Horizon Console の管理

2019 年 12 月
VMware Horizon 7 7.11

vmware®

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

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

ヴ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

VMware Horizon Console の管理

1

『VMware Horizon Console の管理』では、Horizon Console で VMware Horizon® 7 の構成と管理、管理者の作成、ユーザー認証の設定、ポリシーの構成、管理タスクを行う方法を説明します。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。

Horizon Console を使用して クラウド ポッド アーキテクチャ 環境の設定と管理を行う方法については、『Horizon 7 でのクラウド ポッド アーキテクチャの管理』を参照してください。

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。

VMware Horizon Console の使用

2

VMware Horizon Console は、Web インターフェイスの最新バージョンで、仮想デスクトップや公開デスクトップとアプリケーションを作成したり、管理することができます。また、Horizon Console には、VMware Horizon Just-in-Time Management Platform (JMP) 統合ワークフロー機能が統合され、ワークスペースの管理を行うことができます。

Horizon Console は、Horizon Connection Server をインストールして構成した後に使用できます。

JMP 統合ワークフロー機能の詳細については、10 章 JMP Integrated Workflow スタート ガイド を参照してください。

この章には、次のトピックが含まれています。

- サポートされている Horizon 7 機能
- Horizon Console を使用する利点
- Horizon Console のインストールと構成
- Horizon Console へのログイン

サポートされている Horizon 7 機能

Horizon Console は HTML5 技術をベースにしており、Horizon 7 環境全体を管理できます。Horizon Console は、Flash ベースの Horizon Administrator に代わるものです。

Horizon Administrator でサポートされている Horizon 7 機能の詳細については、Horizon 7 の管理ドキュメントを参照してください。

次の機能がサポートされています。

- サーバ
  - Horizon Connection Server の設定
  - イベント データベース
- 資格
  - ユーザーとグループに対する資格
  - デスクトップに対する資格

    - アプリケーションに対する資格
    - グローバル資格
    - グローバル ポリシー
- 認証
    - リモート アクセス認証
    - 公開アプリケーションでの非認証アクセス
    - スマート カード認証
    - ロールベースの委任管理
- 仮想デスクトップ
    - フル仮想マシンの自動専用割り当てプール
    - 自動、インスタント クローン専用割り当て、フローティング割り当てプール
    - 自動化されたリンク クローン デスクトップ プール
    - フル仮想マシンの自動フローティング割り当てプール
    - 手動デスクトップ プール
    - 通常ディスク
- 公開デスクトップ
    - 手動ファーム
    - 自動インスタント クローン ファーム
    - 自動リンク クローン ファーム
    - RDS デスクトップ プール
- 公開アプリケーション
    - 手動アプリケーション プール
    - 既存のアプリケーションのアプリケーション プール
- 仮想マシン
    - vCenter Server で使用可能な仮想マシン
    - vCenter Server で使用できない登録済みのマシン
- クラウド ポッド アーキテクチャ

次の機能はサポートされていません。

- ThinApp アプリケーション
- セキュリティ サーバ
- Mirage サーバ

Horizon Console を使用する利点

Horizon Console を使用すると、デスクトップやアプリケーションのデプロイが簡単になり、ジャストイン タイムのデスクトップ配信が可能になります。セキュリティ リスクを回避するため、より安全な Web インターフェイスも利用できます。

Horizon Console Web インターフェイスを更新すると、使いやすいワークロードを使用して、デスクトップとアプリケーションのデプロイやトラブルシューティングを行うことができます。

Horizon Console には、インスタント クローン、VMware App Volumes、VMware Dynamic Environment Manager テクノロジーを統合ワークフローに組み込む JMP Integrated Workflow 機能も含まれます。この機能を使用すると、オンデマンド デスクトップをすばやくデプロイし、スケーリングできます。詳細については、 JMP Integrated Workflow のバージョン情報を参照してください。

Horizon Console には HTML5 ベースの Web インターフェイスが用意されています。これにより、安全性を強化し、多くのセキュリティ リスクと脆弱性を排除できます。

Horizon Console のインストールと構成

Horizon Connection Server インストーラを使用して Connection Server をインストールして構成すると、Horizon Administrator の Web インターフェイスで Horizon Console URL を使用できます。JMP Server インストーラを使用して JMP Server をインストールして構成すると、Horizon Console で JMP Integrated Workflow を使用できます。

Connection Server のインストールに関する詳細については、『Horizon 7 のインストール』ドキュメントを参照してください。

JMP Server のインストールと設定の詳細については、『VMware Horizon JMP Server 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。

Horizon Console へのログイン

デスクトップまたはアプリケーションのデプロイ タスク、トラブルシューティング タスク、JMP ワークフローの管理を実行するには、Horizon Console にログインする必要があります。Horizon Console には、安全な接続 (TLS) を使用してアクセスします。

前提条件

- Horizon Connection Server 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 Console にログインするには、事前定義ロールか、事前定義ロールの組み合わせをユーザーに割り当てる必要があります。ユーザーにカスタム ロールが割り当てられているか、事前定義ロールとカスタム ロールの組み合わせが割り当てられている場合、Horizon Console にログインすることはできません。ロールベースのアクセスの設定については、ロールベースの委任管理の構成を参照してください。
- Horizon Console 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。サポート対象 Web ブラウザの詳細については、Horizon 7 のインストールドキュメントを参照してください。

手順

1 Web ブラウザを開き、次の URL を入力します。*server* は、Connection Server 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 Connection Server 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、Connection Server 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 Console へのアクセスは、Connection Server 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。

Connection Server 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
Connection Server 用に CA によって署名された証明書を構成しています。	初めて接続するときに、Web ブラウザに [VMware Horizon 7 へようこそ] ページが表示されます。
Connection Server 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 Horizon Console のログイン ページを常に使用するには、[このオプションを常に使用] をクリックします。

注： [このオプションを常に使用] をクリックして [起動] をクリックすると、次に Web ブラウザでタブを開いて **`https://server/admin`** を入力したときに、Horizon Console ログイン ページが常に表示されます。[VMware Horizon 7 へようこそ] ページにアクセスするには、**`https://server/admin/#home`** に移動します。

3 Horizon Console の [起動] をクリックして、Horizon Console のログイン ページを開きます。

4 管理者アカウントにアクセスするための認証情報を持つユーザーとしてログインします。

スタンドアローンの Connection Server 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 Connection Server 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、Connection Server 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。

次のステップ

使用している Connection Server の CPA ポッドまたはクラスタ名を特定するには、Horizon Console ヘッダーと Web ブラウザ タブで名前を確認します。

Horizon Console での Horizon Connection Server の設定

3

Horizon Connection Server 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 Horizon 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。

この章には、次のトピックが含まれています。

Horizon Console での vCenter Server と Horizon Composer の設定

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 Horizon 7 を設定する必要があります。リンク クローン デスクトップ プールを作成して管理するには、Horizon Console で Horizon Composer の設定を行う必要があります。

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 Horizon Storage Accelerator を有効にする必要があります。

Horizon Composer Active Directory 操作のユーザー アカウントの作成

Horizon Composer を使用する場合は、Horizon Composer が Active Directory で特定の操作を行えるよう、Active Directory 内にユーザー アカウントを 1 つ作成する必要があります。Horizon 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。

セキュリティを維持するため、Horizon Composer で使用するユーザー アカウントを別に作成します。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、Horizon 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、Connection Server 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。

次のステップ

[vCenter Server を追加] ウィザードで Horizon 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 プールを構成してデプロイする際に、Horizon Console でこのアカウントを指定します。

Horizon Console での製品のライセンス キーのインストール

Connection Server を使用するには、まず製品のライセンス キーを入力する必要があります。

注： Horizon 7 サブスクリプションのライセンスがある場合、製品のライセンス キーは必要ありません。サブスクリプション ライセンスの詳細については、『Horizon 7 のインストール』の「サブスクリプション ライセンスでの Horizon 7 の有効化」を参照してください。

Horizon Console に初めてログインすると、[ライセンスと使用状況] ペインが表示されます。

複製された Connection Server インスタンスまたはセキュリティ サーバをインストールするときは、ライセンス キーを設定する必要はありません。複製されたインスタンスとセキュリティ サーバは、View の LDAP 構成に格納されている共通ライセンス キーを使用します。

注： Connection Server には有効なライセンス キーが必要です。プロダクト ライセンス キーは 25 文字のキーです。

手順

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

2 [ライセンスの設定] パネルで、[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。

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。

Horizon Console での 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 (TLS) を使用して vCenter Server インスタンスに接続します。

前提条件

- Connection Server 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。Horizon 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 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 Connection Server 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、Connection Server 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 Horizon 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。

手順

1. Horizon Console で、[設定] - [サーバ] の順に移動します。
2. [vCenter Server] 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 （オプション）VMware Cloud on AWS に vCenter Server がデプロイされている場合は、[VMware Cloud on AWS] を選択します。

VMware Cloud on AWS と Horizon 7 の統合の詳細については、『Horizon 7 の統合』を参照してください。

9 [詳細設定] で、vCenter Server と Horizon Composer の同時操作の制限数を設定します。

10 [次へ] をクリックし、指示に従ってウィザードを完了します。

次のステップ

Horizon Composer の設定を行います。

- vCenter Server インスタンスが署名された TLS 証明書で設定されていて、Connection Server 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 [Horizon 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。

Horizon Composer の設定

Horizon Composer を使用するには、Horizon 7 が Horizon Composer サービスに接続できるように設定する必要があります。Horizon 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 Horizon 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 Horizon 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 Horizon Composer サービスにのみ関連付けることができます。

Horizon 7 の初期デプロイが完了した後で、Horizon 7 環境の拡張または変更に対応できるように Horizon Composer サービスを新しいホストに移行できます。初期の Horizon Composer 設定は Horizon Console 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。

前提条件

- 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。Horizon Composer Active Directory 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。 Horizon Console での 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 Horizon 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 Console で、[設定] - [サーバ] の順に移動します。

2 [vCenter Server] タブで [追加] をクリックします。[vCenter Server 設定] ページで、vCenter Server の情報を入力し、[次へ] をクリックします。

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

[Horizon Composer を使用しない] を選択した場合、その他の Horizon 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。

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

オプション	説明
Horizon Composer が vCenter Server と同じホストにインストールされます。	a [Horizon 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 Horizon 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。
Horizon Composer が個別のホストにインストールされます。	a [スタンドアローンの Horizon Composer Server] を選択します。 b Horizon Composer Server アドレスのテキスト ボックスに、Horizon Composer ホストの完全修飾ドメイン名 (FQDN) を入力します。 c Horizon 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 Horizon Composer ユーザーのパスワードを入力します。 e ポート番号が Horizon 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。

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

次のステップ

Horizon Composer ドメインを設定します。

- Horizon 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、Connection Server 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 [Horizon Composer ドメイン] ページが表示されます。
- Horizon 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。

Horizon Composer ドメインの設定

Horizon 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。Horizon Composer の複数のドメインを設定できます。vCenter Server と Horizon Composer の設定を

Horizon 7 に追加した後で、Horizon Console で vCenter Server インスタンスを編集して、より多くの Horizon Composer ドメインを追加できます。

前提条件

- Active Directory 管理者は、Active Directory の操作に必要な Horizon 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、 Horizon Composer Active Directory 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 Console で、[vCenter Server を追加] ウィザードの [vCenter Server 設定] ページと [Horizon Composer の設定] ページを完了していることを確認します。

手順

1 Horizon Console で、[設定] - [サーバ] の順に移動します。

2 [vCenter Server] タブで [追加] をクリックします。[vCenter Server 設定] ページで、vCenter Server の情報を入力し、[次へ] をクリックします。

3 Horizon Composer を使用している場合は、[Horizon Composer の設定] ページで Horizon Composer ホストの場所を選択し、[次へ] をクリックします。

Horizon Composer の詳細については、 Horizon Composer の設定を参照してください。

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

5 Active Directory ドメインのドメイン名を入力します。

例：**`domain.com`**

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

例：**`domain.com\admin`**

7 アカウントのパスワードを入力します。

8 [OK] をクリックします。

9 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。

10 [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。

次のステップ

仮想マシンのディスク容量再利用を有効にして、Horizon 7 の Horizon Storage Accelerator を設定します。

Horizon Console でのインスタント クローンのドメイン管理者の追加

インスタントクローン デスクトップ プールを作成する前に、インスタントクローン ドメイン管理者を Horizon 7 に追加する必要があります。

前提条件

- インスタント クローンのドメイン管理者が、必要な Active Directory ドメイン権限を持っ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』ドキュメントの「インスタントクローン操作用のユーザー アカウントの作成」を参照してください。

手順

1 Horizon Console で、[設定] - [インスタント クローンのドメイン アカウント] の順に選択します。

2 [追加] をクリックします。

3 インスタント クローンのドメイン管理者のドメインを選択します。

4 ユーザー名とパスワードを入力します。

次のステップ

Horizon Console では、インスタント クローンのドメイン管理者を追加または削除できます。また、インスタント クローンの管理者リストを Microsoft Excel ファイルにエクスポートすることもできます。[設定] - [インスタント クローンのドメイン アカウント] の順に移動し、インスタント クローンのドメイン管理者を選択します。[編集] をクリックして、管理者のドメインとログイン情報を編集します。[削除] をクリックして、管理者を削除します。エクスポート アイコンをクリックして、インスタント クローンの管理者リストを Microsoft Excel ファイルにエクスポートします。

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 バージョン 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。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します。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 バージョン 5.1 以降では、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 Console 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。
- Horizon Composer パーシステント ディスクには影響しません。
- vSphere バージョン 5.1 以降で、仮想ハードウェア バージョン 9 以降の仮想マシンでのみ機能します。
- 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（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。

前提条件

- 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 Console で、[設定] - [サーバ] の順に移動します。
2. [vCenter Server] タブで [追加] をクリックし、[vCenter Server を追加] ウィザードを完了して、[ストレージ設定] ページに移動します。
3. [ストレージ設定] ページで、[仮想マシンディスク容量を再利用] を選択します。

   Horizon 7 の新規インストールを実行している場合、このオプションはデフォルトで選択されます。Horizon 7 の新しいリリースにアップグレードする場合は、[仮想マシンディスク容量を再利用] を選択する必要があります。

次のステップ

[ストレージ設定] ページで、Horizon Storage Accelerator を設定します。

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 の Horizon Storage Accelerator の設定

vSphere で、仮想マシンのディスク データをキャッシュするように ESXi ホストを設定できます。この Horizon 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アンチウイルス 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、Horizon 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、Horizon 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 帯域幅が小さくなります。

この手順で説明しているように、Horizon Console の [vCenter Server を追加] ウィザードで Horizon 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。

個々のデスクトップ プールに Horizon Storage Accelerator が設定されていることも確認します。デスクトップ プールで操作するには、Horizon 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。

デフォルトでは、デスクトップ プールで Horizon Storage Accelerator が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 Horizon 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 (VAAI) は、Horizon 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。

Horizon 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 Horizon 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 Horizon 7 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 Horizon 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。

前提条件

- 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 Horizon 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 Console で、[設定] - [サーバ] の順に移動します。

2 [vCenter Server] タブで [追加] をクリックし、[vCenter Server を追加] ウィザードを完了して、[ストレージ設定] ページに移動します。

3 [ストレージ設定] ページで、[Horizon Storage Accelerator を有効にする] を選択します。

このオプションはデフォルトで選択されています。

4 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。

5 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。

6 [ストレージ設定] ページで、[次へ] をクリックします。

7 [設定内容の確認] ページで設定を確認したら、[送信] をクリックします。

次のステップ

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。『Horizon 7 の管理』の「クライアント セッションの設定」を参照してください。

Horizon 7 で Horizon Storage Accelerator の設定を完了するには、デスクトップ プールの Horizon Storage Accelerator を設定します。『Horizon Console 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 Horizon Storage Accelerator を構成する」を参照してください。

vCenter Server と Horizon Composer の同時操作の制限数

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 Horizon 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 を追加] ウィザードの [vCenter Server 設定] ページにある [詳細設定] パネルで設定します。

表 3-1. vCenter Server と Horizon Composer の同時操作の制限数

設定	説明
[最大同時 vCenter プロビジョニング操作数]	Connection Server 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 Connection Server 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 3-1. vCenter Server と Horizon Composer の同時操作の制限数 （続き）

設定	説明
[最大同時 Horizon Composer メンテナンス操作数]	この Horizon 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、Horizon Composer の更新、再構成、再調整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 Horizon Composer プロビジョニング操作数]	この Horizon 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。
[インスタント クローン エンジンの最大同時操作数]	この vCenter Server インスタンスによって管理されているインスタント 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。 この設定はインスタント 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 Horizon Composer インスタンスを Horizon 7 に追加する場合、vCenter Server および Horizon Composer インスタンス用に使用される TLS 証明書が有効で、Connection Server 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 Horizon 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 Horizon Composer インスタンスが認証局 (CA) によって署名された証明書で設定され、ルート証明書が Connection Server 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 Connection Server 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 Horizon 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設定する必要があります。

TLS 証明書の設定方法については、『Horizon 7 のインストール』の「Horizon 7 Server の TLS 証明書の設定」を参照してください。

まず、[vCenter Server を追加] ウィザードを使用して、Horizon Console に vCenter Server と Horizon 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 vCenter Server を追加できません。

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

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 Horizon 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。

手順

1 Horizon Console 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 Horizon Composer インスタンス用に設定された証明書のサムプリントを調べます。

a vCenter Server または Horizon 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 Horizon Composer 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が vCenter Server または Horizon Composer インスタンスのサムプリント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 Horizon 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。

前提条件

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 Console で、[設定] - [サーバ] の順に移動します。

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 メッセージが表示されます。

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 Horizon Composer の削除

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

Horizon Composer との接続を無効にする前に、Horizon 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、Horizon Composer を削除できません。Horizon 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 Horizon 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 Console で、[インベントリ] - [デスクトップ] 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通常ディスクを使用して構成されている場合、通常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 Horizon Composer データベース エントリと Horizon Composer によって作成されたレプリカも削除されます。

   d Horizon Composer によって作成された各リンク クローン デスクトップ プールに次の手順を繰り返します。

2 [設定] - [サーバ] の順に移動します。

3 [vCenter Server] タブで、Horizon 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 [Horizon Composer] タブの [Horizon Composer Server 設定] で、[Horizon 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。

次のステップ

別のホストに Horizon Composer をインストールし、Horizon 7 を再構成して新しい Horizon 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 Horizon Composer を移行する方法については、『Horizon 7 の管理』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] の順にクリックします。

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 Console での Horizon Connection Server のバックアップ

Horizon Connection Server の初期構成が完了したら、Horizon 7 と Horizon 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 7 構成のバックアップと復元については、Horizon Connection Server と Horizon Composer のデータのバックアップを参照してください。

Horizon Console でのクライアント セッションの設定

Connection Server 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。

Horizon Console でのクライアント セッションのグローバル設定

全般的なグローバル設定では、セッション タイムアウトの長さ、SSO の有効性とタイムアウト制限、Horizon Console でのステータス更新を設定します。また、ログイン前メッセージや警告メッセージを表示するかどうか、Horizon Console 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なども設定できます。

Horizon Console でグローバル設定を行うには、[設定] - [グローバル設定] - [一般設定] の順に移動します。

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

表 3-2. 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 Console セッションがどれだけ続くかを決定します。 **重要：** Horizon Console セッション タイムアウトを長く設定すると、Horizon Console が不正に使用されるリスクが増大します。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 Console セッション タイムアウトは 30 分間です。セッション タイムアウトは 10 分から 4320 分（72 時間）の間で設定できます。 セッションがタイムアウトする前に、60 秒間のカウントダウン付きで警告メッセージが表示されます。カウントダウンが終了する前にセッションをクリックすると、セッションが続行します。60 秒後にセッションがタイムアウトすると、再度ログインする必要があることを通知するエラー メッセージが表示されます。
[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 Connection Server 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 Connection Server から切断するか、または Horizon Client を終了し、Horizon 7 Connection Server 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。
[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 Console 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 Console 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。

表 3-2. 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。
[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。**
[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 Console 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 Connection Server、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。

表 3-2. 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
[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。
[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 Connection Server 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ドメイン リストを非表示] 設定を有効にし、Connection Server 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は、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。単一ユーザー ドメインの場合、これは Horizon Client バージョン 5.0 以降に適用されません。 **重要：** この設定のセキュリティと操作性に対する影響については、Horizon 7 のセキュリティを参照してください。
[ドメイン リストを送信]	このチェックボックスは、ユーザー認証の前に、Connection Server がドメイン名のリストをクライアントに送信できるようにする場合に選択します。 **重要：** この設定のセキュリティと操作性に対する影響については、Horizon 7 のセキュリティを参照してください。

Horizon Console のクライアント セッションと接続のグローバル セキュリティ設定

グローバル セキュリティ設定では、中断後にクライアントを再認証するかどうか、メッセージのセキュリティ モードを有効にするかどうか、セキュリティ ステータスを拡張するかどうかを設定します。

Horizon Console でグローバル セキュリティ設定を行うには、[設定] - [グローバル設定] - [セキュリティ設定] の順に移動します。

Horizon 7 に対するすべての Horizon Client 接続と Horizon Console 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 Connection Server 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。

表 3-3. 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。 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。

Horizon Console でのクライアント セッションのグローバル クライアントの制限の設定

グローバル クライアントの制限を設定すると、仮想デスクトップ、公開デスクトップ、公開アプリケーションの起動を特定のクライアントおよびバージョンに限定できます。

Horizon Console でグローバル クライアントの制限設定を行うには、[設定] - [グローバル設定] - [クライアントの制限の設定] の順に移動し、Horizon Client のバージョンを入力します。

Horizon Client はバージョン 4.5.0 以降にする必要があります。ただし、Horizon Client for Chrome はバージョン 4.8.0 以降にする必要があります。この機能が設定されている場合、以前のバージョンの Horizon Client はリモート デスクトップや公開アプリケーションに接続できません。

注： クライアントの制限の設定で制限できるのは、エンド ユーザーによるリモート デスクトップと公開アプリケーションの起動だけです。この機能を有効にしても、エンド ユーザーは Horizon 7 にログインできます。

表 3-4. クライアント セッションのグローバル クライアントの制限の設定

設定	説明
Horizon Client for Windows	バージョン 4.5.0 以降の Horizon Client バージョン番号を入力します。
Horizon Client for Linux	バージョン 4.5.0 以降の Horizon Client バージョン番号を入力します。
Horizon Client for Mac	バージョン 4.5.0 以降の Horizon Client バージョン番号を入力します。
Horizon Client for iOS	バージョン 4.5.0 以降の Horizon Client バージョン番号を入力します。
Horizon Client for Android	バージョン 4.5.0 以降の Horizon Client バージョン番号を入力します。
Horizon Client for UWP	バージョン 4.5.0 以降の Horizon Client バージョン番号を入力します。
Horizon Client for Chrome	バージョン 4.8.0 以降の Horizon Client バージョン番号を入力します。
Horizon Client(HTML Access)	バージョン 4.5.0 以降の Horizon Client バージョン番号を入力します。
追加のクライアントのブロック	このオプションを選択すると、ホワイトリストに登録された た Horizon Client を除き、すべてのクライアント タイプでデスクトップまたは公開アプリケーションの起動がブロックされます。 ただし、エンド ユーザーが他のクライアント タイプを使用してデスクトップまたは公開アプリケーションを起動できるようにするには、該当するクライアント タイプを `pae-AdditionalClientTypes` LDAP 属性に追加し、そのクライアント タイプのブロック設定を回避する必要があります。 ADSI Edit ユーティリティを使用して、Connection Server の LDAP 属性を編集できます。 ADSI Edit ユーティリティでは、`CN=Common`、`OU=Global`、`OU=Properties`、`DC=vdi`、`DC=vmware`、`DC=int` の下にある `pae-AdditionalClientTypes` LDAP 属性を使用できます。
メッセージ	ユーザーがホワイトリストにないクライアント タイプまたはバージョンからデスクトップや公開アプリケーションを起動した場合に表示するメッセージを入力します。

Horizon Console での Horizon Connection Server の無効化または有効化

Connection Server 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。

Connection Server 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 Connection Server 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。Connection Server に接続できません。
- これが複製された Connection Server 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 Console で、[設定] - [サーバ] の順に選択します。

2 [Connection Server] タブで、Connection Server 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。

Horizon Connection Server インスタンスの外部 URL の編集

Horizon Console を使用して、Connection Server インスタンスの外部 URL を編集できます。

デフォルトでは、Connection Server 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 Connection Server 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 Connection Server 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 Connection Server 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。

手順

1 Horizon Console で、[設定] - [サーバ] の順に選択します。

2 [Connection Server] タブで、Connection Server インスタンスを選択して [編集] をクリックします。

3 [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://horizon.example.com:443

注： ホスト名が解決できないときに Connection Server 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、Connection Server 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。

4 [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 Connection Server 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。

5 [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。

6 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。

7 [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。変更を有効にするために Connection Server を再起動する必要はありません。

Horizon Console でのゲートウェイの登録

Horizon Client は、Horizon Console で登録したゲートウェイまたは Unified Access Gateway アプライアンスを介して接続します。

Horizon Console で、ゲートウェイの登録または登録解除ができます。ゲートウェイの登録を解除するには、ゲートウェイまたは Unified Access Gateway アプライアンスを選択して、[登録解除] をクリックします。

手順

1 Horizon Console で、[設定] - [サーバ] の順に選択します。

2 [ゲートウェイ] タブで [登録] をクリックします。

3 ゲートウェイまたは Unified Access Gateway アプライアンスの FQDN を入力します。

4 [OK] をクリックします。

スマート カード認証の設定

4

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。

この章には、次のトピックが含まれています。

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 Connection Server 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 Connection Server 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 Connection Server 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 ボックスに [ユーザー名のヒント] フィールドを表示するには、管理者が Horizon Console の Connection Server 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。Unified Access Gateway アプライアンスでスマート カード ユーザー名のヒント機能を有効にする方法については、『Unified Access Gateway の導入および設定』ドキュメント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 Connection Server 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、Connection Server 構成プロパティを変更する必要があります。

5 Horizon Console でのスマート カードの設定

Horizon Console 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。

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。

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。

前提条件

- 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*

次のステップ

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 Connection Server 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、Connection Server 構成プロパティを変更する必要があります。

前提条件

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 Connection Server 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 Connection Server サービスを再起動して、変更を有効にします。

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
```

次のステップ

Connection Server 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 Console でスマート カード認証の設定をします。

Horizon Console でのスマート カードの設定

Horizon Console 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。

前提条件

- Connection Server ホストの Connection Server 構成プロパティを変更します。
- Horizon Client が Connection Server 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 Console で、[設定] - [サーバ] の順に選択します。

2 [Connection Server] タブで、Connection Server 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、[Horizon 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 メニューから設定オプションを選択します。

オプション	アクション
不許可	Connection Server 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 Connection Server 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	Connection Server 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、Connection Server 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、Connection Server 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。 **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、Connection Server か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 Connection Server 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します。	[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 Connection Server 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 Console へのログインで管理者が使用するスマート カード認証を設定するには、[Horizon Administrator 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 メニューから設定オプションを選択します。

オプション	アクション
不許可	Connection Server 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 Console 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 Console 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 Connection Server 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、Connection Server 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、Connection Server 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。

次のステップ

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。Horizon Console でのスマート カード認証の設定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 カード認証の設定

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 Connection Server 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 Console で SAML 認証子を作成します。

Unified Access Gateway でのスマート カード認証の設定については、『Unified Access Gateway』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 Console での SAML 認証子の設定を参照してください。

2 Connection Server 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。

Connection Server 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、Connection Server 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。

前提条件

- 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。

次のステップ

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。

Horizon Console でのスマート カード認証の設定の検証

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。

- Connection Server 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。

- Connection Server インスタンスでスマート カード認証を設定した場合は、Horizon Console でスマート カード認証の設定を確認します。

  a [設定] - [サーバ] の順に選択します。

  b [Connection Server] タブで、Connection Server 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、Connection Server 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 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。

- Connection Server 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。

前提条件

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。

前提条件

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 4-1. 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 4-1. 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。
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。

他のタイプのユーザー認証の設定

5

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。

この章には、次のトピックが含まれています。

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 Connection Server 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 Console での 2 要素認証の有効化

Horizon Console で Connection Server の設定を変更して、Connection Server インスタンスで RSA SecurID 認証または RADIUS 認証を有効にします。

前提条件

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 Connection Server 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。これらの値は、Horizon Console で入力します。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 Console で、[設定] - [サーバ] の順に移動します。

2 [Connection Server] タブで、Connection Server 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、[高度な認証] セクションの [2 要素認証] ドロップダウン メニューから、[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 メニューから、[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。

- エンド ユーザーの RADIUS 認証ダイアログにカスタムのユーザー名とパスコードのラベルを表示するには、[ユーザー名ラベル] と [パスコード ラベル] フィールドにカスタム ラベルを入力します。
- 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。

Connection Server 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、Connection Server 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。

次のステップ

Connection Server 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 SecureID 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 Console で、[設定] - [サーバ] の順に移動します。

2 [Connection Server] タブで、Connection Server 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、[高度な認証] セクションの [2 要素認証] ドロップダウン メニューから、[RSA SecureID] を選択します。

4 [ノード シークレットをクリア] を選択して、[OK] をクリックします。

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 Connection Server 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。

- Connection Server 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 Connection Server 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。
- Connection Server 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 Connection Server 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、Connection Server インスタンスにアーティファクトを送信します。Connection Server 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。

Connection Server 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 Connection Server 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 Console 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 Console での SAML 認証子の設定

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 Console 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 Connection Server インスタンスと関連付けます。導入環境に複数の Connection Server 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。

Connection Server 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、Connection Server 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』を参照してください。

前提条件

- 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。
- Connection Server 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。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。
- 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 アプライアンス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 Console で、[設定] - [サーバ] の順に移動します。

2 [Connection Server] 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、環境内の各 Connection Server 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 アプライアンス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 アプライアンス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 Connection Server 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。

オプション	説明
SAML メタデータ	（静的認証子の場合）Unified Access Gateway アプライアンス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。
Connection Server 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。

次のステップ

Connection Server 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。Connection Server 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。

前提条件

手順

1 Connection Server 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] の順に選択して、**pae-SAMLProxyName** エントリと **pae-SAMLProxyPort** エントリに値を追加します。

Connection Server 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、Connection Server は 24 時間後に Unified Access Gateway アプライアンスやサードパーティ製の 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、Connection Server 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 Connection Server は有効期間が 90 日間のメタデータを生成します。

前提条件

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 Connection Server 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、Connection Server 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 Connection Server 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。

Connection Server 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、Connection Server 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。

前提条件

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。

手順

1 新規のブラウザ タブを開き、Connection Server 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 Connection Server ホストの完全修飾ドメイン名です。

このページには、Connection Server 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" ...
```

次のステップ

ID プロバイダで適切な手順を使用して、Connection Server 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

Connection Server 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 Connection Server 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 Console 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 Console での SAML 認証子の設定を参照してください。

Horizon Console 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。

前提条件

- 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 Console で公開デスクトップと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 Console で、[設定] - [サーバ] の順に移動します。

2 [Connection Server] 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。

前提条件

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。

ユーザーとグループの認証

6

Horizon Console にログインした後、ユーザーおよびグループに認証を設定し、アプリケーションやデスクトップへのアクセスを制御できます。

ネットワーク外部からデスクトップへのユーザーまたはグループのアクセスを制限するように、リモート アクセスを構成します。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。

この章には、次のトピックが含まれています。

ネットワーク外部のリモート デスクトップ アクセスの制限

資格が付与されている特定のユーザーとグループについて外部ネットワークからのアクセスを許可し、資格が付与されている他のユーザーとグループについてはアクセスを制限することがきます。資格が付与されたすべてのユーザーは、内部ネットワークにある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。特定のユーザーによる外部ネットワークからのアクセスを制限しない場合、資格が付与されているすべてのユーザーが外部ネットワークからアクセスできるようになります。

セキュリティ上の理由で、管理者は外部ネットワークのユーザーとグループによるネットワーク内のリモート 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必要がある場合があります。制限されているユーザーが外部ネットワークからシステムにアクセスすると、ユーザーにシステムを使用する資格が付与されていないことを伝えるメッセージが表示されます。デスクトップおよびアプリケーション プールの資格を取得するには、ユーザーは内部ネットワークの中にいる必要があります。

リモート アクセスの設定

特定のユーザーとグループについてはネットワークの外部から接続サーバ インスタンスへのアクセスを許可し、その他のユーザーとグループについてはアクセスを制限できます。

前提条件

- ユーザーに資格が付与される接続サーバ インスタンスへのゲートウェイとして、Unified Access Gateway アプライアンス、セキュリティ サーバ、またはロード バランサは、ネットワークの外部にデプロイする必要があります。Unified Access Gateway アプライアンスのデプロイの詳細については、『Unified Access Gateway の導入および設定』ドキュメントを参照してください。
- リモートからアクセスするユーザーには、デスクトップやアプリケーション プールへの資格を付与する必要があります。

手順

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

2 [リモート アクセス] タブをクリックします。

3 [追加] をクリックして、1 つ以上の検索基準を選択し、[検索] をクリックして検索基準に基づいてユーザーまたはグループを検索します。

注： 非認証アクセスのユーザーは検索結果に表示されません。

4 非認証アクセスのユーザーまたはグループにリモート アクセスを許可するには、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。

5 特定のユーザーまたはグループからリモート アクセスを削除するには、そのユーザーまたはグループを選択して、[削除] をクリックしてから、[OK] をクリックします。

非認証アクセスの構成

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。

注： 非認証アクセスは、デスクトップ プールの公開アプリケーションでサポートされません。

この機能を実行するには、Horizon 7 バージョン 7.1 環境のセットアップと Horizon Client バージョン 4.4 が必要です。

非認証アクセス ユーザーを構成するルールとガイドラインについては、『Horizon 7 の管理』ドキュメントを参照してください。

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。

前提条件

- 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。
- デスクトップの使用資格を持つユーザーを選択し、ユーザーを非認証アクセス ユーザーにすると、このユーザーは資格のあるデスクトップにアクセスできなくなります。

手順

1 Horizon Console 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。

4 ユーザーを選択し、[次へ] をクリックします。

5 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 [送信] 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、ドメイン、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。

次のステップ

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。『Horizon 7 の管理』ドキュメントで「ユーザーの非認証アクセスを有効にする」を参照してください。

Horizon Console での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、Connection Server 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 Console で、[設定] - [サーバ] の順に選択します。

2 [Connection Server] タブをクリックします。

3 Connection Server 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、Connection Server 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。

次のステップ

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。

前提条件

- RDS ホストのグループに基づいてファームを作成します。ファームの作成の詳細については、『Horizon Console 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。公開アプリケーションの作成の詳細については、『Horizon Console 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。

手順

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

2 [資格] タブで、[資格] ドロップダウン メニューから [アプリケーションに対する資格を追加] 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。[非認証ユーザー] チェックボックスをオンにして [検索] をクリックし、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 プール内のアプリケーションを選択して、[送信] をクリックします。

次のステップ

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 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。デフォルトのユーザーを削除すると、ユーザーが正常に削除されたことを示すメッセージと内部エラー メッセージが Horizon Console に表示されます。ただし、デフォルトのユーザーは、Horizon Console から削除されません。

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 Console で、[ユーザーとグループ] を選択します。

2 [非認証アクセス] タブでユーザーを選択し、[削除] をクリックします。

3 [OK] をクリックします。

次のステップ

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 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。

前提条件

- 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。

Horizon Console でのユーザーへのハイブリッド ログインの設定

非認証アクセス ユーザーを作成した後、ユーザーにハイブリッド ログインを有効にできます。ハイブリッド ログインを有効にすると、非認証アクセス ユーザーが認証情報を入力せずにファイル共有、ネットワーク プリンタなどのサービスにドメイン レベルでアクセスできるようになります。

注： ハイブリッド ログイン機能では、ハイブリッド ログインに設定された特定の非認証アクセス ユーザーのすべてのログイン ユーザーに対して同じドメイン ユーザーを使用します。

注： ユーザー プロファイルのタブを使用して、RDS ホスト マシンからのネットワーク パスとしてホーム ディレクトリを設定した場合、デフォルトの Windows の管理ユーザー インターフェイスでは、ホーム ディレクトリ フォルダの既存の権限がすべて削除され、管理者とフル コントロールを持つローカル ユーザーに権限が追加されます。管理者アカウントを使用して権限リストからローカル ユーザーを削除し、ユーザーに設定にする必要がある権限を持つドメイン ユーザーを追加します。

前提条件

- RDS ホストに Horizon Agent をインストールしたときに、ハイブリッド ログインのカスタム オプションを選択していることを確認します。RDS ホストの Horizon Agent カスタム セットアップ オプションの詳細については、『Horizon Console 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』ドキュメントを参照してください。
- 非認証アクセス ユーザーを作成していることを確認します。非認証アクセス ユーザーの作成を参照してください。
- ドメインのユーザー アカウントで Kerberos DES 暗号化が無効になっていることを確認します。ハイブリッド ログイン機能では、Kerberos DES 暗号化がサポートされていません。

手順

1. Horizon Console 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非認証アクセス 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. 非認証アクセス ユーザーを選択して、[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 Connection Server 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 [ハイブリッド ログインを有効にする] を選択します。

デフォルトでは、[True SSO を有効にする] オプションが選択されています。Horizon 7 環境に True SSO が有効になっている必要があります。次に、ハイブリッド ログインで有効になっている非認証アクセス ユーザーは、True SSO を使用して、Horizon Client から Connection Server インスタンスにログインします。

注： True SSO で Connection Server ポッドが設定されていない場合、ユーザーは資格を付与されたアプリケーションを非認証アクセスで開始できます。ただし、ポッドで True SSO が有効でないため、ユーザーはネットワークにアクセスできません。

8 （オプション） ユーザーが Horizon Client から Connection Server インスタンスにログインできるようにするには、[パスワード ログインを有効にする] を選択して、ユーザーのパスワードを入力します。

Horizon 7 環境に True SSO が設定されていない場合は、この設定を使用します。

CPA 環境の場合、ハイブリッド ログイン ユーザー機能は、ハイブリッド ログイン ユーザーに [パスワード ログインを有効にする] が設定され、公開アプリケーションに対する資格が付与されている Connection Server ポッドでのみ機能します。

たとえば、ポッド A と ポッド B がある CPA 環境で、ハイブリッド ログイン ユーザーに [パスワード ログインを有効にする] が設定され、ポッド A のアプリケーションに対する資格が付与されているとします。ユーザーは、ポッド A またはポッド B のいずれかに接続するクライアントからアプリケーションを表示し、起動できます。ただし、ポッド B で同じユーザーに別のアプリケーションに対する資格が付与されている場合、ユーザーはポッド B に接続するクライアントからアプリケーションを表示し、起動することはできません。ポッド B でハイブリッド ログイン機能を使用するには、別のハイブリッド ログイン ユーザーを作成して [パスワード ログインを有効にする] を設定し、そのユーザーにアプリケーションに対する資格を付与する必要があります。CPA 環境のセットアップ方法の詳細については、『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。

9 [終了] をクリックします。

次のステップ

ユーザーに公開アプリケーションに対する資格を付与します。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。

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

Horizon Client for Windows で、ユーザーが [オプション] メニューの [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 Connection Server インスタンスとリモート デスクトップの認証で使用されます。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 Connection Server 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。

- Connection Server 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。
- Horizon Client の [オプション] メニューで [現在のユーザーとしてログイン] を選択したときに渡されるユーザー ID と認証情報が Connection Server インスタンスで受け入れられるように、Connection Server インスタンスで [現在のユーザーとしてのログインを受け入れる] 設定を有効にします。

  重要： この設定を有効にする前に、セキュリティ リスクを理解しておく必要があります。『Horizon 7 のセキュリティ』の「ユーザー認証のセキュリティ関連のサーバ設定」を参照してください。

- 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、[オプション] メニューの [現在のユーザーとしてログイン] 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] 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 Connection Server 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 Connection Server 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。

- Connection Server 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、Connection Server 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] 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、Connection Server 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、Connection Server 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 Connection Server 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。

Horizon Console でのロールベースの委任管理の構成

7

Horizon 7 環境の重要な管理タスクは、Horizon Console 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。

この章には、次のトピックが含まれています。

ロールと権限の概要

Horizon Console 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 Console 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 Console 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 Console 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。ロールにオブジェクト固有の権限が含まれている場合、アクセス グループへのロールの適用が必要になる場合があります。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。

Horizon Console でのアクセス 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 Console 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 Console 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。

- 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 7-1. 異なるアクセス グループの異なる管理者 に、このタイプの構成の例を示します。

表 7-1. 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 7-2. 同じアクセス グループの異なる管理者 に、このタイプの構成の例を示します。

表 7-2. 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 Console 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 Console 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 Console 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 7-3. 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 Console で同じ権限がどのように表示されるかを示します。

表 7-4. MarketingDesktops の Folders（フォルダ） タブの権限

Admin	ロール	継承
horizon-domain.com\Admin1	インベントリ管理者	
horizon-domain.com\Admin1	管理者（読み取り専用）	はい

最初の権限は、表 7-3. Admin 1 の Administrators and Groups（管理者とグループ） タブでの権限に示す最初の権限と同じです。2 番目の権限は、表 7-3. Admin 1 の Administrators and Groups（管理者とグループ）タブでの権限に示す 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 7-3. Admin 1 の Administrators and Groups（管理者とグループ） タブでの権限 の最初の権限が Horizon Console でどのように表示されるかを示します。

表 7-5. インベントリ管理者の [ロールの権限] タブの権限

Administrator	アクセス グループ
horizon-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 Console 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 Console 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。Connection Server 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、Connection Server 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。

- Horizon Console での管理者の作成

  管理者を作成するには、Horizon Console 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。

- Horizon Console での管理者の削除

  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。

Horizon Console での管理者の作成

管理者を作成するには、Horizon Console 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。

前提条件

- 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。 Horizon Console でのカスタム 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 Console で、[設定] - [管理者] の順に移動します。
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。

Horizon Console での管理者の削除

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 Horizon Console で、[設定] - [管理者] の順に移動します。

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 Console を使用して、特定の管理者ユーザーとグループ、ロール、アクセス グループの権限を追加、削除、確認できます。

- Horizon Console での権限の追加

  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。

- Horizon Console での権限の削除

  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。

- Horizon Console での権限の確認

  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。

Horizon Console での権限の追加

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 Console で、[設定] - [管理者] の順に移動します。

2 権限を作成します。

オプション	アクション
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します。	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します。	a [ロールの権限] 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します。	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。

Horizon Console での権限の削除

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 Console で、[設定] - [管理者] の順に移動します。

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します。	[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します。	[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します。	[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、[権限を削除] をクリックします。

Horizon Console での権限の確認

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 Horizon Console で、[設定] - [管理者] の順に移動します。

2 権限を確認します。

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。	[ロールの権限] 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 Console 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。

- Horizon Console でアクセス グループを追加する

  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。

- Horizon Console での別のアクセス 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。

- Horizon Console でのアクセス 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 グループ内のデオブジェクトの確認

  Horizon Console で、特定のアクセス グループのデスクトップ プール、アプリケーション プール、ファーム、パーシステント ディスクを確認できます。

- アクセス グループ内の vCenter 仮想マシンの確認

  Horizon Console 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。

Horizon Console でアクセス グループを追加する

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 Console で、[アクセス グループ] ダイアログ ボックスに移動します。

オプション	アクション
デスクトップから	■ [インベントリ] - [デスクトップ] の順に選択します。 ■ [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。
ファームから	■ [インベントリ] - [ファーム] の順に選択します。 ■ [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。

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。

次のステップ

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。

Horizon Console での別のアクセス 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 Console で、[インベントリ] - [デスクトップ] の順に選択するか、[インベントリ] - [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 [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 Console が、選択したアクセス グループにプールまたはファームを移動します。

Horizon Console でのアクセス 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。

前提条件

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。 Horizon Console での別のアクセス 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 Console で、[設定] - [管理者] の順に移動します。

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 グループ内のデオブジェクトの確認

Horizon Console で、特定のアクセス グループのデスクトップ プール、アプリケーション プール、ファーム、パーシステント ディスクを確認できます。

手順

1 Horizon Console 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	[インベントリ] - [デスクトップ] の順に選択します。
アプリケーション プール	[インベントリ] - [アプリケーション] の順に選択します。
ファーム	[インベントリ] - [ファーム] の順に選択します。
通常ディスク	[インベントリ] - [パーシステント ディスク] 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 仮想マシンの確認

Horizon Console 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 Console で、[インベントリ] - [マシン] の順に移動します。

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 Console 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。

- Horizon Console でのカスタム 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 Console 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。
- Horizon Console でのカスタム 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。
- Horizon Console でのカスタム 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。

Horizon Console でのカスタム 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 Console 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。

前提条件

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 Console で、[設定] - [管理者] の順に移動します。

2 [ロールの権限] 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。

Horizon Console でのカスタム 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。

前提条件

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 Console で、[設定] - [管理者] の順に移動します。

2 [ロールの権限] タブでロールを選択します。

3 ロールの権限を表示して、[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。

Horizon Console でのカスタム 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。

前提条件

ロールが権限に含まれる場合は、権限を削除します。 Horizon Console での権限の削除を参照してください。

手順

1 Horizon Console で、[設定] - [管理者] の順に移動します。

2 [ロールの権限] 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 Console 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 7-6. Horizon Console の事前定義ロール

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、Connection Server 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 Console 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 7-6. Horizon Console の事前定義ロール （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 Console 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 Console 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、再調整し、デフォルトのプール イメージを変更する。 ■ 自動ファームを管理します。 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 オブジェクトに対してのみこれらの操作を実行できます。 このロールを持つ管理者は、手動ファームまたは管理対象外の手動プールを作成できません。また、ファームまたは管理対象外の手動プールに RDS ホストの追加や削除を行うこともできません。	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 7-7. 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 Console にログインして使用します。 **注：** Horizon 7 バージョン 7.10 以降では、新しいロールに [コンソール操作] 権限が自動的に追加されます。この権限は、Horizon Console のグローバル権限のリストに表示されません。	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。 **注：** Horizon 7 バージョン 7.10 以降では、新しいロールに [直接操作] 権限が自動的に追加されます。この権限は、Horizon Console のグローバル権限のリストに表示されません。	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、Connection Server 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
[vCenter Server 構成の管理（読み取り専用）]	vCenter Server 構成へのアクセスは読み取り専用になります。	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） ローカル管理者 ローカル管理者（読み取り専用）

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 7-8. 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
自動化されたデスクトップとファームでのメンテナンス操作を管理	デスクトップ プールとファームの再構成、更新、再調整、イメージのプッシュとメンテナンスのスケジューリング、デフォルト イメージの変更を行います。	デスクトップ プール、ファーム
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	Horizon Composer パーシステント ディスクの操作を実行します（パーシステント ディスクの接続、接続解除、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 7-9. 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 Console 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 7-10. 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 **注：** 管理対象外のデスクトップ プールを追加する場合は適用されません。管理者は、このタスクを実行するためのグローバル設定およびポリシー管理者 (読み取り専用) ロールを持っている必要があります。
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 **注：** 管理対象外のデスクトップ プールを削除する場合は適用されません。管理者は、このタスクを実行するためのグローバル設定およびポリシー管理者 (読み取り専用) ロールを持っている必要があります。
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 **注：** デスクトップ プールで管理対象外の仮想デスクトップを追加または削除する場合は適用されません。管理者は、このタスクを実行するためのグローバル設定およびポリシー管理者 (読み取り専用) ロールを持っている必要があります。
デフォルトの Horizon Console イメージを更新、再構成、再調整または変更する。	Composer デスクトップ プール イメージの管理と [vCenter Server 構成の管理 (読み取り専用)]。
アクセス グループを変更する。	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 Console 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 7-11. 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 または [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] **注：** デスクトップ プールまたはファームから管理対象外のデスクトップまたは RDS ホストを削除する場合は適用されません。管理者は、このタスクを実行するためのグローバル設定およびポリシー管理者 (読み取り専用) ロールを持っている必要があります。
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か、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か、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 Console でパーシステント 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、一般的な通常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 Console の [パーシステント ディスク] ページで実行します。

表 7-12. 通常ディスク管理タスクと権限

タスク	必要な権限
ディスクを接続解除する。	■ ディスクがセカンダリ ディスクの場合、通常ディスクの管理権限が必要です。 ■ ディスクがプライマリ ディスクの場合、通常ディスクの管理権限とマシンの管理権限が必要です。 ■ 別のデータストアのディスクを接続を解除するには、管理者に [vCenter Server 構成の管理（読み取り専用）] 権限も必要です。
ディスクを接続する。	ディスクに対する通常ディスクの管理およびマシンに対するマシンの管理。
ディスクを編集する。	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。
アクセス グループを変更する。	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、最後のデスクトップ 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 プールの管理または [マシンの管理]。
vCenter Server からインポートする。	ディスクに対する通常ディスクの管理および vCenter Server 構成の管理（読み取り専用）。
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 Console 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 Console 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 Console の [グローバル管理者ビュー] ページで行います。

表 7-13. 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
全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 Console 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 7-14. 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 Console にログインできます。	[コンソール操作] **注：** Horizon 7 バージョン 7.10 以降では、新しいロールに [コンソール操作] 権限が自動的に追加されます。この権限は、Horizon Console のグローバル権限のリストに表示されません。
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 アシスタント。	[リモート アシスタンス]
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 7-15. 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	アクセス グループを削除するには、ルート アクセス グループに対するローカル管理者ロールまたは管理者ロールが必要です。 ルート アクセス グループに対するインベントリ管理者かローカル管理者のロール、または管理者ロールが必要です。
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 **注：** Horizon 7 バージョン 7.10 以降では、新しいロールに直接操作権限が自動的に追加されます。この権限は、Horizon Console のグローバル権限のリストに表示されません。
`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。
vCenter Server 構成へのアクセスは読み取り専用になります。	[vCenter Server 構成の管理（読み取り専用）]

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 Console でのポリシーの設定 8

Horizon Console 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。

この章には、次のトピックが含まれています。

グローバル ポリシーの設定

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。

手順

1 Horizon Console で、[設定] - [グローバル ポリシー] の順に選択します。

[グローバル ポリシー] ペインには、すべてのクライアント セッション、デスクトップ プールまたはユーザーに影響する設定が表示されます。

表 8-1. 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。

2 [ポリシーを編集] をクリックして設定を変更します。

3 [OK] をクリックして変更を保存します。

Horizon 7 コンポーネントのメンテナンス

9

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。

この章には、次のトピックが含まれています。

Horizon 7 構成データのバックアップと復元

Horizon Console で自動バックアップをスケジュールリングするか実行して、Horizon 7 と Horizon Composer の構成データをバックアップできます。Horizon 7 構成をリストアするには、バックアップした View LDAP ファイルと Horizon 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 Connection Server と Horizon Composer のデータのバックアップ

Connection Server の初期構成が完了したら、Horizon 7 と Horizon 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 Console を使用すると、Horizon 7 と Horizon Composer のデータを保持できます。

Horizon 7 は、Connection Server の構成データを View LDAP リポジトリに保存します。Horizon Composer は、Horizon Composer データベースにリンク クローン デスクトップの設定データを保存します。

Horizon Console 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 Horizon 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 の説明については、『Horizon 7 の管理』の「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 Console 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、Connection Server 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 Horizon Console 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 Connection Server 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 Connection Server 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 Connection Server 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。
- Connection Server 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 Connection Server 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。
- Connection Server が複数の Horizon 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 Horizon 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、Connection Server 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、Connection Server 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。

前提条件

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 Console で、[設定] - [サーバ] の順に選択します。

2 [Connection Server] タブで、バックアップ対象の Connection Server インスタンスを選択して [今すぐバックアップ] 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、Connection Server と Horizon Composer の構成データを定期的にバックアップできます。Horizon Console 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 9-1. 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。
バックアップ時間	バックアップをスケジュールリングする時間。
バックアップ時間のオフセット	スケジュールされたバックアップの時間のオフセット。
Max number of backups（バックアップの最大数）	Connection Server 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	Connection Server 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 Connection Server 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 Connection Server 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 Connection Server 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 Connection Server 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。このコマンドは Horizon Composer データベース情報はバックアップしません。

前提条件

- Connection Server 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 Connection Server 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。

次のステップ

`vdmimport` コマンドを使用して、Connection Server 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 Connection Server と Horizon Composer の構成データのリストアを参照してください。

Horizon Connection Server と Horizon Composer の構成データのリストア

Horizon 7 によってバックアップされた Connection Server LDAP 構成ファイルおよび Horizon Composer データベース ファイルを手動でリストアできます。

個別のユーティリティを手動で実行して、Connection Server と Horizon Composer の構成データをリストアします。

構成データをリストアする前に、Horizon Console で構成データをバックアップしたことを確認します。Horizon Connection Server と Horizon 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、Connection Server データを LDIF バックアップ ファイルから Connection Server 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、Horizon Composer データを `.svi` バックアップ ファイルから Horizon 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、Connection Server インスタンスの現在のバージョンをインストールし、Connection Server 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 Connection Server 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、Connection Server 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 Connection Server 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 Console 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 Connection Server と Horizon Composer のデータのバックアップを参照してください。

前提条件

- Connection Server 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 Connection Server 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. Horizon Composer が実行されているサーバで VMware Horizon Composer Windows サービスを停止し、Horizon Composer のすべてのインスタンスを停止します。
2. Horizon Connection Server 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 Connection Server と AD LDS Instance VMwareVDMDS の両方をアンインストールします。
3. 1 つの Connection Server インスタンスをインストールします。
4. Windows サービスの VMware Horizon Connection Server を停止して、Connection Server インスタンスを停止します。
5. [スタート] - [コマンド プロンプト] の順にクリックします。
6. 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：

   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。
7. 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：

8 Connection Server をアンインストールします。

VMware Horizon Connection Server パッケージのみをアンインストールします。

9 Connection Server を再インストールします。

10 Horizon Console にログインして、構成が正しいかどうかを検証します。

11 Horizon Composer インスタンスを開始します。

12 レプリカ サーバ インスタンスを再インストールします。

`vdmimport` コマンドは、Connection Server 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： リストアされる構成が、vCenter Server および Horizon 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、Horizon Composer の構成をバックアップからリストアします。 Horizon Composer データベースのリストアを参照してください。Horizon 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、Horizon Composer 構成をリストアした後に不整合を手動で解決する必要があります。

Horizon Composer データベースのリストア

Horizon 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 Horizon 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 Horizon Composer データベース データをリストアしたり、Horizon 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 Horizon 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、Horizon Composer サービスに関連する問題を解決するためのものです。

前提条件

Horizon 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 Connection Server コンピュータの `C:` ドライブ（`C:\Programdata\VMWare\VDM\backups`）に格納します。

Horizon 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` - Horizon 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 Horizon Composer バックアップ ファイルを、Connection Server コンピュータから、VMware Horizon 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 Horizon Composer がインストールされているコンピュータで、VMware Horizon 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、Horizon 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 Composer サービスを開始します。

次のステップ

`SviConfig restoredata` コマンドの出力結果コードについては、 Horizon Console データベースのリストアの結果コードを参照してください。

Horizon Console データベースのリストアの結果コード

Horizon Console データベースをリストアすると、`SviConfig restoredata` コマンドで結果コードが表示されます。

表 9-2. 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。

表 9-2. restoredata の結果コード （続き）

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

Horizon Composer データベースのデータのエクスポート

Horizon 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 Horizon 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。

前提条件

デフォルトでは、Horizon 7 はバックアップ ファイルを Connection Server 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。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。
- `OutputFilePath` - 出力ファイルへのパス。

手順

1 Horizon Composer がインストールされているコンピュータで、VMware Horizon 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、Horizon Composer アプリケーションと同じ場所にあります。

`Horizon-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_Horizon_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"
```

次のステップ

SviConfig exportdata コマンドのエクスポート結果コードについては、Horizon 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。

Horizon Composer データベースのエクスポートの結果コード

Horizon 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 9-3. 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 Console 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 Console には、Connection Server インスタンス、イベント データベース、ゲートウェイ、Horizon 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 Console 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 Console で、[モニター] - [ダッシュボード] の順に移動します。

2 [システムの健全性] ペインで、[表示] をクリックします。

詳細ペインには、各問題に関連する名前、バージョン、その他の情報が表示されます。

- 緑色のチェック マークは、コンポーネントに問題がないことを示します。
- 赤色の感嘆符は、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。
- 黄色の感嘆符は、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 詳細を表示する問題を選択します。

オプション	説明
コンポーネント	サービス コンポーネントに関する情報を表示します。 [Connection Server]、[ゲートウェイ サーバ]、[イベント データベース]、[View Composer Server] または [True SSO] タブをクリックしてサービス コンポーネントに関する情報を表示し、トラブルシューティング タスクを実行します。 コンポーネントを選択して、次のタスクを実行します。 ■ ステータス、名前、バージョン、その他の詳細を表示します。 ■ Connection Server を選択した場合は、[サービスのステータスの表示] タブをクリックして、ゲートウェイ サービスに関する情報を表示します。 ■ Connection Server を選択した場合は、[セッションの詳細の表示] タブをクリックして、Connection Server セッションに関する情報を表示します。
RDS ファーム	ファームに関する情報を表示します。ファーム ID をクリックして、ファームに関する詳細情報（ファームに属する RDS ホストを含む）を表示します。
vSphere	vSphere に関連するコンポーネントに関する情報が表示されます。 [データストア]、[ESX ホスト]、[vCenter Server] タブをクリックして、各コンポーネントに関する情報を表示します。
その他のコンポーネント	[ドメイン]、[SAML 2.0]、[License Service] タブをクリックして、各コンポーネントに関する情報を表示します。このセクションの説明は Horizon Composer にも適用されます。 **注：** 信頼されていない証明書が原因で SAML 2.0 認証子に警告が表示された場合は、証明書のリンクをクリックして証明書を受け入れ、検証することができます。
リモート ポッド	リモート Horizon 7 ポッドに関する情報を表示します。 **注：** このセクションは、クラウド ポッド アーキテクチャ機能が有効になっている場合にのみ表示されます。

4 [セッション] ペインで、仮想デスクトップ、公開デスクトップ、公開アプリケーションのアクティブなセッション、切断されたセッションまたはアイドル状態のセッション数を棒グラフで表示できます。

5 [セッション] ペインで [表示] をクリックして、セッションを表示します。

[セッション] ページに、セッションに関する情報が表示されます。

6 [ワークロード] ペインで [表示] をクリックして、データストアを表示します。

データストアを選択すると、データストアの現在の使用量などの追加情報を表示できます。Horizon Console は、データストアの空き容量がしきい値を下回ると警告を表示します。選択したデータストアに関連するデスクトップ プールがある場合、そのデータストアを選択すると、デスクトップ プールの情報を表示できます。[その他のデータストア] 列には、複数のデータストアにまたがるデスクトップ プールまたはファームの情報が表示されます。

Horizon Connection Server の負荷ステータスの監視

Horizon Console ダッシュボードで、Connection Server の負荷を監視できます。Connection Server ごとに、CPU とメモリの使用率、表示プロトコル セッション数、Connection Server の接続セッション数、Connection Server に接続できるセッション数の上限しきい値を確認できます。RDS ホストで接続されているセッション数を確認することもできます。

手順

1 Horizon Console で、[モニター] - [ダッシュボード] の順に移動します。

2 [システムの健全性] ペインで、[表示] をクリックします。

[コンポーネント] ペインの [Connection Server] タブで、[セッション] 列に各 Connection Server の Connection Server セッションの割合が表示されます。[CPU 使用量] 列には、各 Connection Server で使用された CPU の割合が表示されます。[メモリ使用量] 列には、各 Connection Server で使用されたメモリの割合が表示されます。

注： Connection Server が、HTTP(s) セキュア トンネル、PCoIP セキュア ゲートウェイ、Blast Secure Gateway 接続とのセキュア ゲートウェイ接続で構成されていない場合、Horizon Console は Connection Server セッションの割合を表示せず、Connection Server の一覧を表示します。

3 Connection Server を選択して [セッションの詳細の表示] をクリックし、Connection Server セッション、Connection Server セッションの最大数、表示プロトコル セッションを表示します。

注： Connection Server が、HTTP(s) セキュア トンネル、PCoIP セキュア ゲートウェイ、Blast Secure Gateway 接続とのセキュア ゲートウェイ接続で構成されていない場合、Connection Server に接続できるセッション数にしきい値がないため、Horizon Console は最大セッション数のしきい値を表示しません。

4 RDS ホストのセッション数を表示するには、[コンポーネント] ペインで [RDS ファーム] をクリックし、ファーム ID をクリックします。

[セッション] 列には、RDS ホストのセッション数が表示されます。

Horizon Connection Server でのサービスの監視

Horizon Console ダッシュボードでは、Connection Server で実行されているゲートウェイ サービス コンポーネントを監視できます。ゲートウェイ サービス コンポーネントには、HTTP(s) セキュア トンネル、PCoIP ゲートウェイ、Blast Secure Gateway 接続で構成されたセキュア ゲートウェイ接続が含まれます。

手順

1 Horizon Console で、[モニター] - [ダッシュボード] の順に移動します。

2 [システムの健全性] ペインで、[表示] をクリックします。

3 Connection Server を選択して、[サービスのステータスの表示] を選択します。

[ゲートウェイ サービスのステータス] ダイアログには、ゲートウェイ サービス コンポーネントのステータスと使用中のゲートウェイ サービス コンポーネントが表示されます。

注： 有効になっていないサービス コンポーネントはグレーアウトされます。

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。

前提条件

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 9-4. 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 9-5. 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。
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。

Horizon Console での製品ライセンス キーまたはライセンス モードの変更

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場合や、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 Console を使用して製品のライセンス キーを変更できます。VMware Horizon Cloud Service の Horizon 7 デプロイに基づいて、Horizon 7 の無期限ライセンスまたはサブスクリプション ライセンスのいずれかを取得できます。Horizon Console を使用して、ポッドのライセンス モードをサブスクリプション ライセンスから無期限ライセンスに変更できます（その逆の変更も可能）。

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。

前提条件

- Horizon 7 と、Horizon Composer や公開アプリケーションなどのアドオン機能を正常に動作させるため、有効な製品のライセンス キーを入手してください。
- サブスクリプション ライセンスを使用するには、サブスクリプション ライセンスで Horizon 7 を有効にしていることを確認します。『Horizon 7 のインストール』を参照してください。[ライセンス] パネルには、Horizon 7 ポッドのサブスクリプション ライセンスに関する情報が表示されます。

手順

1 Horizon Console で、[設定] - [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 キーを編集するには、[ライセンスを編集] をクリックして、ライセンスのシリアル番号を入力し、[OK] をクリックします。

更新されたライセンス情報が [ライセンスの設定] パネルに表示されます。

3 （オプション）Horizon 7 ポッドをサブスクリプション ライセンスから無期限ライセンスに変更するには、[無期限ライセンスを使用する] をクリックして [OK] をクリックします。

更新されたライセンス情報が [ライセンスの設定] パネルに表示されます。

4 （オプション）Horizon 7 ポッドを無期限ライセンスからサブスクリプション ライセンスに変更するには、[サブスクリプション ライセンスを使用する] をクリックして [OK] をクリックします。これで、VMware Horizon Cloud Service 管理者はサブスクリプション ライセンスで Horizon 7 ポッドを有効にできます。

更新されたライセンス情報が [ライセンスの設定] パネルに表示されます。

5 ライセンスの有効期限の日付を確認します。

6 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、Horizon 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。

7 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。

ライセンス使用量の監視

Horizon Console では、Horizon 7 に同時接続しているアクティブなユーザーを監視できます。[使用量の設定] パネルには、現在の使用量と過去の最も高い使用量が表示されます。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 7 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 7 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 7 は、Horizon 7 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、[使用量の設定] パネルの [現在] 列には、Horizon 7 環境を最初に構成してからのユーザー数、または指定ユーザー数を最後にリセットしてから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 7 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。

同時接続ユーザーの場合、[使用量の設定] パネルの [最大] 列には、並列デスクトップ セッションの最大数、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 7 環境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。

ライセンス使用量データのリセット

Horizon Console で、製品使用量データの履歴をリセットして、現在のデータ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。

前提条件

製品ライセンスの使用状況について理解しておきます。ライセンス使用量の監視を参照してください。

手順

1 Horizon Console で、[設定] - [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。

カスタマー エクスペリエンス向上プログラムへの参加

VMware カスタマー エクスペリエンス向上プログラム (CEIP) に参加するように Horizon 7 を設定できます。

CEIP で VMware が収集するデータの種類と VMware がそのデータを使用する方法については、http://www.vmware.com/trustvmware/ceip.html の「Trust & Assurance」を参照してください。

Horizon Client でデータ共有を設定するには、該当する Horizon Client のインストールとセットアップ ガイドを参照してください。たとえば、Windows クライアントの場合は、VMware Horizon Client for Windows のインストールとセットアップ ガイドを参照してください。HTML Access でデータ共有を設定する場合は、VMware Horizon HTML Access のインストールとセットアップ ガイドを参照してください。

手順

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

2 [カスタマー エクスペリエンス プログラム] タブを選択して、[編集設定] をクリックします。

3 CEIP に参加するには、[VMware カスタマー エクスペリエンス向上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 （オプション） 組織の地理的な場所、業種、従業員数を選択します。

5 [OK] をクリックします。

Skyline Collector アプライアンスとの Horizon Connection Server の統合

VMware のテクニカル サポートが Horizon 7 で発生した問題の診断と解決に使用する Skyline Collector アプライアンスを Horizon Connection Server を統合できます。Skyline Collector アプライアンスは、Connection Server のログを取得し、ログ収集に設定された Horizon 7 管理者ユーザーに提供します。

手順

1 Horizon Console で、操作ログの収集権限を持つログ コレクタ管理者というカスタム ロールを作成します。Horizon Console でのカスタム ロールの追加を参照してください。

2 カスタム ロールの説明を追加します。

3 新しい管理者ユーザーを追加し、そのユーザーにインベントリ管理者（読み取り専用）ロールとログ コレクタ管理者カスタム ロールを選択します。

Skyline Collector アプライアンスは、この管理者ユーザーが Horizon 7 の問題を診断して解決できるように Connection Server のログを取得します。

JMP Integrated Workflow スタート ガイド

10

JMP Integrated Workflow 概念の概要を理解し、JMP Integrated Workflow 機能を使用するために必要な作業をよく理解してください。

この章には、次のトピックが含まれています。

JMP Integrated Workflow のバージョン情報

VMware Horizon JMP (Just-in-Time Management Platform) の統合ワークフロー機能を使用すると、ユーザーまたはユーザー グループのデスクトップ ワークスペースを 1 つのコンソールで定義し、管理することができます。

デスクトップ ワークスペースを作成するには、VMware Horizon デスクトップ プール、VMware App Volumes AppStacks、VMware Dynamic Environment Manager の設定などを含む JMP の割り当てを定義します。JMP 割り当てを送信すると、JMP 自動化エンジンが Horizon 7、App Volumes、Dynamic Environment Manager システムと通信を行い、デスクトップの使用資格をユーザーに付与します。

既存の JMP 割り当ては、Horizon Console の [割り当て (JMP)] タブで管理できます。各コンポーネントの割り当ては、それぞれの JMP コンポーネントのコンソールで変更できます。たとえば、JMP 割り当てで定義されたデスクトップ プールを変更するには、Horizon Console で [インベントリ] - [デスクトップ] の順に選択します。

Horizon Console で JMP 割り当てを開くと、JMP 割り当ての各コンポーネントが予測される状態であることが確認されます。違いがあると、影響を受ける領域がコンソールで強調表示されます。現在の状態を受け入れることも、割り当てを変更して必要な状態にし、ユーザーの資格を再度付与することもできます。

VMware Horizon JMP Server をインストールして構成すると、Horizon Console で JMP Integrated Workflow 機能が使用可能になります。詳細について h、 JMP 統合ワークフローの開始と『VMware Horizon JMP Server のインストールとセットアップ ガイド』を参照してください。

注： App Volumes が VMware Cloud をサポートしていないため、JMP Integrated Workflow 機能は AWS の VMware Cloud® をサポートしていません。

JMP 統合ワークフローの開始

JMP Integrated Workflow 機能を使用するには、JMP Server をインストールして設定し、JMP を構成する必要があります。

前提条件

インストールするすべてのテクノロジー コンポーネントの前提条件とシステム要件を確認します。

手順

1 必要であれば、管理者ユーザーおよびグループを Active Directory で設定します。

『Horizon 7 のインストール』ドキュメントの「Active Directory の準備」を参照してください。JMP を構成するには、Active Directory の情報が必要です。

2 Microsoft SQL Server を設定し、JMP Server のインストールで使用するログイン認証情報が作成されていることを確認します。詳細については、『VMware Horizon JMP Server のインストールとセットアップ ガイド』ドキュメントの「 JMP Server のデータベース要件」を参照してください。

3 VMware Horizon7 バージョン 7.5 以降をインストールして設定します。

『Horizon 7 のインストール』ドキュメントを参照してください。

4 （オプション）VMware App Volumes 2.14 以降をインストールして設定します。これにより、アプリケーションをリアルタイムで提供できます。

詳細については、『VMware App Volumes インストール ガイド』ドキュメントを参照してください。

5 （オプション）コンテキスト ポリシーを管理するには、VMware Dynamic Environment Manager 9.2.1 以降をインストールして設定します。

『VMware Dynamic Environment Manager のインストールと設定』ドキュメントを参照してください。

6 JMP Server が組織のネットワーク内にある他のサーバと安全に通信できるように、CA 署名付きの SSL 証明書を取得します。

7 JMP Integrated Workflow 機能に必要な他のサーバと通信できるように、JMP Server をインストールして JMP Server に SSL 証明書を設定します。

詳細については、『VMware Horizon JMP Server のインストールとセットアップ ガイド』を参照してください。

8 初めての場合は、JMP を構成します。詳細については、 JMP の初期構成を参照してください。

次のステップ

前のタスクが正常に終了すると、JMP 割り当ての作成をすぐに始めることができます。詳細については、JMP 割り当ての作成を参照してください。

JMP 設定の管理

11

JMP Server をインストールしたら、JMP 割り当てを作成したり、JMP Integrated Workflow の機能を使用する前に、JMP の設定で必要な資格情報を設定する必要があります。必要であれば、JMP 設定を編集し、新しい設定情報を追加できます。

この章には、次のトピックが含まれています。

JMP の初期構成

JMP 割り当てを作成する前に、Horizon Console を使用して JMP を構成する必要があります。ユーザーまたはグループへのデスクトップ ワークスペースの割り当てで使用する Active Directory ドメインの認証情報を入力する必要があります。JMP 割り当ての作成で App Volumes AppStack と Dynamic Environment Manager 設定共有を使用するときに、認証情報を含めることもできます。

前提条件

- VMware Horizon JMP Server が正常にインストールされ、その URL があることを確認します。詳細については、『VMware Horizon JMP Server のインストールとセットアップ ガイド』を参照してください。
- JMP Server で使用する Horizon 7 バージョン 7.5 以降の管理者アカウントの認証情報を取得します。
- JMP Server で使用する Active Directory 認証情報を取得します。
- JMP 割り当てにアプリケーションを割り当てる場合は、使用する VMware App Volumes Manager インスタンスの URL と管理者アカウントの認証情報があることを確認します。ロード バランサで App Volumes Manager インスタンスを管理する場合は、ロード バランサの URL を取得し、App Volumes Manager 情報を設定するときに使用します。
- VMware Dynamic Environment Manager 設定共有を使用する場合は、その UNC パスとアクセスに必要な管理者アカウントの認証情報を取得します。

手順

1 Horizon Console で、[JMP 設定] をクリックします。

2 JMP Server の情報を入力します。

a [JMP Server] タブで、[JMP Server の追加] をクリックします。

b `https://jmp.yourcompany.com` の形式で JMP Server の URL を入力します。

c [保存] をクリックします。

JMP Server URL が検証されます。`JMP Server が到達不能`というメッセージを受信した場合は、正しい URL を入力していることを確認します。また、JMP Server が正しく構成され、JMP Server が到達可能であることを確認します。

3 JMP Server で使用する Horizon 7 Connection Server バージョン 7.5 以降のアカウント情報を入力します。

a [Horizon 7] タブをクリックします。

b 自動入力されていない場合は、[Connection Server URL] の値を入力します。この URL は、Horizon Console が接続している Horizon 7 Connection Server の URL と同じです。

c Horizon 7 サービス アカウントのユーザー名とパスワードを入力します。

d [サービス アカウント ドメイン] テキスト ボックスに、作成中の JMP 割り当てで使用する有効な名前を入力して、[Enter] を押します。

e [保存] をクリックします。

4 JMP 割り当てで使用する Active Directory の情報を入力します。

a [Active Directory] タブをクリックします。

b [新規] をクリックします。

c [NETBIOS 名] テキスト ボックスで、使用可能な NetBIOS ドメイン名のリストから選択します。

[DNS ドメイン名] テキスト ボックスと [コンテキスト] テキスト ボックスにデフォルト値が表示されます。

d [DNS ドメイン名] テキスト ボックスに追加されたデフォルト値が正しい値かどうか確認します。必要であれば、別の Active Directory の完全修飾ドメイン名を入力します。例：`mycompany.com`

e [プロトコル] セクションで、Active Directory のプロトコルを選択します。

f [バインド ユーザー名] と [バインド パスワード] テキスト ボックスに、バインド識別名 (DN) のユーザー アカウントの認証情報を入力します。例：**`administrator`**

g デフォルトとは異なる値を使用する場合は、[コンテキスト] テキスト ボックスの値を変更します。

この値は、Active Directory データ検索のルートとして使用されます。

h （オプション）[詳細プロパティ] をクリックして、ポート番号のデフォルト値を変更します。

デフォルトのポート値は、以前に選択したプロトコルに基づいて設定されます。ポート値を変更することも、テキスト ボックスを空白にすることもできます。

i [ドメイン コントローラ] テキスト ボックスに、Active Directory トラフィックの処理に使用する 1 つ以上のホスト名または IP アドレスを入力できます。

例：`adserver.mycompany.com, 10.111.XXX.XXX` テキスト ボックスを空白にすると、[DNS ドメイン名] テキスト ボックスに値が使用されます。

j [保存] をクリックします。

5 JMP 割り当ての作成で App Volumes Appstack を使用する場合は、使用する App Volumes Manager を構成します。

a [App Volumes] タブをクリックします。

b [新規] をクリックします。

c App Volumes インスタンスに割り当てる名前を [名前] テキスト ボックスに入力します。テキスト ボックスを空白にすると、[App Volumes サーバ URL] テキスト ボックスに入力した値が使用されます。

d JMP Server ポッドを関連付ける App Volumes Manager に有効な URL を入力します。

重要： 使用する App Volumes Manager をロード バランサが管理する場合は、そのロード バランサの URL を入力します。

e App Volumes Manager またはロード バランサの管理者アカウントの認証情報を入力します。この認証情報は、JMP Server が App Volumes Manager にアクセスするときに使用します。

f JMP 割り当てに使用される App Volumes Manager サービス アカウントのドメイン名を入力します。

g （オプション）1 つ以上の App Volumes Manager を登録する場合は、切り替えボタンを使用して、追加する App Volumes Manager が JMP 割り当ての作成で使用するデフォルトのサーバかどうかを示します。JMP 割り当ての作成時に使用するインスタンスは変更できます。

h [保存] をクリックします。

6 JMP 割り当てを作成するときに Dynamic Environment Manager 構成共有を使用する場合は、JMP 設定にその情報を追加します。

a [UEM] タブをクリックします。

b [新規] をクリックします。

c [ファイル共有の UNC パス] テキスト ボックスに、`\\fileserver-name\UEM-configuration-share-pathname` という形式で値を入力します。例：`\\FileServer\UEMConfig`。

重要： 入力するファイル共有の UNC パスに `General` は含めないでください。

d Dynamic Environment Manager 構成共有への接続に使用する Dynamic Environment Manager 管理者アカウントの認証情報を入力します。

e [Active Directory] リストから、Dynamic Environment Manager 構成共有で使用するドメイン名を選択します。

> **注：** Active Directory に 1 つの Dynamic Environment Manager 構成共有を関連付けることができます。

f [保存] をクリックします。

次のステップ

JMP の初期設定が完了すると、JMP 割り当てを作成できます。詳細については、JMP 割り当ての作成を参照してください。

JMP 設定の管理

Horizon Console では、JMP 設定の情報を変更、追加、削除できます。

- 特定の JMP 設定を変更するために、必要な情報を準備する必要があります。
- JMP 設定を変更するには、適切な管理者権限が必要です。

JMP Server の設定の編集

既存の JMP Server 設定を変更するには、Horizon Console を使用します。

前提条件

- 特定の JMP Server 設定を変更するために、必要な情報を準備する必要があります。
- Horizon Console にログインして JMP Server の設定を変更するには、適切な管理者権限が必要です。

手順

1 Horizon Console で、[JMP 設定] を選択します。

2 [JMP 設定] ペインで、[JMP Server] タブをクリックします。

3 [編集] をクリックします。

4 [JMP Server の URL] に新しい URL を入力します。

5 [保存] をクリックします。

新しい JMP Server URL が検証されます。無効な場合、エラー メッセージが表示されます。

Horizon 7 認証情報の編集

既存の Horizon 7 Connection Server の資格情報を変更するには、Horizon Console を使用します。

手順

1 Horizon Console で、[JMP 設定] をクリックします。

2 [Horizon 7] タブをクリックします。

3 [認証情報の編集] をクリックします。

4 必要であれば、[サービス アカウント ユーザー名] に新しいユーザー名を入力します。

5 必要であれば、[サービス アカウント パスワード] に新しいパスワードを入力します。

6 必要であれば、[サービス アカウント ドメイン] の値を変更します。

7 [保存] をクリックします。

Horizon 接続サーバ URL の編集

既存の JMP 割り当てに別の Horizon Connection Server に関連付けるには、JMP 割り当てに関連付けられている JMP Server の 設定で登録済みの Horizon Connection Server URL を変更する必要があります。

Horizon Console には、Horizon Connection Server の情報を変更できるユーザー インターフェイスがありません。JMP の設定で既存の Horizon Connection Server ホスト URL を変更するには、SQL Server Management Studio を使用する必要があります。

前提条件

- SQL Server Management Studio セッションにログインし、JMP Server に作成した SQL Server データベースにアクセスするには、適切なシステム管理者権限が必要です。
- データベースの変更を行う前に、SQL Server データベースをバックアップします。

手順

1 現在、Horizon Console セッションにログインしている場合は、ログアウトします。

2 sysadmin (SA) として SQL Server Management Studio セッションにログインするか、SA 権限を持つユーザー アカウントにログインします。

3 置換する Horizon Connection Server ホスト URL が別の JMP Server インスタンスに登録されていないことを確認します。

たとえば、置換する Horizon Connection Server ホスト URL が `new-horizon-host.com` の場合、次の SQL ステートメントを使用して、登録されていないことを確認します。

```
SELECT * from  xms_services
WHERE xms_services.host = "new-horizon-host.com"
```

4 前の SQL ステートメントが結果を返さない場合は、次の手順に進みます。それ以外の場合は、次のステートメントを使用して、既存の Horizon Connection Server ホストの情報を削除します。

```
DELETE from xms_services
WHERE xms_services.host = "new-horizon-host.com"
```

5 次のステートメントを使用して、既存の JMP Server の設定を更新します。`new-horizon-server-host.com` は、置換する Horizon Connection Server ホストの URL です。`old-horizon-host.com` は、現在登録されている Horizon Connection Server ホストの URL です。

```
UPDATE xms_service_endpoints
SET host = 'new-horizon-host.com', is_available = 1
```

```
WHERE service_id = (SELECT id FROM xms_services WHERE service_type = 'horizon'
    AND host = 'old-horizon-host.com')
AND host = 'old-horizon-host.com'

UPDATE xms_services
SET [name] = 'horizon-https://new-horizon-host.com', host = 'new-horizon-host.com'
WHERE service_type = 'horizon'
AND host = 'old-horizon-host.com'
```

6 新しい Horizon Connection Server URL を使用して Horizon Console にログインして、新しい Horizon Connection Server ホストが古い Horizon Connection Server ホストの JMP 割り当てに関連付けられたことを確認します。

Active Directory ドメインの追加

最初の Active Directory ドメインを設定した後、別のドメインを追加する場合は、Horizon Console を使用します。

手順

1 Horizon Console で、[JMP 設定] をクリックします。

2 [Active Directory] タブをクリックし、[追加] をクリックします。

3 [NETBIOS 名] テキスト ボックスで、使用可能な NetBIOS ドメイン名のリストから選択します。

[DNS ドメイン名] テキスト ボックスと [コンテキスト] テキスト ボックスにデフォルト値が表示されます。

4 NETBIOS 名の更新後に、[DNS ドメイン名] テキスト フィールドにデフォルト値が追加されていることを確認します。必要であれば、別の Active Directory の完全修飾ドメイン名を入力します。例：`mycompany.com`

5 [プロトコル] セクションで、Active Directory のプロトコルを選択します。

6 [バインド ユーザー名] と [バインド パスワード] テキスト フィールドに、バインド識別名 (DN) のユーザー アカウント（Administrator など）の認証情報を入力します。

7 デフォルトとは異なる値を使用する場合は、[コンテキスト] テキスト フィールドの値を変更します。

8 （オプション）[詳細プロパティ] をクリックして、ポート番号のデフォルト値を変更します。

デフォルトのポート値は、以前に選択したプロトコルに基づいて設定されます。ポート値を変更することも、テキスト フィールドを空白にすることもできます。

9 [ドメイン コントローラ] テキスト フィールドに、Active Directory トラフィックの処理に使用する 1 つ以上のホスト名または IP アドレスを入力できます。

10 [保存] をクリックします。

Active Directory のテーブルに、新しく追加された Active Directory ドメインの情報が表示されます。

Active Directory ドメイン情報の編集

JMP の設定を最初に構成した後に特定の情報が変更されている場合は、Horizon Console を使用して Active Directory ドメインの設定情報を変更します。

手順

1 Horizon Console で、[JMP 設定] をクリックします。

2 [Active Directory] タブをクリックします。

3 Active Directory ドメインのテーブルで 1 つの行を選択し、[編集] をクリックします。

4 更新する必要がある Active Directory 情報を変更します。

5 [保存] をクリックします。

Active Directory ドメイン情報の削除

既存の Active Directory (AD) ドメインの設定情報を削除するには、Horizon Console を使用します。

登録済みの Active Directory ドメインが既存の JMP 割り当てで使用されていない場合、このドメインの情報を JMP の設定から削除できます。

手順

1 Horizon Console で、[JMP 設定] をクリックします。

2 [Active Directory] タブをクリックします。

3 テーブルで、JMP 設定から削除する Active Directory ドメインの行を選択します。

4 削除確認のダイアログが表示されたらメッセージを確認し、[削除] をクリックして、この Active Directory ドメイン情報の削除を確認します。

Active Directory ドメインを使用する JMP 割り当てがない場合、ドメインが削除されます。

Active Directory ドメインが JMP 割り当てで使用されている場合、警告のダイアログ ボックスが表示されます。警告メッセージに、Active Directory ドメインを使用している JMP 割り当てのリストが表示されます。ドメインを JMP 割り当てから削除するか、ドメインを使用している JMP 割り当てを削除した場合にのみ、ドメイン情報を削除できます。

App Volumes 情報の追加

Horizon Console で App Volumes Manager の情報を追加し、JMP 割り当ての作成時に使用できます。

手順

1 Horizon Console で、[JMP 設定] をクリックします。

2 [App Volumes] タブをクリックし、[追加] をクリックします。

[App Volumes インスタンスの追加] ダイアログ ボックスが表示されます。

3 App Volumes インスタンスに割り当てる一意の名前を [名前] テキスト ボックスに入力します。テキスト ボックスを空白にすると、[App Volumes サーバ URL] テキスト ボックスに入力した値が使用されます。

4 [App Volumes サーバ URL] テキスト ボックスに、JMP Server に関連付ける App Volumes Manager に有効な URL を入力します。追加する App Volumes Manager をロード バランサが管理する場合は、そのロード バランサの URL を入力します。

注： 追加した App Volumes Manager が 別の SQL データベースに接続している場合、追加した App Volumes Manager の情報が App Volumes タブに表示されます。App Volumes Manager が同じ SQL データベースに接続している場合は、以前に登録した App Volumes Manager の情報のみが App Volumes タブに表示されます。

5 JMP Server が App Volumes Manager へのアクセスで使用する App Volumes 管理者のユーザー名とパスワードを入力します。

6 JMP 割り当てに使用される App Volumes サービス アカウントのドメイン名を入力します。

7 追加する App Volumes Manager を JMP 割り当ての作成時にデフォルトで使用する App Volumes Manager サーバにするには、切り替えボタンをクリックします。JMP 割り当ての作成時に使用するサーバは変更できます。

切り替えボタンが青色に変わり、[はい] というラベルが表示されます。

8 [保存] をクリックします。

App Volumes インスタンス情報の編集

JMP 割り当てで使用される App Volumes インスタンスの情報を変更する場合は、Horizon Console で 情報を変更します。

手順

1 Horizon Console で、[JMP 設定] をクリックします。

2 [App Volumes] タブをクリックして、変更する App Volumes のインスタンスのテーブル行を選択します。

3 [編集] をクリックします。

[App Volumes インスタンスの追加] ダイアログ ボックスが表示されます。

4 更新する必要がある App Volumes インスタンス情報を変更します。

5 [保存] をクリックします。

App Volumes インスタンス情報の削除

App Volumes インスタンスの既存の設定を削除する場合は、Horizon Console を使用します。

登録済みの App Volumes インスタンスが JMP 割り当てで使用されていない場合、このインスタンスの情報を JMP の設定から削除できます。

手順

1 Horizon Console で、[JMP 設定] をクリックします。

2 [App Volumes] タブをクリックします。

3 JMP の設定から削除する App Volumes インスタンス情報の行を選択します。

4 [削除] をクリックして、この App Volumes インスタンス情報の削除を確認します。

App Volumes インスタンスを使用する JMP 割り当てがない場合、インスタンスが削除されます。

App Volumes インスタンスが JMP 割り当てで使用されている場合は、警告のダイアログ ボックスが表示されます。警告メッセージに、App Volumes インスタンスを使用している JMP 割り当てのリストが表示されます。App Volumes インスタンスを JMP 割り当てから削除するか、インスタンスを使用している JMP 割り当てを削除した場合にのみ、インスタンス情報を削除できます。

Dynamic Environment Manager 構成共有情報の追加

最初の Dynamic Environment Manager 構成共有情報を設定した後に別の共有を追加する場合は、Horizon Console を使用します。

Active Directory ドメインごとに 1 つの Dynamic Environment Manager 構成共有を追加できます。追加する構成共有に、JMP Server 設定の構成共有と同じ IP アドレスまたは DNS アドレスを設定することはできません。

手順

1 Horizon Console で、[JMP 設定] をクリックします。

2 [UEM] タブをクリックして、[追加] をクリックします。

[UEM ファイル共有の追加] ダイアログ ボックスが表示されます。

3 [ファイル共有の UNC パス] テキスト ボックスに、`\\server-name\UEM-configuration-share-pathname` という形式で値を入力します。

たとえば、構成共有の場所が `\\<IP-address>\uemshare\config\general\FlexRepository\..` の場合、[ファイル共有の UNC パス] テキスト ボックスに **`\\<IP-address>\uemshare\config`** を入力する必要があります。

4 Dynamic Environment Manager 構成ファイル共有への接続で使用する Dynamic Environment Manager のユーザー名とパスワードを入力します。

5 [Active Directory] リストから、Dynamic Environment Manager 構成ファイル共有を使用するドメイン名を選択します。

注： Active Directory に 1 つの Dynamic Environment Manager 構成ファイル共有を関連付けることができます。

6 [保存] をクリックします。

Dynamic Environment Manager 構成ファイル共有の情報が JMP 設定に追加され、[UEM] タブのテーブルに新しい行が追加されます。

Dynamic Environment Manager 構成ファイルの共有情報の編集

JMP 割り当てで使用されている Dynamic Environment Manager 構成ファイル共有の情報を変更するには、Horizon Console を使用します。

手順

1 Horizon Console で、[JMP 設定] をクリックします。

2 [UEM] タブをクリックして、既存の情報が保存されているテーブルで、変更する Dynamic Environment Manager 構成ファイル共有の行を選択します。

3 [編集] をクリックします。

[UEM ファイル共有の編集] ダイアログ ボックスが表示されます。

4 更新する必要がある Dynamic Environment Manager 構成ファイル共有の情報を変更します。

5 [保存] をクリックします。

Dynamic Environment Manager 構成共有情報の削除

Dynamic Environment Manager 構成共有の既存の設定を削除する場合は、Horizon Console を使用します。

登録済みの Dynamic Environment Manager 構成共有が JMP 割り当てで使用されていない場合、この構成共有を JMP 設定から削除できます。

手順

1 Horizon Console で、[JMP 設定] をクリックします。

2 [UEM] タブをクリックします。

3 JMP の設定から削除する Dynamic Environment Manager 構成共有情報の行を選択します。

4 [削除] をクリックして、この Dynamic Environment Manager 構成共有情報の削除を確認します。

Dynamic Environment Manager 構成共有を使用する JMP 割り当てがない場合、構成共有が削除されます。

Dynamic Environment Manager 構成共有が JMP 割り当てで使用されている場合は、警告のダイアログ ボックスが表示されます。警告メッセージに、Dynamic Environment Manager 構成共有を使用している JMP 割り当てのリストが表示されます。Dynamic Environment Manager 構成共有を JMP 割り当てから削除するか、構成共有を使用している JMP 割り当てを削除した場合にのみ、その構成共有情報を削除できます。

JMP 割り当ての管理

12

JMP Server をインストールして JMP の構成を行うと、JMP Integrated Workflow 機能を使用して JMP 割り当ての作成、変更、複製、削除を行うことができます。

まず、JMP 割り当ての作成を開始する前に、JMP Server をインストールして JMP の構成を行う必要があります。詳細については、『VMware Horizon JMP Server のインストールとセットアップ ガイド』および JMP の初期構成を参照してください。

JMP 割り当てを作成、編集、複製または削除する前に、次の前提条件が満たされていることを確認します。

- JMP の設定で登録されている Horizon 7 インスタンスが起動し、実行されていることを確認します。
- 1 つ以上の Active Directory ドメインが JMP の設定で登録されていることを確認します。
- JMP の設定で登録されている App Volumes インスタンスが起動し、実行されていることを確認します。
- JMP 設定で定義されている Dynamic Environment Manager 構成共有が起動し、実行されていることを確認します。

注： グローバル資格はサポートされていません。

JMP 割り当ての作成、編集、複製または削除を行っているときに、「アクションが正常に完了しませんでした」というメッセージが表示される場合があります。たとえば、基盤となる JMP テクノロジー コンポーネントの 1 つに接続を試みたときに問題が発生し、割り当ての検証に失敗する場合があります。JMP 割り当てのサマリ画面で、次のオプションのいずれかを選択し、問題を修正を行います。

- 問題を手動で修正するには、[編集] をクリックします。
- 現在の JMP 割り当てで見つかった問題を JMP Server が修正するように設定するには、[修復] をクリックします。
- JMP 割り当てを完全に削除するには、[強制的に削除] をクリックします。

この章には、次のトピックが含まれています。

JMP 割り当ての作成

Horizon Console では、ユーザーまたはユーザー グループのデスクトップ ワークスペースの作成で使用する JMP 割り当てを作成できます。

JMP 割り当てを定義するには、Horizon デスクトップ プール、App Volumes Appstack、User Environment Manager の設定を選択します。

前提条件

12 章 JMP 割り当ての管理に記載されている前提条件を満たしていることを確認します。

手順

1 Horizon Console で、[割り当て (JMP)] をクリックします。

2 [新規] をクリックします。

3 [新しい割り当て] ウィザードの [ユーザー] タブで、[Active Directory] ドロップダウン リストの横に 2、3 文字入力し、新しい JMP 割り当てに追加するユーザーまたはユーザー グループを選択します。

選択した項目が [選択したユーザー/グループ] セクションに追加されます。

4 [次へ] をクリックします。

5 [デスクトップ] タブで、JMP 割り当てに追加するデスクトップ プールを選択し、[次へ] をクリックします。

6 [アプリケーション] タブで、JMP 割り当てに追加するアプリケーション名の横にあるチェック ボックスをクリックします。選択が終了したら、[次へ] をクリックします。

7 [ユーザー環境] タブで、使用可能なユーザー環境設定で JMP 割り当てを設定するかどうかを決めます。

- [UEM の設定を無効にしますか?] を [いいえ] に設定して [スキップ] をクリックすると、User Environment Manager の割り当てファイルが User Environment Manager の構成共有に保存されません。User Environment Manager のすべての設定が、現在作成している JMP 割り当てを使用するユーザーの仮想デスクトップ ワークスペースに適用されます。
- [UEM の設定を無効にしますか?] を [いいえ] に設定した場合は、作成している JMP 割り当てに適用するユーザー環境設定を選択します。[次へ] をクリックすると、選択したユーザー環境設定で User Environment Manager の割り当てファイルが作成されます。選択した設定が、現在作成している JMP 割り当てを使用するユーザーの仮想デスクトップ ワークスペースに適用されます。
- [UEM の設定を無効にしますか?] を [はい] に設定すると、使用可能なユーザー環境設定のリストがビューから消えます。[次へ] をクリックすると、空の割り当てファイルが、User Environment Manager の構成共有に書き込まれます。User Environment Manager の設定を無効にすると、現在作成している JMP 割り当てを使用するユーザーの仮想デスクトップ ワークスペースにユーザー環境設定が適用されません。

8 [定義] タブで、JMP 割り当てのデフォルト名をそのまま使用するか、別の名前で置き換えます。また、必要に応じて説明を追加します。

9 [AppStack の接続] ドロップダウン リストで、AppStack が JMP 割り当てに接続するタイミングを選択し、[次へ] をクリックします。

10 [サマリ] タブで、新しい割り当ての詳細を確認します。問題がなければ、[送信] をクリックします。変更を行う必要がある場合は、[戻る] をクリックして調整します。

新しい JMP 割り当てがキューに入り、JMP データベースへの保存待ち状態になります。また、[JMP 割り当て] ペインの割り当てリストに追加されます。JMP 割り当てが JMP データベースに正常に追加されると、ステータスが保留状態から変わります。これは JMP 割り当てリストで選択可能になり、編集、複製、削除を行うことができます。

また、次の情報を使用すると、新しい JMP 割り当てに作成された割り当てまたは資格を確認できます。

- JMP 割り当てに作成された Horizon デスクトップ プールの情報を確認するには、Horizon Console を使用します。[インベントリ] - [デスクトップ] の順に選択し、JMP Server によって作成されたデスクトップ プールを検索します。
- JMP Server によって新しい JMP 割り当てに作成された AppStack の情報を表示するには、App Volumes Manager コンソールを使用します。[ボリューム] - [AppStack] の順に選択し、JMP Server によって作成された AppStack を検索します。
- JMP 割り当てに設定したユーザー環境設定を確認するには、Dynamic Environment Manager 管理コンソールを使用して [ユーザー環境] タブをクリックします。左側のペインから JMP 割り当てで使用されるユーザー環境設定を選択します。ユーザー環境設定の JMP 割り当て情報が表示されたダイアログ ボックスから、[割り当て] タブをクリックします。

JMP 割り当ての編集

JMP 割り当ての定義に使用されたコンポーネントが変更されると、その割り当ての変更が必要になる場合があります。JMP 割り当てを変更するには、Horizon Console を使用します。

前提条件

- 12 章 JMP 割り当ての管理に記載されている前提条件を満たしていることを確認します。
- 保留状態の JMP 割り当ては編集できません。

手順

1 Horizon Console で、[割り当て (JMP)] をクリックします。

2 チェック ボックスをクリックするか、リストで JMP 割り当ての名前をクリックして、編集する JMP 割り当てを選択します。

3 [編集] をクリックします。

4 [割り当ての編集] ウィザードで、現在の設定を変更します。

編集を中止するには、[キャンセル] をクリックします。

a 現在選択されているユーザーまたはグループを削除するには、削除アイコン ([X]) をクリックします。

b [次へ] をクリックします。

c [デスクトップ] タブで、JMP 割り当てに追加するデスクトップ プールを選択します。[次へ] をクリックします。

d [アプリケーション] タブで、JMP 割り当てに追加するアプリケーションを選択するか、すでに選択されているアプリケーションの選択を解除します。[次へ] をクリックします。

e [ユーザー環境] タブで、使用可能なユーザー環境設定で JMP 割り当てを設定するかどうかを決めます。

- [UEM の設定を無効にしますか?] を [いいえ] に設定して [スキップ] をクリックすると、User Environment Manager の割り当てファイルが User Environment Manager の構成共有に保存されません。User Environment Manager のすべての設定が、現在編集している JMP 割り当てを使用するユーザーの仮想デスクトップ ワークスペースに適用されます。
- [UEM の設定を無効にしますか?] を [いいえ] に設定した場合は、作成している JMP 割り当てに適用するユーザー環境設定を選択します。[次へ] をクリックすると、選択したユーザー環境設定で User Environment Manager の割り当てファイルが作成されます。選択した設定が、現在編集している JMP 割り当てを使用するユーザーの仮想デスクトップ ワークスペースに適用されます。
- [UEM の設定を無効にしますか?] を [はい] に設定すると、使用可能なユーザー環境設定のリストがビューから消えます。[次へ] をクリックすると、空の割り当てファイルが、User Environment Manager の構成共有に書き込まれます。User Environment Manager の設定を無効にすると、現在編集している JMP 割り当てを使用するユーザーの仮想デスクトップ ワークスペースにユーザー環境設定が適用されません。

f 必要であれば、[定義] タブで、[名前]、[説明]、JMP 割り当てに AppStack を接続するタイミングを変更します。

g [次へ] をクリックします。

h 変更内容を確認して [送信] をクリックし、変更を保存します。

成功すると、変更が保存されます。問題が検出されると、追加情報と実行可能なアクションが表示されます。

JMP 割り当ての複製

作成する JMP 割り当てに類似した割り当てを複製すると、JMP 割り当てをより簡単に作成できます。

前提条件

- 12 章 JMP 割り当ての管理に記載されている前提条件を満たしていることを確認します。
- 保留またはエラー状態の JMP 割り当ては複製できません。

手順

1 Horizon Console で、[割り当て (JMP)] を選択します。

2 複製する JMP 割り当てを選択して、[複製] をクリックします。

3 [新しい割り当て] ウィザードを使用して、複製された JMP 割り当てを必要に応じて変更します。

a 新しいユーザーまたはグループを選択するか、現在選択されているユーザーまたはグループを削除します。[次へ] をクリックします。

b [デスクトップ] ペインで、新しいデスクトップ プールを選択します。あるいは、複製された JMP 割り当てに含まれているデスクトップ プールを削除します。[次へ] をクリックします。

c すでに選択されているアプリケーションの選択を解除し、新しい JMP 割り当てに追加するアプリケーションを選択します。[次へ] をクリックします。

d [ユーザー環境] ペインで、新しい JMP 割り当てに適用する User Environment Manager の設定を選択します。[次へ] をクリックします。

e 必要であれば、[定義名] でデフォルトの名前を置き換えます。説明を追加し、AppStack に新しい JMP 割り当てを関連付けるタイミングを指定します。

f [次へ] をクリックして、新しい JMP 割り当てのサマリを確認します。

g 問題がなければ、[送信] クリックします。それ以外の場合は、[戻る] をクリックして、修正を行います。

新しい JMP 割り当てが検証されます。検証に時間がかかる場合があります。検証に成功すると、新しく作成した JMP 割り当てが [JMP 割り当て] ペインのリストに追加されます。名前の上にマウス ポイントを置くと、保留状態であることが通知されます。この状態は、JMP データベースに正常に保存するまで続きます。JMP 割り当てが保留状態でなくなると、割り当てに別のアクションを実行できます。

JMP 割り当ての削除

Horizon Console を使用して、JMP 割り当てを削除します。

JMP 割り当てを削除すると、Horizon プールの資格、AppStack の割り当て、JMP 割り当てに関連付けられている UEM 資格が削除されます。ただし、Horizon プールの資格や JMP 割り当てで使用されている AppStack 割り当てが JMP 割り当ての作成前から存在していた場合、これらの資格や割り当ては削除されません。JMP 割り当てを削除すると、この割り当てはユーザーまたはデスクトップに適用されなくなります。

前提条件

- 12 章 JMP 割り当ての管理に記載されている前提条件を満たしていることを確認します。
- 保留状態の JMP 割り当ては削除できません。

手順

1 Horizon Console で、[割り当て (JMP)] をクリックします。

2 [JMP 割り当て] ペインで、1 つ以上の JMP 割り当てを選択して [削除] をクリックします。

3 確認のダイアログ ボックスで、[削除] をクリックし、割り当てを完全に削除することを確認します。

成功すると、Horizon プールの資格が JMP データベースと [JMP 割り当て] ペインのリストから削除されます。

削除操作の一部が失敗すると、JMP 割り当ては削除されません。ステータス インジケータをクリックすると、削除操作が失敗した原因の詳細が表示されます。

Horizon Console でのイベント レポートの設定 13

イベント データベースを作成し、Horizon 7 イベントについての情報を記録することができます。さらに、Syslog サーバを使用する場合、イベントを Syslog サーバに送信するか、`Syslog` 形式で記述されたイベントのフラット ファイルを作成するように Connection Server を構成できます。

この章には、次のトピックが含まれています。

Horizon Console で Horizon 7 イベント用のデータベースとデータベース ユーザーを追加する

イベント データベースは、既存のデータベース サーバに追加する方法で作成します。続いて、レポート ソフトウェアを使用して、そのデータベース内のイベントを分析できます。

イベント データベース用のデータベース サーバは、専用のサーバにデプロイします。これは、プロビジョニングおよび Horizon 7 のデプロイに対して重要な他のアクティビティにイベントのログ アクティビティが影響を与えないようにするためです。

注： このデータベースのために ODBC データ ソースを作成する必要はありません。

前提条件

- サポートされている Microsoft SQL Server または Oracle データベース サーバが、Connection Server インスタンスでアクセスできるシステム上に存在することを確認します。

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

- データベースとユーザーをデータベース サーバに作成するために必要なデータベース権限があることを確認します。
- Microsoft SQL Server データベース サーバにデータベースを作成する手順に慣れていない場合は、『Horizon 7 のインストール』の「View Composer データベースを SQL Server に追加する」を参照してください。
- Oracle データベース サーバにデータベースを作成する手順に慣れていない場合は、『Horizon 7 のインストール』の「View Composer データベースを Oracle 12c または 11g に追加する」を参照してください。

手順

1 サーバにデータベースを追加し、HorizonEvents のようなわかりやすい名前をこのデータベースに付けます。

Oracle 12c または Oracle 11g データベースの場合は、Oracle システム識別子 (SID) も指定します（この識別子は Horizon Console でイベント データベースを構成する際に使用します）。

2 テーブル、ビュー、Oracle トリガとシーケンスの作成権限とこれらのオブジェクトの読み書き権限を持っているユーザーをこのデータベースに追加します。

Microsoft SQL Server データベースの場合、統合 Windows 認証セキュリティ モデルの認証方法は使用しないでください。認証に SQL Server 認証を使用していることを確認します。

データベースは作成されますが、Horizon Console でデータベースを構成するまでスキーマはインストールされません。

次のステップ

以下の説明に従います。Horizon Console でのイベント データベースの設定

Horizon Console で SQL Server データベースをイベント レポート用に準備する

Horizon Console を使用して Microsoft SQL Server にイベント データベースを設定する前に、正しい TCP/IP プロパティを設定し、サーバが SQL Server 認証を使用していることを確認する必要があります。

前提条件

- イベント レポート用に SQL Server データベースを作成します。Horizon Console で Horizon 7 イベント用のデータベースとデータベース ユーザーを追加するを参照してください。
- データベースを構成するために必要なデータベース権限があることを確認します。
- データベース サーバが SQL Server 認証の認証方法を使用していることを確認します。Windows 認証は使用しないでください。

手順

1 SQL Server 構成マネージャを開き、[SQL Server *YYYY* ネットワークの構成] を展開します。

2 [*server_name* のプロトコル] を選択します。

3 プロトコルのリストで [TCP/IP] を右クリックし、[P プロパティ] を選択します。

4 [有効化] プロパティを [はい] に設定します。

5 ポートが割り当てられていることを確認し、必要であれば割り当てます。

静的および動的なポートおよびポートを割り当てる方法については、SQL Server 構成マネージャのオンライン ヘルプを参照してください。

6 このポートがファイアウォールによってブロックされないことを確認します。

次のステップ

Horizon Console を使用して、データベースを Connection Server に接続します。以下の説明に従います。Horizon Console でのイベント データベースの設定

Horizon Console でのイベント データベースの設定

イベント データベースには、Horizon 7 のイベントに関する情報が、ログ ファイルではなくデータベースのレコードとして格納されます。

Connection Server インスタンスをインストールした後で、イベント データベースを構成します。Connection Server グループ内で構成する必要があるホストは 1 台だけです。グループの他のホストは自動的に構成されます。

注： Connection Server インスタンスと外部データベース間のデータベース接続のセキュリティは、管理者の責任ですが、イベント トラフィックは Horizon 7 環境の 健全性に関する情報に制限されます。さらに慎重を期すのであれば、IPSec などの手段を使用してこのチャネルを保護するか、データベースを Connection Server コンピュータ上でローカルに展開することができます。

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。

また、Horizon 7 イベントを `Syslog` 形式で生成すると、他社製分析ソフトウェアからイベント データにアクセスできます。`vdmadmin` コマンドと `-I` オプションを使用して、Horizon 7 イベント メッセージを `Syslog` 形式でイベント ログ ファイルに記録します。『Horizon 7 の管理』ドキュメントで、「-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。

前提条件

イベント データベースを構成するには、次の情報が必要です。

- データベース サーバの DNS 名または IP アドレス。
- データベース サーバの種類（Microsoft SQL Server または Oracle）。
- データベース サーバへのアクセスに使用するポート番号。デフォルトは、Oracle の場合は 1521、SQL Server の場合は 1433 です。SQL Server では、データベース サーバが名前付きインスタンスの場合、または SQL Server Express を使用している場合は、ポート番号の特定が必要になる場合があります。SQL Server の名前付きインスタンスへの接続については、Microsoft のサポート技術情報（KB）の記事 http://support.microsoft.com/kb/265808 を参照してください。
- データベース サーバに作成したイベント データベースの名前。Horizon Console で Horizon 7 イベント用のデータベースとデータベース ユーザーを追加するを参照してください。

Oracle 12c または 11g データベースの場合、Horizon Console でイベント データベースを設定するときに Oracle System Identifier (SID) をデータベース名として使用する必要があります。

- このデータベース用に作成したユーザーのユーザー名とパスワード。Horizon Console で Horizon 7 イベント用のデータベースとデータベース ユーザーを追加するを参照してください。

  このユーザーに対しては SQL Server 認証を使用します。統合 Windows 認証セキュリティ モデルの認証方法は使用しないでください。

- イベント データベースのテーブルのプレフィックス（VE_ など）。プリフィックスを使用することで、Horizon 7 の複数のインストール間でデータベースを共有できます。

注： 使用しているデータベース ソフトウェアで有効な文字を入力する必要があります。ダイアログ ボックスを終了するときにプレフィックスの構文はチェックされません。使用しているデータベース ソフトウェアで有効でない文字を入力した場合、Connection Server がデータベース サーバへの接続を試行したときにエラーが発生します。ログ ファイルにはすべてのエラーが記録され、このエラーや、データベース名が無効な場合にデータベース サーバから返されるその他すべてのエラーも含まれます。

手順

1 Horizon Console で、[設定] - [イベント設定] の順に選択します。

2 [イベント データベース] セクションで、[編集] をクリックし、提示されるフィールドに情報を入力して、[OK] をクリックします。

  イベント データベース情報をクリアするには、[クリア] をクリックします。

3 （オプション） イベントの設定 ウィンドウで、[編集] をクリックし、イベントを表示する時間の長さ、およびイベントを新規として分類する日数を変更し、[OK] をクリックします。

  これらの設定は、イベントが Horizon Console インターフェイスに表示される期間に関係します。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。

4 [Monitoring（監視）] - [イベント] を選択し、イベント データベースに正常に接続できることを確認します。

  接続できない場合は、エラー メッセージが表示されます。SQL Express を使用している場合、または SQL Server の名前付きインスタンスを使用している場合は、前提条件にあるように、正しいポート番号の特定が必要な場合があります。

Horizon Console でのファイルまたは Syslog サーバへのイベント ログの書き込み

Horizon 7 イベントを `Syslog` 形式で生成すると、分析ソフトウェアからイベント データにアクセスできます。

Connection Server グループ内で構成する必要があるホストは 1 台だけです。グループの他のホストは自動的に構成されます。

イベントのファイル ベースのログ記録を有効にすると、イベントはローカル ログ ファイルに蓄積されます。ファイル共有を指定すると、これらのログ ファイルはその共有に移動されます。

- イベント ログのローカル ディレクトリの最大サイズは、最も古いファイルが削除される前に閉じられたログ ファイルを含めて 300 MB です。Syslog 出力のデフォルトの出力先は `%PROGRAMDATA%\VMware\VDM\events\` です。
- Syslog サーバがない場合や、現在の Syslog サーバまたはイベント データベースではニーズが満たせない場合は、UNC パスを使用して長期的なイベントのレコードのログ ファイルを保存します。

別の方法として、`vdmadmin` コマンドを使用してイベントのファイル ベースのログを Syslog 形式で構成できます。『Horizon 7 の管理』ドキュメントで、`vdmadmin` コマンドの `–I` オプションを使用した Syslog 形式での Horizon 7 イベント ログ メッセージの生成に関するトピックを参照してください。

重要： Syslog サーバに送信されるときに、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間で送信され、ユーザー名などの秘密データが含まれている場合があります。VMware は、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モニターリングする可能性を回避することを推奨します。

前提条件

イベントを Syslog 形式で記録できるようにするか、Syslog サーバに送信できるようにする、またはその両方を実現できるように Connection Server を構成するには、以下の情報が必要です。

- Syslog サーバを使用して UDP ポートで Horizon 7 イベントをリッスンする予定にしている場合、Syslog サーバの DNS 名または IP アドレスと UDP ポート番号が必要です。デフォルトの UDP ポート番号は 514 です。
- フラット ファイル形式でログを収集する予定にしている場合は、ログ ファイルを格納するファイル共有およびフォルダまでの UNC パスが必要で、ファイル共有に書き込む権限を持つアカウントのユーザー名、ドメイン名、パスワードが必要です。

手順

1 Horizon Console で、[設定] - [イベント設定] の順に選択します。

2 （オプション） [Syslog] 領域で、イベントを Syslog サーバに送信するように Connection Server を設定するには、[Syslog サーバに送信] の下にある [追加] をクリックし、サーバ名または IP アドレスと UDP ポート番号を入力します。

3 （オプション） [ファイル システムへのイベント] 領域で、イベント ログ メッセージを生成してログファイルに Syslog 形式で保存するかどうかを選択します。

オプション	説明
Always	イベント ログ メッセージが常に生成され、Syslog 形式で保存されます。
エラー時にファイルにログを記録する（デフォルト）	イベント データベースまたは Syslog サーバにイベントを書き込むときに問題が発生した場合、監査イベントがログ ファイルに記録されます。このオプションは、デフォルトで有効になっています。
実行しない	イベント ログ メッセージが生成されず、Syslog 形式で保存されません。

ログ ファイルは、ファイル共有までの UNC パスを指定しない限り、ローカルで保持されます。

4 （オプション）Horizon 7 イベント ログ メッセージをファイル共有に保存するには、[場所にコピー] の下にある [追加] をクリックして、ログ ファイルを保存するファイル共有またはフォルダまでの UNC パスを入力し、ファイル共有に書き込み権限を持つアカウントのユーザー名、ドメイン名、パスワードを入力します。

以下は、UNC パスの例です。

```
\\syslog-server\folder\file
```

Horizon 7 でのイベントの監視

イベント データベースは、Connection Server ホストまたはグループ、Horizon Agent、Horizon Console 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。[イベント] ページ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 Console 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 Console 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 Connection Server を再起動する必要があります。

Horizon Console 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。Horizon Console でのファイルまたは Syslog サーバへのイベント ログの書き込みと『Horizon 7 のインストール』の「-l 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。

複数の Connection Server にイベント データベースを設定すると、Horizon Console の [イベント] ページにすべての Connection Server のイベントが表示されます。Horizon Console では、実行するタスクに基づいてイベントがフィルタリングされます。これらのイベントは、[デスクトップ プール] や [アプリケーション プール] など、関連するページに表示されます。

前提条件

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 Console で、[監視] - [イベント] の順に選択します。

2 （オプション）[イベント] ページでは、イベントの時間範囲を選択し、イベントにフィルタリングを適用し、一覧表示されたイベントを 1 つ以上の列で並べ替えることができます。

次のステップ

特定のイベントを表示するには、Horizon Console でデスクトップまたはアプリケーション プール、仮想マシン、パーシステント ディスク、ユーザーまたはグループに移動し、[イベント] タブをクリックします。

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 13-1. 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 Console での Horizon Help Desk Tool の使用

14

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 7 の管理ドキュメント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 の管理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 7 の管理ドキュメント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 Connection Server 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 Connection Server 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 Connection Server 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}
  ```

この章には、次のトピックが含まれています。

Horizon Console で Horizon Help Desk Tool を開始します。

Horizon Help Desk Tool は、Horizon Console に統合されています。Horizon Help Desk Tool のトラブルシューティングを行うユーザーを検索できます。

手順

1 [ユーザー検索] テキスト ボックスでユーザー名を検索するか、Horizon Help Desk Tool ツールに直接移動できます。

- Horizon Console で、[ユーザー検索] テキスト ボックスにユーザー名を入力します。
- [監視] - [ヘルプデスク] の順に選択し、[ユーザー検索] テキスト ボックス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。

2 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。

次のステップ

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。

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。

また、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。

注： Linux デスクトップ ユーザーには、Skype for Business の情報は表示されません。

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 14-1. [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。
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。 ■ [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。 ■ [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。 **注：** Linux デスクトップ セッションでは、[アプリケーション] タブにアクセスできません。
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

[デスクトップ] 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 14-2. デスクトップ

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。Linux デスクトップ セッションのデスクトップ プールとして Linux が表示されます。
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。
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

[アプリケーション] 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。

注： Linux デスクトップ セッションでは、[アプリケーション] タブにアクセスできません。

表 14-3. アプリケーション

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。
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： クラウド ポッド アーキテクチャ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 14-4. 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 14-5. 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。
[OS バージョン]	オペレーティング システムのバージョン。
[接続サーバ]	セッションが接続している接続サーバ。
[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。Linux デスクトップ プールの Linux を表示します。
[vCenter Server]	vCenter Server の IP アドレス。
[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。セッションの状態は、アイドル、アクティブまたは切断です。ユーザーが 1 分間非アクティブ状態になると、セッションのステータスがアイドル状態になります。アイドル状態の場合、ステータス アイコンは緑の輪郭で表示されます。アクティブ状態の場合は緑色、切断状態は灰色で表示されます。 **注：** Linux デスクトップ セッションの場合、アイドル状態のステータスは表示されません。
[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。
[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。
[ゲートウェイ/プロキシ名]	セキュリティ サーバ、Unified Access Gateway アプライアンスまたはロード バランサの名前。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。
[ゲートウェイ/プロキシ IP アドレス]	セキュリティ サーバ、Unified Access Gateway アプライアンスまたはロード バランサの 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。
[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。

ユーザー操作性の評価基準

PCoIP または 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、[詳細] をクリックします。これらの詳細を更新するには、更新アイコンをクリックします。

表 14-6. PCoIP 表示プロトコルの詳細

オプション	説明
[Tx バンド幅]	PCoIP セッションの転送バンド幅（キロビット/秒単位）
[フレーム レート]	PCoIP セッションのフレーム率（1 秒あたりのフレーム数）

表 14-6. PCoIP 表示プロトコルの詳細 （続き）

オプション	説明
[パケット ロス]	PCoIP セッションのパケット ロス率。
[Skype の状態]	PCoIP セッションでの Skype for Business のステータス。 ■ 最適化済み ■ フォールバック ■ 最適化済み (バージョン不一致) ■ フォールバック (バージョン不一致) ■ 接続中 ■ 切断されました ■ 未定義 Linux デスクトップ セッションの場合、このオプションは N/A と表示されます。

表 14-7. Blast 表示プロトコルの詳細

オプション	説明
[フレーム レート]	Blast セッションのフレーム率（1 秒あたりのフレーム数）。
[Skype の状態]	Blast セッションでの Skype for Business のステータス。 ■ 最適化済み ■ フォールバック ■ 最適化済み (バージョン不一致) ■ フォールバック (バージョン不一致) ■ 接続中 ■ 切断されました ■ 未定義 Linux デスクトップ セッションの場合、このオプションは N/A と表示されます。
[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 とメモリ使用量、ネットワークとディスクのパフォーマンス

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 表示プロトコルのネットワークまたはディスク パフォーマンスがグラフで表示されます。

注： Horizon Agent デスクトップの起動または再起動後すぐに、パフォーマンス グラフにタイムラインが表示されない場合があります。数分後にタイムラインが表示されます。

表 14-8. CPU 使用率

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。

表 14-9. メモリ使用率

オプション	説明
[セッションのメモリ]	現在のセッションのメモリ使用量。
[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。

表 14-10. ネットワークのパフォーマンス

オプション	説明
[遅延]	PCoIP または Blast セッション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。

表 14-11. ディスクのパフォーマンス

オプション	説明
[読み取り]	1 秒あたりの読み取りの入出力 (I/O) 操作の数。
[書き込み]	1 秒あたりの書き込み I/O 操作の数。
[ディスクの遅延時間]	ディスク遅延のグラフが表示されます。ディスク遅延は、Windows パフォーマンス カウンタから取得した入出力操作/秒 (IOPS) データの時間（ミリ秒）時間です。
[平均読み取り]	1 秒あたりのランダム読み取り I/O 操作の平均数。
[平均書き込み]	1 秒あたりのランダム書き込み I/O 操作の平均数。
[平均の遅延時間]	Windows パフォーマンス カウンタから取得した IOPS データの平均遅延時間（ミリ秒）。

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 14-12. 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。 ■ [プロトコルの接続]。ログインで PCoIP または Blast プロトコル接続の完了にかかった合計時間。 ■ [ログイン スクリプト]。ログイン スクリプトが開始してから完了するまでの合計時間。 ■ [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 のロード] 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。
- セッションが Linux デスクトップ セッションの場合、[GPO のロード] と [プロファイルのロード] のセグメントは表示されません。
- デスクトップ セッションに接続した直後は、ログイン データが使用できない場合があります。数分後にログイン データが表示されます。

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。

RDS ホスト セッションの場合、現在のユーザーまたはシステム プロセスが開始した RDS ホスト セッション プロセスが [プロセス] タブに表示されます。

表 14-13. 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。 Windows コアのプロセスなどの重要なプロセスは終了できません。これらのプロセスも [プロセス] タブに表示される場合があります。重要なプロセスを終了しようとすると、Horizon Help Desk Tool はメッセージを表示し、システム プロセスを終了できないことを通知します。

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。Linux デスクトップ セッションでは、[アプリケーション] タブにアクセスできません。

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。

エンド ユーザーのアプリケーション プロセスを終了できます。アプリケーション プロセスを終了するには、[アプリケーションの終了] をクリックし、変更内容を確認して [OK] をクリックします。

注： データ保存などのユーザー操作の保留中や、その他の例外が発生した場合、アプリケーション プロセスを終了できないことがあります。ただし、アプリケーションの終了時に Horizon Help Desk Tool は成功または失敗を通知するメッセージを表示しません。

表 14-14. 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。

前提条件

- 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。 **注：** Linux デスクトップ ユーザーは、この機能を使用できません。 [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。

vdmadmin コマンドの使用

15

vdmadmin コマンド ライン インターフェイスを使用して、Connection Server 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、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。

- 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。

デフォルトの場合、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。#unique_9 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 15-1. 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 15-2. 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。#unique_186 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。

表 15-2. vdmadmin コマンド オプション （続き）

オプション	説明
–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] -getlogfilelogfile-outfile local_file-d desktop-mmachine
```

```
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 [-mmachine]
```

```
vdmadmin
-A [-b authentication_arguments] -list [-xml] [-w | -n] -d desktop-m machine
```

```
vdmadmin
-A [-b authentication_arguments] -setloglevel level -ddesktop [-mmachine]
```

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 15-3. 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。

表 15-3. Horizon Agent でのログ構成オプション （続き）

オプション	説明
`–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。
`–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 [-bauthentication_arguments] -override-iip_or_dns-ddesktop-mmachine
```

```
vdmadmin
-A [-bauthentication_arguments] -override-list-ddesktop-mmachine
```

```
vdmadmin
-A [-bauthentication_arguments] -override-r-ddesktop [-mmachine]
```

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 15-4. 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 [–bauthentication_arguments] [–udomain\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 [-bauthentication_arguments] -list-xml [-w | -n]
```

```
vdmadmin
-H [-bauthentication_arguments] -list-monitorid monitor_id -xml [-w | -n]
```

```
vdmadmin
-H [-bauthentication_arguments] -monitoridmonitor_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 15-5. 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 15-6. 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 [–bauthentication_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 15-7. 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 15-8. 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。

表 15-8. 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 （続き）

オプション	説明
–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 [–bauthentication_arguments] –ddesktop–m machine–udomain\user
```

```
vdmadmin
–L [–bauthentication_arguments] –ddesktop [–mmachine | –udomain\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 15-9. 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 15-10. 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。#unique_203 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 15-11. 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} -domaindomain-add [-s
connsvr]
```

```
        vdmadmin
        -N [-bauthentication_arguments] -domains-list [-w | -n] [-xml]
```

```
        vdmadmin
        -N [-bauthentication_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 15-12. 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。

表 15-12. ドメイン フィルタの構成のオプション （続き）

オプション	説明
–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 15-13. 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 Connection Server 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 Connection Server 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 Connection Server 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、Connection Server 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 Connection Server 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 Connection Server 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 15-14. 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 15-15. XSL スタイルシート 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 15-15. 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] [-groupgroup_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 [-bauthentication_arguments] [-xml]
```

```
        vdmadmin
        -Q
        -clientauth
        -list [-bauthentication_arguments] [-xml]
```

```
        vdmadmin
        -Q
```

```
        -clientauth
        -remove [-b authentication_arguments] -domain domain_name-clientid client_id
```

```
        vdmadmin
        -Q
        -clientauth
        -removeall [-bauthentication_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 15-16. 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。
–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。

表 15-16. 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
–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} –ownerdomain\user–userdomain\user [–passwordpassword]
```

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 15-17. 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 [-bauthentication_arguments] -e-ddesktop-mmachine [-m machine] ...
```

```
vdmadmin
-V [-bauthentication_arguments] -e-vcdnvCenter_dn-vmpath inventory_path
```

```
vdmadmin
-V [-b authentication_arguments] -p-d desktop -m machine [-mmachine] ...
```

```
vdmadmin
-V [-b authentication_arguments] -p-vcdnvCenter_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 15-18. 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 [–bauthentication_arguments] –collisions [–resolve]
vdmadmin–X [–bauthentication_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 15-19. 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 15-20. 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
```