horizon Administrator に追加できない

Horizon Administrator が ThinApp アプリケーションを Horizon Administrator に追加できません。

問題

Horizon Administrator で [新しい ThinApp をスキャン] をクリックしたときに、MSI パッケージが使用できません。

原因

アプリケーション パッケージが MSI 形式でないか、接続サーバ ホストがネットワーク共有内のディレクトリにアクセスできないかのどちらかです。

解決方法

- アプリケーション リポジトリ内のアプリケーション パッケージが MSI 形式であることを確認します。
- ネットワーク共有が、ThinApp アプリケーションの Horizon 7 要件を満たしていることを確認します。詳細については、「ThinApp アプリケーションに対する Horizon 7 の要件」を参照してください。
- ネットワーク共有内のディレクトリが正しい権限を持つことを確認します。詳細については、「アプリケーション リポジトリを登録できない」を参照してください。

アプリケーション リポジトリのスキャン時に、接続サーバ デバッグ ログ ファイルにメッセージが表示されます。接続サーバ ログ ファイルは接続サーバ ホストの `<drive>:\Documents and Settings\All Users\Application Data\VMware\VDM\logs` ディレクトリにあります。

ThinApp テンプレートを割り当てることができない

ThinApp テンプレートをマシンまたはデスクトップ プールに割り当てることができません。

問題

ThinApp テンプレートをマシンまたはデスクトップ プールに割り当てようとすると、Horizon Administrator が割り当てエラーを返します。

原因

マシンまたはデスクトップ プールにすでに割り当てられているアプリケーションが ThinApp テンプレートに含まれているか、または以前に別のインストール タイプを使用して ThinApp テンプレートがマシンまたはデスクトップ プールに割り当てられています。

解決方法

マシンまたはデスクトップ プールにすでに割り当てられている ThinApp アプリケーションがテンプレートに含まれている場合は、そのアプリケーションが含まれていない新しいテンプレートを作成するか、または既存のテンプレートを編集してそのアプリケーションを削除します。新しいテンプレートまたは変更されたテンプレートをマシンまたはデスクトップ プールに割り当てます。

ThinApp アプリケーションのインストール タイプを変更するには、既存のアプリケーションの割り当てをマシンまたはデスクトップ プールから削除する必要があります。ThinApp アプリケーションがアンインストールされた後、別のインストール タイプを使用してそのアプリケーションをマシンまたはデスクトップ プールに割り当てることができます。

ThinApp アプリケーションがインストールされない

Horizon Administrator が ThinApp アプリケーションをインストールできません。

問題

ThinApp アプリケーションのインストール ステータスに、Pending Install（インストールの保留中） または Install Error（インストール エラー） が表示されます。

原因

この問題の一般的な原因には次のようなものがあります。

- マシン上に、ThinApp アプリケーションをインストールするための十分なディスク領域がなかった。
- 接続サーバ ホストとマシン間または接続サーバ ホストとアプリケーション リポジトリ間のネットワーク接続が切断されている。
- ネットワーク共有内で ThinApp アプリケーションにアクセスできなかった。
- ThinApp アプリケーションが以前にインストールされたか、ディレクトリまたはファイルがすでにマシン上に存在する。

問題の原因に関する詳細は、Horizon Agent と接続サーバのログ ファイルで参照できます。

Horizon Agent ログ ファイルは、マシンの `<drive>:\ProgramData\VMware\VDM\logs` にあります。

接続サーバ ログ ファイルは接続サーバ ホストの `<drive>:\Documents and Settings\All Users\Application Data\VMware\VDM\logs` ディレクトリにあります。

解決方法

1 Horizon Administrator で、[カタログ] - [ThinApps] の順に選択します。

2 ThinApp アプリケーションの名前をクリックします。

3 [マシン] タブで、マシンを選択し、[インストールを再試行] をクリックして ThinApp アプリケーションを再インストールします。

ThinApp アプリケーションがアンインストールされない

Horizon Administrator が ThinApp アプリケーションをアンインストールできません。

問題

ThinApp アプリケーションのインストール ステータスに、Uninstall Error（アンインストール エラー） と表示されます。

原因

このエラーの一般的な原因には次のようなものがあります。

- Horizon Administrator がアンインストールしようとしたときに、ThinApp アプリケーションがビジー状態だった。
- 接続サーバ ホストとマシン間のネットワーク接続が切断されている。

問題の原因に関する詳細は、Horizon Agent と接続サーバのログ ファイルで参照できます。

Horizon Agent ログ ファイルは、マシンの `<drive>:\Documents and Settings\All Users\Application Data\VMware\VDM\logs`（Windows XP システムの場合）または `<drive>:\ProgramData\VMware\VDM\logs`（Windows 7 システムの場合）にあります。

接続サーバ ログ ファイルは接続サーバ ホストの `<drive>:\Documents and Settings\All Users\Application Data\VMware\VDM\logs` ディレクトリにあります。

解決方法

1 Horizon Administrator で、[カタログ] - [ThinApps] の順に選択します。

2 ThinApp アプリケーションの名前をクリックします。

3 [マシン] タブをクリックし、マシンを選択し、[インストールを再試行] をクリックしてアンインストール操作を再試行します。

4 アンインストール操作が依然として失敗する場合は、ThinApp アプリケーションをマシンから手動で削除し、[デスクトップのアプリ ステータスを削除] をクリックします。

このコマンドによって、Horizon Administrator での ThinApp アプリケーション割り当てが解除されます。マシン内のファイルや設定は削除されません。

重要　このコマンドは、ThinApp アプリケーションをマシンから手動で削除した後にのみ使用してください。

MSI パッケージが無効

Horizon Administrator が、アプリケーション リポジトリ内の無効な MSI パッケージを報告します。

問題

Horizon Administrator が、スキャン処理中に MSI パッケージが無効であることを報告します。

原因

この問題の一般的な原因には次のようなものがあります。

- MSI ファイルが破損している。
- MSI ファイルが ThinApp によって作成されていない。
- MSI ファイルがサポートされていないバージョンの ThinApp で作成または再パッケージ化されている。ThinApp バージョン 4.6 以降を使用する必要があります。

解決方法

MSI パッケージに関する問題のトラブルシューティングについては、『ThinApp ユーザーズ ガイド』を参照してください。

ThinApp 構成例

ThinApp 構成例では、アプリケーションのキャプチャとパッケージ化から、インストールのステータスの確認までの標準的な ThinApp 構成を順に実行します。

開始する前に

この例にある手順の実行方法の詳細については、次のトピックを参照してください。

- 「アプリケーション パッケージのキャプチャと格納」
- 「マシンまたはデスクトップ プールへの ThinApp アプリケーションの割り当て」

手順

1 http://www.vmware.com/products/thinapp から ThinApp ソフトウェアをダウンロードし、それをクリーンなコンピュータにインストールします。

Horizon 7 は ThinApp バージョン 4.6 以降をサポートしています。

2 ThinApp **[セットアップ キャプチャ]** ウィザードを使用して、アプリケーションをキャプチャし、MSI 形式でパッケージ化します。

3 接続サーバ ホストとリモート デスクトップの両方にアクセス可能な Active Directory ドメイン内のコンピュータ上に共有フォルダを作成し、その共有フォルダに対するファイルおよび共有権限を構成して、ビルトイン Active Directory グループ ドメイン コンピュータに読み取りアクセス権を与えます。

ThinApp アプリケーションをドメイン コントローラに割り当てる予定がある場合は、ビルトイン Active Directory グループ ドメイン コントローラにも読み取りアクセス権を与えます。

4 MSI パッケージを共有フォルダにコピーします。

5 Horizon Administrator で、共有フォルダをアプリケーション リポジトリとして登録します。

6 Horizon Administrator で、アプリケーション リポジトリ内の MSI パッケージをスキャンし、選択した ThinApp アプリケーションを Horizon Administrator に追加します。

7 ThinApp アプリケーションをマシンまたはデスクトップ プールに割り当てるかどうかを決定します。

マシンに共通する命名規則を使用すると、マシン割り当てを使用して、その命名規則を使用するすべてのマシンにアプリケーションを素早く配布することができます。デスクトップ プールを部門またはユーザーの種類ごとに構成すると、デスクトップ プール割り当てを使用して、特定の部門またはユーザーにアプリケーションを素早く配布することができます。

8 Horizon Administrator で、マシンまたはデスクトップ プールに割り当てる ThinApp アプリケーションを選択し、インストール方法を指定します。

オプション	アクション
ストリーミング	マシンにアプリケーションへのショートカットをインストールします。このショートカットは、リポジトリをホストするネットワーク共有上のアプリケーションを参照します。アプリケーションを実行するには、ユーザーがそのネットワーク共有にアクセスできる必要があります。
フル	マシンのローカル ファイル システムにアプリケーション全体をインストールします。

9 Horizon Administrator で、ThinApp アプリケーションのインストール ステータスを確認します。

キオスク モードのクライアントの設定 10

Horizon 7 からクライアントのデスクトップへのアクセス権を取得できる無人クライアントを設定できます。

キオスク モードのクライアントは、Horizon Client を実行して接続サーバ インスタンスに接続し、セッションを起動するシン クライアントまたはロックダウン PC です。エンド ユーザーは通常、ログインしなくてもクライアント デバイスにアクセスできますが、公開デスクトップの一部のアプリケーションではエンド ユーザーに認証情報の入力を要求する場合があります。利用例には、医療データ入力ワークステーション、空港のチェックイン ステーション、顧客によるセルフサービス ポイント、公共の情報端末などがあります。

安全なトランザクションのための認証メカニズムをデスクトップ アプリケーションで実装し、物理ネットワークを改ざんや傍受から保護し、信頼されたデバイスのみがネットワークに接続するようにする必要があります。

キオスク モードのクライアントは、リモート セッションへの USB デバイス自動リダイレクトやロケーションベースの印刷など、リモート アクセスのための標準機能をサポートします。

Horizon 7 では、Horizon 7 4.5 以降のフレキシブル認証機能を使用して、エンド ユーザーではなくキオスク モードのクライアント デバイスを認証します。MAC アドレスによって、または文字列「custom-」もしくは ADAM で定義した別のプリフィックス文字列で始まるユーザー名によって身元を識別するクライアントを認証するように接続サーバ インスタンスを構成できます。自動生成パスワードが付与されるようにクライアントを構成する場合は、デバイス上でパスワードを指定しなくても Horizon Client を実行できます。明示的パスワードを構成する場合は、このパスワードを Horizon Client に対して指定する必要があります。Horizon Client は通常はスクリプトから実行し、パスワードはスクリプトに平文で記述されるため、権限のないユーザーがスクリプトの内容を読めないようにする対策を講じる必要があります。

文字列「cm-」で始まり MAC アドレスが続くアカウント名、または、文字列「custom-」もしくは定義した別の文字列で始まるアカウント名を使った接続を受け付けることができるのは、キオスク モードのクライアントを認証できるように構成された接続サーバ インスタンスだけです。Horizon 7 4.5 以降の Horizon Client では、これらの形式のユーザー名を手動で入力することはできません。

ベスト プラクティスとして、専用の接続サーバ インスタンスを使用してキオスク モードのクライアントを処理し、Active Directory 内にこれらのクライアントのアカウントのための専用の組織単位とグループを作成してください。この方法により、これらのシステムが不正な侵入から保護されるだけでなく、クライアントの構成および管理が容易になります。

キオスク モードのクライアントの構成

キオスク モードのクライアントをサポートするように Active Directory および Horizon 7 を構成するには、いくつかのタスクを順に実行する必要があります。

開始する前に

構成タスクを実行するために必要な権限があることを確認します。

- Domain Admins または Account Operators の認証情報。ドメイン内のユーザーおよびグループのアカウントに変更を加えるための Active Directory の認証情報です。
- **管理者**、**インベントリ管理者**、またはこれらと同等のロール。Horizon Administrator を使用して、リモート デスクトップを使用する資格をユーザーまたはグループに付与するために必要です。
- **管理者**または同等のロール。`vdmadmin` コマンドを実行するために必要です。

手順

1 キオスク モードのクライアントのための Active Directory および Horizon 7 の準備

クライアント デバイスを認証するために作成するアカウントを受け入れるように Active Directory を構成する必要があります。グループを作成するときは常に、クライアントがアクセスするデスクトップ プールに対する資格をそのグループに付与する必要もあります。クライアントが使用するデスクトップ プールを準備することもできます。

2 キオスク モードのクライアントに対するデフォルト値の設定

`vdmadmin` コマンドを使用して、キオスク モードのクライアントに対する組織単位、パスワード有効期限、および Active Directory グループ メンバーシップのデフォルト値を設定できます。

3 クライアント デバイスの MAC アドレスの表示

クライアントに対してその MAC アドレスに基づいたアカウントを作成する場合は、Horizon Client を使用して、クライアント デバイスの MAC アドレスを調べることができます。

4 キオスク モードのクライアント用アカウントの追加

`vdmadmin` コマンドを使用して、接続サーバ グループの構成にクライアントのアカウントを追加できます。クライアントを追加すると、クライアントの認証を有効にした接続サーバ インスタンスでそのクライアントを使用できるようになります。クライアントの構成を更新したり、クライアントのアカウントをシステムから削除することもできます。

5 キオスク モードのクライアントの認証の有効化

`vdmadmin` コマンドを使用して、接続サーバ インスタンス経由でクライアントのリモート デスクトップに接続しようとするクライアントの認証を有効にすることができます。

6 キオスク モードのクライアントの構成の確認

`vdmadmin` コマンドを使用すると、キオスク モードのクライアントや、そのようなクライアントを認証するように構成されている接続サーバ インスタンスについての情報を表示できます。

7 キオスク モードのクライアントからリモート デスクトップへの接続

コマンド ラインからクライアントを実行するか、またはスクリプトを使用して、クライアントをリモート セッションに接続することができます。

キオスク モードのクライアントのための Active Directory および Horizon 7 の準備

クライアント デバイスを認証するために作成するアカウントを受け入れるように Active Directory を構成する必要があります。グループを作成するときは常に、クライアントがアクセスするデスクトップ プールに対する資格をそのグループに付与する必要もあります。クライアントが使用するデスクトップ プールを準備することもできます。

ベスト プラクティスとして、キオスク モードのクライアントの管理作業を最小限に抑えるために、そのようなクライアント用の独立した組織単位とグループを作成することをお勧めします。どのグループにも属さないクライアントのために個別のアカウントを追加できますが、この方法では、構成するクライアントの数が多くなってくると管理面のオーバーヘッドが大きくなります。

手順

1 Active Directory で、キオスク モードのクライアントのために使用する独立した組織単位およびグループを作成します。

グループには Windows 2000 以前の形式の名前を指定する必要があります。この名前は、`vdmadmin` コマンドでグループを識別するために使用します。

2 ゲスト仮想マシンのイメージまたはテンプレートを作成します。

vCenter Server によって管理される仮想マシンを自動プールのテンプレート、リンク クローン プールの親、または手動デスクトップ プールの仮想マシンとして使用できます。ゲスト OS にアプリケーションをインストールして構成することもできます。

3 無人状態が続いたときにクライアントがロックされないようにゲスト OS を構成します。

キオスク モードで接続するクライアントのログイン前メッセージは Horizon 7 により表示されません。画面のロックを解除して、メッセージを表示するイベントが必要な場合は、ゲスト OS で適切なアプリケーションを構成できます。

4 Horizon Administrator で、クライアントが使用するデスクトップ プールを作成し、このプールに対する資格をグループに付与します。

たとえば、クライアント アプリケーションの要件に最も適したプールとして、フローティング割り当てのリンク クローン デスクトップ プールを作成することができます。1 つ以上の ThinApp アプリケーションをデスクトップ プールと関連付けることもできます。

重要　1 つのクライアントまたはグループに、2 つ以上のデスクトップ プールに対する資格を付与しないでください。そのようにすると、Horizon 7 はクライアントが資格のあるプールの中からランダムにリモート デスクトップを割り当てて、警告イベントを発生させます。

---

5 クライアントに対しロケーションベースの印刷を有効にするには、Active Directory グループ ポリシー設定 `AutoConnect Location-based Printing for VMware View` を構成します。この設定は、Microsoft グループ ポリシー オブジェクト エディタの `Computer Configuration` の下の `Software Settings` フォルダにあります。

6 最適化する必要があるその他のポリシーを構成し、クライアントのリモート デスクトップのセキュリティを設定します。

たとえば、デスクトップの起動時またはデバイスを接続したときにローカル USB デバイスをリモート デスクトップに接続するポリシーをオーバーライドします。Horizon Client for Windows のデフォルトでは、キオスク モードのクライアントに対してこれらのポリシーが有効です。

例: キオスク モードのクライアントのための Active Directory の準備

ある企業のイントラネットに MYORG というドメインがあり、この企業の組織単位の識別名が OU=myorg-ou,DC=myorg,DC=com であるとします。Active Directory で、組織単位 kiosk-ou（識別名は OU=kiosk-ou,DC=myorg,DC=com）とグループ kc-grp を作成して、キオスク モードのクライアント用にこれらを使用できます。

次に進む前に

クライアントに関するデフォルト値を設定します。

キオスク モードのクライアントに対するデフォルト値の設定

vdmadmin コマンドを使用して、キオスク モードのクライアントに対する組織単位、パスワード有効期限、および Active Directory グループ メンバーシップのデフォルト値を設定できます。

vdmadmin コマンドは、クライアントが公開デスクトップへの接続用に使用する接続サーバ インスタンスと同じグループに属するいずれかの接続サーバ インスタンスで実行する必要があります。

パスワード有効期限および Active Directory グループ メンバーシップのデフォルト値を構成すると、これらの設定は同じグループに属するすべての接続サーバ インスタンス間で共有されます。

手順

◆ クライアントに対するデフォルト値を設定します。

```
vdmadmin –Q –clientauth –setdefaults [–b< authentication_arguments>] [–ou <DN>]
[ –expirepassword | –noexpirepassword ] [–group <group_name> | –nogroup]
```

オプション	説明
–expirepassword	クライアント アカウントのパスワード有効期限に、接続サーバ グループの有効期限と同じ値を指定します。グループでパスワード有効期限が定義されていない場合、パスワードは無期限になります。
–group <group_name>	クライアント アカウントを追加するデフォルト グループの名前を指定します。グループの名前は、Active Directory の Windows 2000 以前のグループ名として指定する必要があります。
–noexpirepassword	クライアント アカウントのパスワードを無期限にすることを指定します。

オプション	説明
–nogroup	デフォルト グループの設定をクリアします。
–ou <DN>	クライアント アカウントを追加するデフォルト組織単位の識別名を指定します。 例： OU=kiosk-ou,DC=myorg,DC=com 注　このコマンドを使用して組織単位の構成を変更することはできません。

このコマンドは、接続サーバ グループ内のクライアントのデフォルト値を更新します。

例: キオスク モードのクライアントに対するデフォルト値の設定

クライアントの組織単位、パスワード有効期限、およびグループ メンバーシップのデフォルト値を設定します。

```
vdmadmin –Q –clientauth –setdefaults –ou "OU=kiosk–ou,DC=myorg,DC=com" –noexpirepassword –
group kc–grp
```

次に進む前に

MAC アドレスを認証に使用するクライアント デバイスの MAC アドレスを調べます。

クライアント デバイスの MAC アドレスの表示

クライアントに対してその MAC アドレスに基づいたアカウントを作成する場合は、Horizon Client を使用して、クライアント デバイスの MAC アドレスを調べることができます。

開始する前に

クライアントのコンソールにログインします。

手順

- MAC アドレスを表示するには、プラットフォームに応じて適切なコマンドを入力します。

オプション	アクション
Windows	**C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware–view.exe –printEnvironmentInfo** と入力します クライアントに対して構成したデフォルトの接続サーバ インスタンスが使用されます。デフォルト値を構成していない場合、クライアントから値の入力を求められます。 このコマンドはクライアント デバイスの IP アドレス、MAC アドレス、およびマシン名を表示します。
Linux	次のコマンドを入力します。 **vmware–view ––printEnvironmentInfo –s <connection_server>** クライアントがデスクトップへの接続に使用する接続サーバ インスタンスの IP アドレスまたは FQDN を指定する必要があります。 このコマンドは、クライアント デバイスの IP アドレス、MAC アドレス、マシン名、ドメイン、ログインしているユーザーの名前とドメイン、およびタイムゾーンを表示します。

次に進む前に

クライアントのアカウントを追加します。

キオスク モードのクライアント用アカウントの追加

vdmadmin コマンドを使用して、接続サーバ グループの構成にクライアントのアカウントを追加できます。クライアントを追加すると、クライアントの認証を有効にした接続サーバ インスタンスでそのクライアントを使用できるようになります。クライアントの構成を更新したり、クライアントのアカウントをシステムから削除することもできます。

vdmadmin コマンドは、クライアントが公開デスクトップへの接続用に使用する接続サーバ インスタンスと同じグループに属するいずれかの接続サーバ インスタンスで実行する必要があります。

キオスク モードのクライアントを追加すると、Horizon 7 はそのクライアントのユーザー アカウントを Active Directory に作成します。クライアントの名前を指定する場合は、「custom-」などのわかりやすいプリフィックス文字列または ADAM 内で定義した代替プリフィックス文字列で始まる 20 文字以内の名前にする必要があります。クライアントの名前を指定しない場合、Horizon 7 はクライアント デバイス用に指定した MAC アドレスから名前を生成します。たとえば、MAC アドレスが 00:10:db:ee:76:80 の場合、対応するアカウント名は cm-00_10_db_ee_76_80 になります。これらのアカウントは、クライアントの認証を有効にする接続サーバ インスタンスでのみ使用できます。

重要　同じ名前を複数のクライアント デバイスに使用しないでください。将来のリリースではこの構成がサポートされない可能性があります。

手順

- クライアントのドメインと名前または MAC アドレスを指定するには、**–domain** および **–clientid** オプションを使用して vdmadmin コマンドを実行します。

```
vdmadmin –Q –clientauth –add [–b <authentication_arguments>] –domain <domain_name>
–clientid <client_id> [–password "<password>" | –genpassword] [–ou <DN>]
[–expirepassword | –noexpirepassword] [–group <group_name> | –nogroup]
[–description "<description_text>"]
```

オプション	説明
–clientid <client_id>	クライアントの名前または MAC アドレスを指定します。
–description "<description_text>"	クライアント デバイスのアカウントの説明を Active Directory に作成します。
–domain <domain_name>	クライアントのドメインを指定します。
–expirepassword	クライアント アカウントのパスワード有効期限に、接続サーバ グループの有効期限と同じ値を指定します。グループでパスワード有効期限が定義されていない場合、パスワードは無期限になります。
–genpassword	クライアント アカウントのパスワードを生成します。これは、**–password** も **–genpassword** も指定しない場合のデフォルトの動作です。 生成されるパスワードは長さが 16 文字で、英大文字、英小文字、記号、および数字をそれぞれ 1 つ以上含み、同じ文字を繰り返し含めることができます。より強力なパスワードが必要な場合は、**–password** オプションを使用してパスワードを指定します。
–group <group_name>	クライアント アカウントを追加するグループの名前を指定します。グループの名前は、Active Directory の Windows 2000 以前のグループ名として指定する必要があります。以前にデフォルトのグループを設定した場合、クライアント アカウントはこのグループに追加されます。
–noexpirepassword	クライアント アカウントのパスワードを無期限にすることを指定します。
–nogroup	クライアント アカウントをデフォルトのグループに追加しないことを指定します。

オプション	説明
–ou <DN>	クライアント アカウントを追加する組織単位の識別名を指定します。 例： OU=kiosk-ou,DC=myorg,DC=com
–password "<password>"	クライアント アカウントの明示的パスワードを指定します。

コマンドを実行すると、クライアントの Active Directory ユーザー アカウントが、指定されたドメインおよびグループが存在する場合、その中に作成されます。

例: クライアントのアカウントの追加

MAC アドレスで指定されたクライアントのアカウントを MYORG ドメインに追加します（グループ kc-grp のデフォルト設定を使用）。

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –group kc–grp
```

MAC アドレスで指定されたクライアントのアカウントを MYORG ドメインに追加します（自動生成されたパスワードを使用）。

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –genpassword
```

クライアントの名前を指定してアカウントを追加し、そのクライアントで使用するパスワードを指定します。

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Terminal21 –password "guest" –ou
"OU=kiosk–ou,DC=myorg,DC=com" –description "Terminal 21"
```

クライアントの名前を指定してアカウントを追加します（自動生成されたパスワードを使用）。

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Kiosk11 –genpassword –ou
"OU=kiosk–ou,DC=myorg,DC=com" –description "Kiosk 11"
```

次に進む前に

クライアントの認証を有効にします。

キオスク モードのクライアントの認証の有効化

vdmadmin コマンドを使用して、接続サーバ インスタンス経由でクライアントのリモート デスクトップに接続しようとするクライアントの認証を有効にすることができます。

vdmadmin コマンドは、クライアントがリモート デスクトップへの接続用に使用する接続サーバ インスタンスと同じグループに属するいずれかの接続サーバ インスタンスで実行する必要があります。

個別の接続サーバ インスタンスに対して認証を有効にできますが、グループ内のすべての接続サーバ インスタンスがクライアント認証に関する他のすべての設定を共有します。クライアントのアカウントの追加が必要なのは 1 回だけです。接続サーバ グループ内で、認証が有効されたすべての接続サーバ インスタンスがクライアントを認証できます。

リモート デスクトップ サービス (RDS) ホスト上のセッション ベースのデスクトップでキオスク モードを使用する予定の場合、Remote Desktop User グループにユーザー アカウントを追加する必要があります。

手順

1 接続サーバ インスタンス上でクライアントの認証を有効にします。

```
vdmadmin –Q –enable [–b <authentication_arguments>] –s <connection_server>
[–requirepassword]
```

オプション	説明
–requirepassword	パスワードの入力をクライアントに要求することを指定します。 重要 このオプションを指定した場合、接続サーバ インスタンスは自動生成されたパスワードを使用するクライアントを認証できません。接続サーバ インスタンスの構成を変更してこのオプションを指定すると、そのようなクライアントは認証されず、「**不明なユーザー名または不正確なパスワード**」というエラー メッセージが表示されて認証に失敗します。
–s <connection_server>	クライアントの認証を有効にする接続サーバ インスタンスの NetBIOS 名を指定します。

コマンドを実行すると、指定した接続サーバ インスタンスによるクライアントの認証が有効になります。

2 Microsoft リモート デスクトップ サービス (RDS) ホストにより公開デスクトップが提供される場合、リモート デスクトップ サービス (RDS) ホストにログインし、Remote Desktop User グループにユーザー アカウントを追加します。

たとえば、Horizon 7 Server でユーザー アカウント **custom–11** に、リモート デスクトップ サービス (RDS) ホスト上のセッションベースのデスクトップへの資格を付与するとします。この場合、RDS ホストにログインし、[コントロール パネル] - [システムとセキュリティ] - [システム] - [リモートの設定] - [ユーザーの選択] - [追加]を順に選択して、ユーザー **custom–11** を Remote Desktop User グループに追加する必要があります。

例: キオスク モードのクライアントの認証の有効化

接続サーバ インスタンス csvr-2 に対しクライアントの認証を有効にします。自動生成されたパスワードを使用するクライアントの場合、パスワードを入力せず認証できます。

```
vdmadmin –Q –enable –s csvr–2
```

接続サーバ インスタンス csvr-3 に対しクライアントの認証を有効にして、パスワードを Horizon Client に指定するようクライアントに要求します。自動生成されたパスワードを使用するクライアントは認証されません。

```
vdmadmin –Q –enable –s csvr–3 –requirepassword
```

次に進む前に

接続サーバ インスタンスおよびクライアントの構成を確認します。

キオスク モードのクライアントの構成の確認

vdmadmin コマンドを使用すると、キオスク モードのクライアントや、そのようなクライアントを認証するように構成されている接続サーバ インスタンスについての情報を表示できます。

vdmadmin コマンドは、クライアントがリモート デスクトップへの接続用に使用する接続サーバ インスタンスと同じグループに属するいずれかの接続サーバ インスタンスで実行する必要があります。

手順

- キオスク モードのクライアントおよびクライアント認証についての情報を表示します。

  ```
  vdmadmin –Q –clientauth –list [–b<authentication_arguments>] [–xml]
  ```

  このコマンドは、キオスク モードのクライアントと、クライアント認証を有効にした接続サーバ インスタンスについての情報を表示します。

例: キオスク モードのクライアントに関する情報の表示

クライアントについての情報をテキスト形式で表示します。クライアント cm-00_0c_29_0d_a3_e6 のパスワードは自動生成されており、エンド ユーザーまたはアプリケーション スクリプトにはこのパスワードを Horizon Client に指定する必要はありません。クライアント cm-00_22_19_12_6d_cf のパスワードは明示的に指定されており、エンド ユーザーはこのパスワードを入力する必要があります。接続サーバ インスタンス CONSVR2 は、自動生成されたパスワードを使用するクライアントからの認証要求を受け付けます。CONSVR1 は、キオスク モードのクライアントからの認証要求を受け付けません。

```
C:\ vdmadmin –Q –clientauth –list
Client Authentication User List
================================
GUID               : 94be6344–0c9b–4a92–8d54–1brc1c2dc282
ClientID           : cm–00_0c_29_0d_a3_e6
Domain             : myorg.com
Password Generated: true

GUID               : 471d9d35–68b2–40ee–b693–56a7d92b2e25
ClientID           : cm–00_22_19_12_6d_cf
Domain             : myorg.com
Password Generated: false

Client Authentication Connection Servers
========================================
Common Name                    : CONSVR1
Client Authentication Enabled : false
Password Required              : false

Common Name                    : CONSVR2
Client Authentication Enabled : true
Password Required              : false
```

次に進む前に

クライアントがそのリモート デスクトップに接続できることを確認します。

キオスク モードのクライアントからリモート デスクトップへの接続

コマンド ラインからクライアントを実行するか、またはスクリプトを使用して、クライアントをリモート セッションに接続することができます。

展開先のクライアント デバイス上で Horizon Client を実行するには通常、コマンド スクリプトを使用します。

注　Windows または Mac クライアントで、リモート デスクトップ セッションの開始時にクライアント上の USB デバイスが別のアプリケーションまたはサービスで使用されている場合、デフォルトではそれらのデバイスは自動転送されません。すべてのクライアントで、ヒューマン インターフェイス デバイス (HID) およびスマート カード リーダーはデフォルトでは転送されません。

手順

◆ リモート セッションに接続するには、プラットフォームに応じて適切なコマンドを入力します。

オプション	説明
Windows	次のコマンドを入力します。 **C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended [-serverURL <connection_server>] [-userName <user_name>] [-password <password>]**
	-password <password> クライアント アカウントのパスワードを指定します。アカウントにパスワードを定義した場合は、このパスワードを指定する必要があります。
	-serverURL <connection_server> Horizon Client がそのリモート デスクトップに接続するために使用する接続サーバ インスタンスの IP アドレスまたは FQDN を指定します。クライアントがそのリモート デスクトップへの接続に使用する接続サーバ インスタンスの IP アドレスまたは FQDN を指定しない場合、クライアント用に構成したデフォルトの接続サーバ インスタンスが使用されます。
	-userName <user_name> クライアント アカウントの名前を指定します。クライアントの MAC アドレスを使用せずに、「custom-」などのわかりやすいプレフィックス文字列で始まるアカウント名を使用してクライアントを認証する場合は、この名前を指定する必要があります。
Linux	次のコマンドを入力します。 **vmware-view --unattended -s <connection_server> [--once] [-u <user_name>] [-p <password>]**
	--once エラーが発生した場合に Horizon Client が接続を再試行しないことを指定します。 重要 通常はこのオプションを指定し、終了コードを使ってエラーを処理することをお勧めします。指定しない場合、`vmware-view` プロセスをリモートから強制終了することが難しい場合があります。
	-p <password> クライアント アカウントのパスワードを指定します。アカウントにパスワードを定義した場合は、このパスワードを指定する必要があります。
	-s <connection_server> クライアントがそのデスクトップへの接続に使用する接続サーバ インスタンスの IP アドレスまたは FQDN を指定します。
	-u <user_name> クライアント アカウントの名前を指定します。クライアントの MAC アドレスを使用せずに、「custom-」などのわかりやすいプリフィックス文字列で始まるアカウント名を使用してクライアントを認証する場合は、この名前を指定する必要があります。

サーバがキオスク クライアントを認証し、リモート デスクトップが利用可能であれば、リモート セッションが開始されます。

例: キオスク モードのクライアント上での Horizon Client の実行

アカウント名がクライアントの MAC アドレスに基づいており、自動生成パスワードを使用する Windows クライアント上で Horizon Client を実行します。

```
C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended -
serverURL consvr2.myorg.com
```

割り当てられた名前およびパスワードを使用する Linux クライアント上で Horizon Client を実行します。

```
vmware-view -unattended -s 145.124.24.100 --once -u custom-Terminal21 -p "Secret1!"
```

Horizon 7 のトラブルシューティング 11

Horizon 7 の使用中に発生する可能性のある問題を診断および解決するために、さまざまな手順を使用できます。Horizon Help Desk Tool でトラブルシューティングを行ったり、他のトラブルシューティング手順で問題の調査と修復を行うことができます。また、VMware テクニカル サポートを利用することもできます。

デスクトップとデスクトップ プールのトラブルシューティングの詳細については、『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントを参照してください。

この章では次のトピックについて説明します。

Horizon Help Desk Tool の使用

Horizon Help Desk Tool は、Horizon 7 ユーザー セッションのステータスを取得し、トラブルシューティングとメンテナンス操作を行う Web アプリケーションです。

Horizon Help Desk Tool では、トラブルシューティングを行うためにユーザー セッションを確認し、デスクトップの再起動やリセットなどのデスクトップ メンテナンス操作を実行できます。

Horizon Help Desk Tool を設定するには、次の要件を満たす必要があります。

- Horizon 7 の Horizon Enterprise Edition ライセンスまたは Horizon Apps Advanced Edition ライセンス正しいライセンスがあることを確認するには、「Horizon Help Desk Tool のライセンス確認」を参照してください。

- Horizon 7 コンポーネントの情報を保存するイベント データベースイベント データベースの設定の詳細については、『Horizon 7 のインストール』 ドキュメントを参照してください。
- Horizon Help Desk Tool にログインするヘルプデスク管理者ロールまたはヘルプデスク管理者（読み取り専用）ロールこれらのロールの詳細については、「Horizon Help Desk Tool のロール ベースのアクセスの設定」を参照してください。
- ログイン セグメントを表示するには、各接続サーバ インスタンスでタイミング プロファイラを有効にします。

  各接続サーバ インスタンスでタイミング プロファイラを有効にするには、次の `vdmadmin` コマンドを使用します。

  ```
  vdmadmin -I -timingProfiler -enable
  ```

  管理ポートを使用している接続サーバインスタンスでタイミング プロファイラを有効にするには、次の `vdmadmin` コマンドを使用します。

  ```
  vdmadmin -I -timingProfiler -enable -server {ip/server}
  ```

注 Horizon Administrator で使用する場合、Horizon Help Desk Tool は、Linux デスクトップをサポートしません。Linux デスクトップ セッションで Horizon 7 ユーザー セッションのステータスを取得するには、Horizon Console で Horizon Help Desk Tool を使用してください。

Horizon Help Desk Tool のライセンス確認

有効なプロダクト ライセンス キーがない場合、Horizon Help Desk Tool にログインできません。Horizon Administrator でプロダクト ライセンス キーを確認して、有効なライセンスを適用できます。

開始する前に

- Horizon Enterprise エディション ライセンスまたは Horizon Apps Advanced エディション ライセンスに有効なプロダクト ライセンスキーを入手します。

手順

1. Horizon Administrator で、[View 構成] - [製品のライセンスと使用状況] の順に選択します。

   現在のライセンス キーの最初と最後の 5 文字は、[ライセンス] パネルに表示されます。

2. [ヘルプデスク ライセンス]フィールドで、ライセンスのステータスを確認します。

オプション	説明
無効	プロダクト ライセンス キーが無効です。Horizon Help Desk Tool にログインできません。
有効	プロダクト ライセンス キーが有効です。Horizon Help Desk Tool にログインできます。

3. (オプション) プロダクト ライセンス キーが有効でない場合には、[ライセンスを編集] をクリックして有効なライセンス シリアル番号を入力し、[OK] をクリックして、Horizon Administrator の URL を更新します。

   [製品ライセンス] ウィンドウに更新されたライセンス情報が表示されます。

次に進む前に

Horizon Help Desk Tool にログインします。

Horizon Help Desk Tool のロール ベースのアクセスの設定

Horizon Help Desk Tool 管理者に定義済みの管理者ロールを割り当て、他の管理者ユーザーにトラブルシューティング タスクを委任できます。また、カスタム ロールを作成し、定義済みの管理者ロールに基づいて権限を追加できます。

次の定義済みの管理者ロールを Horizon Help Desk Tool 管理者に割り当てることができます。

- ヘルプデスク管理者
- ヘルプデスク管理者（読み取り専用）

Horizon Help Desk Tool 管理者にカスタム ロールを作成する場合は、ヘルプデスクを管理（読み取り専用）権限の他、ヘルプデスク管理者ロールまたはヘルプデスク管理者（読み取り専用）ロールに応じて、他の権限も割り当てる必要があります。

開始する前に

カスタム ロールの作成に使用できる管理者権限について理解しておきます。「定義済みのロールと権限」を参照してください。

手順

1 Horizon Administrator で、[View 構成] - [管理者] の順に選択して、[ロール] タブをクリックします。

2 [ロール] タブで [ロールを追加] をクリックし、ヘルプデスク管理者ロールまたはヘルプデスク管理者（読み取り専用）ロールのいずれかを選択して、[OK] をクリックします。

   a (オプション) カスタム ロールを追加するには、[ロール] タブで [ロールを追加] をクリックし、ヘルプデスクを管理（読み取り専用）権限を選択します。ヘルプデスク管理者ロールまたはヘルプデスク管理者（読み取り専用）ロールのいずれかに基づいて権限を選択して、[OK] をクリックします。

Horizon Help Desk Tool へのログイン

Horizon Help Desk Tool は、Horizon Console に統合されています。Horizon 7 バージョン 7.5 以降では、Horizon Help Desk Tool URL を使用して Horizon Help Desk Tool にログインできません。

手順

1 Horizon Administrator から Horizon Help Desk Tool にログインするには、右上のパネルで [Horizon Console] をクリックします。これは、Horizon ConsoleWeb インターフェイスへのシングル サインオンです。

2 Horizon Console で、ユーザーの検索フィールドにユーザー名を入力します。

   Horizon Console では、検索結果にユーザーのリストが表示されます。最大で 100 個までの検索結果が返されます。

3 ユーザー名を選択します。

   ユーザー カードにユーザー情報が表示されます。

次に進む前に

問題のトラブルシューティングを行うには、ユーザー カードで関連するタブをクリックします。

Horizon Help Desk Tool でのユーザーのトラブルシューティング

Horizon Help Desk Tool のユーザー カードを使用すると、ユーザーの基本情報を確認できます。ユーザー カードのタブをクリックすると、特定のコンポーネントの詳細が表示されます。

ユーザーの詳細が表に表示されることがあります。これらのユーザーの詳細は、表の列を使って並べ替えることができます。

- 列を昇順で並べ替えるには、列を 1 回クリックします。
- 列を降順で並べ替えるには、列を 2 回クリックします。
- 列を並べ替えない場合は、列を 3 回クリックします。

ユーザーの基本情報

ユーザーのユーザー名、電話番号、メール アドレス、ユーザーの接続状態などのユーザーの基本情報が表示されます。ユーザーにデスクトップまたはアプリケーション セッションがある場合、ユーザーは接続状態になります。ユーザーにデスクトップまたはアプリケーション セッションがない場合、ユーザーは切断状態になります。

電話番号をクリックすると、Skype for Business セッションが開きます。ユーザーとともにトラブルシューティングを行うことができます。

メール アドレスをクリックすると、ユーザーにメッセージを送信できます。

セッション

[セッション] タブには、ユーザーが接続しているデスクトップまたはアプリケーションの情報が表示されます。

[フィルタ] テキスト ボックスを使用すると、デスクトップまたはアプリケーション セッションをフィルタリングできます。

注 [セッション] タブには、Microsoft RDP 表示プロトコルを使用するセッションや、vSphere Client または ESXi からの仮想マシンにアクセスするセッションの情報は表示されません。

[セッション] タブには、次の情報が表示されます。

表 11-1. [セッション] タブ

オプション	説明
状態	デスクトップまたはアプリケーション セッションの状態が表示されます。 ■ セッションが接続されている場合、緑色が表示されます。 ■ セッションがローカル セッションか、ローカルのポッドで実行されているセッションの場合、L が表示されます。 ■ ポッド フェデレーション内の別のポッドでセッションが実行されている場合、G が表示されます。
コンピュータ名	デスクトップまたはアプリケーション セッションの名前。名前をクリックすると、カードにセッション情報が表示されます。 セッション カードでタブをクリックすると、次の追加情報が表示されます。 ■ [詳細] タブには、仮想マシン、CPU またはメモリ使用量などのユーザー情報が表示されます。「Horizon Help Desk Tool のセッションの詳細」を参照してください。 ■ [プロセス] タブには、CPU およびメモリ関連のプロセスに関する情報が表示されます。「Horizon Help Desk Tool のセッション プロセス」を参照してください。 ■ [アプリケーション] タブには、実行中のアプリケーションの詳細が表示されます。「Horizon Help Desk Tool のアプリケーション ステータス」を参照してください。
プロトコル	デスクトップまたはアプリケーション セッションの表示プロトコル。
Type	デスクトップの種類（公開デスクトップ、仮想マシン デスクトップまたはアプリケーション）が表示されます。
接続時間	セッションが接続サーバに接続した時間。
セッションの期間	セッションが接続サーバに接続していた期間。

デスクトップに対する資格

[デスクトップに対する資格] タブには、ユーザーに使用資格が付与されている公開デスクトップまたは仮想デスクトップの情報が表示されます。

表 11-2. デスクトップに対する資格

オプション	説明
状態	デスクトップ セッションの状態が表示されます。 ■ セッションが接続されている場合、緑色が表示されます。
デスクトップ プール名	セッションのデスクトップ プールの名前。
デスクトップ タイプ	デスクトップの種類（公開デスクトップまたは仮想マシン デスクトップ）が表示されます。 注 セッションでポッド フェデレーションの別のポッド実行されている場合、情報は表示されません。
Type	デスクトップの資格のタイプが表示されます。 ■ ローカル資格の場合には、Local が表示されます。 ■ グローバル資格の場合には、Global が表示されます。

表 11-2. デスクトップに対する資格 (続き)

オプション	説明
vCenter	vCenter Server の仮想マシンの名前が表示されます。 注 セッションでポッド フェデレーションの別のポッド実行されている場合、情報は表示されません。
デフォルトのプロトコル	デスクトップまたはアプリケーション セッションのデフォルトの表示プロトコル。

アプリケーションに対する資格

[アプリケーションに対する資格] タブには、ユーザーに使用資格が付与されている公開アプリケーションの情報が表示されます。

表 11-3. アプリケーションに対する資格

オプション	説明
状態	アプリケーション セッションの状態が表示されます。 ■ セッションが接続されている場合、緑色が表示されます。
アプリケーション	アプリケーション プールの公開アプリケーションの名前が表示されます。
ファーム	セッションが接続している RDS ホストを含むファームの名前。 注 グローバル アプリケーション資格の場合、この列にはグローバル アプリケーション資格のファーム数が表示されます。
Type	アプリケーションに対する資格のタイプが表示されます。 ■ ローカル資格の場合には、Local が表示されます。 ■ グローバル資格の場合には、Global が表示されます。
パブリッシャ	公開アプリケーションのソフトウェア メーカー名。

アクティビティ

[アクティビティ] タブには、ユーザーのアクティビティに関するイベント ログ情報が表示されます。過去 12 時間、過去 30 日間などの期間や管理者の名前でアクティビティをフィルタリングできます。[ヘルプデスク イベントのみ] をクリックすると、Horizon Help Desk Tool アクティビティでのみフィルタリングできます。[更新] アイコンをクリックして、イベント ログを更新します。[エクスポート] アイコンをクリックして、イベント ログをファイルにエクスポートします。

注 CPA 環境のユーザーのイベント ログ情報は表示されません。

表 11-4. アクティビティ

オプション	説明
[時間]	時間範囲を選択します。デフォルトは、過去 12 時間です。 ■ [過去 12 時間] ■ [過去 24 時間] ■ [過去 7 日間] ■ [過去 30 日間] ■ [すべて]
[管理者]	管理者ユーザーの名前。
[メッセージ]	ユーザーまたは管理者が実行したアクティビティに固有のユーザーまたは管理者のメッセージが表示されます。
[リソース名]	アクティビティの実行対象のデスクトップ プールまたは仮想マシン名に関する情報が表示されます。

Horizon Help Desk Tool のセッションの詳細

[セッション] タブで [コンピュータ名] オプションのユーザー名をクリックすると、セッション ユーザーの詳細が [詳細] タブに表示されます。Horizon Client、仮想または公開デスクトップ、CPU とメモリの詳細を確認できます。

Horizon Client

Horizon Client のタイプに応じて情報が表示されます。ユーザー名、Horizon Client のバージョン、クライアント マシンの IP アドレス、クライアント マシンのオペレーティング システムなどの詳細が表示されます。

注　Horizon Agent をアップグレードした場合、Horizon Client も最新バージョンにアップグレードする必要があります。それ以外の場合、Horizon Client のバージョンは表示されません。Horizon Client のアップグレードの詳細については、『Horizon 7 のアップグレード』ドキュメントを参照してください。

仮想マシン

仮想デスクトップまたは公開デスクトップに関する情報が表示されます。

表 11-5. 仮想マシンの詳細

オプション	説明
[コンピュータ名]	デスクトップまたはアプリケーション セッションの名前。
[エージェント バージョン]	Horizon Agent のバージョン。
[セッション状態]	デスクトップまたはアプリケーション セッションの状態。
[状態の継続期間]	セッションが同じ状態を継続した時間。
[ログイン時間]	セッションにログインしたユーザーのログイン時間。
[ログインの継続期間]	ユーザーがセッションにログインしていた期間。
[セッションの期間]	セッションが接続サーバと接続していた期間。
[接続サーバ]	セッションが接続している接続サーバ。

表 11-5. 仮想マシンの詳細 (続き)

オプション	説明
[Unified Access Gateway の名前]	Unified Access Gateway アプライアンスの名前。この情報の表示には、セッション接続後、30 ～ 60 秒ほどかかる場合があります。
[Unified Access Gateway の IP アドレス]	Unified Access Gateway アプライアンスの IP アドレス。この情報の表示には、セッション接続後、30 ～ 60 秒ほどかかる場合があります。
[プール]	デスクトップまたはアプリケーション プールの名前。
[ファーム]	公開デスクトップまたはアプリケーション セッションの RDS ホストのファーム。
[vCenter Server]	vCenter Server の IP アドレス。

BLAST メトリックを表示する

VMware Blast 表示プロトコルを使用する仮想または公開デスクトップ セッションのパフォーマンスの詳細が表示されます。これらのパフォーマンスの詳細を表示するには、[BLAST メトリックを表示する] をクリックします。

表 11-6. Blast 表示プロトコルの詳細

オプション	説明
[Blast セッション カウンタ]	■ [推定バンド幅（アップリンク)]。アップリンク シグナルの推定バンド幅。 ■ [パケット損失（アップリンク)]。アップリンク シグナルのパケット損失率。
[Blast イメージング カウンタ]	■ [送信バイト]。Blast セッションで転送されたイメージング データの合計バイト数。 ■ [受信バイト]。Blast セッションで受信したイメージング データの合計バイト数。
[Blast オーディオ カウンタ]	■ [送信バイト]。Blast セッションで転送されたオーディオ データの合計バイト数。 ■ [受信バイト]。Blast セッションで受信したオーディオ データの合計バイト数。
[Blast CDR カウンタ]	■ [送信バイト]。Blast セッションで転送されたクライアント ドライブ リダイレクトの合計バイト数。 ■ [受信バイト]。Blast セッションで受信したクライアント ドライブ リダイレクトの合計バイト数。

CPU、メモリ、遅延

仮想/公開デスクトップまたはアプリケーションの CPU とメモリの使用量や、PCoIP または Blast 表示プロトコルの遅延がグラフで表示されます。

表 11-7. CPU、メモリ、遅延の詳細

オプション	説明
[セッションの CPU]	現在のセッションの CPU 使用率。
[ホストの CPU]	セッションが割り当てられている仮想マシンの CPU 使用率。
[セッションのメモリ]	現在のセッションのメモリ使用量。

表 11-7. CPU、メモリ、遅延の詳細 (続き)

オプション	説明
[ホストのメモリ]	セッションが割り当てられている仮想マシンのメモリ使用量。
[セッションの遅延]	PCoIP または Blast 表示プロトコルの遅延がグラフで表示されます。 Blast 表示プロトコルの場合、遅延時間はラウンドトリップ時間（ミリ秒単位）です。この遅延時間を追跡するパフォーマンス カウンタは、[VMware Blast セッション カウンタ] - [RTT] です。 PCoIP 表示プロトコルの場合、遅延時間はラウンドトリップ遅延時間（ミリ秒単位）です。この遅延時間を追跡するパフォーマンス カウンタは、[PCoIP セッション ネットワーク統計情報] - [ラウンド トリップ遅延時間] です。

セッション ログイン セグメント

ログインの継続時間とログイン時に作成されたセグメントが表示されます。

表 11-8. セッション ログイン セグメント

オプション	説明
[ログインの継続期間]	ユーザーがデスクトップまたはアプリケーション プールをクリックしてから Windows エクスプローラが起動するまでの時間。
[セッション ログイン時間]	ユーザーがセッションにログインしていた期間。
ログイン セグメント	ログイン時に作成されたセグメントが表示されます。 ■ [仲介]。接続サーバがセッションの接続または再接続を処理する時間の合計。ユーザーがデスクトップ プールをクリックしてからトンネル接続が確立するまでの時間で計算されます。ユーザー認証、マシンの選択、トンネル接続を確立に必要なマシンの準備など、接続サーバのタスクの所要時間が含まれます。 ■ [GPO のロード]Windows グループ ポリシーの処理時間の合計。グローバル ポリシーが設定されていない場合、0 が表示されます。 ■ [プロファイルのロード]Windows ユーザー プロファイルの処理時間の合計。 ■ [インタラクティブ]。Horizon Agent がセッションの接続または再接続を処理する時間の合計。PCoIP または Blast Extreme がトンネル接続を使用してから Windows エクスプローラが起動するまでの時間で計算されます。 ■ [認証]。接続サーバがセッションの認証にかかった合計時間。 ■ [仮想マシンの開始]。仮想マシンの起動にかかった合計時間。この時間には、オペレーティング システムの起動、サスペンド状態のマシンの再開、Horizon Agent が接続準備完了通知の送信にかかる時間が含まれます。

トラブルシューティングでログイン セグメントの情報を使用する場合には、次のガイドラインに従ってください。

- セッションが新しい仮想デスクトップ セッションの場合、すべてのログイン セグメントが表示されます。グローバル ポリシーが設定されていない場合、[GPO ロード] のログイン セグメントの時間は 0 になります。
- 切断されたセッションから仮想デスクトップ セッションが再接続された場合には、[ログインの継続期間]、[インタラクティブ]、[仲介] のログイン セグメントが表示されます。

- セッションが公開デスクトップ セッションの場合には、[ログインの継続期間]、[GPO ロード]、[プロファイルのロード] のログイン セグメントが表示されます。新しいセッションの場合には、[GPO ロード] と [プロファイルのロード] のログイン セグメントが表示されます。これらのログイン セグメントが新しいセッションで表示されない場合には、RDS ホストを再起動する必要があります。

Horizon Help Desk Tool のセッション プロセス

[セッション] タブで [コンピュータ名] オプションのユーザー名をクリックすると、セッション プロセスが [プロセス] タブに表示されます。

プロセス

セッションごとに、CPU やメモリ関連プロセスの詳細情報を表示できます。たとえば、セッションの CPU やメモリ使用率が異常に高い場合、[プロセス] タブでプロセスの詳細を確認できます。

表 11-9. セッション プロセスの詳細

オプション	説明
プロセス名	セッション プロセスの名前。たとえば、chrome.exe。
CPU	プロセスの CPU 使用率 (%)。
メモリ	プロセスのメモリ使用量 (KB)。
ディスク	メモリのディスク IOPS。次の式で計算されます。 (現在の時刻の I/O バイト数の合計) - (現在時刻より 1 秒前の I/O バイト数の合計)。 タスク マネージャに正の値が表示されている場合、この計算結果は 1 秒あたり 0 KB と表示されます。
ユーザー名	プロセスを所有するユーザーの名前。
ホストの CPU	セッションが割り当てられている仮想マシンの CPU 使用率。
ホストのメモリ	セッションが割り当てられている仮想マシンのメモリ使用量。
プロセス	仮想マシン内のプロセス数
更新	更新アイコンをクリックすると、プロセスのリストが更新されます。
プロセスの終了	実行中のプロセスを終了します。 注　プロセスを終了するには、ヘルプデスク管理者ロールが必要です。 プロセスを終了するには、プロセスを選択して [プロセスの終了] ボタンをクリックします。

Horizon Help Desk Tool のアプリケーション ステータス

[セッション] タブの [コンピュータ名] オプションでユーザー名をクリックすると、[アプリケーション] タブでアプリケーションのステータスと詳細を確認できます。

アプリケーション

アプリケーションごとに、現在のステータスとその他の詳細を表示できます。

表 11-10. アプリケーションの詳細

オプション	説明
アプリケーション	アプリケーションの名前。
説明	アプリケーションの説明。
ステータス	アプリケーションのステータス。アプリケーションが実行中かどうかが表示されます。
ホストの CPU	セッションが割り当てられている仮想マシンの CPU 使用率。
ホストのメモリ	セッションが割り当てられている仮想マシンのメモリ使用量。
アプリケーション	実行されているアプリケーションのリスト。
更新	更新アイコンをクリックすると、アプリケーションのリストが更新されます。

Horizon Help Desk Tool でのデスクトップまたはアプリケーション セッションのトラブルシューティング

Horizon Help Desk Tool では、ユーザーの接続状態に基づいて、デスクトップまたはアプリケーション セッションのトラブルシューティングを行うことができます。

開始する前に

- Horizon Help Desk Tool を開始します。

手順

1 ユーザー カードで、[セッション] タブをクリックします。

パフォーマンス カードに CPU とメモリの使用量と、Horizon Client、仮想デスクトップ、公開デスクトップに関する情報が表示されます。

2 トラブルシューティングのオプションを選択します。

オプション	アクション
[メッセージを送信]	公開デスクトップまたは仮想デスクトップのユーザーにメッセージを送信します。警告、情報、エラーなどのメッセージの重要度を選択します。 [メッセージの送信] をクリックし、重要度とメッセージの詳細を入力して、[送信] をクリックします。
[リモート アシスタンス]	接続されているデスクトップまたはアプリケーション セッションのリモート アシスタント チケットを生成できます。管理者は、リモート アシスタンス チケットを使用してユーザーのデスクトップを操作し、トラブルシューティングを行うことができます。 [リモート アシスタンス] をクリックして、ヘルプ デスク チケット ファイルをダウンロードします。チケットを開きます。リモート デスクトップでユーザーがチケットを承認するまで待機します。チケットは、Windows デスクトップでのみ開くことができます。ユーザーがチケットを承認すると、ユーザーとチャットを行い、ユーザーのデスクトップの操作を要求できます。 注 ヘルプ デスクのリモート アシスタンス機能は Microsoft Remote Assistance をベースにしています。公開デスクトップに Microsoft Remote Assistance をインストールし、リモート アシスタンス機能を有効にする必要があります。Microsoft Remote Assistance で接続またはアップグレードの問題が発生すると、ヘルプ デスクのリモート アシスタンスが開始しない場合があります。詳細については、Microsoft の Web サイトで Microsoft Remote Assistance のドキュメントを参照してください。
[再起動]	仮想デスクトップで Windows の再起動プロセスを開始します。この機能は、公開デスクトップまたはアプリケーション セッションで使用できません。 [VDI の再起動] をクリックします。
[切断]	デスクトップまたはアプリケーション セッションを切断します。 [詳細] - [切断] の順にクリックします。
[ログオフ]	公開デスクトップまたは仮想デスクトップでログオフ プロセスを開始します。あるいは、アプリケーション セッションでログオフ プロセスを開始します。 [詳細] - [ログオフ] の順にクリックします。
[リセット]	仮想マシンのリセットを開始します。この機能は、公開デスクトップまたはアプリケーション セッションで使用できません。 [詳細] - [仮想マシンのリセット] の順にクリックします。 注 保存していない作業は失われます。

VMware Logon Monitor の使用

VMware Logon Monitor は、Windows ユーザーのログインを監視し、パフォーマンス メトリックを提供します。これにより、管理者、サポート スタッフ、開発者はログイン パフォーマンスの問題を解決することができます。

メトリックには、ログイン時間、ログイン スクリプト時間、CPU やメモリの使用量、ネットワーク接続速度などがあります。Logon Monitor は、他の VMware 製品からメトリックを受け取り、ログイン プロセスに関する詳細情報を提供します。

サポートされているプラットフォーム

Logon Monitor は、Horizon Agent と同じ Windows プラットフォームをサポートします。

主な特長

Logon Monitor の特長は次のとおりです。

- Horizon Agent の一部としてインストールされ、デフォルトで有効になっています。
- Horizon Help Desk Tool タイミング プロファイラと連携します。ログイン関連のメトリックを集計し、Horizon Agent イベント データベースに送信します。
- ユーザーが簡単にアクセスできるように、ログをファイル サーバにアップロードできます。
- Horizon Persona Management、App Volumes、UEM、Horizon Agent など、他の VMware 製品と連携します。これらの製品がログイン関連のイベントを Logon Monitor に送信します。イベントが発生すると、Logon Monitor がイベントをログに記録し、ログイン フローのイベントとその期間を表示します。
- 同じマシンでの同時ログインを監視します。

ログ

Logon Monitor は、サービス ステータス メッセージとユーザー セッションのログ ファイルを書き込みます。デフォルトでは、ログ ファイルはすべて `C:\ProgramData\VMware\VMware Logon Monitor\Logs` に書き込まれます。

- メインのログ：メインのログ ファイル **`vmlm.txt`** には、vmlm サービスのすべてのステータス メッセージと、ログイン監視の前後で発生したセッション イベントが記録されます。Logon Monitor が正常に実行されているかどうかを判断するには、このログを確認します。
- セッション ログ：セッション ログには、ユーザーのログイン セッションに関連するすべてのイベントが記録されます。ログインが開始すると、このログへのイベントの記録が開始します。このイベントは、1 つのユーザー セッションにのみ適用されます。ログの最後に書き込まれるサマリには、最も重要なメトリックの概要が含まれます。ログインに時間がかかる場合のトラブルシューティングでは、このログを確認します。ログインが完了すると、新しいイベントはセッション ログに書き込まれません。

Logon Monitor のメトリック

Logon Monitor は、ログイン、グループ ポリシー、ユーザー プロファイル、パフォーマンスに関連するメトリックを計算します。これらのメトリックにより、管理者は、ログイン時のエンド ユーザー システムの詳細を確認し、パフォーマンス低下の根本原因を判断できます。

表 11-11. Logon Monitor のメトリック

メトリック	パラメータ	説明
ログイン時間	■ 開始 ■ 終了 ■ 合計時間	このメトリックには、ゲストでのログインの開始時間、ログインの完了、プロファイルのロード、デスクトップの表示、ゲストでログインにかかった合計時間が含まれます。ゲスト以外の時間は除外されます。
セッション開始からログイン開始までの時間	合計時間	Windows がユーザー セッションを開始し、ログインが開始するまでの時間。
プロファイルの同期時間	合計時間	Windows がログイン時にユーザー プロファイルの調整に費やした時間。
シェルのロード	■ 開始 ■ 終了 ■ 合計時間	ユーザー シェル ロードの開始時刻は Windows が提供します。エクスプローラ ウィンドウが生成された時間が終了時間になります。
ログインからハイブ ロードまでの時間	合計時間	このメトリックは、ログインの開始からユーザー レジストリ ハイブのロードまでの合計時間を提供します。
Windows フォルダ リダイレクト	■ 開始 ■ 終了 ■ 合計時間	Windows のフォルダ リダイレクトが開始し、完全に適用されるまでの時間に関連するメトリックです。Windows フォルダ リダイレクトを有効にするまでの合計時間も含まれます。フォルダ リダイレクトが初めて適用される場合や、新しいファイルがリダイレクト先の共有にアップロードされている場合は、この値が高くなる可能性があります。
グループ ポリシーの時間	■ ユーザー グループ ポリシーの適用時間 ■ マシン グループ ポリシーの適用時間	ゲストへのグループ ポリシーの適用に関連するメトリック。ユーザー グループ ポリシーとマシン グループ ポリシーの適用にかかる時間も含まれます。
プロファイルのメトリック	■ プロファイル タイプ：ローカル、ローミング、一時 ■ プロファイル サイズ：ファイル数、フォルダ数、合計の MB 数	ユーザー プロファイルに関連するメトリック。ユーザー プロファイルの種類だけでなく、格納先（ローカル コンピュータか中央のプロファイル ストア）、あるいはログアウト後に削除するかどうかも含まれます。 プロファイル サイズには、ファイルの数、フォルダーの合計数、ユーザー プロファイルの合計サイズ (MB) が含まれます。
プロファイル サイズの分布	■ 0 ～ 1 MB のファイル数 ■ 1 MB ～ 10 MB のファイル数 ■ 10 MB ～ 100 MB のファイル数 ■ 100 MB ～ 1 GB のファイル数 ■ 1 GB ～ 10 GB のファイル数	ユーザー プロファイルに含まれる様々なサイズのファイル数。
ログイン時に開始するプロセス	■ 名前 ■ プロセス ID ■ 親プロセス ID ■ セッション ID	これらの値はプロセスごとに記録され、セッションの開始からログイン完了までの時間を表します。

表 11-11. Logon Monitor のメトリック (続き)

メトリック	パラメータ	説明
グループ ポリシー ログイン スクリプトの時間	合計時間	グループ ポリシー ログイン スクリプトの実行に関連するメトリック。グループ ポリシー ログイン スクリプトの実行にかかった合計時間が報告されます。
グループ ポリシー Power Shell スクリプトの時間	合計時間	グループ ポリシー Power Shell スクリプトの実行に関連するメトリック。グループ ポリシー Power Shell スクリプトの実行にかかった時間を表します。
メモリ使用率	■ 使用可能なバイト数：最小、最大、平均 ■ コミット済みのバイト数：最小、最大、平均 ■ ページ プール：最小、最大、平均	ログイン時のメモリ使用量に関連する WMI メトリック。サンプリングは、ログインが完了するまで実行されます。デフォルトで無効になっています。
CPU 使用率	■ アイドル状態の CPU：最小、最大、平均 ■ ユーザー CPU：最小、最大、平均 ■ カーネル CPU：最小、最大、平均	ログイン時の CPU 使用量に関連する WMI メトリック。サンプリングは、ログインが完了するまで実行されます。デフォルトで無効になっています。
ログイン スクリプトを同期するかどうか。		グループ ポリシー ログイン スクリプトが同期で実行されるのか、非同期で処理されるかどうかを報告します。
ネットワーク接続の状態	■ ドロップ ■ 復元	ネットワーク接続が維持されているのか、切断されているのかを報告します。
グループ ポリシーによるソフトウェアのインストール	■ 非同期：True または False ■ エラー コード ■ 合計時間	グループ ポリシーによるソフトウェアのインストールに関連するメトリック。インストールがログインと同期または非同期で実行されたのかどうか、インストールが成功したのか失敗したのかどうか、グループ ポリシーによるソフトウェアのインストールにかかった合計時間を表します。
プロファイルのボリュームのディスク使用量	■ ユーザーが使用可能なディスク容量 ■ 空きディスク容量 ■ ディスク容量の合計	ユーザー プロファイルが保存されているボリューム上のディスク使用量に関連するメトリック。
ドメイン コントローラの検出	■ エラー コード ■ 合計時間	ドメイン コントローラに関連するメトリック。エラー コードは、ドメイン コントローラに被害が及ぶ障害が発生しているかどうかを表します。
推定ネットワーク バンド幅	バンド幅	この値はイベント ID 5327 から収集されます。
ネットワーク接続の詳細	■ バンド幅 ■ 低速リンクのしきい値 ■ 低速リンクの検出：True または False	イベント ID 5314 から収集される値。

表 11-11. Logon Monitor のメトリック (続き)

メトリック	パラメータ	説明
ログイン時間に影響を及ぼす設定	■ コンピュータ\管理用テンプレート\ログイン\コンピュータの起動とログインでネットワークを常に待機 ■ コンピュータ\管理用テンプレート\ログイン\ユーザーのログイン時に次のプログラムを実行 ■ コンピュータ\管理用テンプレート\ユーザー プロファイル\ローミング ユーザー プロファイルを待機 ■ コンピュータ\管理用テンプレート\ユーザー プロファイル\ユーザーにローミング プロファイルまたはリモート ホーム ディレクトリがある場合のネットワークの最大の待機時間を設定 ■ コンピュータ\管理用テンプレート\グループ ポリシー\ログイン スクリプトの遅延を設定 ■ ユーザー\管理用テンプレート\システム\ログイン\ユーザーのログイン時に次のプログラムを実行 ■ ユーザー\管理用テンプレート\システム\ユーザー プロファイル\ログイン、ログアウト時にのみ同期するネットワーク ディレクトリを指定	
Horizon Agent、Persona Management、App Volumes のメトリック		Logon Monitor と対話する VMware 製品は、Logon Monitor ログのカスタム メトリックを報告します。このメトリックは、これらの製品がログイン時間に悪影響を及ぼしているかどうかを判断する場合に役立ちます。

Logon Monitor の構成

Windows レジストリ値を使用して、Logon Monitor を構成できます。

レジストリ設定

設定を変更するには、`HKLM\Software\VMware, Inc.\VMware Logon Monitor` レジストリ キーに移動します。

表 11-12. Logon Monitor の構成値

レジストリ キー	Type	説明
RemoteLogPath	REG_SZ	ログをアップロードするリモート共有へのパス。ログがリモートのログ共有にコピーされると、RemoteLogPath レジストリ キーで指定されたフォルダに配置されます。 例: `\\server\share\%username%.%userdomain%`. Logon Monitor が必要に応じてフォルダを作成します。デフォルトで無効になっています。 ■ リモート ログ フォルダの UNC パス ■ オプションです。構成しない場合、ログはアップロードされません。 ■ オプションで使用可能なローカル環境変数です。
フラグ	REG_DWORD	この値は、Logon Monitor の動作に影響を及ぼすビットマスクです。 ■ CPU とメモリのメトリックを有効または無効にする場合、設定または削除する値は 0x4 です。デフォルトで無効になっています。 ■ プロセス イベントとログイン スクリプトのメトリックを有効にする場合、設定または削除する値は 0x8 です。デフォルトで無効になっています。 ■ Horizon 7 との統合を有効または無効にする場合、設定する値は 0x2 です。デフォルトで有効になっています。 ■ クラッシュ ダンプを無効にするには、値を 0x1 に設定します。ダンプは、`C:\ProgramData\VMware\VMware Logon Monitor\Data` に書き込まれます。デフォルトで無効になっています。 ■ リモート パスにユーザーごとのフォルダを作成する場合、設定する値は 0x10 です。デフォルトで無効になっています。
LogMaxSizeMB	REG_DWORD	メイン ログの最大サイズ (MB)。デフォルトは 100 MB です。
LogKeepDays	REG_DWORD	ローリング前にメイン ログを保持する最大日数。デフォルトは 7 日です。

タイミング プロファイラの設定

Logon Monitor と Horizon Help Desk タイミング プロファイラを統合します。デフォルトでは、タイミング プロファイラは無効になっています。

- Logon Monitor で、タイミング プロファイラを使用してイベントをイベント データベースに書き込むには、`vdmadmin -I -timingProfiler -enable` を実行します。
- Logon Monitor でタイミング プロファイラの使用を無効にするには、`vdmadmin -I -timingProfiler -disable` を実行します。

VMware Horizon Performance Tracker の使用

VMware Horizon Performance Tracker は、リモート デスクトップで実行され、表示プロトコルのパフォーマンスとシステム リソースの使用量を監視するユーティリティです。アプリケーション プールを作成して、Horizon Performance Tracker を公開アプリケーションとして実行することもできます。

VMware Horizon Performance Tracker の構成

リモート デスクトップで Horizon Performance Tracker を実行できます。Horizon Performance Tracker は、公開アプリケーションとしても実行できます。

Horizon Performance Tracker の機能

Horizon Performance Tracker には、次の機能の重要なデータが表示されます。

表 11-13. Horizon Performance Tracker の機能

パフォーマンスのモニタリング	詳細
プロトコル固有のデータ	■ エンコーダの名前：表示プロトコルで使用されるエンコーダの名前 ■ バンド幅の使用状況：受信および送信の全体バンド幅。表示プロトコル（PCoIP または Blast）ごとに、サンプリング期間中の平均バンド幅が表示されます。 ■ 1 秒あたりのフレーム レート：1 秒のサンプリング期間中にエンコードされたイメージング フレームの数 ■ オーディオ有効：オーディオ機能が有効かどうか ■ オーディオの開始：オーディオ機能が開始しているかどうか ■ CPU 使用率: 　■ エンコーダの CPU 使用率：現在のユーザー セッションの表示プロトコル エンコーダの CPU 使用率 　■ システムの CPU 使用率：システムの CPU 使用率の合計
転送タイプ	■ クライアントからリモート セッション：クライアントからリモート ピアへの転送で使用された UDP または TCP プロトコル転送パッケージ ■ リモート セッションからクライアント：リモート ピアからクライアントへの転送で使用された UDP または TCP プロトコル転送パッケージ ■ Horizon Connection Server：接続サーバ インスタンスとの接続に使用される UDP または TCP プロトコル転送パッケージ
システムの健全性ステータス	■ 推定バンド幅：Horizon Client と Horizon Agent の間で使用可能な推定全体バンド幅。 ■ ラウンド トリップ：Horizon Agent と Horizon Client の間のラウンド トリップの待ち時間（ミリ秒）
セッション コンテキスト	■ サーバの詳細。DNS 名、ドメイン名、トンネリングの有無、URL、リモート IP アドレスなど。 ■ クライアント コンピュータの詳細。ディスプレイ番号、IP アドレス、キーボードとマウスのレイアウト、言語、タイムゾーンなど。
リアルタイムのプロトコルの切り替え	

注　Horizon Agent が仮想デスクトップ セッションで実行されている場合、Horizon Performance Tracker はデータの収集と表示のみを行います。

Horizon Performance Tracker のシステム要件

Horizon Performance Tracker は、次の構成をサポートしています。

表 11-14. Horizon Performance Tracker のシステム要件

システム	要件
仮想デスクトップのオペレーティング システム	Horizon Agent をサポートするすべてのオペレーティング システム
クライアント マシンのオペレーティング システム	すべての Horizon Client バージョンがサポートされます。ただし、公開アプリケーションとして実行される Horizon Client for Linux と Horizon Client for Windows 10 UWP はサポートされません。
表示プロトコル	VMware Blast および PCoIP

Horizon Performance Tracker のインストール

Horizon Performance Tracker は、Horizon Agent インストーラのカスタム セットアップ オプションです。デフォルトでは選択されていないため、オプションを選択する必要があります。Horizon Performance Tracker は、IPv4 と IPv6 の両方に対応しています。

Horizon Performance Tracker は、仮想デスクトップまたはリモート デスクトップ サービス (RDS) ホストにインストールできます。リモート デスクトップ サービス (RDS) ホストにインストールした場合は、公開アプリケーションとして公開し、Horizon Client から実行することもできます。『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』を参照してください。

インストールすると、デスクトップにショートカットが作成されます。

Horizon Performance Tracker グループ ポリシー設定

デフォルトの設定を変更するには、グループ ポリシーを構成します。「VMware Horizon Performance Tracker のポリシー設定」を参照してください。

VMware Horizon Performance Tracker のポリシー設定

Horizon Performance Tracker ADMX テンプレート ファイル (`perf_tracker.admx`) に、Horizon Performance Tracker 関連のポリシー設定が含まれています。

Horizon Performance Tracker をインストールすると、エージェント マシンの `C:\Program Files\vmware\Horizon Performance Tracker\admx` ディレクトリに `perf_tracker.admx` ファイルがインストールされます。対応する ADML ファイルは、同じディレクトリのサブフォルダにあります。ポリシー設定を編集するには、エージェント マシンの `gpedit.msc` を使用します。

手順

1 `C:\Program Files\vmware\Horizon Performance Tracker\admx` のファイルをエージェント マシンの `C:\Windows\PolicyDefinitions` にコピーします。

2 `gpedit.msc` を実行します。

3 [コンピュータの構成] - [管理用テンプレート] - [VMware Horizon Performance Tracker] の順に移動して、設定を編集します。

表 11-15. Horizon Performance Tracker のポリシー設定

設定	説明
Horizon Performance Tracker の基本設定	有効にした場合、Horizon Performance Tracker がデータを収集する頻度を秒単位で設定できます。
リモート デスクトップ接続で Horizon Performance Tracker の自動開始を有効にする	有効にした場合、ユーザーがリモート デスクトップ接続にログインすると、Horizon Performance Tracker は自動的に開始します。この環境設定の GPO 設定をクリアするには、[無効にする] を選択します。
リモート アプリケーション接続で Horizon Performance Tracker の自動開始を有効にする	有効にした場合、ユーザーがリモート アプリケーション接続にログインすると、Horizon Performance Tracker は自動的に開始します。この環境設定の GPO 設定をクリアするには、[無効にする] を選択します。

4 変更内容を有効にするには、Horizon Performance Tracker を再起動します。

Horizon Performance Tracker の実行

Horizon Client を使用すると、Horizon Performance Tracker をリモート デスクトップ内で実行できます。また、公開アプリケーションとして実行することもできます。

使用している Horizon Client プラットフォームで複数のセッションがサポートされている場合は、異なるファームから複数の Horizon Performance Tracker 公開アプリケーションを実行できます。複数のセッションをサポートしている Windows クライアントと Mac クライアントの場合、概要ウィンドウに表示されるコンピュータ名で、公開アプリケーションの実行元のファームを確認できます。iOS クライアントと Android クライアントの場合、HTML Access で同時に実行可能なセッションは 1 つだけです。別のファームから 2 番目のセッションを開くと、最初のセッションが終了します。

開始する前に

- Horizon Performance Tracker をインストールして構成します。「VMware Horizon Performance Tracker の構成」を参照してください。
- Horizon Performance Tracker のグループ ポリシーを設定します。「VMware Horizon Performance Tracker のポリシー設定」を参照してください。

手順

- リモート デスクトップで Horizon Performance Tracker を実行するには、Horizon Client または HTML Access を使用してサーバに接続し、リモート デスクトップを開始します。

  リモート デスクトップを開いたとき Horizon Performance Tracker が自動的に開始しない場合は、Windows デスクトップにある [VMware Horizon Performance Tracker] のショートカットをダブルクリックするか、他の Windows アプリケーションと同じ方法で Horizon Performance Tracker を開始します。

  概要ウィンドウまたはフローティング バーを表示してアプリケーションを終了するには、リモート デスクトップのシステム トレイで VMware Horizon Performance Tracker のアイコンを右クリックしてオプションを選択します。

- Horizon Performance Tracker を公開アプリケーションとして実行するには、Horizon Client または HTML Access を使用してサーバに接続し、Horizon Performance Tracker の公開アプリケーションを開始します。

  Horizon Performance Tracker の公開アプリケーションを使用する方法は、使用するクライアントの種類によって異なります。Horizon Client for Linux または Horizon Client for Windows 10 UWP では、Horizon Performance Tracker を公開アプリケーションとして実行できません。

  - Horizon Client for Windows の場合、Windows クライアント システムのシステム トレイに VMware Horizon Performance Tracker のアイコンが表示されます。このアイコンをダブルクリックすると、Windows クライアントで Horizon Performance Tracker が開きます。概要ウィンドウまたはフローティング バーを表示してアプリケーションを終了するには、このアイコンを右クリックしてオプションを選択します。
  - Horizon Client for Mac の場合、Mac クライアント システムのメニュー バーに VMware Horizon Performance Tracker のアイコンが表示されます。このアイコンをダブルクリックすると、Mac クライアントで Horizon Performance Tracker が開きます。また、概要ウィンドウまたはフローティング バーを表示してアプリケーションを終了するには、このアイコンを右クリックしてオプションを選択することもできます。
  - Horizon Client for Android、Horizon Client for iOS の場合は、Horizon Client の Unity Touch サイドバーに VMware Horizon Performance Tracker のアイコンが表示されます。概要ウィンドウまたはフローティング バーを表示してアプリケーションを終了するには、このアイコンをタッチしたままオプションを選択します。
  - HTML Access では、HTML Access サイドバーに VMware Horizon Performance Tracker のアイコンが表示されます。概要ウィンドウまたはフローティング バーを表示してアプリケーションを終了するには、このアイコンを右クリックしてオプションを選択します。

次に進む前に

Horizon Performance Tracker に表示されるデータの詳細については、「VMware Horizon Performance Tracker の構成」を参照してください。

システム健全性の監視

Horizon Administrator のシステム健全性ダッシュボードを使用すると、Horizon 7 の動作またはエンド ユーザーによるリモート デスクトップへのアクセスに影響を及ぼす可能性のある問題を素早く調べることができます。

Horizon Administrator の表示の左上にあるシステム健全性ダッシュボードには、Horizon 7 の動作に関するレポートを表示するために使用できるリンクがいくつかあります。

セッション	[セッション] 画面へのリンクを提供します。この画面には、リモート デスクトップおよびアプリケーション セッションのステータスに関する情報が表示されます。
問題のある vCenter 仮想マシン	[マシン] 画面へのリンクを提供します。この画面には、Horizon 7 が問題があるとフラグ付けした vCenter 仮想マシン、RDS ホスト、その他のマシンに関する情報が表示されます。

問題のある RDS ホスト	[マシン] 画面の [RDS ホスト] タブへのリンクを提供します。このタブには、Horizon 7 が問題があるとフラグ付けした RDS ホストに関する情報が表示されます。
イベント	エラー イベントおよび警告イベントを表示するようにフィルタ処理された Events（イベント） 画面へのリンクを提供します。
システムの健全性	[ダッシュボード] 画面へのリンクを提供します。この画面には、Horizon 7 コンポーネント、vSphere コンポーネント、ドメイン、デスクトップのステータス、およびデータストア使用量の概要が表示されます。

システム健全性ダッシュボードには、各項目に対して番号付きのリンクが表示されます。この番号は、リンク先のレポートによって詳細情報が提供される項目の数を示します。

Horizon 7 でのイベントの監視

イベント データベースは、接続サーバ ホストまたはグループ、Horizon Agent、および Horizon Administrator で発生したイベントの情報を格納し、ダッシュボードでイベントの数をユーザーに通知します。Events（イベント） 画面でイベントの詳細を調べることができます。

注　イベントは、一定の時間、Horizon Administrator インターフェイスに一覧表示されます。この時間が経過すると、イベントは履歴データベース テーブルにのみ表示されます。データベース テーブル内のイベントを調べるには、Microsoft SQL Server または Oracle データベース レポート ツールを使用できます。詳細については、『Horizon 7 の統合』を参照してください。

注　イベント データベースが使用できない場合、Horizon 7 がイベントの監査証跡を維持し、データベースが使用可能になると、これらの監査証跡をイベント データベースに保存します。これらのイベントを Horizon Administrator インターフェイスに表示するには、イベント データベースと接続サーバを再起動する必要があります。

Horizon Administrator でのイベントの監視に加えて、イベント データが分析ソフトウェアからアクセスできるように、Horizon 7 イベントを `Syslog` 形式で生成できます。「-I オプションを使用した Syslog 形式での Horizon 7 イベント ログ メッセージの生成」および『Horizon 7 のインストール』ドキュメントの「Syslog サーバのイベント ログを構成する」を参照してください。

開始する前に

イベント データベースを作成して設定します。『Horizon 7 のインストール』ドキュメントを参照してください。

手順

1. Horizon Administrator で、[監視] - [イベント] を選択します。
2. (オプション) Events（イベント） ウィンドウでは、イベントの時間範囲を選択し、イベントにフィルタ処理を適用し、一覧表示されたイベントを 1 つ以上の列によって並べ替えることができます。

Horizon 7 イベント メッセージ

Horizon 7 では、システムの状態が変更されるか、システムに問題が発生した場合は、常にイベントが報告されます。それらのイベント メッセージの情報を使用して、適切な処置を取ることができます。

次の表に、Horizon 7 が報告するイベントのタイプを示します。

表 11-16. Horizon 7 が報告するイベントのタイプ

イベントのタイプ	説明
監査失敗または監査成功	管理者またはユーザーが Horizon 7 の動作または構成に対して行った変更の成否を報告します。
エラー	失敗した Horizon 7 の動作を報告します。
情報	Horizon 7 内の正常な動作を報告します。
警告	時間の経過とともにより深刻な問題を引き起こす可能性がある、動作または設定の小さな問題を報告します。

監査失敗、エラー、または警告イベントに関連付けられたメッセージが表示された場合は、何らかの処置が必要になることがあります。監査成功または情報イベントについては、処置は必要ありません。

Horizon 7 の診断情報の収集

VMware のテクニカル サポートが Horizon 7 の問題を診断して解決する際に役立つ診断情報を収集できます。

Horizon 7 の各種コンポーネントから診断情報を収集できます。この情報の収集方法は、Horizon 7 のコンポーネントによって異なります。

- Horizon Agent 用のデータ収集ツール バンドルの作成

  VMware のテクニカル サポートによる Horizon Agent のトラブルシューティングを支援するため、`vdmadmin` コマンドを使用してデータ収集ツール (DCT) バンドルを作成することが必要になる場合があります。`vdmadmin` を使用せずに、手動で DCT バンドルを取得することもできます。

- Horizon Client の診断情報の保存

  Horizon Client の使用中に問題が発生し、一般的なネットワーク トラブルシューティング テクニックでそれらを解決できない場合は、ログ ファイルのコピーと構成に関する情報を保存できます。

- サポート スクリプトを使用した View Composer の診断情報の収集

  View Composer のサポート スクリプトを使用して、View Composer の構成データを収集し、ログ ファイルを生成することができます。この情報は、View Composer で発生した問題を VMware カスタマー サポートで診断する際に役立ちます。

- Horizon 接続サーバの診断情報の収集

  サポート ツールを使用して、Horizon 接続サーバのログ レベルを設定し、ログ ファイルを生成することができます。

- コンソールからの Horizon Agent、Horizon Client、または Horizon 接続サーバの診断情報の収集

  コンソールに直接アクセスできる場合、サポート スクリプトを使用して、接続サーバまたは Horizon Client のログ ファイル、あるいは Horizon Agent が動作しているリモート デスクトップのログ ファイルを生成できます。この情報は、これらのコンポーネントで発生した問題を VMware のテクニカル サポートで診断する際に役立ちます。

Horizon Agent 用のデータ収集ツール バンドルの作成

VMware のテクニカル サポートによる Horizon Agent のトラブルシューティングを支援するため、vdmadmin コマンドを使用してデータ収集ツール (DCT) バンドルを作成することが必要になる場合があります。vdmadmin を使用せずに、手動で DCT バンドルを取得することもできます。

vdmadmin コマンドを接続サーバ インスタンスで使用して、DCT バンドルをリモート デスクトップから要求すると便利です。バンドルは接続サーバに返されます。

別の方法として、特定のリモート デスクトップにログインし、そのデスクトップ上に DCT バンドルを作成する support コマンドを実行することもできます。ユーザー アカウント制御 (UAC) をオンにした場合は、この方法で DCT バンドルを取得する必要があります。

手順

1 必要な権限を持つユーザーとしてログインします。

オプション	アクション
View 接続サーバで vdmadmin を使用	接続サーバの標準インスタンスまたはレプリカ インスタンスに **管理者**ロールを持つユーザーとしてログインします。
リモート デスクトップ上	管理者権限を持つユーザーとしてリモート デスクトップにログインします。

2 コマンド プロンプトを開き、DCT バンドルを生成するコマンドを実行します。

オプション	アクション
View 接続サーバで vdmadmin を使用	出力バンドル ファイル、デスクトップ プール、マシンの名前を指定するには、vdmadmin コマンドで –outfile、–d、および –m オプションを使用します。 `vdmadmin –A [–b <authentication_arguments>] –getDCT –outfile <local_file> –d <desktop> –m <machine>`
リモート デスクトップ上	ディレクトリを c:\Program Files\VMware\VMware View\Agent\DCT に変更して、次のコマンドを実行します。 `support`

このコマンドを実行すると、指定した出力ファイルにバンドルが書き込まれます。

例: vdmadmin を使用した Horizon Agent のバンドル ファイルの作成

デスクトップ プール dtpool2 のマシン machine1 用の DCT バンドルを作成して、zip ファイル C:¥myfile.zip に書き込みます。

```
vdmadmin –A –d dtpool2 –m machine1 –getDCT –outfile C:\myfile.zip
```

次に進む前に

既存のサポート要求がある場合は、この DCT バンドル ファイルを添付してサポート要求を更新できます。

Horizon Client の診断情報の保存

Horizon Client の使用中に問題が発生し、一般的なネットワーク トラブルシューティング テクニックでそれらを解決できない場合は、ログ ファイルのコピーと構成に関する情報を保存できます。

診断情報を保存して VMware のテクニカル サポートに問い合わせる前に、Horizon Client の接続の問題の解決を試みることができます。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』ドキュメントの「Horizon Client と Horizon 接続サーバの接続の問題」を参照してください。

手順

1 Horizon Client で [サポート情報] をクリックするか、リモート デスクトップ メニューで [オプション] - [サポート情報] の順に選択します。

2 **[サポート情報]** ウィンドウで、[サポートデータの収集] をクリックし、確認が求められたら、[はい] をクリックします。

   コマンド ウィンドウに、情報の収集の進捗が表示されます。このプロセスには数分かかることがあります。

3 コマンド ウィンドウで、Horizon Client の構成をテストする Horizon 接続サーバ インスタンスの URL を入力し、必要に応じて Horizon 7 プロセスの診断ダンプを生成するように選択して、プロンプトに応答します。

   情報がクライアント マシンのデスクトップ上のフォルダ内の zip ファイルに書き込まれます。

4 VMware Web サイト上の Support（サポート） ページでサポート要求を提出し、出力 zip ファイルを添付します。

サポート スクリプトを使用した View Composer の診断情報の収集

View Composer のサポート スクリプトを使用して、View Composer の構成データを収集し、ログ ファイルを生成することができます。この情報は、View Composer で発生した問題を VMware カスタマー サポートで診断する際に役立ちます。

開始する前に

View Composer がインストールされているコンピュータにログインします。

サポート スクリプトを実行するには、Windows Script Host ユーティリティ（`cscript`）を使用する必要があるため、`cscript` の使い方を理解しておきます。http://technet.microsoft.com/library/bb490887.aspx を参照してください。

手順

1 コマンド プロンプト ウィンドウを開いて、`C:\Files\\View Composer` ディレクトリに移動します。

   デフォルト ディレクトリにソフトウェアをインストールしなかった場合は、該当するドライブ文字とパスで置き換えてください。

2 `svi-support` スクリプトを実行するコマンドを入力します。

```
cscript ".\svi-support.wsf" /zip
```

`/?` オプションを使用して、スクリプトで使用可能な他のコマンド オプションに関する情報を表示できます。

スクリプトの実行が終了すると、出力ファイルの名前と場所が通知されます。

3 VMware の Web サイト上の Support（サポート） ページでサポート要求を提出し、出力ファイルを添付します。

Horizon 接続サーバの診断情報の収集

サポート ツールを使用して、Horizon 接続サーバのログ レベルを設定し、ログ ファイルを生成することができます。

サポート ツールは接続サーバのログ データを収集します。この情報は、接続サーバで発生した問題を VMware のテクニカル サポートで診断する際に役立ちます。サポート ツールは、Horizon Client または Horizon Agent の診断情報の収集には使用できません。その代わりに、サポート スクリプトを使用する必要があります。「コンソールからの Horizon Agent、Horizon Client、または Horizon 接続サーバの診断情報の収集」を参照してください。

開始する前に

接続サーバの標準インスタンスまたはレプリカ インスタンスに **管理者**ロールを持つユーザーとしてログインします。

手順

1 [スタート] - [すべてのプログラム] - [VMware] - [View 接続サーバ ログ レベルの設定] の順に選択します。

2 [選択] テキスト ボックスに数値を入力してログ レベルを設定し、Enter キーを押します。

オプション	説明
0	ログ レベルをデフォルト値にリセットします。
1	通常のログ レベルを選択します。
2	デバッグのログ レベルを選択します（デフォルト）。
3	完全なログを選択します。

選択した詳細レベルでのログ情報の記録が開始されます。

3 接続サーバの動作に関する十分な情報を収集したら、[スタート] - [すべてのプログラム] - [VMware] - [View 接続サーバ ログ バンドルの生成] の順に選択します。

サポート ツールによって、接続サーバ インスタンスのデスクトップ上の `vdm-sdct` フォルダにログ ファイルが書き込まれます。

4 VMware の Web サイト上の Support（サポート） ページでサポート要求を提出し、出力ファイルを添付します。

コンソールからの Horizon Agent 、Horizon Client、または Horizon 接続サーバの診断情報の収集

コンソールに直接アクセスできる場合、サポート スクリプトを使用して、接続サーバまたは Horizon Client のログ ファイル、あるいは Horizon Agent が動作しているリモート デスクトップのログ ファイルを生成できます。この情報は、これらのコンポーネントで発生した問題を VMware のテクニカル サポートで診断する際に役立ちます。

開始する前に

情報を収集するシステムにログインします。管理権限を持つユーザーとしてログインする必要があります。

- Horizon Agent の場合、Horizon Agent がインストールされている仮想マシンにログインします。
- Horizon Client の場合、Horizon Client がインストールされているシステムにログインします。
- 接続サーバの場合、接続サーバ ホストにログインします。

手順

1 コマンド プロンプト ウィンドウを開いて、診断情報を収集する Horizon 7 コンポーネントの該当するディレクトリに移動します。

オプション	説明
Horizon Agent	`C:¥Files¥View¥¥` ディレクトリに移動します。
Horizon Client	`C:¥Files¥View¥¥` ディレクトリに移動します。
View 接続サーバ	`C:¥Files¥View¥¥` ディレクトリに移動します。

デフォルト ディレクトリにソフトウェアをインストールしなかった場合は、該当するドライブ文字とパスで置き換えてください。

2 サポート スクリプトを実行するコマンドを入力します。

```
.\support.bat [loglevels]
```

詳細ログを有効にする場合は、`loglevels` オプションを指定し、ログ レベルの数値の入力が求められたら入力します。

オプション	説明
0	ログ レベルをデフォルト値にリセットします。
1	通常のログ レベルを選択します。
2	デバッグのログ レベルを選択します（デフォルト）。
3	完全なログを選択します。
4	PCoIP の情報ログを選択します（Horizon Agent および Horizon Client のみ）。
5	PCoIP のデバッグ ログを選択します（Horizon Agent および Horizon Client のみ）。
6	仮想チャネルの情報ログを選択します（Horizon Agent および Horizon Client のみ）。
7	仮想チャネルのデバッグ ログを選択します（Horizon Agent および Horizon Client のみ）。
8	仮想チャネルのトレース ログを選択します（Horizon Agent および Horizon Client のみ）。

スクリプトによって、デスクトップ上の `vdm-sdct` フォルダに、zip 形式ログ ファイルが書き込まれます。

3 VMware View Composer Guest Agent ログは `C:¥Files¥Files¥¥Composer Guest Agent svi-ga-support` ディレクトリにあります。

4 VMware の Web サイト上の Support（サポート） ページでサポート要求を提出し、出力ファイルを添付します。

サポート要求の更新

サポート Web サイトで、既存のサポート要求を更新できます。

サポート要求を提出すると、VMware のテクニカル サポートから、`support` スクリプトまたは `svi-support` スクリプトの出力ファイルの提供を依頼する電子メールが送信される場合があります。スクリプトを実行すると、出力ファイルの名前と場所が通知されます。この出力ファイルを添付して電子メール メッセージに返信してください。

添付ファイルとしては出力ファイルが大きすぎる（10 MB 以上）場合は、VMware のテクニカル サポートに連絡し、サポート要求番号を伝え、FTP アップロードの方法を確認してください。または、サポート Web サイトで、既存のサポート要求に出力ファイルを添付できます。

手順

1 VMware の Web サイトの [サポート] ページに移動して、ログインします。

2 [サポート要求履歴] をクリックして、該当するサポート要求番号を見つけます。

3 サポート要求を更新し、`support` スクリプトまたは `svi-support` スクリプトを実行して取得した出力を添付します。

セキュリティ サーバと Horizon 接続サーバのペアリングの失敗のトラブルシューティング

セキュリティ サーバは、接続サーバ インスタンスとのペアリングに失敗すると、動作しない場合があります。

問題

セキュリティ サーバが 接続サーバとのペアリングに失敗すると、次のセキュリティ サーバ問題が発生する可能性があります。

- 2 度目にセキュリティ サーバをインストールしようとすると、セキュリティ サーバは接続サーバに接続できません。
- Horizon Client が Horizon 7 に接続できません。次のエラー メッセージが表示されます。**View 接続サーバ認証に失敗しました。デスクトップへの安全な接続に利用できるゲートウェイがありません。ネットワーク管理者にお問い合わせください。**
- Horizon Administrator ダッシュボードで、セキュリティ サーバが **停止** と表示されます。

原因

セキュリティ サーバのインストールを開始し、セキュリティ サーバの ペアリング パスワードを入力した後に、セキュリティ サーバ操作がキャンセルまたは中止された場合に、この問題が発生する可能性があります。

解決方法

セキュリティ サーバを Horizon 7 環境に保持する場合は、次の手順を実行します。

1 Horizon Administrator で、[View 構成] - [サーバ] を選択します。

2 [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] ドロップダウン メニューから [アップグレードまたは再インストールを準備] を選択して [OK] をクリックします。

3 [接続サーバ] タブで、セキュリティ サーバとペアリングする接続サーバ インスタンスを選択し、[その他のコマンド] ドロップダウン メニューから [セキュリティ サーバのペアリング パスワードを指定] を選択し、パスワードを入力して [OK] をクリックします。

4 セキュリティ サーバを再度インストールします。

Horizon 7 環境からセキュリティ サーバ エントリを削除する場合は、`vdmadmin -S` コマンドを実行します。

例：**`vdmadmin -S -r -s <security_server_name>`**

Horizon 7 Server の証明書失効チェックのトラブルシューティング

サーバの TLS 証明書で証明書失効チェックを実行できない場合、安全な Horizon Client 接続に使用されるセキュリティ サーバまたは接続サーバ インスタンスが View Administrator で赤色に表示されます。

問題

セキュリティ サーバまたは接続サーバ アイコンが、Horizon Administrator ダッシュボードで赤色で表示されます。Horizon 7 Server の状態には、次のメッセージが表示されます。**サーバ証明書はチェックできません。**

原因

組織がインターネット アクセスにプロキシ サーバを使用しているか、接続サーバ インスタンスが、ファイアウォールなどの制御が原因で証明書失効チェックを提供するサーバにアクセスできない場合は、証明書失効チェックに失敗することがあります。

接続サーバ インスタンスは、自身の証明書とペアにされたセキュリティ サーバの証明書について証明書失効チェックを実行します。デフォルトでは、VMware Horizon View 接続サーバ サービスは `LocalSystem` アカウントで開始されます。サービスが `LocalSystem` で実行されると、接続サーバ インスタンスは、Internet Explorer で構成されているプロキシ設定を使用して CRL DP URL にアクセスしたり、OCSP レスポンダを使用して証明書の失効ステータスを判断することはできません。

Microsoft `Netshell` コマンドを使用してプロキシ設定を接続サーバ インスタンスにインポートすると、サーバはインターネット上の証明書失効チェック サイトにアクセスできるようになります。

解決方法

1 接続サーバ コンピュータで、[管理者として実行] 設定を使用してコマンドライン ウィンドウを開きます。

たとえば、[スタート] をクリックし、「**`cmd`**」と入力し、`cmd.exe` アイコンを右クリックして、[管理者として実行] を選択します。

2 「**`netsh`**」と入力し、Enter キーを押します。

3 「**`winhttp`**」と入力し、Enter キーを押します。

4 「**`show proxy`**」と入力し、Enter キーを押します。

`Netshell` により、プロキシが直接接続に設定されたことが示されます。この設定では、組織でプロキシが使用されている場合は、接続サーバ コンピュータはインターネットに接続できません。

5 プロキシ設定を構成します。

たとえば、**netsh winhttp>** プロンプトで **import proxy source=ie** と入力します。

プロキシ設定が接続サーバ コンピュータにインポートされます。

6 「**show proxy**」と入力して、プロキシ設定を確認します。

7 VMware Horizon View 接続サーバ サービスを再起動します。

8 Horizon Administrator ダッシュボードで、セキュリティ サーバまたは接続サーバ アイコンが緑色になっていることを確認します。

スマート カードでの証明書失効チェックのトラブルシューティング

スマート カードが接続されている接続サーバ インスタンスまたはセキュリティ サーバは、スマート カード証明書失効チェックを構成しない限り、サーバの TLS 証明書で証明書失効チェックを実行できません。

問題

組織でインターネット アクセスのためにプロキシ サーバを使用している場合や接続サーバ インスタンスまたはセキュリティ サーバが、ファイアウォールまたは他の制御が理由で失効チェックを提供するサーバに到達できない場合、証明書失効チェックは失敗する可能性があります。

重要 CRL ファイルが最新であることを確認します。

原因

Horizon 7 は、証明書失効リスト (CRL) およびオンライン証明書状態プロトコル (OCSP) による証明書失効チェックをサポートします。CRL は、証明書を発行した認証局 (CA) によって公開される、失効した証明書のリストです。OCSP は、X.509 証明書の失効ステータスを取得するために使用される証明書検証プロトコルです。認証局 (CA) は、接続サーバまたはセキュリティ サーバ ホストからにアクセスできる必要があります。この問題は、スマート カード証明書の失効チェックを構成した場合に限って発生します。「スマート カードでの証明書失効チェックの使用」を参照してください。

解決方法

1 Horizon 7 Server のパスを使用して認証局 (CA) の Website から最新の CRL をダウンロードするための自分用の手順を（手動で）作成します。

2 接続サーバ ホストまたはセキュリティ サーバ ホスト上で、TLS/SSL ゲートウェイ構成フォルダ内の `locked.properties` ファイルを作成または編集します。

例：`<install_directory>\VMware\VMware View\Server\SSLgateway\conf\locked.properties`

3 `locked.properties` ファイルの `enableRevocationChecking` および `crlLocation` プロパティを CRL が保存されているローカル パスに追加します。

4 変更を反映するため、接続サーバ サービスまたはセキュリティ サーバ サービスを再起動してください。

トラブルシューティングの追加情報

トラブルシューティングの追加情報は、VMware ナレッジベースの記事に掲載されています。

VMware ナレッジベース（KB）は、VMware 製品の新しいトラブルシューティング情報が追加されて継続的に更新されています。

Horizon 7 のトラブルシューティングの詳細については、VMware KB の Web サイトで利用可能な KB の記事を参照してください。

http://kb.vmware.com/selfservice/microsites/microsite.do

vdmadmin コマンドの使用

12

vdmadmin コマンド ライン インターフェイスを使用して、接続サーバ インスタンスに対するさまざまな管理タスクを実行できます。

vdmadmin を使用すると、Horizon Administrator のユーザー インターフェイス内からは実行できない管理タスクや、スクリプトから自動的に実行する必要がある管理タスクを実行できます。

Horizon Administrator、Horizon 7 コマンドレット、**vdmadmin** で実行可能な操作の比較については、『Horizon 7 の統合』を参照してください。

- vdmadmin コマンドの使用方法

  vdmadmin コマンドの構文によって、コマンドの動作が制御されます。

- -A オプションを使用した Horizon Agent のログの構成

  vdmadmin コマンドと **–A** オプションを使用して、Horizon Agent によるログの記録を構成できます。

- -A オプションを使用した IP アドレスの上書き

  vdmadmin コマンドと **–A** オプションを使用して、Horizon Agent によって報告される IP アドレスを上書きできます。

- -F オプションを使用した外部セキュリティ プリンシパルの更新

  vdmadmin コマンドと **–F** オプションを使用して、デスクトップの使用が許可されている Active Directory 内の Windows ユーザーの外部セキュリティ プリンシパル（FSP）を更新できます。

- -H オプションを使用した健全性モニターの一覧表示および詳細表示

  vdmadmin コマンドと **–H** オプションを使用して、既存の健全性モニターを一覧表示し、Horizon 7 コンポーネントのインスタンスを監視し、特定の健全性モニターまたはモニター インスタンスの詳細を表示することができます。

- -I オプションを使用した Horizon 7 の動作レポートの一覧表示および結果表示

  vdmadmin コマンドと **–I** オプションを使用して、Horizon 7 の動作について利用可能なレポートを一覧表示し、いずれかのレポートの実行結果を表示することができます。

- -I オプションを使用した Syslog 形式での Horizon 7 イベント ログ メッセージの生成

  vdmadmin コマンドと **–I** オプションを使用して、Horizon 7 イベント メッセージを **Syslog** 形式でイベント ログ ファイルに記録できます。サードパーティ製分析製品の多くでは、分析操作のために入力としてフラット ファイル **Syslog** データが必要です。

- -L オプションを使用した専用マシンの割り当て

  vdmadmin コマンドと –L オプションを使用して、専用プールのマシンをユーザーに割り当てることができます。

- -M オプションを使用したマシンに関する情報の表示

  vdmadmin コマンドと –M オプションを使用して、仮想マシンまたは物理コンピュータの構成に関する情報を表示できます。

- -M オプションを使用した仮想マシン上のディスク容量の再利用

  vdmadmin コマンドと –M オプションを使用すると、リンク クローン仮想マシンをディスク容量再利用の対象として指定することができます。Horizon 7 は、リンク クローン OS ディスク上の未使用容量が Horizon Administrator で指定した最小しきい値に達するのを待たずに、ESXi ホストにその OS ディスク上のディスク容量を再利用するように指示します。

- -N オプションを使用したドメイン フィルタの構成

  vdmadmin コマンドと –N オプションを使用して、Horizon 7 によって、エンド ユーザーからアクセス可能にするドメインを制御できます。

- ドメイン フィルタの構成

  ドメイン フィルタを構成して、接続サーバ インスタンスまたはセキュリティ サーバによって、エンド ユーザーからアクセス可能にするドメインを制限することができます。

- -O および -P オプションを使用して資格を持たないユーザーのマシンとポリシーを表示する

  vdmadmin コマンドと –O および –P オプションを使用して、システムを使用する資格を失ったユーザーに割り当てられている仮想マシンとポリシーを表示できます。

- -Q オプションを使用したキオスク モードのクライアントの構成

  vdmadmin コマンドと –Q オプションを使用すると、キオスク モードのクライアントのデフォルト値を設定してアカウントを作成し、これらのクライアントの認証を可能にし、それらの構成に関する情報を表示することができます。

- -R オプションを使用したマシンの最初のユーザーの表示

  vdmadmin コマンドと –R オプションを使用して、管理対象仮想マシンの初期の割り当てを確認できます。たとえば、LDAP データが失われた場合、仮想マシンを再度ユーザーに割り当てるためにこの情報が必要になることがあります。

- -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

  vdmadmin コマンドと –S オプションを使用して、接続サーバ インスタンスまたはセキュリティ サーバのエントリを Horizon 7 の構成から削除できます。

- -T オプションの使用による管理者の 2 番目の認証情報の提供

  vdmadmin コマンドを使用するときに –T オプションを指定すると、Active Directory の 2 番目の認証情報を管理者ユーザーに提供できます。

- -U オプションを使用したユーザーに関する情報の表示

  vdmadmin コマンドと –U オプションを使用して、ユーザーに関する詳細情報を表示できます。

- -V オプションを使用した仮想マシンのロック解除またはロック

  vdmadmin コマンドと –V オプションを使用して、データセンター内の仮想マシンをロック解除またはロックできます。

- -X オプションを使用して LDAP エントリおよびスキーマの競合を検出して解決する

  vdmadmin コマンドの –X オプションを使用すると、グループ内の複製接続サーバ インスタンスで発生している LDAP エントリ競合および LDAP スキーマ競合を検出して解決することができます。また、クラウド ポッド アーキテクチャ 環境内の LDAP スキーマ競合の検出と解決を行うこともできます。

vdmadmin コマンドの使用方法

vdmadmin コマンドの構文によって、コマンドの動作が制御されます。

Windows コマンド プロンプトで、次の形式の vdmadmin コマンドを使用します。

```
vdmadmin <command_option> [<additional_option> <argument>] ...
```

使用できる追加のオプションは、コマンド オプションによって異なります。

デフォルトでは、vdmadmin コマンドの実行可能ファイルのパスは C:¥Program Files¥VMware¥VMware View¥Server¥tools¥bin です。コマンド ラインにパスを入力するのを避けるには、<PATH> 環境変数にパスを追加します。

- vdmadmin コマンドでの認証

  指定した操作を正常に実行するためには、vdmadmin コマンドを Administrators（管理者） ロールのユーザーとして実行する必要があります。

- vdmadmin コマンドの出力形式

  一部の vdmadmin コマンド オプションでは、出力情報の形式を指定できます。

- vdmadmin コマンド オプション

  vdmadmin コマンドで実行する操作を指定するには、コマンド オプションを使用します。

vdmadmin コマンドでの認証

指定した操作を正常に実行するためには、vdmadmin コマンドを Administrators（管理者） ロールのユーザーとして実行する必要があります。

Horizon Administrator を使用して**管理者**ロールをユーザーに割り当てることができます。第 6 章「ロールベースの委任管理の構成」を参照してください。

十分な権限を持たないユーザーとしてログインしている場合に、–b オプションを使用して、Administrators（管理者） ロールが割り当てられているユーザーとしてコマンドを実行できます。ただし、そのユーザーのパスワードを知っている必要があります。–b オプションを指定すると、特定のドメインで特定のユーザーとして vdmadmin コマンドを実行できます。次に示す –b オプションの使用形式は同等です。

```
–b <username> <domain> [<password> | *]
```

```
–b <username>@<domain> [<password> | *]
```

```
–b <domain>\<username> [<password> | *]
```

パスワードの代わりにアスタリスク (*) を指定した場合は、パスワードを入力するように求められます。vdmadmin コマンドは、機密パスワードがコマンド行のコマンド履歴に残らないようにします。

–b オプションは、–R および –T オプションを除くすべてのコマンド オプションとともに使用できます。

vdmadmin コマンドの出力形式

一部の vdmadmin コマンド オプションでは、出力情報の形式を指定できます。

次の表に、出力テキストの形式を指定できる vdmadmin コマンド オプションを示します。

表 12-1. 出力形式を選択するためのオプション

オプション	説明
–csv	出力の形式をカンマ区切り値として指定します。
–n	ASCII（UTF-8）文字を使用して出力を表示します。これは、カンマ区切り値およびテキスト形式出力のデフォルトの文字セットです。
–w	Unicode（UTF-16）文字を使用して出力を表示します。これは、XML 出力のデフォルトの文字セットです。
–xml	出力形式を XML として指定します。

vdmadmin コマンド オプション

vdmadmin コマンドで実行する操作を指定するには、コマンド オプションを使用します。

次の表に、Horizon 7 の処理を制御および確認するために vdmadmin コマンドで使用できるコマンド オプションを示します。

表 12-2. vdmadmin コマンド オプション

オプション	説明
–A	Horizon Agent がログ ファイルに記録する情報を管理します。「-A オプションを使用した Horizon Agent のログの構成」を参照してください。 Horizon Agent によりレポートされる IP アドレスを上書きします。「-A オプションを使用した IP アドレスの上書き」を参照してください。
–C	接続サーバ グループの名前を設定します。GUID-3AD7B00C-43C4-417E-A06B-7251805657D6#GUID-3AD7B00C-43C4-417E-A06B-7251805657D6 を参照してください。
–F	Active Directory 内のすべてのユーザーまたは指定されたユーザーの外部セキュリティ プリンシパル（FSP）を更新します。「-F オプションを使用した外部セキュリティ プリンシパルの更新」を参照してください。
–H	Horizon 7 サービスの健全性についての情報を表示します。「-H オプションを使用した健全性モニターの一覧表示および詳細表示」を参照してください。
–I	Horizon 7 の動作に関するレポートを生成します。「-I オプションを使用した Horizon 7 の動作レポートの一覧表示および結果表示」を参照してください。
–L	ユーザーに専用デスクトップを割り当てます。または割り当てを削除します。「-L オプションを使用した専用マシンの割り当て」を参照してください。
–M	仮想マシンまたは物理コンピュータの情報を表示します。「-M オプションを使用したマシンに関する情報の表示」を参照してください。
–N	接続サーバ インスタンスまたはグループで Horizon Client に提供されるドメインを構成します。「-N オプションを使用したドメイン フィルタの構成」を参照してください。
–O	ユーザーに割り当てられたリモート デスクトップのうち、ユーザーが資格を失っているデスクトップを表示します。「-O および -P オプションを使用して資格を持たないユーザーのマシンとポリシーを表示する」を参照してください。
–P	資格のないユーザーのリモート デスクトップに関連付けられているユーザー ポリシーを表示します。「-O および -P オプションを使用して資格を持たないユーザーのマシンとポリシーを表示する」を参照してください。
–Q	キオスク モードのクライアント デバイスの Active Directory アカウントおよび Horizon 7 構成を設定します。「-Q オプションを使用したキオスク モードのクライアントの構成」を参照してください。
–R	リモート デスクトップに最初にアクセスしたユーザーを報告します。「-R オプションを使用したマシンの最初のユーザーの表示」を参照してください。
–S	接続サーバ インスタンスの構成エントリを Horizon 7 の構成から削除します。「-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。
–T	Active Directory の 2 番目の認証情報を管理者ユーザーに提供します。「-T オプションの使用による管理者の 2 番目の認証情報の提供」を参照してください。
–U	ユーザーに関する情報（リモート デスクトップに対する資格や ThinApp 割り当て、管理者のロールなど）を表示します。「-U オプションを使用したユーザーに関する情報の表示」を参照してください。
–V	仮想マシンをロック解除またはロックします。「-V オプションを使用した仮想マシンのロック解除またはロック」を参照してください。
–X	複製された接続サーバ インスタンス上で重複する LDAP エントリを検出して解決します。「-X オプションを使用して LDAP エントリおよびスキーマの競合を検出して解決する」を参照してください。

-A オプションを使用した Horizon Agent のログの構成

`vdmadmin` コマンドと –A オプションを使用して、Horizon Agent によるログの記録を構成できます。

構文

```
vdmadmin –A [–b< authentication_arguments>] –getDCT–outfile< local_file> –d< desktop >–m< machine>
```

```
vdmadmin –A [–b< authentication_arguments>] –getlogfile <logfile> –outfile< local_file> –d< desktop> –m <machine>
```

```
vdmadmin –A [–b< authentication_arguments>] –getloglevel [–xml] –d< desktop> [–m< machine>]
```

```
vdmadmin –A [–b< authentication_arguments>] –getstatus [–xml] –d< desktop> [–m< machine>]
```

```
vdmadmin –A [–b< authentication_arguments>] –getversion [–xml] –d< desktop> [–m <machine>]
```

```
vdmadmin –A [–b< authentication_arguments>] –list [–xml] [–w | –n] –d< desktop> –m< machine>
```

```
vdmadmin –A [–b< authentication_arguments>] –setloglevel< level> –d <desktop> [–m <machine>]
```

使用上の注意

VMware のテクニカル サポートによる Horizon Agent のトラブルシューティングを支援するため、データ収集ツール (DCT) バンドルを作成することができます。さらに、ログ レベルを変更し、Horizon Agent のバージョンおよびステータスを表示して、各ログ ファイルをローカル ディスクに保存することもできます。

オプション

次の表に、Horizon Agent でのログを構成するためのオプションを示します。

表 12-3. Horizon Agent でのログ構成オプション

オプション	説明
–d <desktop>	デスクトップ プールを指定します。
–getDCT	データ収集ツール（DCT）バンドルを作成して、ローカル ファイルに保存します。
–getlogfile <logfile>	コピーを保存するログ ファイルの名前を指定します。
–getloglevel	Horizon Agent の現在のログ レベルを表示します。
–getstatus	Horizon Agent ステータスを表示します。
–getversion	Horizon Agent のバージョンを表示します。

表 12-3. Horizon Agent でのログ構成オプション (続き)

オプション	説明	
`–list`	Horizon Agent のログ ファイルを表示します。	
`–m` <machine>	デスクトップ プール内のマシンを指定します。	
`–outfile` <local_file>	DCT バンドルまたはログ ファイルのコピーを保存するローカル ファイルの名前を指定します。	
`–setloglevel` <level>	Horizon Agent のログ レベルを設定します。	
	デバッグ	エラー、警告、およびデバッグ イベントをログに記録します。
	正常	エラーおよび警告イベントをログに記録します。
	トレース	エラー、警告、情報、およびデバッグ イベントをログに記録します。

例

デスクトップ プール dtpool2 に属するマシン machine1 の Horizon Agent のログ レベルを表示します。

```
vdmadmin –A –d dtpool2 –m machine1 –getloglevel
```

デスクトップ プール dtpool2 に属するマシン machine1 の Horizon Agent のログ レベルを debug に設定します。

```
vdmadmin –A –d dtpool2 –m machine1 –setloglevel debug
```

デスクトップ プール dtpool2 に属するマシン machine1 の Horizon Agent ログ ファイルのリストを表示します。

```
vdmadmin –A –d dtpool2 –m machine1 –list
```

デスクトップ プール dtpool2 に属するマシン machine1 の Horizon Agent ログ ファイル `log–2009–01–02.txt` のコピーを、`C:¥mycopiedlog.txt` として保存します。

```
vdmadmin –A –d dtpool2 –m machine1 –getlogfile log–2009–01–02.txt –outfile C:\mycopiedlog.txt
```

デスクトップ プール dtpool2 に属するマシン machine1 の Horizon Agent のバージョンを表示します。

```
vdmadmin –A –d dtpool2 –m machine1 –getversion
```

デスクトップ プール dtpool2 に属するマシン machine1 の Horizon Agent のステータスを表示します。

```
vdmadmin –A –d dtpool2 –m machine1 –getstatus
```

デスクトップ プール dtpool2 のマシン machine1 用の DCT バンドルを作成して、zip ファイル C:¥myfile.zip に書き込みます。

```
vdmadmin –A –d dtpool2 –m machine1 –getDCT –outfile C:\myfile.zip
```

-A オプションを使用した IP アドレスの上書き

vdmadmin コマンドと –A オプションを使用して、Horizon Agent によって報告される IP アドレスを上書きできます。

構文

```
vdmadmin –A [–b <authentication_arguments>] –override –i <ip_or_dns> –d <desktop> –m
<machine>
```

```
vdmadmin –A [–b <authentication_arguments>] –override –list –d <desktop> –m <machine>
```

```
vdmadmin –A [–b <authentication_arguments>] –override –r –d <desktop> [–m <machine>]
```

使用上の注意

Horizon Agent は、自身が実行されているマシンの検出済み IP アドレスを、接続サーバ インスタンスに報告します。Horizon Agent によって報告された値を接続サーバ インスタンスが信頼することができない安全な構成では、Horizon Agent によって提供された値を上書きして、管理対象マシンで使用する IP アドレスを指定することができます。Horizon Agent によって報告されたマシンのアドレスが、定義されたアドレスと一致しない場合は、Horizon Client を使用してそのマシンにアクセスできません。

オプション

次の表に、IP アドレスを上書きするためのオプションを示します。

表 12-4. IP アドレスの上書きのためのオプション

オプション	説明
–d <desktop>	デスクトップ プールを指定します。
–i <ip_or_dns>	IP アドレスまたは DNS で解決できるドメイン名を指定します。
–m <machine>	デスクトップ プールのマシンの名前を指定します。
–override	IP アドレスの上書きの操作を指定します。
–r	上書きされた IP アドレスを削除します。

例

デスクトップ プール dtpool2 のマシン machine2 の IP アドレスをオーバーライドします。

```
vdmadmin –A –override –i 10.20.54.165 –d dtpool2 –m machine2
```

デスクトップ プール dtpool2 のマシン machine2 に定義されている IP アドレスを表示します。

```
vdmadmin –A –override –list –d dtpool2 –m machine2
```

デスクトップ プール dtpool2 のマシン machine2 に定義されている IP アドレスを削除します。

```
vdmadmin –A –override –r –d dtpool2 –m machine2
```

デスクトップ プール dtpool3 のデスクトップに定義されている IP アドレスを削除します。

```
vdmadmin –A –override –r –d dtpool3
```

-F オプションを使用した外部セキュリティ プリンシパルの更新

vdmadmin コマンドと –F オプションを使用して、デスクトップの使用が許可されている Active Directory 内の Windows ユーザーの外部セキュリティ プリンシパル（FSP）を更新できます。

構文

```
vdmadmin –F [–b <authentication_arguments>] [–u <domain>\<user>]
```

使用上の注意

ローカル ドメイン以外のドメインを信頼する場合は、外部ドメインのセキュリティ プリンシパルがローカル ドメインのリソースにアクセスするのを許可します。Active Directory では、信頼された外部ドメインのセキュリティ プリンシパルを表すために FSP を使用します。信頼された外部ドメインのリストを変更する場合は、ユーザーの FSP を更新できます。

オプション

–u オプションは、FSP を更新するユーザーの名前およびドメインを指定します。このオプションを指定しない場合、コマンドは Active Directory 内のすべてのユーザーの FSP を更新します。

例

EXTERNAL ドメインのユーザー Jim の FSP を更新します。

```
vdmadmin –F –u EXTERNAL\Jim
```

Active Directory 内の全ユーザーの FSP を更新します。

```
vdmadmin –F
```

-H オプションを使用した健全性モニターの一覧表示および詳細表示

vdmadmin コマンドと –H オプションを使用して、既存の健全性モニターを一覧表示し、Horizon 7 コンポーネントのインスタンスを監視し、特定の健全性モニターまたはモニター インスタンスの詳細を表示することができます。

構文

```
vdmadmin –H [–b<authentication_arguments>] –list –xml [–w | –n]
```

```
vdmadmin –H [–b<authentication_arguments>] –list –monitorid< monitor_id >–xml [–w | –n]
```

```
vdmadmin –H [–b<authentication_arguments>] –monitorid <monitor_id >–instanceid<
instance_id >–xml [–w | –n]
```

使用上の注意

次の表に、Horizon 7 のコンポーネントの健全性を監視するために使用される健全性モニターを示します。

表 12-5. 健全性モニター

モニター	説明
CBMonitor	接続サーバ インスタンスの健全性を監視します。
DBMonitor	イベント データベースの健全性を監視します。
DomainMonitor	接続サーバ ホストのローカル ドメインおよび信頼されるすべてのドメインの健全性を監視します。
SGMonitor	セキュリティ ゲートウェイ サービスおよびセキュリティ サーバの健全性を監視します。
VCMonitor	vCenter サーバの健全性を監視します。

コンポーネントに複数のインスタンスがある場合、コンポーネントの各インスタンスを監視するための別個のモニター インスタンスが Horizon 7 によって作成されます。

このコマンドを実行すると、健全性モニターおよびモニター インスタンスに関するすべての情報が XML 形式で出力されます。

オプション

次の表に健全性モニターを一覧表示し、詳細を表示するためのオプションを示します。

表 12-6. 健全性モニターの一覧表示と詳細表示のためのオプション

オプション	説明
`–instanceid` <instance_id>	健全性モニター インスタンスを指定します。
`–list`	健全性モニター ID を指定しない場合は、既存の健全性モニターが表示されます。
`–list –monitorid` <monitor_id>	指定した健全性モニター ID のモニター インスタンスを表示します。
`–monitorid` <monitor_id>	健全性モニター ID を指定します。

例

既存のすべての健全性モニターを、Unicode 文字を使用した XML で一覧表示します。

```
vdmadmin –H –list –xml
```

vCenter モニター（VCMonitor）のすべてのインスタンスを、ASCII 文字を使用した XML で一覧表示します。

```
vdmadmin –H –list –monitorid VCMonitor –xml –n
```

指定した vCenter モニター インスタンスの健全性を表示します。

```
vdmadmin –H –monitorid VCMonitor –instanceid 4aec2c99–4879–96b2–de408064d035 –xml
```

-I オプションを使用した Horizon 7 の動作レポートの一覧表示および結果表示

`vdmadmin` コマンドと `–I` オプションを使用して、Horizon 7 の動作について利用可能なレポートを一覧表示し、いずれかのレポートの実行結果を表示することができます。

構文

```
vdmadmin –I [–b<authentication_arguments>] –list [–xml] [–w | –n]
```

```
vdmadmin –I [–b< authentication_arguments>] –report< report >–view< view> [–startdate<
yyyy–MM–dd–HH:mm:ss>][–enddate< yyyy–MM–dd–HH:mm:ss>] [–w | –n] –xml | –csv
```

使用上の注意

このコマンドを使用して、利用可能なレポートおよびビューを表示し、指定したレポートおよびビューに Horizon 7 によって記録された情報を表示できます。

`vdmadmin` コマンドと `–I` オプションを使用して、`syslog` 形式の Horizon 7 ログ メッセージを生成することもできます。「-I オプションを使用した Syslog 形式での Horizon 7 イベント ログ メッセージの生成」を参照してください。

オプション

次の表に、レポートおよびビューを一覧表示し、結果を表示するために指定できるオプションを示します。

表 12-7. レポートおよびビューの一覧表示と結果表示のためのオプション

オプション	説明
–enddate <yyyy-MM-dd-HH:mm:ss>	表示する情報の日付の上限を指定します。
–list	利用可能なレポートおよびビューを一覧表示します。
–report <report>	レポートを指定します。
–startdate <yyyy-MM-dd-HH:mm:ss>	表示する情報の日付の下限を指定します。
–view <view>	ビューを指定します。

例

利用可能なレポートおよびビューを、Unicode 文字を使用した XML で一覧表示します。

```
vdmadmin –I –list –xml –w
```

2010 年 8 月 1 日以降に発生したユーザー イベントのリストを、ASCII 文字を使用したカンマ区切り値として表示します。

```
vdmadmin –I –report events –view user_events –startdate 2010–08–01–00:00:00 –csv –n
```

-I オプションを使用した Syslog 形式での Horizon 7 イベント ログ メッセージの生成

vdmadmin コマンドと –I オプションを使用して、Horizon 7 イベント メッセージを Syslog 形式でイベント ログ ファイルに記録できます。サードパーティ製分析製品の多くでは、分析操作のために入力としてフラット ファイル Syslog データが必要です。

構文

```
vdmadmin –I –eventSyslog –disable
```

```
vdmadmin –I –eventSyslog –enable –localOnly
```

```
vdmadmin –I –eventSyslog –enable –path <path>
```

```
vdmadmin –I –eventSyslog –enable –path <path>
 –user <DomainName\username> –password <password>
```

使用上の注意

このコマンドを使用して、Horizon 7 イベント ログ メッセージを Syslog 形式で生成できます。Syslog ファイルで、Horizon 7 イベント ログ メッセージはキーと値のペアでフォーマットされるため、ログ データに分析ソフトウェアからアクセスできます。

vdmadmin コマンドと -I オプションを使用して、使用可能なレポートおよびビューを一覧にして、指定したレポートの内容を表示することもできます。「-I オプションを使用した Horizon 7 の動作レポートの一覧表示および結果表示」を参照してください。

オプション

eventSyslog オプションは無効または有効にできます。Syslog 出力はローカル システムのみまたは別の場所にダイレクトできます。Syslog サーバへの直接 UDP 接続は、Horizon 7 5.2 以降でサポートされています。『Horizon 7 のインストール』の「Syslog サーバのイベント ログを構成する」を参照してください。

表 12-8. Syslog 形式で Horizon 7 イベント ログ メッセージを生成するためのオプション

オプション	説明
-disable	Syslog ログを無効にします。
-e|-enable	Syslog ログを有効にします。
-eventSyslog	Horizon 7 イベントが Syslog 形式で生成されるように指定します。
-localOnly	Syslog 出力をローカル システムのみに保存します。-localOnly オプションを使用した場合、Syslog 出力のデフォルトの宛先は %PROGRAMDATA%\VMware\VDM\events\ です。
-password <password>	Syslog 出力の指定された宛先パスへのアクセスを認証するユーザーのパスワードを指定します。
-path	Syslog 出力の宛先 UNC パスを決定します。
-u|-user <DomainName\username>	Syslog 出力の宛先パスにアクセスできるドメインとユーザー名を指定します。

例

Syslog 形式での Horizon 7 イベントの生成を無効にします。

```
vdmadmin -I -eventSyslog -disable
```

Horizon 7 イベントの Syslog 出力をローカル システムのみにダイレクトします。

```
vdmadmin -I -eventSyslog -enable -localOnly
```

Horizon 7 イベントの Syslog 出力を指定されたパスにダイレクトします。

```
vdmadmin -I -eventSyslog -enable -path <path>
```

Horizon 7 イベントの Syslog 出力を、認証されたドメイン ユーザーによるアクセスを必要とする指定されたパスにダイレクトします。

```
vdmadmin –I –eventSyslog –enable –path \\logserver\share\ViewEvents –user <mydomain\myuser>
 –password <mypassword>
```

-L オプションを使用した専用マシンの割り当て

vdmadmin コマンドと –L オプションを使用して、専用プールのマシンをユーザーに割り当てることができます。

構文

```
vdmadmin –L [–b <authentication_arguments>] –d <desktop> –m  <machine> –u <domain>\<user>
```

```
vdmadmin –L [–b <authentication_arguments>] –d <desktop> [–m <machine> | –u
<domain>\<user>] –r
```

使用上の注意

Horizon 7 は、ユーザーが初めて専用デスクトップ プールに接続するときに、そのユーザーにマシンを割り当てます。状況によっては、事前にマシンをユーザーに割り当てた方がよい場合があります。たとえば、ユーザーが最初に接続する前に、ユーザーのシステム環境を準備しておくことができます。Horizon 7 によって専用プールから割り当てられたリモート デスクトップにユーザーが接続すると、そのデスクトップをホストする仮想マシンは、その有効期間を通して同じユーザーに割り当てられたままになります。専用プールに属する単一のマシンにユーザーを割り当てることができます。

資格のある任意のユーザーにマシンを割り当てることができます。これは、接続サーバ インスタンス上での View LDAP データの損失から復旧する場合、または特定のマシンの所有権を変更する場合に行うことをお勧めします。

Horizon 7 によって専用プールから割り当てられたリモート デスクトップにユーザーが接続すると、そのリモート デスクトップは、デスクトップをホストする仮想マシンの有効期間を通して同じユーザーに割り当てられたままになります。ユーザーが組織を離れた場合、デスクトップへのアクセスが不要になった場合、または今後別のデスクトップ プールのデスクトップを使用する場合は、そのユーザーへのマシンの割り当てを削除する必要があることがあります。特定のデスクトップ プールにアクセスするすべてのユーザーへの割り当てを削除することもできます。

注 vdmadmin –L コマンドは、所有権を View Composer パーシステント ディスクに割り当てません。パーシステント ディスクを含むリンク クローン デスクトップをユーザーに割り当てるには、Horizon Administrator で [ユーザーの割り当て] メニュー オプションを使用します。

vdmadmin –L を使用してパーシステント ディスクを含むリンク クローン デスクトップをユーザーに割り当てる場合、状況によっては予期しない結果になる場合があります。たとえば、パーシステント ディスクを切断し、それを使用してデスクトップを再作成した場合、再作成されたデスクトップは元のデスクトップの所有者に割り当てられません。

オプション

次の表に、デスクトップをユーザーに割り当てたり、割り当てを削除したりするためのオプションを示します。

表 12-9. 専用デスクトップの割り当てのオプション

オプション	説明
–d <desktop>	デスクトップ プールの名前を指定します。
–m <machine>	リモート デスクトップをホストする仮想マシンの名前を指定します。
–r	指定したユーザーへの割り当て、または指定したマシンへのすべての割り当てを削除します。
–u <domain\user>	ユーザーのログイン名およびドメインを指定します。

例

デスクトップ プール dtpool1 のマシン machine2 を、CORP ドメインのユーザー Jo に割り当てます。

```
vdmadmin –L –d dtpool1 –m machine2 –u CORP\Jo
```

CORP ドメインのユーザー Jo に対する、プール dtpool1 のデスクトップの割り当てを削除します。

```
vdmadmin –L –d dtpool1 –u Corp\Jo –r
```

デスクトップ プール dtpool3 のマシン machine1 に対するユーザーの割り当てをすべて削除します。

```
vdmadmin –L –d dtpool3 –m machine1 –r
```

-M オプションを使用したマシンに関する情報の表示

vdmadmin コマンドと –M オプションを使用して、仮想マシンまたは物理コンピュータの構成に関する情報を表示できます。

構文

```
vdmadmin –M [–b< authentication_arguments>] [–m< machine> | [–u< domain\user>][–d<
desktop>]] [–xml | –csv] [–w | –n]
```

使用上の注意

このコマンドを実行すると、リモート デスクトップの基盤となる仮想マシンまたは物理コンピュータに関する情報が表示されます。

- マシンの表示名
- デスクトップ プールの名前

- マシンの状態

  マシンの状態は、UNDEFINED、PRE_PROVISIONED、CLONING、CLONINGERROR、CUSTOMIZING、READY、DELETING、MAINTENANCE、ERROR、LOGOUT のいずれかの値になります。

  このコマンドでは、Horizon Administrator では表示される **接続済み** や **切断されました** などのすべての動的なマシンの状態が表示されるわけではありません。
- 割り当てられているユーザーの SID
- 割り当てられているユーザーのアカウント名
- 割り当てられているユーザーのドメイン名
- 仮想マシンのインベントリ パス（該当する場合）
- マシンが作成された日付
- マシンのテンプレート パス（該当する場合）
- vCenter Server の URL（該当する場合）

オプション

次の表に、詳細を表示するマシンを指定するためのオプションを示します。

表 12-10. マシンに関する情報を表示するためのオプション

オプション	説明
–d <desktop>	デスクトップ プールの名前を指定します。
–m <machine>	仮想マシンの名前を指定します。
–u <domain\user>	ユーザーのログイン名およびドメインを指定します。

例

CORP ドメインのユーザー Jo に割り当てられているプール dtpool2 内のリモート デスクトップの基盤となるマシンに関する情報を表示し、出力の形式を ASCII 文字を使用した XML に設定します。

```
vdmadmin –M –u CORP\Jo –d dtpool2 –xml –n
```

マシン machine3 に関する情報を表示し、出力の形式をカンマ区切り値に設定します。

```
vdmadmin –M –m machine3 –csv
```

-M オプションを使用した仮想マシン上のディスク容量の再利用

vdmadmin コマンドと –M オプションを使用すると、リンク クローン仮想マシンをディスク容量再利用の対象として指定することができます。Horizon 7 は、リンク クローン OS ディスク上の未使用容量が Horizon Administrator で指定した最小しきい値に達するのを待たずに、ESXi ホストにその OS ディスク上のディスク容量を再利用するように指示します。

構文

```
vdmadmin –M [–b< authentication_arguments>] –d< desktop> –m< machine>
–markForSpaceReclamation
```

使用上の注意

このオプションを使用すると、デモまたはトラブルシューティングの目的で特定の仮想マシン上でディスク容量再利用を開始することができます。

停電期間が有効なときは、このコマンドを実行しても、容量の再利用は行われません。

vdmadmin コマンドと **–M** オプションを使用してディスク容量を再利用するには、以下の前提条件を満たしている必要があります。

- Horizon 7 が vCenter Server および ESXi バージョン 5.1 以降を使用していることを確認します。
- vSphere バージョン 5.1 以降で提供される VMware Tools が仮想マシンにインストールされていることを確認します。
- 仮想マシンが仮想ハードウェア バージョン 9 以降であることを確認します。
- Horizon Administrator で、vCenter Server に対して、[容量再利用を有効にする] オプションが選択されていることを確認します。「vSphere でリンク クローン仮想マシンのディスク領域を再利用できるようにする」を参照してください。
- Horizon Administrator で、デスクトップ プールに対して [VM ディスク スペースを再利用] オプションが選択されていることを確認します。『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントの「View Composer リンク クローンでのディスク容量の再利用」を参照してください。
- 容量再利用操作を開始する前に、仮想マシンがパワーオンされていることを確認します。
- 停電期間が有効でないことを確認します。『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントの「View Composer リンク クローン用の Storage Accelerator と領域再利用の停電期間の設定」を参照してください。

オプション

表 12-11. 仮想マシンのディスク容量を再利用するためのオプション

オプション	説明
–d <desktop>	デスクトップ プールの名前を指定します。
–m <machine>	仮想マシンの名前を指定します。
–MarkForSpaceReclamation	仮想マシンをディスク容量再利用の対象として指定します。

例

デスクトップ プール pool1 の仮想マシン machine3 を、ディスク容量再利用の対象として指定します。

```
vdmadmin –M –d pool1 –m machine3 –markForSpaceReclamation
```

-N オプションを使用したドメイン フィルタの構成

vdmadmin コマンドと –N オプションを使用して、Horizon 7 によって、エンド ユーザーからアクセス可能にするドメインを制御できます。

構文

```
vdmadmin –N [–b< authentication_arguments>] –domains {–exclude | –include | –search}
–domain <domain> –add [–s< connsvr>]
```

```
vdmadmin –N [–b<authentication_arguments>] –domains –list [–w | –n] [–xml]
```

```
vdmadmin –N [–b <authentication_arguments>] –domains –list –active [–w | –n] [–xml]
```

```
vdmadmin –N [–b< authentication_arguments>] –domains {–exclude | –include | –search}
–domain< domain >–remove [–s< connsvr>]
```

```
vdmadmin –N [–b< authentication_arguments>] –domains {–exclude | –include | –search}
–removeall [–s< connsvr>]
```

使用上の注意

–exclude、–include、または –search オプションのいずれかを指定して、それぞれ除外リスト、包含リスト、または検索除外リストに操作を適用します。

ドメインを検索除外リストに追加すると、そのドメインは自動ドメイン検索から除外されます。

ドメインを包含リストに追加すると、そのドメインは検索結果に含まれます。

ドメインを除外リストに追加すると、そのドメインは検索結果から除外されます。

オプション

次の表に、ドメイン フィルタを構成するためのオプションを示します。

表 12-12. ドメイン フィルタの構成のオプション

オプション	説明
–add	ドメインをリストに追加します。
–domain <domain>	フィルタ処理するドメインを指定します。 ドメインを指定する場合は、ドメインの DNS 名ではなく NetBIOS 名を使用する必要があります。
–domains	ドメイン フィルタ処理を指定します。
–exclude	除外リストへの操作を指定します。
–include	包含リストへの操作を指定します。
–list	各接続サーバ インスタンスと接続サーバ グループの検索除外リスト、除外リスト、および包含リストに構成されているドメインを表示します。
–list –active	コマンドを実行した接続サーバ インスタンスに使用可能なドメインを表示します。
–remove	ドメインをリストから削除します。
–removeall	すべてのドメインをリストから削除します。
–s <connsvr>	接続サーバ インスタンスのドメイン フィルタに操作を適用することを指定します。接続サーバ インスタンスは名前または IP アドレスで指定できます。 このオプションを指定しないと、検索構成に対して行った変更が、グループ内のすべて接続サーバ インスタンスに適用されます。
–search	検索除外リストへの操作を指定します。

例

接続サーバ インスタンス csvr1 の検索除外リストにドメイン FARDOM を追加します。

```
vdmadmin –N –domains –search –domain FARDOM –add –s csvr1
```

接続サーバ グループの除外リストにドメイン NEARDOM を追加します。

```
vdmadmin –N –domains –exclude –domain NEARDOM –add
```

グループ内の接続サーバ インスタンスとグループの両方のドメイン検索構成を表示します。

```
C:\ vdmadmin –N –domains –list

Domain Configuration
====================
Cluster Settings
   Include:
   Exclude:
   Search :
     FARDOM
     DEPTX
```

```
Broker Settings: CONSVR-1
   Include:
(*)Exclude:
     YOURDOM
   Search :

Broker Settings: CONSVR-2
   Include:
   Exclude:
   Search :
```

Horizon 7 によって、グループ内の各接続サーバ ホストでのドメイン検索が制限され、ドメイン FARDOM および DEPTX が除外されます。CONSVR-1 の除外リストの横にある文字 (*) は、CONSVR-1 でのドメイン検索の結果から Horizon 7 によって YOURDOM ドメインが除外されることを示しています。

ASCII 文字を使用した XML で、ドメイン フィルタを表示します。

```
vdmadmin -N -domains -list -xml -n
```

ローカル接続サーバ インスタンス上の Horizon 7 で使用できるドメインを表示します。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS:fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

ASCII 文字を使用した XML で、使用可能なドメインを表示します。

```
vdmadmin -N -domains -list -active -xml -n
```

接続サーバ グループの除外リストからドメイン NEARDOM を削除します。

```
vdmadmin -N -domains -exclude -domain NEARDOM -remove
```

接続サーバ インスタンス csvr1 の包含リストからすべてのドメインを削除します。

```
vdmadmin -N -domains -include -removeall -s csvr1
```

ドメイン フィルタの構成

ドメイン フィルタを構成して、接続サーバ インスタンスまたはセキュリティ サーバによって、エンド ユーザーからアクセス可能にするドメインを制限することができます。

Horizon 7 は、接続サーバ インスタンスまたはセキュリティ サーバが存在するドメインから始めて、信頼関係をたどってアクセスできるドメインを決定します。ドメインのセットが小さく、適切に接続されている場合、Horizon 7 は短時間でドメインの完全なリストを決定できますが、ドメインの数が増えたり、ドメイン間の接続が不十分であったりすると、この処理に要する時間は長くなります。Horizon 7 では、リモート デスクトップにログインしたユーザーに提供しない方がよいドメインも検索結果に含まれる場合があります。

ドメイン列挙の繰り返しを制御する Windows レジストリ キー（HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RecursiveDomainEnum）の値を以前に false に設定した場合は、ドメイン検索の繰り返しが無効になっているため、接続サーバ インスタンスによってプライマリ ドメインのみが使用されます。ドメインのフィルタ処理機能を使用するには、そのレジストリ キーを削除するか、値を true に設定して、システムを再起動します。このキーを設定したすべての接続サーバ インスタンスに対して、この操作を実行する必要があります。

次の表に、ドメインのフィルタ処理を構成するために指定できるドメイン リストのタイプを示します。

表 12-13. ドメイン リストのタイプ

ドメイン リストのタイプ	説明
検索除外リスト	自動検索中に Horizon 7 でたどることができるドメインを指定します。検索除外リストに含まれるドメインは検索で無視され、除外されたドメインに信頼されるドメインの特定は試行されません。プライマリ ドメインは検索から除外できません。
除外リスト	Horizon 7 でのドメイン検索の結果から除外するドメインを指定します。プライマリ ドメインは除外できません。
包含リスト	Horizon 7 でのドメイン検索の結果から除外しないドメインを指定します。その他のドメインは、プライマリ ドメイン以外すべて除外されます。

自動ドメイン検索では、検索除外リストで指定したドメインと、それらの除外ドメインに信頼されるドメイン以外のドメインのリストを取得します。Horizon 7 によって、空でない最初の除外リストまたは包含リストが次の順序で選択されます。

1 接続サーバ インスタンスに構成されている除外リスト

2 接続サーバ グループに構成されている除外リスト

3 接続サーバ インスタンスに構成されている包含リスト

4 接続サーバ グループに構成されている包含リスト

Horizon 7 によって最初に選択されたリストのみが検索結果に適用されます。

結果に含めるようにドメインを指定しても、そのドメインのドメイン コントローラに現在アクセスできない場合、そのドメインは Horizon 7 によりアクティブ ドメインのリストに含められません。

接続サーバ インスタンスまたはセキュリティ サーバが属するプライマリ ドメインは除外できません。

ドメインを含めるフィルタ処理の例

包含リストを使用して、Horizon 7 でのドメイン検索の結果から除外しないドメインを指定できます。その他のドメインは、プライマリ ドメイン以外すべて除外されます。

ある接続サーバ インスタンスがプライマリの MYDOM ドメインに属していて、YOURDOM ドメインとの信頼関係があるとします。YOURDOM ドメインには、DEPTX ドメインとの信頼関係があるとします。

この接続サーバ インスタンスについて、現在アクティブなドメインを表示します。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS: fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

DEPTY および DEPTZ ドメインがこのリストに表示されるのは、DEPTX ドメインに信頼されるドメインであるためです。

この接続サーバ インスタンスで、プライマリの MYDOM ドメイン以外に YOURDOM および DEPTX ドメインのみを使用可能にするように指定します。

```
vdmadmin -N -domains -include -domain YOURDOM -add
vdmadmin -N -domains -include -domain DEPTX -add
```

YOURDOM および DEPTX ドメインを含めた後、現在アクティブなドメインを表示します。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM
Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
```

Horizon 7 によって包含リストがドメイン検索の結果に適用されます。ドメイン階層が非常に複雑で、ネットワーク接続に問題のあるドメインがある場合は、ドメイン検索に時間がかかることがあります。そのような場合は、代わりに検索除外を使用します。

ドメイン除外のフィルタ処理の例

除外リストを使用して、Horizon 7 でのドメイン検索の結果から除外するドメインを指定できます。

CONSVR-1 および CONSVR-2 という 2 つの接続サーバ インスタンスのグループが、プライマリの MYDOM ドメインに属していて、YOURDOM ドメインとの信頼関係があるとします。YOURDOM ドメインには、DEPTX および FARDOM ドメインとの信頼関係があるとします。

FARDOM ドメインは地理的に離れた場所にあり、このドメインへのネットワーク接続は低速で高レイテンシーのリンクを経由しています。FARDOM ドメインのユーザーが MYDOM ドメインの接続サーバ グループにアクセスできるようにする必要はありません。

この接続サーバ グループのメンバーについて、現在アクティブなドメインを表示します。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-1)
============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS: fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

DEPTY および DEPTZ ドメインは DEPTX ドメインに信頼されるドメインです。

Horizon Client の接続パフォーマンスを向上させるために、接続サーバ グループによる検索から FARDOM ドメインを除外します。

```
vdmadmin -N -domains -search -domain FARDOM -add
```

検索から FARDOM ドメインを除外した後、次のコマンドを実行して現在アクティブなドメインを表示します。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-1)
============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

検索除外リストを拡張して、グループ内のすべての接続サーバ インスタンスでのドメイン検索から、DEPTX ドメインとそのドメインに信頼されるすべてのドメインを除外します。さらに、YOURDOM ドメインも CONSVR-1 で使用可能なドメインから除外します。

```
vdmadmin -N -domains -search -domain DEPTX -add
vdmadmin -N -domains -exclude -domain YOURDOM -add -s CONSVR-1
```

ドメイン検索の新しい構成を表示します。

```
C:\ vdmadmin -N -domains -list

Domain Configuration
====================
Cluster Settings
   Include:
```

```
   Exclude:
   Search :
     FARDOM
     DEPTX

Broker Settings: CONSVR-1
   Include:
(*)Exclude:
     YOURDOM
   Search :

Broker Settings: CONSVR-2
   Include:
   Exclude:
   Search :
```

Horizon 7 によって、グループ内の各接続サーバ ホストでのドメイン検索が制限され、ドメイン FARDOM および DEPTX が除外されます。CONSVR-1 の除外リストの横にある文字 (*) は、CONSVR-1 でのドメイン検索の結果から Horizon 7 によって YOURDOM ドメインが除外されることを示しています。

CONSVR-1 で、現在アクティブなドメインを表示します。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-1)
============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
```

CONSVR-2 で、現在アクティブなドメインを表示します。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-2)
============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
```

-O および -P オプションを使用して資格を持たないユーザーのマシンとポリシーを表示する

vdmadmin コマンドと –O および –P オプションを使用して、システムを使用する資格を失ったユーザーに割り当てられている仮想マシンとポリシーを表示できます。

構文

```
vdmadmin -O [-b< authentication_arguments>] [-ld | -lu] [-w | -n] [-xml [-noxslt |
-xsltpath< path>]]
```

```
vdmadmin -P [-b< authentication_arguments>] [-ld | -lu] [-w | -n] [-xml [-noxslt |
-xsltpath< path>]]
```

使用上の注意

通常の仮想マシンまたは物理システムに対するユーザーの資格を失効させても、関連付けられたリモート デスクトップの割り当ては自動的に失効しません。ユーザーのアカウントを一時的にサスペンドする場合やユーザーが長期休暇中の場合は、この状況でも問題がない可能性があります。資格を再度有効にすると、そのユーザーは以前と同じ仮想マシンを引き続き使用することができます。ユーザーが組織を離れた場合は、他のユーザーはその仮想マシンにアクセスできないため、その仮想マシンは実体なしとみなされます。資格のないユーザーに割り当てられているポリシーを調べることも必要になります。

オプション

次の表に、資格のないユーザーの仮想マシンとポリシーの表示に指定できるオプションを示します。

表 12-14. 資格のないユーザーのマシンおよびポリシーを表示するためのオプション

オプション	説明
-ld	出力エントリの順序をマシン別に設定します。
-lu	出力エントリの順序をユーザー別に設定します。
-noxslt	XML 出力にデフォルトのスタイルシートを適用しないことを指定します。
-xsltpath <path>	XML 出力を変換するために使用するスタイルシートのパスを指定します。

表 12-15 に、XML 出力を HTML に変換するために適用できるスタイルシートを示します。これらのスタイルシートは、ディレクトリ C:\Program Files\VMware\VMware View\server\etc にあります。

表 12-15. XSL スタイルシート

スタイルシート ファイル名	説明
unentitled-machines.xsl	ユーザーまたはシステム別にグループ化された、現在ユーザーに割り当てられている資格のない仮想マシンのリストを含むレポートを変換します。これはデフォルトのスタイルシートです。
unentitled-policies.xsl	資格のないユーザーに適用されているユーザー レベルのポリシーのある仮想マシンのリストを含むレポートを変換します。

例

資格のないユーザーに割り当てられている仮想マシンを仮想マシン別にグループ化して、テキスト形式で表示します。

```
vdmadmin -O -ld
```

資格のないユーザーに割り当てられている仮想マシンをユーザー別にグループ化して、ASCII 文字を使用した XML 形式で表示します。

```
vdmadmin -O -lu -xml -n
```

独自のスタイルシート `C:\tmp\unentitled-users.xsl` を適用して、出力をファイル `uu-output.html` にリダイレクトします。

```
vdmadmin -O -lu -xml -xsltpath "C:\tmp\unentitled-users.xsl" > uu-output.html
```

資格のないユーザーの仮想マシンに関連付けられているユーザー ポリシーをデスクトップ別にグループ化して、Unicode 文字を使用した XML 形式で表示します。

```
vdmadmin -P -ld -xml -w
```

独自のスタイルシート `C:\tmp\unentitled-policies.xsl` を適用して、出力をファイル `up-output.html` にリダイレクトします。

```
vdmadmin -P -ld -xml -xsltpath "C:\tmp\unentitled-policies.xsl" > up-output.html
```

-Q オプションを使用したキオスク モードのクライアントの構成

`vdmadmin` コマンドと `-Q` オプションを使用すると、キオスク モードのクライアントのデフォルト値を設定してアカウントを作成し、これらのクライアントの認証を可能にし、それらの構成に関する情報を表示することができます。

構文

```
vdmadmin –Q –clientauth –add [–b< authentication_arguments>] –domain<
domain_name>–clientid< client_id> [–password "<password>" | –genpassword] [–ou< DN>]
[–expirepassword | –noexpirepassword] [–group <group_name> | –nogroup] [–description
"<description_text>"]
```

```
vdmadmin –Q –disable [–b< authentication_arguments>] –s< connection_server>
```

```
vdmadmin –Q –enable [–b< authentication_arguments>] –s< connection_server>
[–requirepassword]
```

```
vdmadmin –Q –clientauth –getdefaults [–b<authentication_arguments>] [–xml]
```

```
vdmadmin –Q –clientauth –list [–b<authentication_arguments>] [–xml]
```

```
vdmadmin –Q –clientauth –remove [–b< authentication_arguments>] –domain<
domain_name>–clientid< client_id>
```

```
vdmadmin –Q –clientauth –removeall [–b<authentication_arguments>] [–force]
```

```
vdmadmin –Q –clientauth –setdefaults [–b< authentication_arguments>] [–ou< DN>]
[ –expirepassword | –noexpirepassword ] [–group< group_name> | –nogroup]
```

```
vdmadmin –Q –clientauth –update [–b< authentication_arguments>] –domain<
domain_name>–clientid< client_id> [–password "<password>" | –genpassword] [–description
"<description_text>"]
```

使用上の注意

vdmadmin コマンドは、クライアントがリモート デスクトップへの接続用に使用する接続サーバ インスタンスと同じグループに属するいずれかの接続サーバ インスタンスで実行する必要があります。

パスワード有効期限および Active Directory グループ メンバーシップのデフォルト値を構成すると、これらの設定は同じグループに属するすべての接続サーバ インスタンス間で共有されます。

キオスク モードのクライアントを追加すると、Horizon 7 はそのクライアントのユーザー アカウントを Active Directory に作成します。クライアントの名前を指定する場合は、文字列「custom-」、または ADAM で定義可能な別の文字列で始まる 20 文字以内の名前にする必要があります。指定した各名前は 1 台のクライアント デバイスでのみ使用します。

「custom-」の代わりに使用するプリフィックスは、接続サーバ インスタンスの ADAM 内の **cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int** で、**pae-ClientAuthPrefix** 複数値属性で定義できます。これらプレフィックスを通常のユーザー アカウントと一緒に使用しないようにしてください。

クライアントの名前を指定しない場合、Horizon 7 はクライアント デバイス用に指定した MAC アドレスから名前を生成します。たとえば、MAC アドレスが 00:10:db:ee:76:80 の場合、対応するアカウント名は cm-00_10_db_ee_76_80 になります。これらのアカウントは、クライアントの認証を有効にする接続サーバ インスタンスでのみ使用できます。

一部のシン クライアントは、キオスク モードで使用されるアカウント名として、文字列「custom-」または「cm-」で始まるもののみ許可しています。

自動生成されるパスワードは長さが 16 文字で、大文字、小文字、記号、および数字をそれぞれ 1 文字以上含み、同じ文字を繰り返し含めることができます。より強力なパスワードが必要な場合は、**–password** オプションを使用してパスワードを指定する必要があります。

–group オプションを使用してグループを指定するか、以前にデフォルトのグループを設定している場合は、Horizon 7 がこのグループにクライアントのアカウントを追加します。**–nogroup** オプションを指定して、アカウントがグループに追加されないようにすることができます。

接続サーバ インスタンスでキオスク モードのクライアントを認証できるようにする場合は、オプションでクライアントがパスワードを入力する必要があることを指定できます。認証を無効にすると、クライアントはリモート デスクトップに接続できません。

個別の接続サーバ インスタンスに対して認証を有効または無効にできますが、グループ内のすべての接続サーバ インスタンスがクライアント認証に関する他のすべての設定を共有します。グループ内のすべての接続サーバ インスタンスに対しクライアントを 1 回追加するだけで、クライアントからの要求を受け付けることができるようになります。

認証を有効にする場合に **–requirepassword** オプションを指定すると、接続サーバ インスタンスは自動生成パスワードを使用するクライアントを認証できません。接続サーバ インスタンスの構成を変更してこのオプションを指定すると、そのようなクライアントは認証されず、「**不明なユーザー名または不正確なパスワード**」というエラー メッセージが表示されて認証に失敗します。

オプション

次の表に、キオスク モードのクライアントを構成するためのオプションを示します。

表 12-16. キオスク モードのクライアントの構成のオプション

オプション	説明
–add	キオスク モードのクライアントのアカウントを追加します。
–clientauth	キオスク モードのクライアントの認証を構成する操作を指定します。
–clientid <client_id>	クライアントの名前または MAC アドレスを指定します。
–description "<description_text>"	クライアント デバイスのアカウントの説明を Active Directory に作成します。
–disable	指定した接続サーバ インスタンスでのキオスク モードのクライアントの認証を無効にします。

表 12-16. キオスク モードのクライアントの構成のオプション (続き)

オプション	説明
–domain <domain_name>	クライアント デバイスのアカウントのドメインを指定します。
–enable	指定した接続サーバ インスタンスでのキオスク モードのクライアントの認証を有効にします。
–expirepassword	クライアント アカウントのパスワード有効期限に、接続サーバ グループの有効期限と同じ値を指定します。グループでパスワード有効期限が定義されていない場合、パスワードは無期限になります。
–force	キオスク モードのクライアントのアカウントを削除する場合に、確認のプロンプトを無効にします。
–genpassword	クライアント アカウントのパスワードを生成します。これは、–password も –genpassword も指定しない場合のデフォルトの動作です。
–getdefaults	クライアント アカウントの追加に使用されるデフォルト値を取得します。
–group <group_name>	クライアント アカウントを追加するデフォルト グループの名前を指定します。グループの名前は、Active Directory の Windows 2000 以前のグループ名として指定する必要があります。
–list	キオスク モードのクライアントと、キオスク モードのクライアントの認証を有効にした接続サーバ インスタンスに関する情報を表示します。
–noexpirepassword	アカウントのパスワードを無期限にすることを指定します。
–nogroup	クライアントのアカウントを追加する場合は、クライアントのアカウントをデフォルト グループに追加しないことを指定します。 クライアントのデフォルト値を設定する場合は、デフォルト グループの設定をクリアします。
–ou <DN>	クライアント アカウントを追加する組織単位の識別名を指定します。 例： OU=kiosk-ou,DC=myorg,DC=com 注 –setdefaults オプションを使用して組織単位の構成を変更することはできません。
–password "<password>"	クライアント アカウントの明示的パスワードを指定します。
–remove	キオスク モードのクライアントのアカウントを削除します。
–removeall	キオスク モードのすべてのクライアントのアカウントを削除します。
–requirepassword	キオスク モードのクライアントはパスワードを入力する必要があることを指定します。Horizon 7 は新しい接続に対して生成されたパスワードを受け付けません。
–s <connection_server>	キオスク モードのクライアントの認証を有効または無効にする接続サーバ インスタンスの NetBIOS 名を指定します。
–setdefaults	クライアント アカウントの追加に使用されるデフォルト値を設定します。
–update	キオスク モードのクライアントのアカウントを更新します。

例

クライアントの組織単位、パスワード有効期限、およびグループ メンバーシップのデフォルト値を設定します。

```
vdmadmin –Q –clientauth –setdefaults –ou "OU=kiosk–ou,DC=myorg,DC=com" –noexpirepassword –
group kc–grp
```

クライアントの現在のデフォルト値をテキスト形式で取得します。

```
vdmadmin –Q –clientauth –getdefaults
```

クライアントの現在のデフォルト値を XML 形式で取得します。

```
vdmadmin –Q –clientauth –getdefaults –xml
```

MAC アドレスで指定されたクライアントのアカウントを MYORG ドメインに追加し、グループ kc-grp のデフォルト設定を使用します。

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –group kc–grp
```

MAC アドレスで指定されたクライアントのアカウントを MYORG ドメインに追加し、自動生成されたパスワードを使用します。

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –genpassword –ou
"OU=kiosk–ou,DC=myorg,DC=com" –group kc–grp
```

クライアントの名前を指定してアカウントを追加し、そのクライアントで使用するパスワードを指定します。

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Terminal21 –password "guest" –ou
"OU=kiosk–ou,DC=myorg,DC=com" –description "Terminal 21"
```

新しいパスワードと説明のテキストを指定してクライアントのアカウントを更新します。

```
vdmadmin –Q –clientauth –update –domain MYORG –clientid custom–Terminal21 –password
"Secret1!" –description "Foyer Entry Workstation"
```

MAC アドレスで指定されたキオスク クライアントのアカウントを MYORG ドメインから削除します。

```
vdmadmin –Q –clientauth –remove –domain MYORG –clientid 00:10:db:ee:54:12
```

削除の確認を求めずに、すべてのクライアントのアカウントを削除します。

```
vdmadmin –Q –clientauth –removeall –force
```

接続サーバ インスタンス csvr-2 に対しクライアントの認証を有効にします。自動生成されたパスワードを使用するクライアントの場合、パスワードを入力せず認証できます。

```
vdmadmin –Q –enable –s csvr–2
```

接続サーバ インスタンス csvr-3 に対しクライアントの認証を有効にして、パスワードを Horizon Client に指定するようクライアントに要求します。自動生成されたパスワードを使用するクライアントは認証されません。

```
vdmadmin –Q –enable –s csvr–3 –requirepassword
```

接続サーバ インスタンス csvr-1 に対しクライアントの認証を無効にします。

```
vdmadmin –Q –disable –s csvr–1
```

クライアントについての情報をテキスト形式で表示します。クライアント cm-00_0c_29_0d_a3_e6 のパスワードは自動生成されており、エンド ユーザーまたはアプリケーション スクリプトにはこのパスワードを Horizon Client に指定する必要はありません。クライアント cm-00_22_19_12_6d_cf のパスワードは明示的に指定されており、エンド ユーザーはこのパスワードを入力する必要があります。接続サーバ インスタンス CONSVR2 は、自動生成されたパスワードを使用するクライアントからの認証要求を受け付けます。CONSVR1 は、キオスク モードのクライアントからの認証要求を受け付けません。

```
C:\ vdmadmin –Q –clientauth –list
Client Authentication User List
================================
GUID              : 94be6344–0c9b–4a92–8d54–1brc1c2dc282
ClientID          : cm–00_0c_29_0d_a3_e6
Domain            : myorg.com
Password Generated: true

GUID              : 471d9d35–68b2–40ee–b693–56a7d92b2e25
ClientID          : cm–00_22_19_12_6d_cf
Domain            : myorg.com
Password Generated: false

Client Authentication Connection Servers
========================================
Common Name                   : CONSVR1
Client Authentication Enabled : false
Password Required             : false

Common Name                   : CONSVR2
Client Authentication Enabled : true
Password Required             : false
```

-R オプションを使用したマシンの最初のユーザーの表示

vdmadmin コマンドと –R オプションを使用して、管理対象仮想マシンの初期の割り当てを確認できます。たとえば、LDAP データが失われた場合、仮想マシンを再度ユーザーに割り当てるためにこの情報が必要になることがあります。

注　vdmadmin コマンドでの –R オプションの使用は、View Agent 5.1 より前の仮想マシンでのみ動作します。View Agent 5.1 以降および Horizon Agent 7.0 以降のバージョンが実行される仮想マシンでは、このオプションは動作しません。仮想マシンの最初のユーザーを検索するには、イベント データベースを使用してマシンにログインしたユーザーを指定します。

構文

```
vdmadmin –R –i <network_address>
```

使用上の注意

特権ユーザーとして、–b オプションを使用してこのコマンドを実行することはできません。**管理者**ロールを持つユーザーとしてログインします。

オプション

–i オプションで、仮想マシンの IP アドレスを指定します。

例

IP アドレス 10.20.34.120 の仮想マシンに最初にアクセスしたユーザーを表示します。

```
vdmadmin –R –i 10.20.34.120
```

-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

vdmadmin コマンドと –S オプションを使用して、接続サーバ インスタンスまたはセキュリティ サーバのエントリを Horizon 7 の構成から削除できます。

構文

```
vdmadmin –S [–b< authentication_arguments>] –r –s< server>
```

使用上の注意

高可用性を確保するため、Horizon 7 では接続サーバ グループ内に 1 つ以上のレプリカの接続サーバ インスタンスを構成できます。グループの接続サーバ インスタンスを無効にしても、そのサーバのエントリは Horizon 7 の構成内に存続します。

また、vdmadmin コマンドと –S オプションを使用して、セキュリティ サーバを Horizon 7 環境から削除することもできます。セキュリティ サーバを恒久的に削除せずにアップグレードまたは再インストールする予定がある場合は、このオプションを使用する必要はありません。

恒久的に削除するには、次のタスクを実行します。

1 接続サーバ インストーラを実行して、Windows Server コンピュータから接続サーバ インスタンスまたはセキュリティ サーバをアンインストールします。

2 プログラムの追加と削除 ツールを実行して、Windows Server コンピュータから Adam Instance VMwareVDMDS プログラムを削除します。

3 別の接続サーバ インスタンスで、vdmadmin コマンドを使用して、アンインストールした接続サーバ インスタンスまたはセキュリティ サーバのエントリを構成から削除します。

元のグループの Horizon 7 構成を複製しないで、削除したシステムに Horizon 7 を再インストールする場合は、再インストールを実行する前に、元のグループのすべての接続サーバ ホストを再起動します。これにより、再インストールされた接続サーバ インスタンスは元のグループから構成の更新を受け取りません。

オプション

–s オプションは、削除する接続サーバ インスタンスまたはセキュリティ サーバの NetBIOS 名を指定します。

例

接続サーバ インスタンス connsvr3 のエントリを削除します。

```
vdmadmin –S –r –s connsvr3
```

-T オプションの使用による管理者の 2 番目の認証情報の提供

vdmadmin コマンドを使用するときに –T オプションを指定すると、Active Directory の 2 番目の認証情報を管理者ユーザーに提供できます。

構文

```
vdmadmin –T [–b< authentication_arguments>] –domainauth
 {–add | –update | –remove | –removeall | –list} –owner <domain\user> –user
<domain\user> [–password <password>]
```

使用上の注意

接続サーバ ドメインと一方向の信頼関係を持つドメイン内にユーザーとグループが存在する場合は、Horizon Administrator で管理者ユーザーの 2 番目の認証情報を指定する必要があります。2 番目の認証情報がないと、管理者は一方向で信頼されているドメインへのアクセス権を付与できません。一方向で信頼されているドメインは、外部ドメインまたは推移的なフォレストの信頼のドメインになります。

2 番目の認証情報は、エンド ユーザーのデスクトップまたはアプリケーション セッションではなく、Horizon Administrator セッションでのみ必要になります。2 番目の認証情報が必要なのは管理者ユーザーだけです。

2 番目の認証情報をユーザーごとに構成するには、`vdmadmin` コマンドを使用します。グローバルに指定された 2 番目の認証情報を構成することはできません。

フォレストの信頼の場合、通常はフォレストのルート ドメインのみに 2 番目の認証情報を構成します。こうすることで、接続サーバはフォレストの信頼の子ドメインを列挙できるようになります。

一方向で信頼されているドメインのユーザーが最初にログオンした場合にのみ、Active Directory アカウントのロック、無効化、およびログオン時間のチェックを実行できます。

ユーザーの PowerShell 管理およびスマート カード認証は、一方向で信頼されているドメインではサポートされません。一方向で信頼されているドメインのユーザーの SAML 認証はサポートされません。

2 番目の認証情報のアカウントには次の権限が必要です。標準のユーザー アカウントには、デフォルトでこれらの権限が付与されています。

- 内容の一覧表示
- すべてのプロパティの読み取り
- アクセス許可の読み取り
- tokenGroupsGlobalAndUniversal の読み取り（[すべてのプロパティの読み取り] により暗黙に含まれる）

制限

- 一方向で信頼されているドメインでのユーザーのスマート カード認証および PowerShell 管理はサポートされません。
- 一方向で信頼されているドメインのユーザーの SAML 認証はサポートされません。

オプション

表 12-17. 2 番目の認証情報を提供するためのオプション

オプション	説明
–add	所有者アカウントの 2 番目の認証情報を追加します。 Windows ログインが実行され、指定した認証情報が有効かどうかが検証されます。View LDAP のユーザーに対して Foreign Security Principal (FSP) が作成されます。
–update	所有者アカウントの 2 番目の認証情報を更新します。 Windows ログインが実行され、更新済みの認証情報が有効かどうかが検証されます。
–list	所有者アカウントのセキュリティ認証情報を表示します。パスワードは表示されません。
–remove	所有者アカウントからセキュリティ認証情報を削除します。
–removeall	所有者アカウントからセキュリティ認証情報をすべて削除します。

例

指定した所有者アカウントの 2 番目の認証情報を追加します。Windows ログインが実行され、指定した認証情報が有効かどうかが検証されます。

```
vdmadmin –T –domainauth –add –owner <domain\user> –user <domain\user> –password <password>
```

指定した所有者アカウントの 2 番目の認証情報を更新します。Windows ログインが実行され、更新済みの認証情報が有効かどうかが検証されます。

```
vdmadmin –T –domainauth –update –owner <domain\user> –user <domain\user> –password <password>
```

指定した所有者アカウントの 2 番目の認証情報を削除します。

```
vdmadmin –T –domainauth –remove –owner <domain\user> –user <domain\user>
```

指定した所有者アカウントの 2 番目の認証情報をすべて削除します。

```
vdmadmin –T –domainauth –removeall –owner <domain\user>
```

指定した所有者アカウントの 2 番目の認証情報をすべて表示します。パスワードは表示されません。

```
vdmadmin –T –domainauth –list –owner <domain\user>
```

-U オプションを使用したユーザーに関する情報の表示

vdmadmin コマンドと –U オプションを使用して、ユーザーに関する詳細情報を表示できます。

構文

```
vdmadmin
–U [–b< authentication_arguments>] –u< domain\user> [–w | –n] [–xml]
```

使用上の注意

このコマンドは、Active Directory および Horizon 7 から取得したユーザーに関する情報を表示します。

- Active Directory から取得したユーザーのアカウントの詳細
- Active Directory グループのメンバーシップ
- マシンに対する資格（マシン ID、表示名、説明、フォルダ、およびマシンが無効になっているかどうかなど）
- ThinApp 割り当て
- 管理者のロール（ユーザーの管理者権限、その権限が付与されているフォルダなど）

オプション

–u オプションは、ユーザーの名前およびドメインを指定します。

例

ASCII 文字を使用した XML で、CORP ドメインのユーザー Jo に関する情報を表示します。

```
vdmadmin –U –u CORP\Jo –n –xml
```

-V オプションを使用した仮想マシンのロック解除またはロック

vdmadmin コマンドと **–V** オプションを使用して、データセンター内の仮想マシンをロック解除またはロックできます。

構文

```
vdmadmin –V [–b <authentication_arguments>] –e –d <desktop> –m <machine> [–m< machine>] ...
```

```
vdmadmin –V [–b <authentication_arguments>] –e –vcdn <vCenter_dn> –vmpath< inventory_path>
```

```
vdmadmin –V [–b< authentication_arguments>] –p –d< desktop >–m< machine> [–m <machine>] ...
```

```
vdmadmin –V [–b< authentication_arguments>] –p –vcdn <vCenter_dn> –vmpath< inventory_path>
```

使用上の注意

vdmadmin コマンドは、リモート デスクトップを不正な状態にする問題が発生した場合に、仮想マシンをロック解除またはロックするためにのみ使用してください。正常に動作しているリモート デスクトップを管理する目的ではこのコマンドを使用しないでください。

リモート デスクトップがロックされ、その仮想マシンのエントリが ADAM に存在しなくなった場合は、–vmpath および –vcdn オプションを使用して、仮想マシンおよび vCenter Server のインベントリ パスを指定します。vCenter Server Client を使用して、Home/Inventory/VMs and Templates の下にリモート デスクトップの仮想マシンのインベントリ パスを見つけることができます。ADAM ADSI Edit を使用して、OU=Properties 見出しの下に vCenter Server の識別名を見つけることができます。

オプション

次の表に、仮想マシンをロック解除またはロックするためのオプションを示します。

表 12-18. 仮想マシンをロック解除またはロックするためのオプション

オプション	説明
–d <desktop>	デスクトップ プールを指定します。
–e	仮想マシンをロック解除します。
–m <machine>	仮想マシンの名前を指定します。
–p	仮想マシンをロックします。
–vcdn <vCenter_dn>	vCenter Server の識別名を指定します。
–vmpath <inventory_path>	仮想マシンのインベントリ パスを指定します。

例

デスクトップ プール dtpool3 の仮想マシン machine1 および machine2 のロックを解除します。

```
vdmadmin –V –e –d dtpool3 –m machine1 –m machine2
```

デスクトップ プール dtpool3 の仮想マシン machine3 をロックします。

```
vdmadmin –V –p –d dtpool3 –m machine3
```

-X オプションを使用して LDAP エントリおよびスキーマの競合を検出して解決する

vdmadmin コマンドの –X オプションを使用すると、グループ内の複製接続サーバ インスタンスで発生している LDAP エントリ競合および LDAP スキーマ競合を検出して解決することができます。また、クラウド ポッド アーキテクチャ 環境内の LDAP スキーマ競合の検出と解決を行うこともできます。

構文

```
vdmadmin -X [-b <authentication_arguments>] -collisions [-resolve]
vdmadmin -X [-b <authentication_arguments>] -schemacollisions [-resolve] [-global]
```

使用上の注意

重複する LDAP エントリが複数の接続サーバ インスタンス上に作成された場合、Horizon 7 内の LDAP データの整合性に問題が発生する可能性があります。この競合状態は、アップグレード中、LDAP レプリケーションが機能していないときに発生する可能性があります。競合状態が発生しているかどうかは Horizon 7 によって定期的にチェックされますが、`vdmadmin` コマンドをグループ内のいずれかの接続サーバ インスタンスで実行することで LDAP エントリの競合を手動で検出して解決することもできます。

また、LDAP スキーマの競合も同様に、アップグレード中、LDAP レプリケーションが機能していないときに発生する可能性があります。Horizon 7 はスキーマの競合状態が発生しているかについてはチェックしないため、LDAP スキーマの競合は `vdmadmin` コマンドを実行して手動で検出と解決を行う必要があります。

オプション

次の表に、LDAP エントリ競合の検出と解決を指定できるオプションを示します。

表 12-19. LDAP エントリ競合の検出および解決を行うオプション

オプション	説明
`-collisions`	接続サーバ グループ内の LDAP エントリ競合の検出を指定します。
`-resolve`	LDAP インスタンス内のすべての LDAP 競合を解決します。このオプションを指定しないと、問題を一覧表示するだけで、解決は行われません。

次の表に、LDAP スキーマ競合の検出と解決に指定できるオプションを示します。

表 12-20. LDAP スキーマ競合の検出および解決を行うオプション

オプション	説明
`-schemacollisions`	接続サーバ グループまたは クラウド ポッド アーキテクチャ 環境内の LDAP スキーマ競合の検出を指定します。
`-resolve`	LDAP インスタンス内のすべての LDAP スキーマ競合を解決します。このオプションを指定しないと、問題を一覧表示するだけで、解決は行われません。
`-global`	クラウド ポッド アーキテクチャ 環境下のグローバルの LDAP インスタンスにチェックと修正を適用します。このオプションを指定しないと、チェックはローカルの LDAP インスタンスに対して実行されます。

例

接続サーバ グループ内の LDAP エントリ競合を検出します。

```
vdmadmin –X –collisions
```

ローカルの LDAP インスタンスの LDAP エントリ競合を検出して解決します。

```
vdmadmin –X –collisions –resolve
```

グローバルの LDAP インスタンスの LDAP スキーマ競合を検出して解決します。

```
vdmadmin –X –schemacollisions –resolve –global
```