VMware Horizon FLEX 管理ガイド

Horizon FLEX 1.6

このドキュメントは新しいエディションに置き換わるまで、ここで書いてある各製品と後続のすべてのバージョンをサポートします。このドキュメントの最新版をチェックするには、http://www.vmware.com/jp/support/pubs を参照してください。

JA-001873-00

vmware®

最新の技術ドキュメントは VMware の Web サイト（http://www.vmware.com/jp/support/）にあります
VMware の Web サイトでは最新の製品アップデートも提供されています。
このドキュメントに関するご意見およびご感想がある場合は、docfeedback@vmware.com までお送りください。

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

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

目次

VMware Horizon FLEX 管理ガイド

VMware Horizon FLEX 管理ガイド では、VMware Horizon® FLEX™ のインストールおよび管理方法について説明します。

対象者

この情報は、Horizon FLEX をインストールするユーザーを対象としています。この情報は、仮想マシン テクノロジーに習熟している経験豊富な Windows システム管理者向けに記述されています。

1 Horizon FLEX の紹介

Horizon FLEX は、IT 管理者がエンド ユーザー用のローカル デスクトップを作成、保護、管理できる、ポリシーベースでコンテナ型のデスクトップ ソリューションです。エンド ユーザーは、自分のコンピュータ上の Horizon FLEX 仮想マシンと呼ばれる制限付きの仮想マシン内で作業を実行します。Horizon FLEX 仮想マシンはエンドユーザーのコンピュータ上にローカルで保存されるため、オフラインのユーザーであっても企業のアプリケーションにアクセスできます。

この章では次のトピックについて説明します。

Horizon FLEX のコンポーネント

Horizon FLEX は、Mirage、Fusion Pro、および Workstation Player を含む、VMware 製品の組み合わせです。

Horizon FLEX の VMware Mirage

Horizon FLEX によって使用される Mirage Server。 このサーバによって、Horizon FLEX 仮想マシンを管理します。Mirage を Horizon FLEX レイヤのテクノロジに使用することで、仮想マシンの管理、バックアップ、およびパッチの適用を行うことができます。Mirage for Horizon FLEX の使用はオプションです。その他のイメージ管理ツールを使用して、Horizon FLEX 仮想マシンを管理することもできます。

Horizon FLEX ポリシー サーバ

Horizon FLEX 固有の機能によって拡張された標準の Mirage サーバ。Horizon FLEX ライセンスを Horizon FLEX 用に Mirage に適用した後に、Horizon FLEX ポリシー サーバ がアクティベートされます。

Horizon FLEX 管理コンソール

Horizon FLEX ポリシー サーバ の Web 管理ユーザー インターフェイス。Horizon FLEX 管理コンソールは、Mirage Web Manager コンポーネント内にあります。Horizon FLEX 管理コンソール を使用して、次のような仮想マシン管理タスクを実行します。

- 仮想マシンのインベントリを管理する
- Active Directory サービスのユーザーやグループのリストを参照する
- ユーザーやグループに 1 つ以上の仮想マシンの資格を付与する
- 特定の資格に仮想マシン ポリシーを指定する

- リモート ロックを使用して、ユーザーが仮想マシンにアクセスできないようにする
- いつでも仮想マシンの詳細とステータスを確認する

Horizon FLEX Client

エンド ユーザーが自分のローカル コンピュータに Horizon FLEX 仮想マシンをダウンロードするために使用するクライアント ソフトウェア。クライアントは、VMware Fusion Pro® for Mac コンピュータと VMware Workstation Player™ for Windows コンピュータを含みます。Fusion Pro と Workstation Player が Horizon FLEX パッケージに含まれます。Fusion Pro と Workstation Player の両方に対して 1 つのライセンス キーが提供されます。

Horizon FLEX 仮想マシン

エンド ユーザーが自分のコンピュータで実行する仮想マシンです。Fusion Pro を使用して、Horizon FLEX 仮想マシンのソース仮想マシンを作成します。Fusion Pro が Horizon FLEX パッケージに含まれます。Horizon FLEX Server は最大で 1,000 ユーザーをサポートできます。

注意　VMware Workstation Pro™ を使用してソース仮想マシンを作成することもできます。Workstation Pro は Horizon FLEX パッケージに含まれません。

Mirage の概要

Mirage は、Horizon FLEX 仮想マシンを操作・使用するために必要となります。

Horizon FLEX は、Mirage で使用できる以下の機能のサブセットを使用します。

- Mirage Server
  - Mirage Management Server
- Mirage Web Manager
  - Mirage Management Console

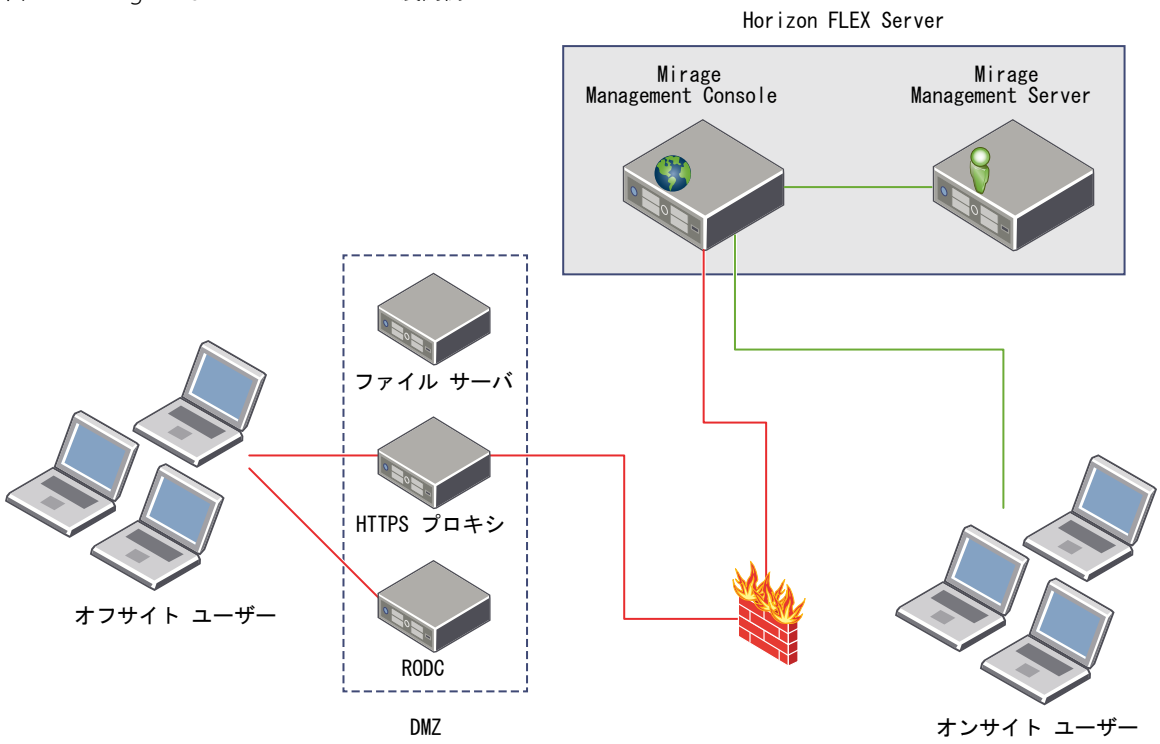
このドキュメントでは、Mirage に関連する一部の情報のみを説明します。Mirage の詳細については、https://www.vmware.com/support/pubs/mirage_pubs.html にある Mirage のドキュメントを参照してください。

Horizon FLEX のアーキテクチャ

一般的な Horizon FLEX の展開環境には、Horizon FLEX Server、ファイル サーバ、HTTPS プロキシ、読み取り専用ドメイン コントローラ (RODC)、およびオフサイトとオンサイトのエンドユーザー システムが存在します。

図 1-1 に、Horizon FLEX の展開環境の主要コンポーネントの関係を示します

図 1-1. Mirage がない Horizon FLEX の展開例



Horizon FLEX サーバ

Horizon FLEX Server は、Horizon FLEX Admin Console と Horizon FLEX Policy Server から構成されます。Horizon FLEX Server の機能は以下のとおりです。

- Horizon FLEX 仮想マシンをディレクトリ サービスのユーザーやグループに割り当てる
- 各ユーザーの使用中の Horizon FLEX 仮想マシンのレコードを保守する
- 展開されている Horizon FLEX 仮想マシンと Horizon FLEX Server 間で、安全で信頼される通信を確実に確立するために、セキュリティ証明書の管理を提供します。
- ポリシー設定をクライアントに強制する
- 特定のユーザーと Horizon FLEX 仮想マシンの組み合わせに対するポリシー設定の変更を可能にする
- Horizon FLEX 仮想マシンの状態を監視する

Mirage Management Console は、展開されたエンドポイントのスケーラブルな保守、管理、およびモニタリングを行うために使用されるグラフィカル ユーザー インターフェイス (GUI) です。Mirage Web Manager は Mirage Management Console の機能をミラーリングします。

デフォルトでは、ポート 7443 が Horizon FLEX Policy Server の外部アクセスで使用され、 ポート 8443 は Horizon FLEX Policy Server と通信するために Mirage Management Server によって使用されます。 必要なポートを利用できるようにするためにファイアウォール ポリシーを構成する必要があります。Mirage によって使用されるポートの詳細なリストについては、https://www.vmware.com/support/pubs/mirage_pubs.html にある Mirage のドキュメントを参照してください。

ファイル サーバ

ファイル サーバは、Horizon FLEX 仮想マシンのソース仮想マシン ファイルを含む TAR ファイルを保存します。ファイル サーバは、クライアント ユーザーが認証情報を入力せずにアクセスできるサーバに配置できます。この例ではファイル サーバが DMZ 内に配置されていますが、これは必須ではありません。

HTTPS プロキシ

HTTPS プロキシは、オフサイトのエンド ユーザー システムによる Mirage Management Console へのアクセスとポリシー更新の取得を可能にします。

RODC

RODC によって、オフィスのエンドユーザー システムが、Horizon FLEX 仮想マシンにログインできるようになり、仮想マシンを最初に起動するときに Active Directory ドメインに参加できるようになります。RODC は、VPN を使用せずに外部ユーザーがログインすることを許可している場合のみ必要です。RODC は DMZ 内に存在します。

負荷分散

Horizon FLEX は、複数のポリシー サーバを使用する負荷分散をサポートします。Horizon FLEX トポロジのフォールトトレランスのためにアクティブ/パッシブ構成の Windows サーバをセットアップします。

Horizon FLEX のシステム要件

Horizon FLEX パッケージの製品ごとに、システム要件が異なります。

Horizon FLEX Server および Mirage Server の要件	詳細については、「Horizon FLEX Server のシステム要件 (P. 10)」を参照してください。
Horizon FLEX の Mirage	Horizon FLEX 1.6 のシステム要件は Mirage 5.5 の場合と同じです。https://www.vmware.com/support/pubs/mirage_pubs.html にある Mirage のドキュメントを参照してください。
Horizon FLEX Client for Mac	Horizon FLEX 1.6 は、Fusion Pro 8.0 を Mac クライアント向けのクライアント ソフトウェアとして使用します。Horizon FLEX 1.6 は、Fusion Pro の以前のバージョンとは互換性がありません。 Fusion Pro のハードウェアとソフトウェアの要件については、「VMware Horizon FLEX Client ユーザー ガイド」を参照してください。
Horizon FLEX Client for Windows	Horizon FLEX 1.6 は、Workstation Player 12.0 を Windows クライアント向けのクライアント ソフトウェアとして使用します。Horizon FLEX 1.6 は、Player Pro の以前のバージョンとは互換性がありません。 Workstation Player のハードウェアとソフトウェアの要件については、「VMware Horizon FLEX Client ユーザー ガイド」を参照してください。
Workstation Pro	Workstation Pro 12.0 を使用してソース仮想マシンを作成し、開くことができますが、Workstation Pro は Horizon FLEX 仮想マシンをダウンロードできません。 Workstation Pro は Horizon FLEX インストール パッケージに含まれません。 Workstation Pro のハードウェアとソフトウェアの要件については、https://www.vmware.com/support/pubs/ws_pubs.html にある Workstation Pro のドキュメントを参照してください。

Horizon FLEX Server のシステム要件

Horizon FLEX 環境には、Horizon FLEX Server と Mirage Server の両方のシステム要件が含まれます。

Horizon FLEX Server のシステム要件

- CPU：クアッドコア プロセッサ 1 基、または vCPU 2 基
- Intel コア速度 2.26 GHz、または同等

- RAM：512 MB（4 GB を推奨）
- ディスク容量：10 GB 以上（40 GB 以上を推奨）
- Windows 2008 R2、Windows 2012 以降
- .NET 4.5.1 以降
- IIS6 の管理互換性があり、ASP および ASP.NET を組み込むバージョン 7.0 以降の IIS
- Active Directory：ドメインにコンピュータ オブジェクトを追加する権限を持つ管理者アカウント
- SQL 2008 Express または SQL Server 2008（Mirage のインストールで必要）
- ソース仮想マシン用の空き容量のある HTTP ファイル共有または IIS 仮想ディレクトリ
- Horizon FLEX Admin Console 向けのファイアウォール ポート
  - IIS および Horizon FLEX Web アプリケーションのデフォルト ポート：HTTP - 7080、HTTPS - 7443（HTTP ポートにダイレクトされる呼び出しは HTTPS ポートにリダイレクトされます。）
  - Mirage Management Server が Windows Communication Foundation (WCF) 要求を認識するポートは、HTTP - 8443 です。
- SSL を使用する場合は、Horizon FLEX Server の証明書が必要です。

Mirage Server の要件

- CPU：vCPU 4 基（vCPU 8 基を推奨）
- RAM：8 GB（16 GB を推奨）
- ディスク容量：146 GB
- Windows 2008 R2、Windows 2012 以降
- .NET 4.5.1 以降

Horizon FLEX のネットワーク要件

Horizon FLEX を使用すると、ネットワークに接続されていない状態であっても、エンド ユーザーが企業のアプリケーションを実行できます。Horizon FLEX 仮想マシンは、ネットワーク接続を必要としないデスクトップ環境を実現するために、ローカルに保存されます。

次の状況では、Horizon FLEX ポリシー サーバ と Horizon FLEX Client の間にネットワーク接続が必要です。

- Horizon FLEX 仮想マシンをユーザーのローカル コンピュータに初めてダウンロードする場合。
- USB デバイスで提供された、またはユーザーのローカル コンピュータに展開された Horizon FLEX 仮想マシンを登録する場合。
- Horizon FLEX 仮想マシンの制限およびポリシーの更新を受け取る場合。

Horizon FLEX 仮想マシンのソース仮想マシンを登録する場合は、仮想マシン パッケージのダウンロード場所となる URL を指定します。仮想マシンをダウンロードするには、エンド ユーザーがダウンロード フォルダにアクセスできる必要があります。

サポートされるホストおよびゲスト OS

エンド ユーザーが Horizon FLEX Client を使用するローカル コンピュータには、サポートされるホスト OS をインストールしておく必要があります。Horizon FLEX 仮想マシンは、サポートされているゲスト OS を使用する必要があります。

サポートされるホスト OS

エンド ユーザーは、次のいずれかのオペレーティング システムがインストールされている物理コンピュータを使用して、Horizon FLEX Client を実行し、Horizon FLEX 仮想マシンにアクセスできます。

表 1-1. サポートされるホスト OS

Horizon FLEX Client	サポートされるオペレーティング システム
Workstation Player	■ Windows 7 ■ Windows 8.1 Enterprise ■ Windows Server 2012 R2 ■ Windows 8 ■ Windows 8.1 Pro ■ Windows 10 注意　Workstation Player は、64 ビットのオペレーティング システムのみをサポートします。
Fusion Pro	■ Mac OS X 10.11 ■ Mac OS X 10.10 ■ Mac OS X 10.9

サポートされるゲスト OS

Horizon FLEX 仮想マシンでは、次のいずれかのゲスト OS を追加できます。

- Windows 10
- Windows 8.1
- Windows 7
- Windows XP
- Windows Server 2012 R2
- Ubuntu 14.04

Horizon FLEX のインストール 2

Horizon FLEX のインストールでは、Horizon FLEX Server とクライアントのコンポーネントをインストールし、Horizon FLEX 仮想マシンを保存するフォルダを作成し、Active Directory を準備し、証明書をセットアップし、Horizon FLEX 仮想マシンを作成して展開します。

この章では次のトピックについて説明します。

Horizon FLEX のインストールの概要

Horizon FLEX は、Mirage、Fusion Pro、および Workstation Player を含む、VMware 製品の組み合わせです。Horizon FLEX のインストールでは、これらの各コンポーネントをインストールし、Horizon FLEX 固有の追加のタスクを実行します。Horizon FLEX を正しく展開するには、必要なタスクを実行する順序を把握しておく必要があります。

Horizon FLEX をインストールする前に、ハードウェアとソフトウェアのすべての要件を満たしていること、有効なライセンスがあること、Horizon FLEX コンポーネント インストーラを VMware Horizon FLEX 製品ダウンロード ページからダウンロードしていることを確認します。

これらの手順を実行して、Horizon FLEX をインストールします。

1 Mirage システムをインストールします。

「Horizon FLEX の Mirage コンポーネントのインストールと構成 (P. 14)」を参照してください。

2 Horizon FLEX 仮想マシンの認証情報をセットアップします。

第 3 章「Horizon FLEX 仮想マシンの証明書のセットアップ (P. 21)」を参照してください。

3 Horizon FLEX 仮想マシン パッケージを保存するダウンロード フォルダを作成します。

「Horizon FLEX 仮想マシン パッケージ用のダウンロード フォルダの作成 (P. 15)」を参照してください。

4 Horizon FLEX 仮想マシンのダウンロード フォルダの仮想ディレクトリを IIS に追加し、サイト バインディングを編集します。

「Horizon FLEX Server の IIS SSL サーバ証明書の構成 (P. 16)」を参照してください。

5 (オプション) 選択した Active Directory の組織単位 (OU) のみのエンティティを同期するように、Horizon FLEX を構成します。

「Active Directory の設定を構成する (P. 16)」を参照してください。

6 Horizon FLEX 管理コンソール への接続をテストします。

「Horizon FLEX 管理コンソール の接続をテストする (P. 17)」を参照してください。

7 Horizon FLEX Client を各エンドユーザー ホストにインストールするか、エンド ユーザーに自分のコンピュータに Horizon FLEX Client をインストールするように指示します。

「エンド ユーザー向けの Horizon FLEX Client のインストール (P. 18)」を参照してください。

8 Horizon FLEX 仮想マシンを作成し、展開します。

第 4 章「Horizon FLEX 仮想マシンの作成とデプロイ (P. 31)」を参照してください。

Horizon FLEX の Mirage コンポーネントのインストールと構成

最初の Horizon FLEX のインストール手順では、Mirage システムをインストールして構成します。

Horizon FLEX パッケージには、次のコンポーネントが含まれます。

- VMware Mirage for Horizon FLEX (Mirage Core Software)
- Mirage PowerCLI for Windows
- Mirage Gateway Appliance Software

Horizon FLEX Server 製品ダウンロード ページからインストール ファイルをダウンロードします。

Mirage をデプロイするには、次のコンポーネントをインストールします。

1 Mirage Management Server

2 Mirage Server

3 Mirage Management Console

4 Mirage Web Manager

Mirage システムをインストールして構成するには、https://www.vmware.com/support/pubs/mirage_pubs.html にある Mirage のドキュメントに記載されているインストール手順に従って操作します。

Mirage システムをインストールするときには、Horizon FLEX Server が正しく動作するように特定のオプションを選択する必要があります。

- ソース仮想マシンに Mirage クライアントをインストールする場合にのみ、Mirage Server と Mirage コンソールが必要となります。
- Horizon FLEX Server と同じシステムに仮想マシン イメージを配置する場合、IIS の「デフォルト Web」サーバにイメージを配置します。
- Web Management Server と Mirage Management Server は同じサーバにインストールできますが、異なるサーバにインストールすることでスケーラビリティが向上します。SQL サーバは Web Management Server および Mirage Management Server とは異なるサーバにインストールすべきです。
- Mirage Server のインストール時に、Mirage Server 転送に SSL を選択します。SSL は、外部アクセスと Horizon FLEX システムの管理に Mirage ゲートウェイ機能を使用するために必要になります。Mirage Server で SSL を構成する前に、サーバ SSL 証明書をインストールする必要があります。
- Mirage Web Manager をインストールする前に、.NET Framework 4.5.1 がサーバにインストールされていることを確認します。
- Mirage Management Server は、Active Directory の読み取り権限があるユーザーとして実行する必要があります。Horizon FLEX 仮想マシンを Active Directory ドメインに参加させる予定がある場合、Mirage Management Server を、ドメインに参加する権限があるユーザーとして実行する必要があります。

Horizon FLEX 仮想マシン パッケージ用のダウンロード フォルダの作成

Horizon FLEX 仮想マシンのデプロイプロセスで、ソース仮想マシン パッケージを TAR (`.tar`) 形式に圧縮して、エンドユーザーが自分の Horizon FLEX 仮想マシンを簡単にダウンロードできるようにします。これらの TAR ファイルを保存するダウンロード フォルダを作成する必要があります。

手順

1 Horizon FLEX Server または別のサーバにダウンロード フォルダを作成します。

ダウンロード フォルダは Horizon FLEX Server になくても構いませんが、フォルダ内のファイルは認証手続きなしでダウンロードできるようにする必要があります。Horizon FLEX Server と同じ IIS サーバにダウンロード フォルダを作成する場合、デフォルト Web サイトのデフォルト IIS ドキュメント ルート フォルダの下にフォルダを作成できます。VMware Mirage Management Web サイトにダウンロード フォルダを作成しないでください。

2 ダウンロード フォルダにアクセス権を割り当てて、ユーザーがフォルダ内のファイルをダウンロードできるようにします。

3 (オプション) ダウンロード フォルダを Horizon FLEX Admins などの管理グループと共有します。これは、Horizon FLEX のデプロイを管理するユーザーの管理グループにすることができます。

この手順によって、ソース仮想マシンを Horizon FLEX ポリシー サーバ に簡単に登録できるようになります。

次に進む前に

「Horizon FLEX Server の IIS SSL サーバ証明書の構成 (P. 16)」を参照してください。

OpenSSL を使用した Horizon FLEX Server の証明書のセットアップ

OpenSSL を使用して、Horizon FLEX Server の自己署名証明書を作成できます。

開始する前に

OpenSSL 構成ファイルは、Mirage Gateway サーバで作成されます。
https://www.vmware.com/support/pubs/mirage_pubs.html で、Mirage のドキュメントを参照してください。

手順

1 OpenSSL コマンド プロンプトで、次の証明書を作成します： **`$ openssl req –new –days <expiration time> –x509 –newkey rsa:2048 – keyout <key filename> –out<certificate filename> –nodes`**

<expiration time> は証明書が有効である必要がある日数を、<key filename> はキーのファイル名を、<certificate filename> は新しい証明書の名前を表します。

自己署名証明書とプライベート キーが生成されます。証明書では 2048 ビット RSA キーを使用しており、パスフレーズによってキーを保護しません。

2 プロンプトが表示されたら、国名、都道府県名、市区町村名、組織名、および部署名を入力します。

3 [共通名] テキスト ボックスに、保護対象の Horizon FLEX Server のホスト名を入力します。

このテキスト ボックスには必ず値を入力する必要があります。

4 電子メール アドレスを入力します。

自己署名証明書および関連付けられたプライベート キーが生成されます。

5 プライベート キーを **.pfx** 形式にする必要がある場合は、前の手順で生成された証明書名とキー ファイル名を使用して次のコマンドを入力します：
$ openSSL pkcs12 –export –out<output pfx filename> –inkey <key filename> –in <certificate name>

パスワード保護された新しい **.pfx** ファイルが生成されます。このファイルは、PEM 証明書の代わりに **.pfx** 証明書を必要とするすべてのデバイスにデプロイできます。

Horizon FLEX Server の IIS SSL サーバ証明書の構成

Horizon FLEX Server の IIS SSL サーバ証明書を構成して、Horizon FLEX Server から Horizon FLEX 仮想マシンへの証明書チェーンを設定する必要があります。

開始する前に

- Horizon FLEX のために Mirage をインストールします。「Horizon FLEX の Mirage コンポーネントのインストールと構成 (P. 14)」を参照してください。
- Mirage サーバにサーバ SSL 証明書をインストールします。https://www.vmware.com/support/pubs/mirage_pubs.html で、Mirage のドキュメントを参照してください。
- Horizon FLEX 仮想マシンの証明書認証を構成します。第 3 章「Horizon FLEX 仮想マシンの証明書のセットアップ (P. 21)」を参照してください。
- Horizon FLEX 仮想マシン パッケージのダウンロード フォルダを作成します。「Horizon FLEX 仮想マシン パッケージ用のダウンロード フォルダの作成 (P. 15)」を参照してください。

手順

1 IIS マネージャーを開きます。

2 [VMware Mirage Management Web サイト] に移動して、ダウンロード フォルダの場所を選択します。

3 フォルダの場所を右クリックして、[仮想ディレクトリを追加] を選択します。

4 名前を [エイリアス] テキストボックスに入力し、Horizon FLEX 仮想マシン パッケージを追加するために作成したフォルダを参照して、[OK] をクリックします。

5 Mirage サーバで定義されている接続ノードであるルート ノードに移動します。

6 Mirage の [ホーム] ページの IIS で、[サーバ証明書] をダブルクリックします。

[IIS SSL サーバ証明書] ウィンドウが開きます。

7 右の列の [インポート] をクリックします。

このステップにより、作成された SSL 証明書がインポートされ、その証明書を識別するキーが割り当てられます。

8 [VMware Mirage Management Web サイト] を選択し、右の列の [バインディングの編集] をクリックします。

9 Horizon FLEX Server 証明書を使用する HTTPS ポートを設定し、[OK] をクリックします。

Active Directory の設定を構成する

Horizon FLEX 仮想マシンの資格を付与する場合は、既存の Active Directory インフラストラクチャからユーザーとグループを資格に追加します。デフォルトでは、Horizon FLEX は、Active Directory インフラストラクチャ全体を Horizon FLEX データベースと同期します。オプションで、特定の組織単位 (OU) のみを同期するように Horizon FLEX を構成することもできます。

開始する前に

Horizon FLEX のために Mirage をインストールします。「Horizon FLEX の Mirage コンポーネントのインストールと構成 (P. 14)」を参照してください。

手順

1 Horizon FLEX 管理コンソール を起動します。

   a Web ブラウザに **`https://<WebManagerServer>:7443/rvm`**（<WebManagerServer> は Mirage Web Manager がインストールされているホストの DNS 名または IP アドレス）と入力します。

   b Mirage にアクセスできるドメイン アカウントのユーザー名とパスワードを入力します。

   c [ログイン] をクリックします。

2 Horizon FLEX 管理コンソールで、[システム全般設定] アイコンをクリックし、[Active Directory 設定] をクリックします。

3 同期する組織単位を [組織単位] テキスト ボックスに入力します。

   テキスト ボックスへの入力を開始すると、Active Directory インフラストラクチャで利用可能な組織単位がドロップダウン メニューに表示され、適切な組織単位を選択できます。

4 [OK] をクリックして組織単位の設定を保存します。

   Horizon FLEX Server は、その組織単位が存在し、アクセスできることを確認します。

Horizon FLEX Server は、ユーザーが選択した組織単位のすべての子の組織単位に属するエンティティを含め、選択した組織単位のみに属する Active Directory エンティティを同期します。

新しい組織単位を構成するときにはいつでも、Horizon FLEX Server は、以前に同期されたエンティティをデータベースから削除し、完全な同期プロセスを新しく開始します。

最初の起動後にパワーオン パスワードをユーザーの Active Directory パスワードと照合するようにクライアント仮想マシンのポリシーを構成できます。「Horizon FLEX イメージの一般的なポリシーを構成する (P. 38)」を参照してください。

Horizon FLEX 管理コンソール の接続をテストする

Horizon FLEX 管理コンソール の接続をテストして、Horizon FLEX のデプロイ環境を検証できます。

開始する前に

- Horizon FLEX のために Mirage をインストールします。「Horizon FLEX の Mirage コンポーネントのインストールと構成 (P. 14)」を参照してください。
- 証明書の認証を構成します。第 3 章「Horizon FLEX 仮想マシンの証明書のセットアップ (P. 21)」を参照してください。

手順

1 Horizon FLEX 管理コンソール を起動します。

   a Web ブラウザに **`https://<WebManagerServer>:7443/rvm`**（<WebManagerServer> は Mirage Web Manager がインストールされているホストの DNS 名または IP アドレス）と入力します。

   b Mirage にアクセスできるドメイン アカウントのユーザー名とパスワードを入力します。

   c [ログイン] をクリックします。

2 Horizon FLEX 管理コンソールのページが正しく表示されることを検証します。

   [イメージ]、[ポリシー]、[資格]、および [仮想マシン] ボタンが、左側のナビゲーション パネルに表示されます。

エンド ユーザー向けの Horizon FLEX Client のインストール

Horizon FLEX 仮想マシンをダウンロードできるようにするには、エンド ユーザーは Horizon FLEX Client ソフトウェアをローカル コンピュータにインストールしておく必要があります。Horizon FLEX パッケージに含まれるサポートされるクライアントは、Mac OS X マシン向けの Fusion Pro と Windows マシン向けの Workstation Player です。

大規模デプロイパッケージを作成して一度に多数のシステムに Horizon FLEX Client をインストールできます。また、Horizon FLEX Client を VMware Web サイトから入手して自分でインストールするようにエンド ユーザーに指示することもできます。複数の Windows マシンで自動 Workstation Player インストールを実行することもできます。

大規模デプロイパッケージを作成して Fusion Pro をインストールする

Fusion Pro の大規模デプロイパッケージを作成して、Fusion Pro を任意の数のエンドユーザー用 Mac にインストールできます。Apple Remote Desktop Admin などの標準的なパッケージデプロイツールを使用して、大規模なデプロイパッケージをデプロイできます。

大規模デプロイパッケージを構成するときには、`Deploy.ini` ファイルの `[Volume License]` セクションで Horizon FLEX のライセンス キーを指定し、Fusion Pro アプリケーションのコピーを `00Fusion_Deployment_Items` フォルダにコピーします。

オプションの `connectAtStartupURL` パラメータを `Deploy.ini` ファイルの `[Locations]` セクションで使用して、ユーザー名と Horizon FLEX Server のホスト名を、次のように指定します。

```
connectAtStartupURL = vmware-rvm://johndoe@yourflexserver.com:7443
```

Fusion Pro を起動するときに、ユーザーの Mac にインストールされている仮想マシンがない場合、[接続] ダイアログ ボックスが開き、[サーバ] および [ユーザー名] テキスト ボックスには、ユーザーが `connectAtStartupURL` パラメータに指定したホスト名とユーザー名が自動入力されます。

大規模デプロイパッケージを作成する手順については、http://kb.vmware.com/kb/2058680 にある VMware ナレッジ ベースの記事を参照してください。

エンド ユーザーへの Workstation Player インストール パッケージの提供

コマンド ラインを使用して Workstation Player をエンド ユーザーのマシンにインストールし、URI (Unified Resource Identifier) を使用して Horizon FLEX Server の接続設定を指定できます。Workstation Player のインストールが完了すると、サーバに接続して Horizon FLEX 仮想マシンをダウンロードするように求めるプロンプトがエンド ユーザーに表示されます。

開始する前に

- エンド ユーザーに、サーバのパスワードと、Horizon FLEX で使用する Workstation Player のライセンス キーを提供します。

手順

- URI を作成して、カスタマイズされた Workstation Player のインストールおよび展開パッケージを作成します。

  コマンド ラインは次のように構成されます。

  ```
  VMware-player-x.x.x-xxxxxxx.exe /v PLAYER_RVM_URI="vmware-
  rvm://username@myserver.com:7443"
  ```

  Workstation Player の .exe ファイルのバージョンとビルド番号を指定します。<username> はユーザーのログイン名で、<myserver.com> はサーバのホスト名です。`vmware-rvm://` と `:7443` をサーバ アドレスに含める必要があります。http や https はサーバ アドレスに追加しないでください。

自動 Workstation Player インストールの実行

Microsoft Windows Installer (MSI) の自動インストール機能を使用すれば、ウィザードのプロンプトに応答することなく、複数の Windows ホストに Workstation Player をインストールできます。これは、大規模な組織でインストールを実施する場合に有用です。

開始する前に

- ホスト システムがホスト システムの要件を満たすことを確認します。
- ホスト コンピュータに MSI 2.0 以降のランタイム エンジンが搭載されていることを確認します。このバージョンのインストーラは Windows XP 以降のバージョンの Windows に組み込まれています。また、Microsoft 社から入手することもできます。詳細は、Microsoft 社の Web サイトを参照してください。

手順

1 Administrator ユーザーまたはローカルの Administrators グループのメンバーとしてホスト システムにログインします。

ドメインにログインする場合、ドメイン アカウントもローカル管理者である必要があります。

2 Workstation Player セットアップ ファイルから管理用インストール イメージをデプロイします。

セットアップ ファイルには **VMware-player-<xxxx-xxxx>.exe** のようなファイル名が付けられています。<xxxx-xxxx> にはバージョン番号とビルド番号を表す数字が入ります。

例：**setup.exe /s /e <install_temp_path>**

3 インストール コマンドは 1 行で入力してください。

次の例は、コマンドに追加できるオプションを示しています。

```
VMware-player-full-x.x.x-xxxxxx.exe /s /pass /v/qn REBOOT=ReallySuppress
"EULAS_AGREED=1 INSTALLDIR=""path_to_program_directory"" ADDLOCAL=ALL
SERIALNUMBER=""xxxxx-xxxxx-xxxxx-xxxxx-xxxxx"" "
```

```
VMware-player-full-x.x.x-xxxxxx.exe /s /v/qn EULAS_AGREED=1 SERIALNUMBER="xxxxx-
xxxxx-xxxxx-xxxxx-xxxxx"
```

```
VMware-player-full-x.x.x-xxxxxx.exe /s /v/qn PLAYER_RVM_URI="vmware-
rvm://username@myserver.com:7443"
```

オプションで **INSTALLDIR** プロパティを使用して、インストール用にデフォルトの場所とは異なるファイル パスを指定できます。

注意　ファイル パスを囲む引用符は重要です。MSI 引数はすべて **/v** オプションで渡されます。外側の引用符で MSI 引数をグループ化し、内側の引用符でその引数に引用符を 1 つ配置します。

オプションで **REMOVE** プロパティを使用して、特定の機能のインストールを省略できます。

Workstation Player 自動インストールのプロパティ

Workstation Player の自動インストール実行時にインストール プロパティをインストール コマンドで指定すると、インストールをカスタマイズできます。

インストール コマンドでインストール プロパティを指定する形式は **Property**= "<value>" です。値 1 は True を、値 0 は False を意味します。

表 2-1. インストール プロパティ

プロパティ	説明	デフォルト値
AUTHD_PORT	「VMware 認証サービス」の通信で使用するポートを指定します。	902
AUTOSOFTWAREUPDATE	新しいビルドが利用可能になった場合は、Workstation Player の自動アップグレードができます。	1
DATACOLLECTION	VMware へユーザー エクスペリエンス情報を送信します。	1
DESKTOP_SHORTCUT	Workstation Player のインストール時に、デスクトップにショートカットを追加します。	1
EULAS_AGREED	製品 EULA をそのまま受け入れることを許可します。インストールまたはアップグレードを完了するには 1 に設定します。	0
INSTALL_DIR	Workstation Player のデフォルトのインストール場所とは異なるディレクトリに Workstation Player をインストールします。	C:\Program Files (x86)\VMware\VMware Player
KEEP_LICENSE	Workstation Player のインストール時にライセンス キーを保持するか削除するかを指定します。	1
KEEP_SETTINGFILES	Workstation Player のアンインストール時に設定ファイルを保持するか削除するかを指定します。	1
PLAYER_RVM_URI	Horizon FLEX Server の URI (Unified Resource Identifier) を指定します。	VMware-player-full-x.x.x-xxxxxx.exe /s /v/qn PLAYER_RVM_URI="vmware-rvm://username@myserver.com:7443"
SERIALNUMBER	Workstation Player のインストール時に、ライセンス キーを入力できます。ライセンス キーにハイフンを含めて入力してください（例：xxxxx-xxxxx-xxxxx-xxxxx-xxxxx）。	
SIMPLIFIEDUI	Workstation Player の特定の UI 機能を有効または無効にします。	0
SOFTWAREUPDATEURL	ソフトウェアに更新管理用の特定 URL を指定します (vmware.com から分離)。	
STARTMENU_SHORTCUT	Workstation Player のインストール時に [スタート] メニューを追加します。	1
SUPPORTURL	Workstation Player の [ヘルプ] メニューから製品不具合について連絡するためのサポート URL またはメール エイリアスを設定します。	

Horizon FLEX 仮想マシンの証明書のセットアップ 3

Horizon FLEX 仮想マシンを作成およびデプロイする前に、証明書をセットアップして、エンド ユーザーが、仮想マシンを確実かつ正常にダウンロードして使用できるようにする必要があります。

Entrust や Go Daddy などの証明書機関 (CA) によって発行された証明書か、サードパーティの証明書を、Horizon FLEX Server で使用することを推奨します。一般的に信頼される証明書の代わりに自己署名の証明書や内部 CA の証明書を使用している場合、Horizon FLEX 仮想マシンをダウンロードして使用するすべてのエンドユーザーのコンピュータで証明書が確実に信頼されるようにする手順を実行する必要があります。

Mirage での Horizon FLEX Server の証明書のセットアップについては、
https://www.vmware.com/support/pubs/mirage_pubs.html で Mirage のドキュメントを参照してください。

この章では次のトピックについて説明します。

信頼される証明書リストの作成

Horizon FLEX 仮想マシン向けに信頼される証明書リストを作成し、リストを Horizon FLEX ポリシー サーバ にインポートできます。信頼される証明書リストを使用する場合、証明書をエンド ユーザーのホストにインストールする必要はありません。

信頼される証明書リストを使用すると、悪意のあるユーザーによって同じホスト名の独自の自己署名証明書が作成され、それらの証明書をホストの信頼される証明書リストに追加されるのを防止できます。

信頼される証明書リストを使用するように Horizon FLEX ポリシー サーバ を構成すると、クライアント ホストはホストの証明書リストを無視し、代わりに信頼される証明書リストを使用してサーバ接続を検証します。クライアント ホストが信頼される証明書リストを使用して証明書を検証できない場合、サーバ接続は失敗します。

ソース仮想マシンの信頼される証明書リストが空の場合、Workstation Player と Fusion Pro は、ホストの信頼される証明書リストに対して認証を行います。

信頼される証明書リストを作成するには、各証明書を個別のファイルにエクスポートしてから、すべてのファイルを 1 つのファイルに連結します。そして、Horizon FLEX 管理コンソール を使用して、連結した証明書ファイルを Horizon FLEX ポリシー サーバ にインポートします。

PEM (Privacy Enhanced Mail) 形式で証明書をエクスポートする必要があります。Windows システムでは、PEM 証明書エンコーディングを Base-64 エンコードの X.509 (.CER) と呼びます。PEM エンコードの証明書のみがサポートされます。他の証明書形式（DER、シリアル化された証明書ストア/SST、PKCS #12/PFX、PKCS #7/P7B）はサポートされません。

PEM 形式について

PEM 形式は、Base64 でエンコードされる標準の証明書形式です。

PEM 形式の証明書の例を以下に記載します。

```
-----BEGIN CERTIFICATE-----
MIIDojCCAwugAwIBAgIJAMLM0CJRzPyzMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD
VQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJUGFsbyBBbHRv
MS8wLQYDVQQKEyZWTXdhcmUsIEluYy4gLSBXb3Jrc3RhdGlvbiBTU0wgVGVzdGlu
ZzEqMCgGA1UEAxMhV29ya3N0YXRpb24gQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTExMDcxNTAyMjY0OFoXDTE1MDcxNDAyMjY0OFowgZMxCzAJBgNVBAYTAlVTMRMw
EQYDVQQIEwpDYWxpZm9ybmlhMRIwEAYDVQQHEwlQYWxvIEFsdG8xLzAtBgNVBAoT
JlZND2FyZSwgSW5jLiAtIFdvcmtzdGF0aW9uIFNTTCBUZXN0aW5nMSowKAYDVQQD
EyFXb3Jrc3RhdGlvbiBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAL/tBlngiEkCK7ssCBe8lZ30FlIHmpECmwEm3AaID1C0
lncb+LdRt2AmmQiknXBPxGBGyRNRNnashrzp1XXR/wL2b2AybT7NX+P/XSH2srDb
cGGCTNa/bwh/ArcirTLCjRwY55lAAH9xwzortRYR84IBJQpHzxcopTSI9o4ZVIqx
AgMBAAGjgfswgfgwHQYDVR0OBBYEFMoT527dtvlgR1EzYK4EnQHS6T2ZMIHIBgNV
HSMEgcAwgb2AFMoT527dtvlgR1EzYK4EnQHS6T2ZoYGZpIGWMIGTMQswCQYDVQQG
EwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJUGFsbyBBbHRvMS8w
LQYDVQQKEyZWTXdhcmUsIEluYy4gLSBXb3Jrc3RhdGlvbiBTU0wgVGVzdGluZzEq
MCgGA1UEAxMhV29ya3N0YXRpb24gQ2VydGlmaWNhdGUgQXV0aG9yaXR5ggkAwszQ
IlHM/LMwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOBgQBcoiwDWGWXzI+j
0gG/7BNzpNHzR1RGAF4nB9JrnCYWvB313kgYDMHogfiAoQchsu/py/OYBYVRjjFJ
YVaTJ7DVl/3Gpk3+tcdJfEmqIz76PVWfWbTnhuJEMYrMM4W06B/K2cs24bkZtcXQ
h8b4FYTVCg/l6TP5SWgei4VWgRfxgA==
-----END CERTIFICATE-----
```

信頼される証明書リストを作成する場合、複数の PEM 形式の証明書を連結し、1 ファイルにします。行末は自動検出されます。次の例は、2 つの証明書を含む連結された証明書リストの形式を示しています。

```
-----BEGIN CERTIFICATE-----
<<ここには base64 のコンテンツが表示されます>>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<<ここには base64 のコンテンツが表示されます>>
-----END CERTIFICATE-----
```

PEM 形式の証明書の作成

CA の Web サイトから証明書をダウンロードするか、ホスト システムから証明書をエクスポートすることで、PEM 形式の証明書を作成できます。

たとえば、Verisign の証明書は https://www.symantec.com/page.jsp?id=roots にある Symantec 社の Web サイトからダウンロードできます。

Mac から PEM 形式の証明書をエクスポートする

PEM 形式の証明書を Mac からエクスポートできます。

開始する前に

Mac におけるキーチェーン アクセスの使用方法について確認しておきます。詳細については、http://support.apple.com の Apple Support Web サイトを参照してください。

手順

1 Mac でキーチェーン アクセスを開きます。

2 サイドバーから [システム ルート] を選択します。

3 エクスポートする証明書を指定します。

4 [ファイル] - [項目のエクスポート] を選択します。

5 証明書を保存する場所を選択し、[PEM 形式（.pem）] ファイル形式を選択します。

Windows システムからの PEM 形式の証明書のエクスポート

PEM 形式の証明書を Windows システムからエクスポートできます。Windows では、PEM 証明書のエンコーディングを Base-64 エンコードの X.509 (.CER) と呼びます。

開始する前に

Windows システムにおける証明書マネージャの使用方法を確認しておきます。詳細については、http://technet.microsoft.com の Microsoft TechNet Web サイトを参照してください。

手順

1 Windows システムで証明書マネージャ (**`certmgr.exe`**) を開きます。

2 エクスポートする証明書を右クリックして、[すべてのタスク] - [エクスポート] を選択します。

3 証明書のエクスポート ウィザードでオプションを選択します。

   a エクスポートするファイル形式として [Base-64 encoded X.509 (.CER)] を選択します。

   Horizon FLEX で証明書を使用できるようにするには、このオプションを選択する必要があります。

   b 証明書を保存する場所とファイル名を指定します。

   c 選択した設定を確認してから、[終了] をクリックします。

   指定した場所に証明書ファイルが保存されます。

信頼される証明書リスト ファイルを作成およびインポートする

PEM 形式の証明書をエクスポートした後に、信頼される証明書リストを作成し、その証明書リスト ファイルを Horizon FLEX ポリシー サーバ にインポートする必要があります。

開始する前に

各証明書を PEM 形式でエクスポートします。「PEM 形式の証明書の作成 (P. 22)」を参照してください。

手順

1 信頼される証明書リスト ファイルを作成するには、各 PEM 形式の証明書ファイルを 1 つのファイルに連結します。

   `cat` コマンドを使用するか、証明書ファイルの内容をコピーしてテキスト ファイルにペーストします。Base64 の内容はテキスト エディタで安全に編集できます。

   例： **`$ cat mycert1.pem mycert2.pem mycert3.pem > list.pem`**

2 Horizon FLEX 管理コンソール を起動します。

   a Web ブラウザに **`https://<WebManagerServer>:7443/rvm`**（<WebManagerServer> は Mirage Web Manager がインストールされているホストの DNS 名または IP アドレス）と入力します。

   b Mirage にアクセスできるドメイン アカウントのユーザー名とパスワードを入力します。

   c [ログイン] をクリックします。

3 Horizon FLEX 管理コンソールで、[システム全般設定] アイコンをクリックし、[証明書] を選択します。

4 [インポート] をクリックし、信頼される証明書リスト ファイルを参照し、[開く] をクリックしてファイルをインポートします。

サーバでの証明書の更新

証明書の有効期限が切れ、新しい証明書の有効期限が遠い未来に設定されている場合、この新しい証明書を Horizon FLEX ポリシー サーバ で信頼される証明書リストに第 2 証明書として追加できます。

信頼される証明書リストに新しい証明書を追加すると、すべての Horizon FLEX 仮想マシンがこの新しい証明書をダウンロードできるようになります。その後、証明書の切り替えが発生する場合、証明書の新しいリストを受け取ったすべての Horizon FLEX 仮想マシンが Horizon FLEX Server に接続でき、信頼される古い証明書はポリシー ファイルから削除できます。

Horizon FLEX 仮想マシンがすでに登録され実行された後でサーバ証明書が変更された場合、エンド ユーザーは、変更された証明書が Fusion Pro または Workstation Player によって信頼されていることを検証する必要があります。新しいサーバ証明書が自己署名の場合、Horizon FLEX Client は Horizon FLEX Server に対してインスタンスのステータスを正しく報告しません。エンド ユーザーは、Horizon FLEX 仮想マシンを開き、[接続] をクリックしてサーバに接続する必要があります。エンド ユーザーに次のエラー メッセージが表示される場合があります。

無効なセキュリティ証明書です

この場合エンド ユーザーは、管理者に確認して証明書が有効であることを検証する必要があります。証明書が有効な場合は、[この証明書を持つこのホストを常に信頼する] チェック ボックスを選択して、[接続する] をクリックします。

自己署名証明書の使用

準備しているソース仮想マシンで自己署名証明書を構成しない場合、Horizon FLEX 仮想マシンが正しく動作するように、各エンドユーザー ホストに証明書をインストールする必要があります。

ポリシー ファイルで証明書のリストが空になっている場合、Workstation Player および Fusion Pro は、ホストの信頼される証明書リストに戻って認証します。

Horizon FLEX ポリシー サーバ でソース仮想マシンの自己署名証明書を追加し、Horizon FLEX Client の自己署名証明書を構成またはインストールしている場合（ソース仮想マシンのポリシー ファイルまたはホストの信頼される証明書リストのいずれかに）、たとえば、証明書の有効期限が切れる場合など、証明書の更新が必要となる場合でも、エンドユーザー ホストに証明書をインストールする必要はありません。

ソース仮想マシンにおける証明書の構成の詳細については、「「Fusion Pro でのソース仮想マシンの作成 (P. 32)」」を参照してください。

信頼される証明書リストの作成と Horizon FLEX ポリシー サーバ へのインポートの詳細については、「「信頼される証明書リストの作成 (P. 21)」」を参照してください。

証明書の更新の詳細については、「「サーバでの証明書の更新 (P. 24)」」を参照してください。

Windows コンピュータへの自己署名証明書のインストール

自己署名証明書を Windows ホストにインストールするには、証明書を Horizon FLEX Server からエクスポートして、Windows コンピュータにインポートします。

開始する前に

- Windows システムにおける MMC 証明書スナップインのインストールと使用の方法を確認しておきます。詳細については、http://technet.microsoft.com の Windows TechNet Web サイトを参照してください。
- Windows IIS をインストールします。

手順

1 自己署名証明書を Horizon FLEX サーバからエクスポートします。

   a Horizon FLEX サーバで MMC (`mmc.exe`) を起動し、コンピュータ アカウントの証明書スナップインを追加し、ローカル コンピュータの証明書を管理します。

   b [ファイル] - [スナップインの追加と削除] を選択します。

c [証明書] スナップインをクリックして、[追加] をクリックします。

d [証明書スナップイン] 画面で、[コンピュータ ーアカウント] を選択し、[次へ] をクリックします。

この設定は、Horizon FLEX サーバで必要となります。

e [ローカル コンピューター] を選択して、[完了] をクリックして [OK] をクリックします。

f 左側のナビゲーション パネルで[証明書（ローカル コンピューター）] をデプロイします。

g [信頼されたルート証明機関] を右クリックして、[すべてのタスク] - [インポート] の順に選択します。

[証明書のインポート ウィザード] が開きます。

h [次へ] をクリックします。

i ルート証明書ファイルを見つけて、[次へ] をクリックします。

j [証明書をすべて次のストアに配置する：信頼されたルート証明機関]を選択し、[次へ] をクリックしてから、[完了] をクリックします。

k [中間ルート証明機関] を右クリックして、[すべてのタスク] - [インポート] を選択します。

l [証明書のインポート ウィザード] が開きます。

m ルート証明書ファイルを見つけて、[次へ] をクリックします。

n [証明書をすべて次のストアに配置する：中間ルート証明機関] を選択し、[次へ] をクリックしてから、[完了] をクリックします。

o インストールする中間証明書ごとに、手順 m と n を繰り返します。

p [信頼されたルート証明機関] - [証明書] に移動します。

q 自己署名証明書を選択し、エクスポートします。

証明書を DER エンコードのバイナリ X.509 (.CER) 形式でエクスポートします。

2 自己署名証明書をクライアント Windows コンピュータにコピーします。

3 自己署名証明書をクライアント Windows コンピュータにインポートします。

a Windows コンピュータで、MMC (`mmc.exe`) を起動します。

b コンピュータ アカウントの証明書スナップインを追加し、ローカル コンピュータの証明書を管理します。

c 自己署名証明書を [信頼されたルート証明機関] - [証明書] にインポートします。

自己署名証明書がすべてのユーザーに対して信頼されるようになりました。

Mac への自己署名証明書のインストール

自己署名証明書を Mac ホストにインストールするには、証明書を Horizon FLEX Server からエクスポートして、Mac にインポートします。

開始する前に

- Windows システムにおける MMC 証明書スナップインのインストールと使用の方法を確認しておきます。詳細については、http://technet.microsoft.com の Windows TechNet Web サイトを参照してください。
- Mac におけるキーチェーン アクセスの使用方法について確認しておきます。詳細については、http://support.apple.com の Apple Support Web サイトを参照してください。
- Windows IIS をインストールします。

手順

1 自己署名証明書を Horizon FLEX サーバからエクスポートします。

   a Horizon FLEX サーバで MMC (`mmc.exe`) を起動し、コンピュータ アカウントの証明書スナップインを追加し、ローカル コンピュータの証明書を管理します。

   b [ファイル] - [スナップインの追加と削除] を選択します。

   c [証明書] スナップインをクリックして、[追加] をクリックします。

   d [証明書スナップイン] 画面で、[コンピュータ ーアカウント] を選択し、[次へ] をクリックします。

   この設定は、Horizon FLEX サーバで必要となります。

   e [ローカル コンピューター] を選択して、[完了] をクリックして [OK] をクリックします。

   f 左側のナビゲーション パネルで[証明書（ローカル コンピューター）] をデプロイします。

   g [信頼されたルート証明機関] を右クリックして、[すべてのタスク] - [インポート] の順に選択します。

   [証明書のインポート ウィザード] が開きます。

   h [次へ] をクリックします。

   i ルート証明書ファイルを見つけて、[次へ] をクリックします。

   j [証明書をすべて次のストアに配置する：信頼されたルート証明機関]を選択し、[次へ] をクリックしてから、[完了] をクリックします。

   k [中間ルート証明機関] を右クリックして、[すべてのタスク] - [インポート] を選択します。

   l [証明書のインポート ウィザード] が開きます。

   m ルート証明書ファイルを見つけて、[次へ] をクリックします。

   n [証明書をすべて次のストアに配置する：中間ルート証明機関] を選択し、[次へ] をクリックしてから、[完了] をクリックします。

   o インストールする中間証明書ごとに、手順 m と n を繰り返します。

   p [信頼されたルート証明機関] - [証明書] に移動します。

   q 自己署名証明書を選択し、エクスポートします。

   証明書を DER エンコードのバイナリ X.509 (.CER) 形式でエクスポートします。

2 自己署名証明書を Mac にコピーします。

3 自己署名証明書を Mac にインポートします。

   a 自己署名証明書をダブルクリックして、キーチェーン アクセスで開きます。

   自己署名証明書が [ログイン] に表示されます。

   b 自己署名証明書を [システム] にコピーします。

   証明書を [システム] にコピーし、すべてのユーザーと、Fusion Pro の仮想マシン (vmware-vmx) プロセスを含むローカル システム プロセスによって信頼されるようにする必要があります。

   c [システム] の自己署名証明書を開いて [信頼] をデプロイし、[システムデフォルトを使用] を選択し、変更を保存します。

   d [システム] の自己署名証明書をもう 1 度開いて [信頼] をデプロイし、[常に信頼] を選択し、変更を保存します。

   e 自己署名証明書を [ログイン] から削除します。

内部 CA 証明書の使用

Entrust や Go Daddy のような商用 CA からではなく、内部 CA の証明書を使用し、準備しているソース仮想マシンで証明書を構成しない場合、Horizon FLEX 仮想マシンが正しく動作するように、各エンドユーザー ホストにルート CA 証明書をインストールする必要があります。

注意　サーバ証明書はルート CA によって署名されるため、エンドユーザー ホストにサーバ証明書をインポートする必要はありません。

ポリシー ファイルで証明書のリストが空になっている場合、Workstation Player および Fusion Pro は、ホストの信頼される証明書リストに戻って認証します。

Horizon FLEX ポリシー サーバ にソース仮想マシンの内部 CA の証明書を追加しており、Horizon FLEX Client の証明書を構成またはインストールしている場合（ソース仮想マシンのポリシー ファイルまたはホストの信頼される証明書リストのいずれかに）、たとえば、証明書の有効期限が切れる場合など、証明書の更新が必要となる場合でも、エンドユーザー ホストにルート CA 証明書をインストールする必要はありません。

ソース仮想マシンにおける証明書の構成の詳細については、「「Fusion Pro でのソース仮想マシンの作成 (P. 32)」」を参照してください。

信頼される証明書リストの作成と Horizon FLEX ポリシー サーバ へのインポートの詳細については、「「信頼される証明書リストの作成 (P. 21)」」を参照してください。

証明書の更新の詳細については、「「サーバでの証明書の更新 (P. 24)」」を参照してください。

Windows コンピュータに内部ルート CA 証明書をインストールする

内部ルート CA 証明書を Windows ホストにインストールするには、証明書を Horizon FLEX サーバからエクスポートして、Windows コンピュータにインポートします。

開始する前に

- Windows システムにおける MMC 証明書スナップインのインストールと使用の方法を確認しておきます。詳細については、http://technet.microsoft.com の Windows TechNet Web サイトを参照してください。
- 内部 CA 証明書を入手し、インストールします。Windows MMC 証明書スナップインを使用して証明書を要求できます。
- Windows IIS をインストールします。

手順

1　ルート CA 証明書を Horizon FLEX サーバからエクスポートします。

   a　Horizon FLEX サーバで MMC (`mmc.exe`) を起動し、コンピュータ アカウントの証明書スナップインを追加し、ローカル コンピュータの証明書を管理します。

   b　[[ファイル] > [スナップインの追加と削除]] を選択します。

   c　[証明書] スナップインをクリックして、[追加] をクリックします。

   d　[証明書スナップイン] 画面で、[コンピュータ ーアカウント] を選択し、[次へ] をクリックします。

   この設定は、Horizon FLEX サーバで必要となります。

   e　[ローカル コンピューター] を選択して、[完了] をクリックして [OK] をクリックします。

   f　左側のナビゲーション パネルで[証明書（ローカル コンピューター）] をデプロイします。

   g　[信頼されたルート証明機関] を右クリックして、[[すべてのタスク] > [インポート]] を選択します。

   [証明書のインポート ウィザード] が開きます。

   h　[次へ] をクリックします。

i ルート証明書ファイルを見つけて、[次へ] をクリックします。

j [証明書をすべて次のストアに配置する：信頼されたルート証明機関]を選択し、[次へ] をクリックしてから、[完了] をクリックします。

k [中間ルート証明機関] を右クリックして、[すべてのタスク > インポート] を選択します。

l [証明書のインポート ウィザード] が開きます。

m ルート証明書ファイルを見つけて、[次へ] をクリックします。

n [証明書をすべて次のストアに配置する：中間ルート証明機関] を選択し、[次へ] をクリックしてから、[完了] をクリックします。

o インストールする中間証明書ごとに、手順 m と n を繰り返します。

p [信頼されたルート証明機関] - [証明書] に移動します。

q ルート CA 証明書を選択し、エクスポートします。

証明書を DER エンコードのバイナリ X.509 (.CER) 形式でエクスポートします。

2 ルート CA 証明書を Windows コンピュータにコピーします。

3 ルート CA 証明書を Windows コンピュータにインポートします。

a Windows コンピュータで、MMC (**mmc.exe**) を起動します。

b コンピュータ アカウントの証明書スナップインを追加し、ローカル コンピュータの証明書を管理します。

c ルート CA 証明書を [信頼されたルート証明機関] - [証明書] にインポートします。

ルート CA 証明書がすべてのユーザーに対して信頼されるようになりました。

Mac への内部ルート CA 証明書のインストール

内部ルート CA 証明書を Mac ホストにインストールするには、証明書を Horizon FLEX Server からエクスポートして、Mac にインポートします。

開始する前に

- Windows システムにおける MMC 証明書スナップインのインストールと使用の方法を確認しておきます。詳細については、http://technet.microsoft.com の Windows TechNet Web サイトを参照してください。
- Mac におけるキーチェーン アクセスの使用方法について確認しておきます。詳細については、http://support.apple.com の Apple Support Web サイトを参照してください。
- Windows IIS をインストールします。

手順

1 ルート CA 証明書を Horizon FLEX サーバからエクスポートします。

a Horizon FLEX サーバで MMC (**mmc.exe**) を起動し、コンピュータ アカウントの証明書スナップインを追加し、ローカル コンピュータの証明書を管理します。

b [[ファイル] > [スナップインの追加と削除]] を選択します。

c [証明書] スナップインをクリックして、[追加] をクリックします。

d [証明書スナップイン] 画面で、[コンピュータ ーアカウント] を選択し、[次へ] をクリックします。

この設定は、Horizon FLEX サーバで必要となります。

e [ローカル コンピューター] を選択して、[完了] をクリックして [OK] をクリックします。

f 左側のナビゲーション パネルで[証明書（ローカル コンピューター）] をデプロイします。

g [信頼されたルート証明機関] を右クリックして、[[すべてのタスク] > [インポート]] を選択します。

[証明書のインポート ウィザード] が開きます。

h [次へ] をクリックします。

i ルート証明書ファイルを見つけて、[次へ] をクリックします。

j [証明書をすべて次のストアに配置する：信頼されたルート証明機関]を選択し、[次へ] をクリックしてから、[完了] をクリックします。

k [中間ルート証明機関] を右クリックして、[すべてのタスク > インポート] を選択します。

l [証明書のインポート ウィザード] が開きます。

m ルート証明書ファイルを見つけて、[次へ] をクリックします。

n [証明書をすべて次のストアに配置する：中間ルート証明機関] を選択し、[次へ] をクリックしてから、[完了] をクリックします。

o インストールする中間証明書ごとに、手順 m と n を繰り返します。

p [信頼されたルート証明機関] - [証明書] に移動します。

q ルート CA 証明書を選択し、エクスポートします。

証明書を DER エンコードのバイナリ X.509 (.CER) 形式でエクスポートします。

2 ルート CA 証明書を Mac にコピーします。

3 ルート CA 証明書を Mac にインポートします。

a ルート CA 証明書をダブルクリックして、キーチェーン アクセスで開きます。

ルート CA 証明書が [ログイン] に表示されます。

b ルート CA 証明書を [システム] にコピーします。

証明書を [システム] にコピーし、すべてのユーザーと Fusion の仮想マシン (`.vmx`) プロセスを含むローカル システム プロセスによって信頼されるようにする必要があります。

c ルート CA 証明書を開いて [信頼] をデプロイし、[システムデフォルトを使用] を選択し、変更を保存します。

d ルート CA 証明書をもう 1 度開いて [信頼] をデプロイし、[常に信頼] を選択し、変更を保存します。

e ルート CA 証明書を [ログイン] から削除します。

Horizon FLEX 仮想マシンの作成とデプロイ 4

複数の Horizon FLEX 仮想マシンを作成し、それらの仮想マシンの資格を Mac ユーザーを含む複数のタイプのエンド ユーザーに付与できます。Horizon FLEX 仮想マシンを使用する場合、ユーザーをエンタープライズ ネットワークから接続または切断できます。Horizon FLEX 仮想マシンのソース仮想マシンを作成する場合、いくつかのオプションを選択して、仮想マシンが Horizon FLEX で正しく機能するようにする必要があります。

Fusion Pro または Workstation Pro（Horizon FLEX パッケージには含まれません）を使用して、ソース仮想マシンを作成できます。

この章では次のトピックについて説明します。

Horizon FLEX 仮想マシン展開の概要

Horizon FLEX 仮想マシンを展開するには、特定の順序でタスクを実行します。

1 ソース仮想マシンを作成して構成します。

「Fusion Pro でのソース仮想マシンの作成 (P. 32)」または「Workstation Pro でのソース仮想マシンの作成（Horizon FLEX に含まれていない） (P. 33)」を参照してください。

2 (オプション) ソース仮想マシンを Active Directory ドメインに参加させる準備を行います。

「Active Directory ドメインに参加させるためにソース仮想マシンを準備する (P. 35)」を参照してください。

3 ソース仮想マシン パッケージを圧縮し、自分のダウンロード ディレクトリに保存します。

「ソース仮想マシン パッケージを圧縮する (P. 36)」を参照してください。

4 ソース仮想マシンを Horizon FLEX ポリシー サーバ に登録します。

「Horizon FLEX ポリシー サーバ でのソース仮想マシンの登録 (P. 37)」を参照してください。

5 Horizon FLEX イメージのポリシーを作成し、Active Directory のユーザーとグループにイメージの資格を付与します。

「ポリシーと資格の作成 (P. 38)」を参照してください。

6 (オプション) Horizon FLEX 仮想マシンを展開するための URI を作成します。

「URI を作成して Horizon FLEX 仮想マシンをデプロイする (P. 45)」を参照してください。

Fusion Pro でのソース仮想マシンの作成

Fusion Pro を使用すると、Horizon FLEX 仮想マシンのソース仮想マシンを作成できます。ソース仮想マシンを作成する場合は、暗号化と制限の情報を設定して、仮想マシンが Horizon FLEX で正しく機能するようにする必要があります。

Workstation Pro を使用してソース仮想マシンを作成することもできます。Workstation Pro は Horizon FLEX パッケージに含まれません。

仮想マシンの作成時に USB デバイスの使用、ドラッグ アンド ドロップ、およびコピー アンド ペースト機能を有効にすると、Horizon FLEX 管理コンソール でポリシーを設定することで、これらの機能をエンド ユーザーに対して有効または無効にできます。ただし、仮想マシンの作成時にこれらの機能を無効にすると、ポリシーを設定することでこれらの機能を有効にし、仮想マシンの設定を無効化することはできません。

Horizon FLEX は、英語の文字を使用する仮想マシン名のみをサポートします。.vmx または .tar のファイル名には非 ASCII 文字を使用しないでください。Fusion Pro は、日本語または簡体字中国語で Horizon FLEX 仮想マシンを作成できません。

注意 Horizon FLEX 仮想マシンを準備する際は、すべての仮想マシン ディスク (.vmdk) ファイルと同じフォルダに .vmx ポリシー ファイルが含まれることを確認してください。クライアント ユーザーのマシン上で .vmx ファイルと仮想マシン ディスクファイルが異なるディレクトリに含まれる場合、ユーザーが Horizon FLEX 仮想マシンを起動しようとするとエラー メッセージが表示されます。

開始する前に

- Fusion Pro での仮想マシンの作成方法を確認しておきます。https://www.vmware.com/support/pubs/fusion_pubs.html の Fusion のドキュメントを参照してください。
- Horizon FLEX 仮想マシンでサポートされるゲスト OS を確認しておきます。「サポートされるホストおよびゲスト OS (P. 12)」を参照してください。
- Horizon FLEX のライセンス キーで Fusion Pro をインストールします。

手順

1 Fusion Pro を開いて、仮想マシンを作成します。

Horizon FLEX でサポートされるゲスト OS を選択します。仮想マシンが作成されるとき、Fusion Pro は VMware Tools のインストールを試行します。エンド ユーザーへの配布用の仮想マシンを構成します。

2 仮想マシン ライブラリで新しい仮想マシンを選択し、[設定] - [暗号化と制限] を選択します。

3 [暗号化の有効化] を選択し、仮想マシンを開くためのパスワードを設定します。

6 文字以上のパスワードを設定する必要があります。エンド ユーザーが仮想マシンを開くことができるようにするためには、この暗号化のパスワードをエンド ユーザーに提供する必要があります。

暗号化のパスワードを保持する必要があります。このパスワードがないと仮想マシンにアクセスできません。

4 [制限の有効化] を選択し、仮想マシンの制限を編集するためのパスワードを設定します。

このパスワードは、仮想マシンの暗号化のパスワードとは別にしてください。

制限のパスワードを保持する必要があります。このパスワードがないと、仮想化マシンの制限を編集できません。

5 [構成] をクリックします。

[制限の構成] ウィンドウが開きます。

6 [制限のタイプ] を [管理] に設定します。

仮想マシンを配布して Horizon FLEX で使用するには、制約のタイプを [管理] に設定する必要があります。

7 仮想マシンをホストする Horizon FLEX Server の URL を [制約管理サーバ] テキスト ボックスに入力します。

8 [サーバの確認] をクリックして、Horizon FLEX Server の URL を確認します。

9 (オプション) 信頼される証明書を仮想マシンに追加するには、[+] ボタンをクリックして、それぞれの証明書ファイルの場所に移動します。

証明書を仮想マシンに追加すると、Horizon FLEX Client は仮想マシンの証明書を使用し、ホストの証明書を使用しなくなります。Horizon FLEX ポリシー サーバ で、すべての Horizon FLEX 仮想マシンの証明書の管理とセットアップを行うには、証明書ボックスを空白のままにします。

10 [保存] をクリックします。

11 [ロック] アイコンをクリックして、仮想マシンの制限を変更できないようにします。

制限のパスワードを使用すれば、仮想マシンの制限を編集できます。

次に進む前に

Horizon FLEX 仮想マシンを Active Directory ドメインに参加させる場合は、仮想マシンがドメインに参加できるようにしておきます。「Active Directory ドメインに参加させるためにソース仮想マシンを準備する (P. 35)」を参照してください。

Mirage クライアントをソース仮想マシンにインストールする方法については、「ソース仮想マシンへの Mirage クライアントのインストール (P. 34)」を参照してください。

Workstation Pro でのソース仮想マシンの作成（Horizon FLEX に含まれていない）

Workstation Pro を使用すると、Horizon FLEX 仮想マシンのソース仮想マシンを作成できます。Workstation Pro は Horizon FLEX パッケージに含まれません。Workstation Pro 用の Horizon FLEX のライセンス キーは不要です。

Horizon FLEX は、英語の文字を使用する仮想マシン名のみをサポートします。.vmx または .tar のファイル名には非 ASCII 文字を使用しないでください。

注意 Horizon FLEX 仮想マシンを準備する際は、すべての仮想マシン ディスク (.vmdk) ファイルと同じフォルダに .vmx ポリシー ファイルが含まれることを確認してください。クライアント ユーザーのマシン上で .vmx ファイルと仮想マシン ディスクファイルが異なるディレクトリに含まれる場合、ユーザーが Horizon FLEX 仮想マシンを起動しようとするとエラー メッセージが表示されます。

開始する前に

- Workstation Pro での仮想マシンの作成方法を確認します。https://www.vmware.com/support/pubs/ws_pubs.html で Workstation Pro のドキュメントを参照してください。
- Horizon FLEX 仮想マシンでサポートされるゲスト OS を確認します。「サポートされるホストおよびゲスト OS (P. 12)」を参照してください。
- Workstation をインストールします。

手順

1 Workstation Pro を開いて、仮想マシンを作成します。仮想マシンが作成されるとき、Workstation Pro は VMware Tools のインストールを試行します。

2 ゲスト OS をインストールします。

Horizon FLEX でサポートされるゲスト OS を選択します。エンド ユーザーへの配布用の仮想マシンを構成します。

3 仮想マシンを暗号化して制限します。仮想マシンを選択して、[VM] - [設定] を選択します。

4 [オプション] タブで [アクセス コントロール] を選択します。

5 [暗号化] をクリックして暗号化パスワードを入力し、[暗号化] をクリックします。

仮想マシンへのアクセスを得るには、暗号化のパスワードが必要になります。ユーザーがマシンの構成を変更できないように保護されていません。ユーザーがマシンの構成を変更できないようにするには、制限を有効にしてパスワードを入力します。

重要　使用する暗号化パスワードを記録します。パスワードを忘れた場合、Workstation にはパスワードを取得する方法は用意されていません。

仮想マシンの暗号化が開始されます。暗号化プロセスが完了した後、制限のパスワードを設定できます。

6 [制限の有効化] チェック ボックスを選択し、仮想マシンの制限を編集するためのパスワードを設定します。

仮想マシンの暗号化パスワードとは異なるパスワードを設定してください。

制限のパスワードを保持する必要があります。このパスワードがないと、仮想マシンの制限を編集できません。

7 [制限のタイプ] を [管理] に設定します。

仮想マシンを配布して Horizon FLEX で使用するには、制約のタイプを [管理] に設定する必要があります。

8 仮想マシンをホストする Horizon FLEX Server の URL を [制約管理サーバ] テキスト ボックスに入力します。

9 [サーバの確認] をクリックして、Horizon FLEX Server の URL を確認します。

10 (オプション) 信頼された証明書を仮想マシンに追加するには、[証明書の管理] アイコンをクリックし、それぞれの証明書ファイルの場所に移動します。

証明書を仮想マシンに追加すると、Horizon FLEX Client は仮想マシンの証明書を使用し、ホストの証明書を使用しなくなります。Horizon FLEX ポリシー サーバ で、すべての Horizon FLEX 仮想マシンの証明書の管理とセットアップを行うには、証明書ボックスを空白のままにします。

11 [保存] をクリックします。

次に進む前に

Horizon FLEX 仮想マシンを Active Directory ドメインに参加させる場合は、仮想マシンがドメインに参加できるようにしておきます。「Active Directory ドメインに参加させるためにソース仮想マシンを準備する (P. 35)」を参照してください。

Mirage クライアントをソース仮想マシンにインストールする方法については、「「ソース仮想マシンへの Mirage クライアントのインストール (P. 34)」」を参照してください。

ソース仮想マシンへの Mirage クライアントのインストール

ソース仮想マシンに Windows ゲスト オペレーティング システムがある場合は、Mirage クライアントを仮想マシンにインストールできます。Mirage クライアントのインストールはオプションです。

Mirage クライアントをソース仮想マシンにインストールする場合は、仮想マシンの資格を付与するときに、ディザスタリカバリのシナリオを選択できます。たとえば、エンド ユーザーがダウンロードする Horizon FLEX 仮想マシンの CVD を Mirage サーバに作成させるオプションを選択できます。Mirage は、選択された Mirage ポリシーに基づいて、エンドユーザーのデータをデーターセンターと定期的に同期します。メインの Mirage Management Console の Mirage File Portal を使用すると、このデータを使用して CVD を復元したり、仮想マシンのファイルにアクセスしたりできます。

注意　Mirage Server をディザスタ リカバリ向けに構成する際は、MongoDB ポートが正しく構成されていることを確認してください。詳細については、『VMware Mirage インストール ガイド』を参照してください。

開始する前に

- ソース仮想マシンを作成します。「Fusion Pro でのソース仮想マシンの作成 (P. 32)」または「Workstation Pro でのソース仮想マシンの作成（Horizon FLEX に含まれていない） (P. 33)」を参照してください。
- Mirage クライアントのインストール手順に従って VMware Mirage インストール ガイド を入手します。

手順

1 Fusion Pro または Workstation Pro で、ソース仮想マシンを開始して、ゲスト OS にログインします。

2 VMware Tools の最新バージョンをインストールします。

   a メニューバーから、[仮想マシン] - [VMware Tools のインストール] を選択します。

   b [次へ] をクリックして、インストールを続行します。

   c VMware Tools の一部の機能を除外する必要がある場合を除き、[完了] を選択し、[次へ] をクリックします。

   d [インストール] をクリックします。

   e インストールが終了したら、[はい] をクリックして仮想マシンを再起動します。

3 Mirage クライアントを ソース仮想マシンにインストールします。

   詳細については、『VMware Mirage インストール ガイド』を参照してください。

4 Mirage Management Console で、エンドポイントが [割り当て保留中] として表示されていることを確認します。

   注意 ソース仮想マシンを配布している間は、この保留の記録を削除しないでください。

5 Mirage Management Console で、CVD 自動作成を有効化します。

   a [システム構成] を右クリックして、[設定] を選択します。

   b [CVD 自動作成] タブをクリックします。

   c [CVD 自動作成を有効にする] を選択します。

      必要に応じてユーザー メッセージを変更できます。

   d [OK] をクリックします。

6 ソース仮想マシンが [割り当て保留中] の状態にある場合には、Mirage でパワーオフします。

   ユーザー名とパスワードを指定しないでください。Mirage クライアント プロンプトでソース仮想マシンを登録しないでください。Mirage にソース仮想マシンを登録すると、エンド ユーザーがアクセスするときに Horizon FLEX 仮想マシンが複製されます。

Mirage クライアントがアクティブになり、このソース仮想マシンに新しい Horizon FLEX の資格を作成すると、この仮想マシンについて Mirage のコントロールを使用できるようになります。

Active Directory ドメインに参加させるためにソース仮想マシンを準備する

Horizon FLEX 仮想マシンを特定の Active Directory ドメインに参加させる場合、Horizon FLEX ポリシー サーバ に登録する前に、ドメインに参加するように、ソース仮想マシンを準備する必要があります。

開始する前に

- ソース仮想マシンを作成します。「Fusion Pro でのソース仮想マシンの作成 (P. 32)」または「Workstation Pro でのソース仮想マシンの作成（Horizon FLEX に含まれていない） (P. 33)」を参照してください。

   注意 ソース仮想マシンには Windows 7 Home エディションや Windows 以外のゲスト OS をインストールしないでください。Windows 7 Home エディション オペレーティング システムや Windows 以外のゲスト OS をドメインに参加させることはできません。

- ソース仮想マシンに管理者パスワードが設定されていることを確認します。
- Horizon FLEX Admin Console で、仮想マシンを Active Directory ドメインに参加させるためのポリシーを設定します。Horizon FLEX 管理者アカウントには、Active Directory でオブジェクトを作成する権限が必要です。
- RODC が DMZ にインストールされている必要があります。
- ドメイン参加をサポートするように Active Directory を構成します。

手順

1. Fusion Pro で、ソース仮想マシンを開始して、ゲスト OS にログインします。
2. (オプション) [Windows アップデート] をオフにします。
3. VMware Tools の最新バージョンをインストールします。
   a. メニューバーから、[仮想マシン] - [VMware Tools のインストール] を選択します。
   b. [次へ] をクリックして、インストールを続行します。
   c. VMware Tools の一部の機能を除外する必要がある場合を除き、[完了] を選択し、[次へ] をクリックします。
   d. [インストール] をクリックします。
   e. インストールが終了したら、[はい] をクリックして仮想マシンを再起動します。
4. 管理者として **`install-rvmsetup.cmd`** を実行して、VMware RVM Setup サービスをソース仮想マシンにインストールします。

   VMware RVM Setup サービスによってドメインへの参加操作が実行されます。**`install-rvmsetup.cmd`** は、VMware Tools に含まれています。
5. Windows の [サービス] スナップイン (**`services.msc`**) を開いて、VMware RVM Setup サービスのスタートアップの種類が [自動] に設定されていることを確認します。
6. ソース仮想マシンをシャットダウンします。

   ソース仮想マシンを次回起動するときに、VMware RVM Setup サービスが起動します。

ソース仮想マシン パッケージを圧縮する

エンド ユーザーが簡単に仮想マシンをダウンロードできるように、ソース仮想マシン パッケージを TAR (**`.tar`**) 形式で圧縮する必要があります。仮想マシン パッケージ（バンドルとも呼ばれます）には、仮想マシンの実行に必要なすべての仮想マシン ファイルが含まれます。

開始する前に

- ソース仮想マシンを作成します。「Fusion Pro でのソース仮想マシンの作成 (P. 32)」または「Workstation Pro でのソース仮想マシンの作成（Horizon FLEX に含まれていない） (P. 33)」を参照してください。
- Horizon FLEX 仮想マシン パッケージのダウンロード フォルダを作成および構成します。「Horizon FLEX 仮想マシン パッケージ用のダウンロード フォルダの作成 (P. 15)」および「Horizon FLEX Server の IIS SSL サーバ証明書の構成 (P. 16)」を参照してください。

手順

1. ソース仮想マシンが実行中の場合は、シャットダウンします。
2. Fusion Pro または Workstation Pro で、ソース仮想マシンに移動します。
3. [ファイル] - [TAR にエクスポート] を選択し、ソース仮想マシン パッケージを TAR ファイルにエクスポートします。

   TAR ファイル名に含まれているすべてのスペースを削除します。ファイル名からスペースを削除すると、仮想マシンのダウンロード URL に簡単に接続できるようになります。
4. TAR ファイルを Horizon FLEX 仮想マシン パッケージのダウンロード フォルダにエクスポートします。

次に進む前に

ソース仮想マシンを Horizon FLEX ポリシー サーバ に登録します。「Horizon FLEX ポリシー サーバ でのソース仮想マシンの登録 (P. 37)」を参照してください。

Horizon FLEX ポリシー サーバ でのソース仮想マシンの登録

Horizon FLEX ポリシー サーバ でソース仮想マシンを Horizon FLEX イメージとして登録しなければ、仮想マシンをエンド ユーザーに配布できません。

開始する前に

- ソース仮想マシンを TAR (`.tar`) アーカイブ ファイルに圧縮します。「ソース仮想マシン パッケージを圧縮する (P. 36)」を参照してください。
- Horizon FLEX 仮想マシン パッケージのダウンロード ディレクトリが適切にセットアップされていることを確認します。「Horizon FLEX 仮想マシン パッケージ用のダウンロード フォルダの作成 (P. 15)」および「Horizon FLEX Server の IIS SSL サーバ証明書の構成 (P. 16)」を参照してください。
- ソース仮想マシンの構成 (`vmx`) ファイルで制限がすでに設定されていることを確認します。制限が設定されていない仮想マシンを選択すると、Horizon FLEX ポリシー サーバ は、`.vmx` ファイルを無効であるとして拒否します。仮想マシンにおける制限の設定の詳細については、「「Fusion Pro でのソース仮想マシンの作成 (P. 32)」」を参照してください。

手順

1 ソース仮想マシンが Mac 上にある場合、これらの手順を実行します。

   a 仮想マシンの仮想マシン パッケージ (`.vmwarevm`) ファイルを見つけて、そのファイル名を右クリックし、[パッケージ コンテンツを表示] を選択します。

   b 仮想マシン構成 (`.vmx`) ファイルを、Horizon FLEX Server がアクセスできる場所にコピーします。

2 Horizon FLEX 管理コンソール を起動します。

   a Web ブラウザに **`https://<WebManagerServer>:7443/rvm`**（<WebManagerServer> は Mirage Web Manager がインストールされているホストの DNS 名または IP アドレス）と入力します。

   b Mirage にアクセスできるドメイン アカウントのユーザー名とパスワードを入力します。

   c [ログイン] をクリックします。

3 左側のナビゲーション パネルで [イメージ] をクリックします。

4 [新規] ([+]) ボタンをクリックします。

5 [イメージ ファイルの選択] テキスト ボックスの横の [選択] をクリックし、ソース仮想マシンの仮想マシン構成 (`.vmx`) ファイルを参照します。

6 Horizon FLEX 仮想マシン ファイルのユーザー フレンドリ名を [イメージ名] テキスト ボックスに入力します。

   たとえば、**`Windows 7 VM`** のように入力します。

7 (オプション) Horizon FLEX 仮想マシンの説明を [説明] テキスト ボックスに入力します。

8 (オプション) [アイコン]の横にある [変更] ボタンをクリックして、Horizon FLEX 仮想マシンのアイコンをアップロードします。

   アップロードするアイコンは、PNG (`.png`) ファイルである必要があります。

9 (オプション) [イメージ URL] テキスト ボックスで、ソース仮想マシン パッケージが含まれる TAR ファイルの完全修飾パスを入力します。

エンド ユーザーは Horizon FLEX 仮想マシンをこの URL からダウンロードします。 URL の形式は `http://<server>:<port>/<download_directory>/<filename.tar>` になります。<server> には、TAR ファイルを保存したサーバのホスト名または IP アドレス、port にはサーバのポート番号、<download_folder> には、TAR ファイルを含む Horizon FLEX 仮想マシンのダウンロード フォルダの名前、<filename.tar> には、ソース仮想マシン パッケージを含む TAR ファイルの名前を指定します。URL は、http と https のいずれかで始めることができます。

例：`https://flexserver.demo.local:7443/flexdownloads/windows7vm.tar`

10 (オプション) [免責事項（オプション）] テキスト ボックスにテキストを入力します。

テキストを指定しない場合、ユーザーが Horizon FLEX 仮想マシンをダウンロードするときに、Horizon FLEX Client には免責事項のテキストが表示されません。

11 [OK] をクリックして、ソース仮想マシンを Horizon FLEX イメージとして登録します。

12 (オプション) イメージ URL を Web ブラウザに入力して、URL を検証します。

例：`https://flexserver.demo.local:7443/flexdownloads/windows7vm.tar`

ファイルを保存するように求められます。権限エラーが表示される場合、ダウンロード フォルダの NTFS 権限を調整する必要がある場合があります。

次に進む前に

Horizon FLEX イメージにポリシーを追加します。「Horizon FLEX イメージの一般的なポリシーを構成する (P. 38)」を参照してください。

ポリシーと資格の作成

ポリシーを使用して、Horizon FLEX イメージから作成された仮想マシンの有効期限を設定したり、機能を制御したりします。資格を使用して、特定のユーザーとグループが特定の Horizon FLEX イメージから仮想マシンのインスタンスを作成できるようにします。

ポリシーには作成する各資格を関連付けます。このポリシーは、Horizon FLEX イメージから作成された仮想マシン インスタンスの、資格におけるデフォルトの制限の設定を定義します。

同じ Horizon FLEX イメージを複数の資格に含めることができ、各資格には異なるポリシーを関連付けることができます。同じユーザーが、複数の資格のメンバーになることができます。

仮想マシン インスタンスが作成されると、資格に関連付けられているポリシーによってインスタンスの初期の制限が決定されます。管理者として、特定の仮想マシン インスタンスの制限設定を変更できます。インスタンス固有の制限は、特定のユーザーと仮想マシンの組み合わせについて制限として機能します。仮想マシンの制限設定の詳細については、「「Horizon FLEX 仮想マシンのトラブルシューティング (P. 47)」」を参照してください。

Horizon FLEX イメージの一般的なポリシーを構成する

一般的なポリシーを構成して、Horizon FLEX イメージから作成された仮想マシンの有効期限を設定したり、機能を制御したりします。

重要　コピーアンドペースト、ドラッグアンドドロップ、およびフォルダ共有設定がソース仮想マシンで有効である場合は、ユーザーが仮想マシンのインスタンスをダウンロードするときにこれらの機能を有効または無効にするようにポリシーを構成できます。これらの機能がソース仮想マシンで無効である場合は、これらの機能をポリシーで有効にして、仮想マシンの設定を無効にすることはできません。

ユーザーにイメージの資格を付与するときに Horizon FLEX イメージに割り当てるポリシーを選択します。同じポリシーを複数の資格で使用できます。

手順

1 Horizon FLEX 管理コンソール を起動します。

   a Web ブラウザに **`https://<WebManagerServer>:7443/rvm`**（<WebManagerServer> は Mirage Web Manager がインストールされているホストの DNS 名または IP アドレス）と入力します。

   b Mirage にアクセスできるドメイン アカウントのユーザー名とパスワードを入力します。

   c [ログイン] をクリックします。

2 左側のナビゲーション画面で [ポリシー] を選択します。

3 [全般] タブをクリックしてポリシーを追加するか、既存のポリシーを選択してから [編集] をクリックして変更します。

4 ポリシーの名前を [ポリシー名] テキスト ボックスに入力します。

5 (オプション) ポリシーの説明を [説明] テキスト ボックスに入力します。

6 [一般的な制限] で、仮想マシンの制限を構成します。

オプション	操作
有効期限の日付	カレンダ ウィジェットを使用して、仮想マシンの有効期限を設定します。
コピー アンド ペースト操作	仮想マシンでコピーアンドペースト操作を許可するかどうかを指定します。このポシリーは、仮想マシン ゲストとホスト間のコピーアンドペースト操作を制御します。仮想マシンでのコピーアンドペースト操作は制御しません。
ドラッグ アンド ドロップ操作	仮想マシンでドラッグアンドドロップ操作を許可するかどうかを指定します。このポシリーは、仮想マシン ゲストとホスト間のドラッグアンドドロップ操作を制御します。仮想マシンでのドラッグアンドドロップ操作は制御しません。
フォルダ共有設定	管理者が仮想マシンで共有フォルダを構成している場合、仮想マシン ゲスト OS で共有フォルダの使用を許可するかどうかを指定します。
メモリおよびプロセッサ設定の変更	仮想マシンのメモリおよび CPU 設定のユーザーによる変更を許可するかどうかを指定します。
仮想マシンを移動またはコピーするときには、パワーオンのパスフレーズを変更するようにユーザーに要求する	ユーザーが仮想マシンを移動またはコピーした場合に暗号化パスワードの変更をユーザーに要求するかどうかを指定します。
最初の起動後に、ユーザーの AD パスフレーズと照合するパワーオン パスフレーズを設定する	仮想マシンをパワーオンするときにユーザーが入力したパスワードを Active Directory パスワードと照合するかどうかを指定します。
仮想マシンの複数コピーをユーザーが作成できないように制限する	仮想マシンへの複数のインスタンスのダウンロードや、すでに登録されている仮想マシンのコピーをユーザーに許可するかどうかを指定します。

7 (オプション) [エンド ユーザー メッセージ] で、仮想マシンの有効期限設定を構成します。

   デフォルトのメッセージは、**この仮想マシンは期限切れになっています。**です。

   a 仮想マシンが期限切れになったときに、ユーザーに表示する追加のカスタム メッセージを入力します。

   b [このメッセージを表示する] チェック ボックスを選択し、仮想マシンの有効期限が切れる何日前にカスタム メッセージを表示するのかを選択し、カスタム メッセージ テキストを入力します。

8 [サーバ設定] で、Horizon FLEX サーバの設定を構成します。

オプション	操作
FLEX サーバの URL	仮想マシン パッケージをホストする Horizon FLEX サーバの URL を入力します。例：**`https://flexserver.demo.local:7443`** 重要　URL の末尾に **`/rvm`** を追加しないでください。
サーバ接続頻度	仮想マシンが同期のためのサーバに接続する頻度を選択します。
オフライン時間制限	仮想マシンが Horizon FLEX サーバに接続することなく、ユーザーが仮想マシンを使用できる日数を設定します。 オフライン時間の制限を超過すると、仮想マシンが Horizon FLEX サーバーに接続しないと、パワーオンできません。

9 [OK] をクリックしてポリシーを保存します。

新しいポリシーがポリシー リストに表示されます。

次に進む前に

Horizon FLEX 仮想マシンに資格を付与します。「Horizon FLEX イメージの資格を付与する (P. 43)」を参照してください。

Horizon FLEX イメージの USB デバイス ポリシーを構成する

ポリシーを構成して、Horizon FLEX イメージから作成した仮想マシンで USB デバイスを使用できるようにするかどうかを制御できます。

重要　USB デバイス コントローラがソース仮想マシンに存在する場合は、ユーザーが仮想マシンのインスタンスをダウンロードするときにこの機能を有効または無効にするようにポリシーを構成できます。この機能がソース仮想マシンで無効である場合は、この機能をポリシーで有効にして、仮想マシンの設定を無効にすることはできません。

手順

1 Horizon FLEX 管理コンソール を起動します。

a Web ブラウザに **`https://<WebManagerServer>:7443/rvm`**（<WebManagerServer> は Mirage Web Manager がインストールされているホストの DNS 名または IP アドレス）と入力します。

b Mirage にアクセスできるドメイン アカウントのユーザー名とパスワードを入力します。

c [ログイン] をクリックします。

2 左側のナビゲーション画面で [ポリシー] を選択します。

3 [デバイス制御] タブをクリックして、新しいデバイス ポリシーを追加します。

4 [USB デバイスのグローバル使用] ドロップダウン メニューを選択して、ポリシーですべての USB デバイスを許可するか、仮想マシンのすべての USB デバイスをブロックするかどうかを設定します。

すべての USB デバイス クラスは灰色で表示され、変更できません。特定の USB デバイス クラスを許可するカスタム ポリシーを作成するには、「Horizon FLEX イメージのカスタム USB デバイス ポリシーを構成する (P. 41)」を参照してください。

5 [OK] をクリックしてポリシーを保存します。

新しいまたは更新されたポリシーがポリシー リストに表示されます。

次に進む前に

Horizon FLEX 仮想マシンに資格を付与します。「Horizon FLEX イメージの資格を付与する (P. 43)」を参照してください。

Horizon FLEX イメージのカスタム USB デバイス ポリシーを構成する

カスタム デバイス ポリシーを構成して、Horizon FLEX イメージから作成した仮想マシンで固有のタイプの USB デバイスを使用できるようにするかどうかを制御できます。

重要　USB デバイス コントローラがソース仮想マシンに存在する場合は、ユーザーが仮想マシンのインスタンスをダウンロードするときにこの機能を有効または無効にするようにポリシーを構成できます。この機能がソース仮想マシンで無効である場合は、この機能をポリシーで有効にして、仮想マシンの設定を無効にすることはできません。

手順

1 Horizon FLEX 管理コンソール を起動します。

   a Web ブラウザに **`https://<WebManagerServer>:7443/rvm`**（<WebManagerServer> は Mirage Web Manager がインストールされているホストの DNS 名または IP アドレス）と入力します。

   b Mirage にアクセスできるドメイン アカウントのユーザー名とパスワードを入力します。

   c [ログイン] をクリックします。

2 左側のナビゲーション画面で [ポリシー] を選択します。

3 [デバイス制御] タブをクリックして、新しいデバイス ポリシーを追加します。

4 [USB デバイスのグローバル使用] ドロップダウン メニューを [カスタム] に設定し、仮想マシンでの特定クラスの USB デバイスを許可またはブロックします。

   USB デバイス クラスのテキスト ボックスが表示され、特定のクラスを許可またはブロックできます。

5 仮想マシンで許可またはブロックする USB クラスを選択します。

表 4-1. USB デバイス タイプ

USB クラス	基本クラス	例
オーディオ	01h	USB サウンド カード
通信および CDC デバイス	02h	USB ネットワーク アダプタ、RS-232 シリアル デバイス
物理操作	05h	ジョイスティック
画像	06h	USB カメラ、USB スキャナ、Web カメラ
プリンタ	07h	USB プリンタ
大容量ストレージ	08h	USB ディスク
スマート カード	0Bh	USB スマート カード リーダー
コンテンツ セキュリティ	0Dh	指紋リーダー
ビデオ	0Eh	Web カメラ
ワイヤレス コントローラ	E0h	Bluetooth アダプタ、Microsoft RNDIS
その他	EFh	[その他] オプションを選択して、前のクラスに含まれていない USB デバイスを許可またはブロックします。[その他] 設定が必要な USB クラスについては、表 4-2 を参照してください。

表 4-2. その他の USB デバイス クラス

USB クラス	基本クラス	例
ヒューマン インターフェイス デバイス (HID)	03h	USB キーボード、USB ジョイスティック、USB マウス
ハブ	09h	USB ハブ

表 4-2. その他の USB デバイス クラス (続き)

USB クラス	基本クラス	例
パーソナル ヘルスケア	0Fh	脈拍監視（ウォッチ）
診断デバイス	DCh	USB 互換テスト デバイス
アプリケーション固有	FEh	IrDA ブリッジ、テストおよび測定クラス (USBTMC)、USB デバイス ファームウェア アップグレード (DFU)

6 オプションで、特定の USB デバイスを許可するデバイス ポリシーを構成できます。

a [次の USB デバイスの使用を仮想マシンで許可する] テキスト ボックスの下にある、[追加] をクリックします。

b [名前] テキスト ボックスに USB デバイスの名前を入力します。

c [ベンダー ID] テキスト ボックスに 16 進数でベンダー ID を入力します。

d [プロダクト ID] テキスト ボックスに 16 進数でプロダクト ID を入力します。

e [追加] をクリックして、[更新] をクリックします。

Windows マシンで USB デバイス情報を取得するには、[システム ツール] をクリックしてから、[デバイス マネージャー] をクリックします。Mac で USB デバイス情報を取得するには、[Apple] アイコンをクリックし、[この Mac について] を選択し、[システム レポート] を選択してから、[USB] を選択して、デバイス項目をクリックします。

7 [OK] をクリックしてポリシーを保存します。

新しいまたは更新されたポリシーがポリシー リストに表示されます。

次に進む前に

Horizon FLEX 仮想マシンに資格を付与します。「Horizon FLEX イメージの資格を付与する (P. 43)」を参照してください。

デプロイされた Horizon FLEX イメージのポリシーを更新する

Horizon FLEX イメージがユーザーにデプロイされたら、既存の仮想マシン インスタンスに適用するポリシーを更新できます。

重要 左側のナビゲーション パネルで [ポリシー] ボタンを使用して既存のポリシーを編集すると、編集は新しいユーザーにのみ適用されます。編集されたポリシーは、デプロイされた仮想マシン インスタンスが関連付けられている既存のユーザーには適用されません。 たとえば、元のポリシーがユーザーによる仮想マシンの複数コピーの作成を制限しない状況で、ポリシーを編集してこの制限を追加した場合、既存の仮想マシンには制限が適用されません。元のポリシーの適用対象となる仮想マシンを持つユーザーは、引き続き仮想マシンのコピーを作成できます。編集されたポリシーの適用対象となる 2 番目の仮想マシンをダウンロードすると、このユーザーによる 2 番目の仮想マシンのコピーは制限されます。

手順

1 Horizon FLEX 管理コンソール を起動します。

a Web ブラウザに **`https://<WebManagerServer>:7443/rvm`**（<WebManagerServer> は Mirage Web Manager がインストールされているホストの DNS 名または IP アドレス）と入力します。

b Mirage にアクセスできるドメイン アカウントのユーザー名とパスワードを入力します。

c [ログイン] をクリックします。

2 左側のナビゲーション パネルで [仮想マシン] をクリックします。

3 仮想マシンを選択します。

4 [編集] をクリックします。

5 仮想マシンのポリシーを更新し、完了したら [OK] をクリックします。

次に進む前に

「Horizon FLEX イメージの一般的なポリシーを構成する (P. 38)」および「Horizon FLEX イメージの USB デバイス ポリシーを構成する (P. 40)」を参照してください。

Horizon FLEX イメージの資格を付与する

資格を使用して、特定の Horizon FLEX イメージから仮想マシンのインスタンスをダウンロードおよび作成することを特定のユーザーとグループに許可します。

ユーザーは、資格が付与されている任意の Horizon FLEX 仮想マシンをダウンロードできます。最初に Horizon FLEX 仮想マシンを登録して使用できるようにするには、ユーザーは Active Directory の認証情報を入力する必要があります。ユーザーは Horizon FLEX Server にログインして、仮想マシンをダウンロードできます。または、Horizon FLEX 仮想マシンを USB からコピーして、仮想マシンの初回起動時に Active Directory の認証情報を入力できます。

開始する前に

- 適切な Active Directory のユーザーとグループが Horizon FLEX データベースで同期されていることを確認します。「Active Directory の設定を構成する (P. 16)」を参照してください。
- ソース仮想マシンを Horizon FLEX ポリシー サーバ に登録します。「Horizon FLEX ポリシー サーバ でのソース仮想マシンの登録 (P. 37)」を参照してください。
- Horizon FLEX イメージのポリシーを構成します。「Horizon FLEX イメージの一般的なポリシーを構成する (P. 38)」を参照してください。

手順

1 Horizon FLEX 管理コンソール を起動します。

   a Web ブラウザに **`https://<WebManagerServer>:7443/rvm`**（<WebManagerServer> は Mirage Web Manager がインストールされているホストの DNS 名または IP アドレス）と入力します。

   b Mirage にアクセスできるドメイン アカウントのユーザー名とパスワードを入力します。

   c [ログイン] をクリックします。

2 左のパネルで [資格] を選択します。

3 [新規] ([+]) ボタンをクリックして資格を作成するか、既存の資格を選択してから [編集] をクリックして変更します。また、既存の資格を選択してから [複製] をクリックして複製します。

4 資格名を作成して、これを Horizon FLEX イメージに割り当てます。

   a 資格の名前を [資格名] テキスト ボックスに入力します。

   b 資格に追加する Horizon FLEX イメージを選択します。

   検索フィールドを使用すると、Horizon FLEX イメージのリストをフィルタリングできます。

   既存の資格を複製する場合は、保存する前に複製した資格の名前を変更する必要があります。

   Horizon FLEX イメージを選択すると、そのイメージの URL が自動的に [ダウンロード URL] テキスト ボックスに表示されます。

   c [ダウンロード URL] テキスト ボックスで、クライアントが Horizon FLEX イメージのダウンロードに使用する URL を変更します。

   d [次へ] をクリックします。

5 資格に追加する Active Directory のユーザーとグループを選択します。

a 検索フィールドを使用して、資格に追加するユーザーとグループを検索し、選択します。

新しい Active Directory のユーザーやグループは、最長 15 分間経過しないと検索結果に表示されません。

b [追加] をクリックして、ユーザーまたはグループを [資格メンバー] リストに追加します。

[削除] または [すべて消去] ボタンを使用すると、メンバーのリストを管理できます。

c [次へ] をクリックします。

6 資格のポリシーを選択し、[次へ] をクリックします。

検索フィールドを使用してポリシーのリストをフィルタリングし、[フィルタの消去] と [フィルタの表示] ボタンを使用して検索を管理できます。

7 (オプション) 仮想マシンの命名パターンを使用するには、[マシン名の構成を使用] を選択して、命名パターンを構成します。

a 使用するマシン名パターンを [マシン名パターン] テキスト ボックスに入力します。

各仮想マシンに異なる名前が付けられ、ドメインに参加できるようにするには、{<username>} プレースホルダを使用します。このプレースホルダは、ユーザーが仮想マシンをダウンロードするときに個々のユーザーの名前に置換されます。また、{<n>} プレースホルダを使用して連続番号パターンを作成すると、ユーザー名に仮想マシン番号を順番に付けることができます。

詳細については、「仮想マシン名のパターンを作成する (P. 45)」を参照してください。

b ドメイン名を [ドメイン名] ドロップダウン メニューから選択します。

c [組織単位] テキスト ボックスに OU を入力します。

たとえば、**`OU=hr1, OU=hr, OU=flex, DC=ws, DC=test, DC=com`** のように指定します。

8 (オプション) Mirage クライアントを仮想マシンにインストールした場合は、仮想マシンを Mirage で管理するかどうかを選択します。

オプション	説明
VMware Mirage をディザスタ リカバリやイメージ管理のシナリオに使用する	このオプションを選択して、CVD ポリシー、ベース レイヤ、アプリケーション レイヤ、およびその他の構成を選択します。 Mirage サーバは、エンド ユーザーがダウンロードする仮想マシンの CVD を自動的に作成します。Mirage は、選択された Mirage ポリシーに基づいて、エンドユーザーのデータをデーター センターと定期的に同期します。メインの Mirage Management Console で Mirage File Portal を使用すると、このデータを使用して CVD を復元したり、仮想マシンのファイルにアクセスしたりできます。Mirage サーバはさらに、イメージのコンプライアンスとリモート アプリケーションの配信のために仮想マシンがプロビジョニングされた後に、ベース レイヤとアプリケーション レイヤーを仮想マシンに自動的に展開します。
VMware Mirage をディザスタ リカバリのシナリオに使用する	このオプションを選択して、CVD ポリシーを選択します。Mirage サーバは、エンド ユーザーがダウンロードする仮想マシンの CVD を作成します。メインの Mirage Management Console の Mirage File Portal を使用すると、このデータを使用して CVD を復元したり、仮想マシンのファイルにアクセスしたりできます。
VMware Mirage を仮想マシンの管理に使用しない	このオプションを選択して、仮想マシンを Mirage で管理しないことを指定します。

Mirage クライアントがインストールされている仮想マシンを削除すると、削除された仮想マシンの CVD を Mirage サーバがアーカイブします。

9 [次へ] をクリックし、権限の設定を確認します。

10 [終了] をクリックして権限を保存するか、[戻る] をクリックして前ページに戻って権限を編集します。

仮想マシン名のパターンを作成する

Horizon FLEX イメージの資格を付与する際、仮想マシン名のパターンを作成すると、仮想マシンが同じユーザー資格向けに作成されるときに Horizon FLEX が一意の仮想マシン名を作成します。

仮想マシン名のパターンには、{<username>} または {<n>} のパラメータを含める必要があります。{<n>} パラメータにより、仮想マシン名に順番に番号を追加する連続番号パターンが作成されます。以下のパターンが有効です。

- VM-{<username>}
- VM-{<n>}

以下のパターンは有効ではありません。

- VM-(<username>}-{<username>}
- VM-{<username>}-{<n>}
- VM-{<n>}-{<n>}

マシン名の上限は 15 文字です。マシン名が 15 文字以上である場合、最初の 15 文字だけが使用されます。たとえば、パターンが VM-1234567890-<username> でユーザー名が Jack の場合、マシン名は VM-1234567890-J に切り詰められます。

各仮想マシンに異なる名前が付けられ、ドメインに参加できるようにするには、{<username>} または {<n>} プレースホルダを使用する必要があります。{<username>} プレースホルダは、ユーザーが仮想マシンをダウンロードするときに個々のユーザーの名前に置換されます。{<n>} については、Active Directory で名前がパターンに一致するコンピュータの検索が行われます。パターンに一致する名前が見つからない場合は、連続番号の値は 1 となります。パターンに一致する名前が見つかった場合は、次の連続番号は、パターンに位置するすべての名前の中で最大の数字に続く数字となります。

たとえば、ある仮想マシンの資格が user1 に付与され、仮想マシン名のパターンが VM-<username>- <n> に設定されている場合、user1 がこの仮想マシンをダウンロードすると、VM-user1-<x>（<x> は割り当てられる数字）のような名前パターンにマシン名が一致するかどうか判断するための検索が Active Directory で行われます。最大のマッピング番号が 25（仮想マシン名が VM-user1-25）の場合、このマシン名は VM-user1-26 に設定されます。パターンに一致する仮想マシンがない場合、Horizon FLEX はこのマシンを VM-user1-1 として設定します。

複数の仮想マシンの資格を同じユーザーに付与できます。たとえば、3 台の仮想マシンの資格を user1 に付与できます。user1 が仮想マシンをダウンロードすると、仮想マシン名は vm-<x>-user1 に変更されます。仮想マシンの番号は、各ユーザー名について順番に割り当てられるのではなく、仮想マシンが登録された時期に基づいて割り当てられます。

たとえば、user1 に 3 台の仮想マシンが割り当てられている場合、他のユーザーへの他の仮想マシンの資格の割り当てと、各仮想マシンを user1 がダウンロードした時期に応じて、vm-10-user1、vm-26-user1、および vm-39-user1 といったマシン名が設定されます。順番に割り当てられた番号は、Horizon FLEX の管理者による追跡目的にのみ使用されます。クライアント ユーザーには、順番に割り当てられた番号は表示されません。

URI を作成して Horizon FLEX 仮想マシンをデプロイする

URI (Unified Resource Identifier) を作成して、Horizon FLEX 仮想マシンをデプロイできます。URI を使用すると、エンド ユーザーがサーバに接続して Horizon FLEX 仮想マシンをダウンロードするためにクリックするリンクを含む電子メールを作成できます。

開始する前に

- Horizon FLEX Client がエンド ユーザーのシステムにインストールされていることを確認します。
- サーバのパスワードと仮想マシンの暗号化パスワードをエンド ユーザーに提供します。

手順

1 エンド ユーザー用の URI を作成します。

URI は以下の構造になります。

`vmware-rvm://<username>@<myserver.com>:7443`

<username> はユーザーのログイン名で、<myserver.com> はサーバのホスト名です。`vmware-rvm://` と `:7443` をサーバ アドレスに追加する含める必要があります。http や https はサーバ アドレスに追加しないでください。

2 リンク テキストを電子メールに入力し、URI のハイパーリンク情報を入力します。

任意の電子メール システムを使用して、リンクを送信できます。ただし、URI の形式は標準の URL として認識されないため、ハイパーリンク情報を手動で入力する必要があります。

3 ユーザー宛の電子メールを作成し、リンク テキストを入力します。

例：**Horizon FLEX 仮想マシン**

4 リンク テキストを選択し、選択したテキストを右クリックして [ハイパーリンク] を選択します。

5 [リンク先：既存のファイルまたは Web ページ] を選択します。

6 [アドレス] テキスト ボックスに URI を入力します。

例：**vmware-rvm://johndoe@yourserver.com:7443**

これで、リンクがアクティブになりました。

7 [OK] をクリックします。

8 電子メールをユーザーに送信します。

ユーザーが電子メールのリンクをクリックすると、ユーザーの Horizon FLEX Client が起動し、サーバ接続ダイアログ ボックスが開きます。サーバとユーザー名のテキスト ボックスには、ユーザーが URI に指定した値が自動入力されます。ユーザーがパスワードを入力し、サーバーに接続して、仮想マシンをダウンロードします。

Horizon FLEX 仮想マシンの管理 5

編集、ロックアウト、再アクティベート、ワイプ、アーカイブ、または削除などの操作を実行して、展開した Horizon FLEX 仮想マシンを管理できます。

Horizon FLEX 仮想マシンのトラブルシューティング

Horizon FLEX 仮想マシンを展開したら、さまざまな操作を実行して管理できます。 展開されている Horizon FLEX 仮想マシンのインベントリを Horizon FLEX 管理コンソールで表示できます。

[検索] テキスト ボックスを使用して、仮想マシン リストやソート可能な列見出しをフィルタリングして、特定の仮想マシンを見つけることができます。列見出しのドロップダウン メニューを使用して、列を選択して表示または非表示にします。

仮想マシンをリストで選択するときに、ページの下部にある [プロパティ] ウィンドウを展開して、仮想マシンの全般設定や仮想マシンに適用されているポリシーを表示できます。

手順

1 Horizon FLEX 管理コンソール を起動します。

   a Web ブラウザに **`https://<WebManagerServer>:7443/rvm`**（<WebManagerServer> は Mirage Web Manager がインストールされているホストの DNS 名または IP アドレス）と入力します。

   b Mirage にアクセスできるドメイン アカウントのユーザー名とパスワードを入力します。

   c [ログイン] をクリックします。

2 左側のナビゲーション パネルで [仮想マシン] をクリックします。

   展開されている Horizon FLEX 仮想マシンのインベントリが、[仮想マシン] ページに表示されます。

3 特定の仮想マシンを管理するには、リストで仮想マシンを選択します。

オプション	操作
編集	仮想マシンを選択し、[編集] をクリックして、仮想マシンに割り当てられているポリシーを変更します。
ロックアウト	仮想マシンを選択して、[ロックアウト] をクリックして、特定の仮想マシンへのユーザー アクセスを無効にします。
再アクティベート	有効期限が切れたまたはロックアウトされている仮想マシンを選択して、[再アクティベート] をクリックして、仮想マシンをリセットします。
ワイプ	仮想マシンを選択して、[ワイプ] をクリックして、ファイル システムから削除します。

オプション	操作
アーカイブ	仮想マシンを選択し、[アーカイブ] をクリックし、使用している仮想マシンを無効にして、仮想マシンのオフライン レコードを保持します。 [仮想マシン] ページの下部にある [アーカイブされたインスタンスの表示] ボックスを選択して、アーカイブされている仮想マシンを表示します。[再アクティベート] をクリックして、アーカイブされている仮想マシンを有効にできます。
Delete	アーカイブされている仮想マシンを選択して、[削除] をクリックします。ステータスが [アーカイブ済み] 以外の仮想マシンは削除できません。

4 仮想マシンで実行できるアクションを判別するには、[ステータス] 列で仮想マシンのステータスを確認します。

ステータス	説明
アクティブ	仮想マシンは使用されており、サーバと通信し、有効期限が切れていません。
非アクティブ	ユーザーが仮想マシンを開くために使用した Horizon FLEX Client が、オフライン作業に関するポリシーで設定されているよりも長い期間、サーバと通信できていません。
期限切れ	有効期限に達しており、仮想マシンがオフになっています。
期限切れを保留中	サーバは、仮想マシンの有効期限が切れた Horizon FLEX Client からの確認を待機しています。
ロックアウト	管理者は、仮想マシンのユーザーをロックアウトしています。
ロックアウトを保留中	ロックアウトが開始されています。Horizon FLEX Client が仮想マシンがロック アウトされていることを確認するまで、ステータスは [保留中] のままになります。
再アクティベートを保留中	サーバは、仮想マシンが再アクティベートされた Horizon FLEX Client からの確認を待機しています。
ダウンロード中	ユーザーは、仮想マシンをダウンロードしています。
ダウンロードのキャンセル	ユーザーがダウンロードをキャンセルしました。
ダウンロードの一時停止	ユーザーがダウンロードを一時停止しました。
ドメインへの参加に失敗	仮想マシンがドメインへの参加に失敗しました。仮想マシンがドメインへの参加に失敗する最も一般的な理由は、オブジェクトが Active Directory にすでに存在していることです。この場合には、オペレーティング システムで保持されているオフラインのドメイン参加ログを確認して、障害の解決方法を決定します。
ユーザーによる削除	ユーザーがクライアントにある仮想マシンを削除しました。
ワイプ	仮想マシンが管理者によってワイプされ、ユーザーのシステムから削除されました。
ワイプを保留中	仮想マシンがユーザーのシステムから削除されていることの Horizon FLEX Client からの確認をサーバが待機しています。
アーカイブ済み	仮想マシンはアーカイブされています。 注意　アーカイブされている仮想マシンを表示するには、[アーカイブされているインスタンスの表示] チェック ボックスを選択する必要があります。

Horizon FLEX システムの維持 6

以前の Horizon FLEX バージョンからのアップグレードなどのメンテナンス操作を Horizon FLEX システムで実行できます。

この章では次のトピックについて説明します。

以前の Horizon FLEX バージョンからアップグレードする

以前の Horizon FLEX バージョンから Horizon FLEX システムをアップグレードできます。

開始する前に

- すべての Mirage Server がシャットダウンしていること。
- デプロイされているすべての Horizon FLEX 仮想マシンがシャットダウンしていること。

手順

1 バージョンをアップグレードするための Horizon FLEX Server と Horizon FLEX Client インストール ファイルをダウンロードします。

2 Horizon FLEX Server コンポーネントをアップグレードします。

   a Mirage Management Server をアップグレードするには、サーバ フォルダの mirage.management.server.64x.<buildnumber>.msi ファイルをダブルクリックします。

   デフォルトでは、初回のインストール時に選択した構成設定が適用されます。この構成設定はアップグレード手順の実行時に変更できます。

   b Mirage Server をアップグレードするには、mirage.server.64x.<buildnumber>.msi ファイルをダブルクリックします。

   デフォルトでは、初回のインストール時に選択した構成設定が適用されます。この構成設定はアップグレード手順の実行時に変更できます。

   c Mirage Web Manager (Web Management Console) をアップグレードするには、WebManagement フォルダの mirage.WebManagement.console.x64.<buildnumber>.msi ファイルをダブルクリックします。

   変更せずに続行します。

   d Mirage を使用して Windows 仮想マシンを管理する場合は、『VMware Mirage 管理者ガイド』で説明している旧バージョンの Mirage からのアップグレード手順に従って操作します。

3 アップグレードした Horizon FLEX Server と互換性があるバージョンにすべての Horizon FLEX Client をアップグレードします。

- Fusion Pro または Workstation Player のアップグレード バージョンのインストーラ ファイルをエンド ユーザーに提供するか、VMware Web サイトからソフトウェアをダウンロードするように指示します。
- 大規模デプロイパッケージを使用して Horizon FLEX Client をアップグレードします。

次に進む前に

Mirage のアップグレードに関する詳細な手順は、https://www.vmware.com/support/pubs/mirage_pubs.html にある VMware Mirage のドキュメントを参照してください。

注意 Mirage Management Server のアップグレード時には、[新しいストレージ領域の作成] を選択しないでください。このオプションを選択して元のストレージ領域へのパスを入力すると、基本レイヤ、アプリ レイヤ、CVD データなどを含むすべての Mirage インストールが削除され、バックアップを利用できない場合には復元できなくなります。

大規模デプロイパッケージを使用して Horizon FLEX Client をエンド ユーザーに提供する方法については、「エンド ユーザー向けの Horizon FLEX Client のインストール (P. 18)」を参照してください。

Horizon FLEX のシステム ログ

Horizon FLEX のログ ファイルは、システムのトラブルシューティングに使用できます。

Horizon FLEX のシステム ログは、次の場所で利用できます。

- Web アプリケーションのログ ファイル

  `C:\ProgramData\Wanova Mirage\rvm\logs\webapp.log`

- Horizon FLEX Server のログ

  `C:\Program Files\Wanova\Mirage Management Server\logs`

  最も重要なログ ファイルは、`mgmtservice.log` ファイルです。

- Horizon FLEX は、Microsoft のオフライン ドメイン参加機能を使用します。オフライン ドメイン参加のログ ファイルは次の場所にあります。

  `C:\Windows\debug\NetSetup.LOG`

インデックス