VMware Workspace Portal のインストールと構成

Workspace Portal 2.1

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-001538-02

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 Workspace Portal のインストールと構成

1

『VMware Workspace Portal インストールおよび構成ガイド』では、Workspace アプライアンスのインストールおよび構成のプロセスを説明しています。インストールが終了したら、VMware Workspace™ Portal を使用して、組織のアプリケーション（Windows アプリケーション、SaaS （サービスとしてのソフトウェア）アプリケーション、および View デスクトップなど）への管理対象マルチ デバイス アクセス権限をユーザーに付与できます。

対象者

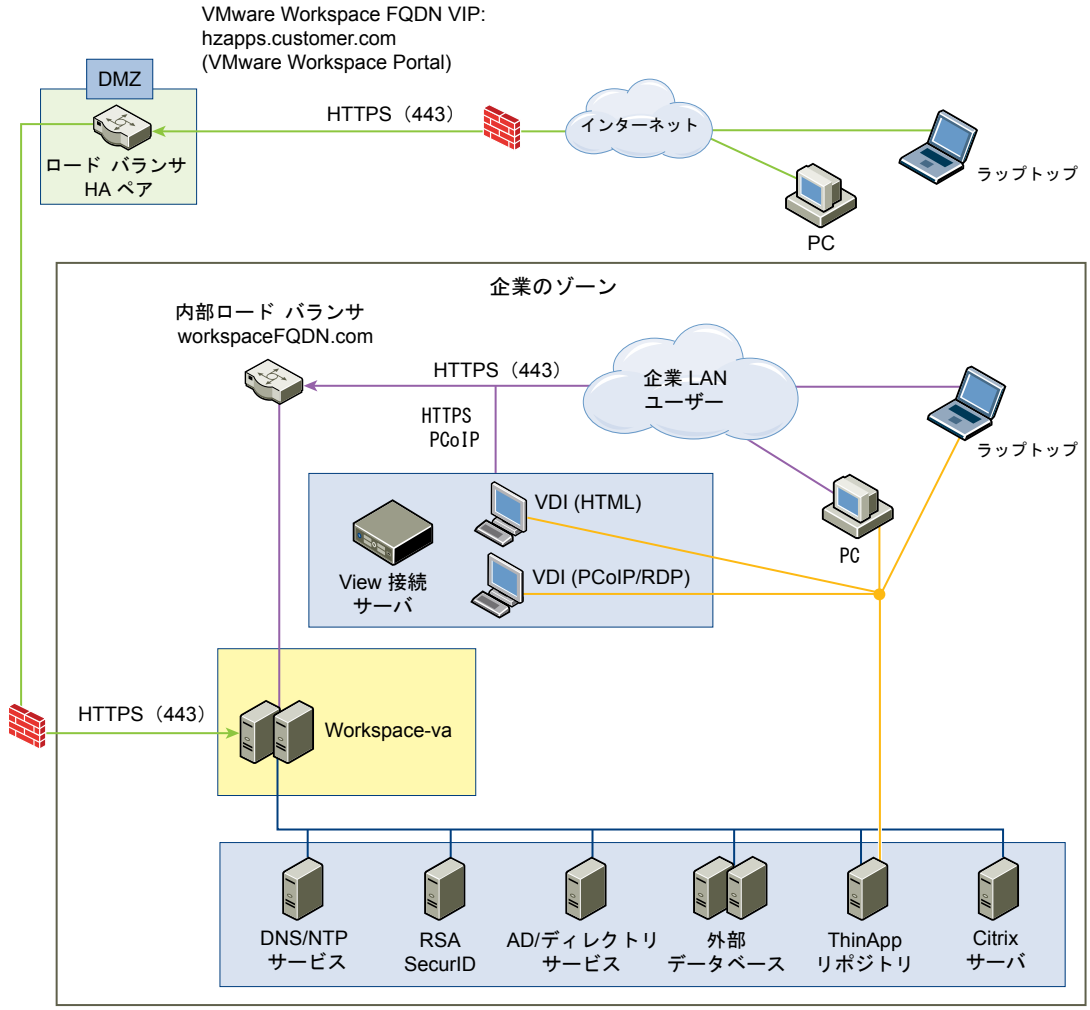
ここに記載する情報は、VMware Workspace™ Portal のシステム管理者および機能管理者向けの情報です。VMware テクノロジ、特に vCenter™、ESX™、vSphere®、View™、ネットワーキングの概念、Active Directory サーバ、SMTP (Simple Mail Transfer Protocol)、および NTP サーバに精通している、Windows および Linux のシステム管理者向けに記述されています。SUSE Linux 11 は、仮想アプライアンスの基本オペレーティング システムです。VMware ThinApp®、RSA SecurID および Active Directory など、その他のテクノロジの知識も、これらの機能の実装を計画している場合に役立ちます。

VMware Workspace Portal のインストールの準備

2

VMware Workspace Portal を展開およびセットアップするタスクでは、前提条件を満たし、Workspace OVF ファイルを展開して Workspace セットアップ ウィザードでのセットアップを完了する必要があります。

図 2-1. 一般的な展開の VMware Workspace Portal アーキテクチャ図



この章では次のトピックについて説明します。

- Workspace システムとネットワークの構成の要件 (P. 8)
- Workspace の展開の準備 (P. 10)

Workspace システムとネットワークの構成の要件

ハードウェア、リソース、およびネットワークの要件を決定する場合は、Workspace の統合方法を含めて、Workspace の展開環境全体を考慮します。

Workspace 仮想アプライアンスの要件

Workspace 仮想アプライアンスに割り当てられているリソースが最小要件を満たしていることを確認します。

表 2-1. VMware Workspace Portal 仮想アプライアンス (workspace-va) の要件

コンポーネント	最小要件
CPU	2
ランダム アクセス メモリ	6GB
ディスク容量	36GB
その他の注意	■ PostgreSQL データベースが workspace-va 構成に含まれているので、外部データベース サーバを使用できます。Workspace でサポートされる特定のデータベース バージョンとサービス パックの構成の詳細については、「VMware 製品の相互運用性マトリックス」（http://www.vmware.com/resources/compatibility/sim/interop_matrix.php）を参照してください。 ■ 外部データベースのサイズに関する情報： 最初の 100,000 ユーザーに対して 64GB、その後は、10,000 ユーザーごとに 20GB を追加します。 ■ ストレージ： 32GB

ネットワーク構成の要件

Kerberos、View、または ThinApp 機能が有効な場合、Workspace サーバを Windows ドメインに参加させる必要があります。この場合、Workspace のホスト名は、参加する Active Directory ドメインと同じドメインに含める必要があります。

表 2-2. ネットワーク構成の要件

コンポーネント	最小要件
DNS レコードおよび IP アドレス	IP アドレスおよび DNS レコード
ファイアウォール ポート	インバウンド ファイアウォール ポート 443 がエンタープライズ ネットワークの外側のユーザーから Workspace に対して開いていることを確認します。

ポートの要件

以下に、Workspace で使用するポートを示します。展開環境には、これらのサブネットのみが含まれる場合があります。次の 2 つのシナリオが想定されます。

- ユーザーとグループを同期するには、Workspace 仮想アプライアンスを Active Directory に接続する必要があります。
- ThinApp と同期するには、Workspace 仮想マシンを Active Directory ドメインに参加させて、ThinApp リポジトリ共有に接続する必要があります。

表 2-3. Workspace で使用するポート

ポート	vCenter サーバの IP アドレス	ターゲット	説明
443	ロード バランサ	Workspace-va	SSL 経由のハイパーテキスト トランスポート プロトコル (HTTPS
443	Workspace-va	Workspace-va 2、3 など	SSL 経由のハイパーテキスト トランスポート プロトコル (HTTPS

表 2-3. Workspace で使用するポート (続き)

ポート	vCenter サーバの IP アドレス	ターゲット	説明
443	ブラウザ	Workspace-va	SSL 経由のハイパーテキスト トランスポート プロトコル (HTTPS
8443	ブラウザ	Workspace-va	管理者ポート SSL 経由のハイパーテキスト トランスポート プロトコル (HTTPS
25	Workspace-va	SMTP	送信メールをリレーする TCP ポート
389、636、3268、3269	Workspace-va	Active Directory	デフォルト値が表示されています。これらのポートは構成可能です。
5432	Workspace-va	データベース	PostgreSQL のデフォルト ポートは 5432 です。Oracle のデフォルト ポートは 1521 です。
389, 443	Workspace-va	View server	View server へのアクセス
443	Workspace-va	VMware ThinApp リポジトリ	ThinApp リポジトリへのアクセス
5500	Workspace-va	RSA SecurID システム	デフォルト値が表示されています。このポートは構成可能です。
53	Workspace-va	DNS サーバ	TCP/UDP すべての workspace-va は、ポート 53 で DNS サーバにアクセスでき、ポート 22 で着信 SSH トラフィックを許可する必要があります。
88, 465, 135	Workspace-va	ドメイン コントローラ	TCP/UDP
TCP: 9300-9400 UDP: 54328	Workspace-va	Workspace-va	要監査

ESX サーバのハードウェア要件

Workspace 仮想アプライアンスが動作するホストと vSphere インスタンスの環境が最小ハードウェア要件を満たしていることを確認します。ストレージ要件は、ユーザー数を基準とし、展開環境によって異なります。

注意　NTP サーバを使用して、ESX ホスト レベルで時刻同期をオンにする必要があります。オンにしないと、仮想アプライアンス間で時間のずれが発生します。

表 2-4. Workspace のハードウェア最小要件

コンポーネント	最小要件
プロセッサ	2 x Intel クアッド コア、3.0GHz、4MB キャッシュ
RAM	16GB DDR2 1066 MHz、ECC およびレジスタード
オンボード LAN	1 x 10/100/1000Base-TX ポート
ストレージ	500GB

Workspace でサポートされる Web ブラウザ

Workspace 管理者コンソールは、Workspace をインストールするときにインストールされる Web ベース アプリケーションです。Workspace 管理コンソール は次のブラウザからアクセスして使用することができます。

- Internet Explorer 10 および 11（Windows システムの場合）

- Google Chrome 34.0 以降（Windows および Mac システムの場合）
- Mozilla Firefox 28 以降（Windows および Mac システムの場合）
- Safari 6.1.3 以降（Mac システムの場合）

Workspace の展開の準備

Workspace を展開する前に、環境を準備する必要があります。この準備には、Workspace OVF ファイルのダウンロード、DNS レコードおよび IP アドレスの作成が含まれます。

開始する前に

Workspace のインストールを開始するには、まず前提条件のタスクを完了します。

- Workspace 仮想アプライアンスを展開する 1 台以上の ESX サーバ。

  注意　サポートされている vSphere および ESX サーバのバージョンの詳細については、「VMware 製品の相互運用性マトリックス」（http://www.vmware.com/resources/compatibility/sim/interop_matrix.php）を参照してください。

- VMware vSphere Client または vSphere Web Client で OVF ファイルを展開し、展開した仮想アプライアンスにリモートでアクセスしてネットワークを構成する必要があります。
- VMware Web サイトの Workspace OFV ファイル。
- DNS レコードと IP アドレスの作成 (P. 10)

  Workspace アプライアンス用の DNS エントリおよび固定 IP アドレスが利用できる必要があります。会社ごとに管理する IP アドレスや DNS レコードが異なるため、インストールを開始する前に、使用する DNS レコードおよび IP アドレスを確認します。

- Workspace のデータベース オプション (P. 11)

  Workspace は、内部データベースまたは外部データベースを使用して設定できます。vPostgres データベースは Workspace アプライアンスに組み込まれています。内部データベースがデフォルトです。外部データベースへの接続は、Workspace セットアップ ウィザードを構成する際に選択できます。

- Active Directory への接続 (P. 11)

  Workspace は、ユーザーの認証や管理に既存の Active Directory インフラストラクチャを使用します。ユーザーとグループを同期するには、Workspace 仮想アプライアンスを Active Directory に接続する必要があります。

- 展開チェックリスト (P. 11)

  Workspace 展開チェックリストを使用して、Workspace のインストールに必要な情報を収集できます。

DNS レコードと IP アドレスの作成

Workspace アプライアンス用の DNS エントリおよび固定 IP アドレスが利用できる必要があります。会社ごとに管理する IP アドレスや DNS レコードが異なるため、インストールを開始する前に、使用する DNS レコードおよび IP アドレスを確認します。

（オプション）逆引きと IP アドレス

Workspace では、オプションで逆引きの構成が可能です。逆引きを実装する場合には、DNS サーバに PTR レコードを定義して、仮想アプライアンスが正しいネットワーク構成を使用するようにする必要があります。

ネットワーク管理者に相談する際に、下記の DNS レコードのサンプル リストを使用できます。サンプル リストの情報を、それぞれの環境に合わせて書き換えてください。次のサンプルには、DNS の正引きレコードと IP アドレスが記載されています。

表 2-5. DNS の正引きレコードと IP アドレスの例

ドメイン名	リソース タイプ	IP アドレス
my-workspace-va.company.com	A	10.28.128.3

次のサンプルには、DNS の逆引きレコードと IP アドレスが記載されています。

表 2-6. DNS の逆引きレコードと IP アドレスの例

IP アドレス	リソース タイプ	ドメイン名
128.28.10.in-addr.arpa	IN	PTR my-workspace-va.company.com

DNS 構成の終了後に、DNS の逆引きが正しく構成されていることを確認します。たとえば、仮想アプライアンスのコマンド <host IP_address> は DNS 名を解決する必要があります。

Unix/Linux ベースの DNS サーバの使用

Unix/Linux ベースの DNS サーバを使用していて、Workspace を Active Directory ドメインに参加させる予定がある場合は、Active Directory ドメイン コントローラごとに正しいサービス（SRV）リソース レコードが作成されていることを確認します。

Workspace のデータベース オプション

Workspace は、内部データベースまたは外部データベースを使用して設定できます。vPostgres データベースは Workspace アプライアンスに組み込まれています。内部データベースがデフォルトです。外部データベースへの接続は、Workspace セットアップ ウィザードを構成する際に選択できます。

組み込みの vPostgres データベース構成は小規模な展開に役立ち、デフォルトで使用できます。内部データベースは Workspace の外部での追加構成は不要ですが、 高可用性を実現するには、内部データベースを構成することをお勧めします。「KB 2094258, Using embedded vPostgres database for VMware Workspace Portal 2.1（VMware Workspace Portal 2.1 用の組み込み vPostgres データベースの使用）」を参照してください。

外部データベースを使用するには、外部データベースに接続する前に、データベース管理者が空の外部データベースとスキーマを準備する必要があります。ライセンスを保有するユーザーは、外部の vPostgres 仮想アプライアンスまたは Oracle データベースを使用して高可用性外部データベース環境を設定できます。「外部データベースへの接続 (P. 22)」を参照してください。

Active Directory への接続

Workspace は、ユーザーの認証や管理に既存の Active Directory インフラストラクチャを使用します。ユーザーとグループを同期するには、Workspace 仮想アプライアンスを Active Directory に接続する必要があります。

Active Directory は、Workspace 仮想アプライアンスと同一の LAN ネットワークでアクセス可能である必要があります。「Active Directory への接続の確立 (P. 32)」を参照してください。

展開チェックリスト

Workspace 展開チェックリストを使用して、Workspace のインストールに必要な情報を収集できます。

展開環境によっては、インストール前や Workspace のインストール時に DNS に固定 IP アドレスを作成する際に、仮想アプライアンスのネットワーク情報の一部のみが必要になる場合があります。

完全修飾ドメイン名の情報

詳細については、「ロード バランサを使用した Workspace への外部アクセスの有効化 (P. 39)」を参照してください。

表 2-7. Workspace 完全修飾ドメイン名 (FQDN) 情報チェックリスト

収集する情報	情報を記入
Workspace FQDN	

Workspace 仮想アプライアンスのネットワーク情報

表 2-8. Workspace ネットワーク情報チェックリスト

収集する情報	情報を記入
IP アドレス	
この仮想アプライアンスの DNS 名	
デフォルト ゲートウェイ アドレス	
ネットマスクまたはプリフィックス	

Active Directory ドメイン コントローラ

表 2-9. Active Directory ドメイン コントローラ情報チェックリスト

収集する情報	情報を記入
Active Directory サーバ名	
Active Directory ドメイン名	
バインド DN ユーザー名とパスワード	
ベース DN	
Active Directory ユーザー名とパスワード（コンピュータをドメインに参加させる権限が必要）	

SSL 証明書（オプション）

表 2-10. SSL 証明書情報チェックリスト

収集する情報	情報を記入
SSL 証明書	
秘密キー	

注意　SSL 証明書はオプションです。Workspace の展開後に、SSL 証明書を追加できます。

Workspace ライセンス キー

表 2-11. Workspace ライセンス キー情報チェックリスト

収集する情報	情報を記入
ライセンス キー	

注意　インストールが完了したら、[設定] > [グローバル設定] タブで Workspace 管理コンソールにライセンス キー情報を入力します。

外部データベース

表 2-12. 外部データベース情報チェックリスト

収集する情報	情報を記入
データベース ホスト名	
ポート	
ユーザー名	
パスワード	

Workspace のパスワード

表 2-13. Workspace で使用する管理パスワード

収集する情報	情報を記入
Workspace 管理者アカウントのパスワード	
仮想アプライアンスのルート アカウントのパスワード	
リモート ログイン用 Sshuser アカウントのパスワード	

3 Workspace の展開

vSphere Client または vSphere Web Client を使用して Workspace を展開および設定するタスクには、OVF テンプレートの展開、Workspace 仮想アプライアンスの起動、Workspace の設定が含まれます。

Workspace 仮想アプライアンスを展開したら、Workspace セットアップ ウィザードを使用して Workspace 環境を設定します。

展開チェックリストの情報を使用して、インストールを完了します。「展開チェックリスト (P. 11)」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。

Workspace OVF ファイルのインストール

Workspace のインストールを開始するには、VMware vSphere Client または vSphere Web Client を使用して OVF ファイルを展開する必要があります。vSphere Client にアクセス可能なローカル ファイルまたは Web URL から OVF ファイルをダウンロードおよび展開できます。

開始する前に

- vSphere Web Client を使用する場合は、Firefox ブラウザまたは Chrome ブラウザを使用します。Internet Explorer を使用して OVF ファイルを展開しないでください。
- Workspace OVF ファイルをダウンロードします。

手順

1 vSphere Client または vSphere Web Client で [OVF テンプレート] を選択して Workspace OVF ファイルを展開します。

2 [OVF テンプレートの展開] ページで、使用環境の Workspace の展開に固有の情報を入力します。

ページ	説明
vCenter サーバの IP アドレス	OVF パッケージの場所を参照するか、または特定の URL を入力します。
OVF テンプレートの詳細	正しいバージョンの Workspace を選択していることを確認します。
ライセンス	エンド ユーザー使用許諾契約を読み、[同意する] をクリックします。

ページ	説明
名前と場所	この Workspace 仮想アプライアンスを識別する名前を入力します。この名前は、仮想マシン フォルダ内で一意である必要があります。名前の大文字と小文字は区別されます。
ホスト/クラスタ	ホストまたはクラスタを選択して展開したテンプレートを実行します。
リソース プール	リソース プールを選択します。
ストレージ	仮想マシン ファイルを格納する場所を選択します。
ディスク形式	Workspace ファイルを保存するディスク形式を選択します。本番環境の場合は、シック プロビジョニング形式を選択します。評価やテストにはシン プロビジョニング形式を使用します。
ネットワークのマッピング	Workspace で使用されているネットワークをインベントリのネットワークにマップします。
プロパティ	注意　Workspace を展開するには、[アプリケーション] セクションのチェック ボックスをオフにします。 [タイムゾーンの設定] フィールドで、正しいタイム ゾーンを選択します。 デフォルトでは、カスタマー エクスペリエンス改善プログラムは有効になっています。VMware はお客様のご要望への対応を向上させるために、お客様の展開環境に関する匿名データを収集します。 [ホスト名] フィールドに、使用するホスト名を入力します。このフィールドを空白にすると、逆引き DNS を使用してホスト名が参照されます。 Workspace に固定 IP アドレスを構成するには、デフォルト ゲートウェイ、DNS、IP アドレス、およびネットマスクの各フィールドにそれぞれのアドレスを入力します。 重要　ホスト名を含む 4 つのアドレス フィールドのいずれかが空白の場合は、DHCP が使用されます。 DHCP を構成する場合は、アドレス フィールドを空白のままにしておきます。 （オプション） Workspace のインストール後に、IP プールを構成できます。「（オプション） Workspace での IP プールの追加 (P. 16)」を参照してください。
終了準備の完了	選択したオプションを確認します。内容が正しければ、[終了] をクリックします。

進捗バーが表示されます。ネットワークの速度によっては、この展開に数分かかることがあります。

3 展開が完了したら、進捗バーで [閉じる] をクリックします。

4 展開したばかりの Workspace 仮想アプライアンスを選択して [仮想マシンをパワーオン] をクリックします。

Workspace 仮想アプライアンスは初期化されます。[コンソール] タブで詳細を確認できます。仮想アプライアンスの初期化が完了すると、コンソール画面に Workspace のバージョンと、Workspace Web インターフェイスにログインして Workspace のセットアップを完了するための URL が表示されます。

次に進む前に

Active Directory への接続や Workspace と同期するユーザーおよびグループの選択などの Workspace の設定を構成します。

（オプション） Workspace での IP プールの追加

IP プールを使用するネットワーク構成は、Workspace ではオプションです。Workspace のインストール後に、Workspace に手動で IP プールを追加できます。workspace-va 仮想アプライアンス ネットワークのプロパティを編集してプロパティを動的プロパティに変更し、ネットマスク、ゲートウェイ、および DNS 設定を構成します。

IP プールは DHCP (Dynamic Host Configuration Protocol) サーバのような役割を果たし、プールから workspace-va 仮想アプライアンスに IP アドレスを割り当てます。Workspace アプライアンスで IP プールを使用できるようにするには、アプライアンスの OVF プロパティを編集する必要があります。

開始する前に

workspace-va 仮想アプライアンスをパワーオフして IP プール設定を追加する必要があります。

手順

1 vSphere Client または vSphere Web Client で、IP プールに構成されている仮想アプライアンスを右クリックして [設定の編集] を選択します。

2 このページの [プロパティ] セクションで [プロパティ] をクリックします。

3 [詳細なプロパティ構成] ページで、vami.DNS.WorkspacePortal、vami.netmask0.WorkspacePortal、および vami.gateway.WorkspacePortal のキー ラベルを構成します。

   a [詳細なプロパティ構成] ページで、キー ラベルを 1 つ選択して [編集] をクリックします。

   b [プロパティ設定の編集] ページで、[タイプ] フィールドの横にある [編集] をクリックします。

   c [プロパティ タイプの編集] ページで [動的プロパティ] を選択し、ネットマスク、ゲートウェイ、DNS サーバそれぞれのドロップダウン メニューから適切な値を選択します。

   d すべてのページが閉じるまで、[OK] をクリックします。

4 仮想アプライアンスをパワーオンします。

IP プールから選択するようにプロパティを構成します。

Workspace 設定の構成

Workspace OVF を展開してインストールしたら、Workspace セットアップ ウィザードを実行して情報を構成し、Active Directory に接続します。内部データベースを作成するか、または外部データベースを使用している場合は外部データベースを選択し、Workspace と同期するユーザーとグループを選択します。

開始する前に

- Workspace 仮想アプライアンスがパワーオンされている。
- Workspace 管理者、Workspace ルート アカウントおよび Workspace Sshuser アカウントに使用するパスワードのリスト。
- 外部データベースを使用している場合は、外部データベースが設定され、接続情報が使用可能である必要があります。
- Active Directory の接続情報。
- マルチフォレスト Active Directory が構成され、ドメイン ローカル グループに異なるフォレストのドメインのメンバが含まれる場合、Workspace ディレクトリ ページで使用されるバインド DN ユーザーをドメイン ローカル グループが存在するドメインの管理者グループに追加する必要があります。これを行わなければ、これらのメンバはドメイン ローカル グループに含まれなくなります。
- フィルタとして使用する Active Directory ユーザー属性のリスト、および Workspace に追加するグループのリスト。

手順

1 OVF を展開した後で Workspace を構成するには、Workspace URL (`https://<workspacehostname>.com`) にアクセスします。

   ようこそ画面で、[続行] をクリックします。

2 [パスワードの設定] 画面で、次の管理者アカウントのパスワードを作成します。

   - アプライアンス管理者。Workspace 管理者のパスワードを作成します。ユーザー名は admin です。変更することはできません。このアカウントは、Workspace の初回インストール時に作成したアカウントです。
   - root アカウント。デフォルトの VMware root パスワードが Workspace のセットアップ時に使用されました。新しい root パスワードを作成します。
   - Sshuser アカウント。workspace-va 仮想アプライアンスにリモート アクセスするために使用するパスワードを作成します。

   [続行] をクリックします。

3 使用するデータベースを選択します。

- 内部データベースを使用している場合は、[続行] をクリックします。
- 外部データベースを使用している場合は、[外部データベース] を選択し、以前に設定したデータベース サーバの外部データベース接続情報、ユーザー名、パスワードを入力します。Workspace がデータベースに接続できることを確認するには、[接続のテスト] をクリックします。

[続行] をクリックします。

データベースへの接続を構成し、データベースを初期化します。

4 [ディレクトリ] ページで、Active Directory 情報を入力して [検証] をクリックします。

情報のタイプ	説明
ディレクトリ タイプ	Active Directory のままにします。
SSL を使用する	ディレクトリ接続に SSL を使用する場合は、このチェック ボックスをオンにします。
DNS サービスの場所の使用	ディレクトリ接続に DNS サービスの場所を使用する場合はこのチェック ボックスをオンにします。
サーバ ホスト	Active Directory ホスト アドレスを入力します。ホスト名の入力には、ASCII 以外の文字を使用しないでください。
サーバ ポート	Active Directory ホストのポート番号を入力します。単一ドメインの Active Directory の場合、デフォルト ポートは 389 です。SSL を選択した場合、デフォルト ポートは 636 です。
属性を検索	ユーザー名を含む Active Directory アカウント属性を入力します。ほとんどの展開では、**sAMAccouontName** を選択します。
ベース DN	ディレクトリ サーバの検索の開始点である DN を入力します。たとえば、OU-myunit,DC=mycompany,DC=com のように入力します。
バインド DN	共通名 (CN) など、ユーザーを検索する権限がある Active Directory ユーザー アカウントのバインド DN を入力します。このユーザーは、Workspace 展開の管理者になります。
バインド パスワード	バインド DN アカウントの Active Directory パスワードを入力します。

バインド DN 情報を確認し、Workspace のユーザーとして管理者のアカウントを追加します。

[続行] をクリックします。

5 [ユーザー属性をマップ] ページで、Workspace ディレクトリ属性にマップする、Active Directory で使用する属性を選択します。

View と統合する予定がある場合は、userPrincipal Name 属性の横にある [必須] を選択します。Horizon DaaS と統合する予定がある場合は、distinguishedName 属性の横にある [必須] を選択します。Connector Services Admin ページで、後でこの操作を行うこともできます。

6 [ユーザーを選択] ページで、ドロップダウン メニューからユーザー属性を選択してフィルタを作成し、Workspace と同期するユーザーのタイプを制限します。[続行] をクリックします。

7 Active Directory のグループは、Workspace と自動的には同期されません。[選択したグループ] ページで、グループの DN の説明の横にある [追加] をクリックして、グループを追加します。[続行] をクリックします。

[Workspace にプッシュ] ページに、Workspace と同期するユーザー数とグループ数に関する情報が表示されます。

[Workspace にプッシュ] をクリックして同期を開始します。

8 [セットアップが完了しました] ページが表示されたら、[Workspace にログイン] をクリックして管理コンソールにログインします。

Workspace ログイン画面が表示されます。Active Directory への接続を設定するときに入力したバインド DN ユーザー名とパスワードを入力します。Workspace 管理コンソール で、Workspace を使用するリソースを設定して、ユーザーをそのリソースに割り当てることができます。

注意　ネットワーク エラーが発生し、逆引き DNS を使用してホスト名を一意に解決できない場合は、Configurator プロセスが停止します。ネットワークの問題を解決して workspace-va 仮想アプライアンスを再起動する必要があります。その後に、展開プロセスを続行できます。新しいネットワーク設定は、workspace-va 仮想アプライアンスを再起動しないと使用できません。

次に進む前に

Workspace 管理コンソールにログインし、組織のアプリケーションのリソース カタログをカスタマイズしてユーザーがこれらのリソースにアクセスできるようにします。

View、ThinApp、Horizon DaaS、および Citrix ベースのアプリケーションなど、他のリソースをセットアップします。『VMware Workspace Portal ガイド』の「リソースのセットアップ」を参照してください。

Workspace のプロキシ サーバ設定

Workspace 仮想アプライアンスは、インターネット上のクラウド アプリケーション カタログおよびその他の Web サービスにアクセスします。HTTP プロキシを使用するインターネット アクセスをネットワーク構成で指定している場合は、Workspace アプライアンスでプロキシ設定を調整する必要があります。

インターネット トラフィックのみを処理するプロキシを有効にします。プロキシが正しく設定されていることを確認するために、ドメイン内の内部トラフィック用のパラメータを `no-proxy` に設定します。

手順

1. vSphere Client で、root ユーザーとして workspace-va 仮想アプライアンスにログインします。
2. [YaST2] と入力します。
3. [ネットワーク サービス] を選択してから、[プロキシ] ページを選択します。
4. 正しいプロキシ URL を [HTTP] フィールドに入力します。

   http://proxy.<example>.com:3128
5. 正しいプロキシ URL を [HTTPS] フィールドに入力します。

   https://proxy.<example>.com:3128
6. workspace-va 仮想マシンで Tomcat サーバを再起動して新しいプロキシ設定を使用します。

   ```
   #service horizon-workspace restart
   ```

クラウド アプリケーション カタログおよびその他の Web サービスを Workspace で使用できるようになりました。

Workspace 管理サービス

Workspace のユーザー、グループ、リソース、認証、同期セットアップ、およびデータベース接続は、別の Workspace 管理サービスから管理します。

サービス	説明
Workspace 管理コンソール	Workspace 管理コンソール インターフェイスで、リソースカタログをセットアップし、ユーザーおよびグループ、使用資格、レポートを管理します。Active Directory から割り当てられた管理者ユーザー ロールとしてログインします。管理コンソールに直接ログインする場合の URL は https://<WorkspaceFQDN>/SAAS/admin です。
Connector Services Admin	[Connector Services Admin] ページでは、ディレクトリの構成、認証アダプタのセットアップ、仮想デスクトップやリモート アプリケーションなどその他のエンタープライズ統合の管理を行います。これには、View 接続サーバ、ThinApp リポジトリ、Citrix 公開アプリケーション リソースとの統合のセットアップが含まれます。これらのページから、ディレクトリの同期状態とアラートを確認することもできます。セットアップ時に作成したユーザー名 **admin** および管理者パスワードを使用して、Workspace 管理者としてログインします。Workspace[Connector Services Admin] ページへのリンクは https://<Workspace_FQDN>.com:8443 にあります。
Appliance Configurator	[Appliance Configurator] ページでは、Workspace データベースの管理、証明書の更新、Syslog の有効化、Workspace およびシステム パスワードの変更、その他のインフラストラクチャ機能の管理を実行できます。セットアップ時に作成したユーザー名 **admin** および管理者パスワードを使用して、Workspace 管理者としてログインします。WorkspaceAppliance Configurator ページへのリンクは https://<Workspace_FQDN>.com:8443 にあります。Workspace 管理コンソール から Appliance Configurator に移動し、[設定] > [仮想アプライアンス システムの構成] ページにアクセスすることもできます。

カスタマー エクスペリエンス改善プログラム

Workspace をインストールすると、VMware カスタマー エクスペリエンス改善プログラムに参加できます。

プログラムに参加すると、VMware はお客様のご要望への対応を向上させるために、お客様の展開環境に関する匿名データを収集します。お客様の組織を特定するデータは収集されません。

VMware はデータを収集する前に、お客様の組織に特有の情報を含むすべてのフィールドを匿名にします。

注意　この情報を送信するために、ネットワークで HTTP プロキシを使用するインターネット アクセスを構成している場合は、Workspace アプライアンスのプロキシ設定を調整する必要があります。「Workspace のプロキシ サーバ設定 (P. 19)」を参照してください。

4 Workspace アプライアンス構成設定の管理

Workspace の構成後、[Appliance Configurator] のページで現在の構成を更新し、仮想アプライアンスのシステム情報を監視できます。

また、Appliance Configurator ページで、データベース、FQDN および SSL 証明書などの設定も更新または変更できます。

表 4-1. Appliance Configurator の設定

ページ名	設定説明
データベース接続	データベース接続の設定です。内部または外部のいずれかが有効です。データベース タイプは変更できます。外部データベースを選択する場合には、外部データベース URL、ユーザー名、パスワードを入力します。外部データベースをセットアップするには、「外部データベースへの接続 (P. 22)」を参照してください。
証明書のインストール	このページで Workspace のカスタムまたは自己署名証明書をインストールします。Workspace がロード バランサとともに構成されている場合、ロード バランサのルート証明書をインストールできます。Workspace のルート CA 証明書の場所もこのページに表示されます。「Workspace での SSL 証明書の使用 (P. 27)」を参照してください。
Workspace FQDN	Workspace の FQDN がこのページに表示されます。これは変更できます。Workspace FQDN はユーザーが Workspace へのアクセスに使用する URL です。
Syslog の構成	このページで外部 syslog サーバを有効にできます。Workspace ログはこの外部サーバに送信されます。「Syslog サーバの有効化 (P. 26)」を参照してください。
パスワードの変更	このページで Workspace 管理者パスワードを変更できます。
システム セキュリティ	このページで Workspace アプライアンスの root パスワードと、リモートで管理者としてログインするときに使用するパスワードを変更できます。
ログ ファイルの場所	Workspace のログ ファイルのリストとそのディレクトリの場所がこのページに表示されます。ログ ファイルを tar や zip ファイルにバンドルしてこのページからダウンロードできます。 「ログ ファイル情報 (P. 28)」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。

■ ログ ファイル情報 (P. 28)

Workspace アプライアンスの構成設定の変更

Workspace を構成した後で、[Appliance Configurator] ページにアクセスして現在の構成を更新し、仮想アプライアンスのシステム情報を監視できます。

手順

1 [Appliance configurator] ページにアクセスするには、Workspace 管理コンソール にログオンします。

2 [設定] タブを開いて [仮想アプライアンス システムの構成] をクリックします。

3 Workspace 管理者パスワードを使用して Appliance Configurator にログオンします。

4 左側のナビゲーション ペインを使用して、表示するページを選択します。

次に進む前に

設定や更新が有効になっていることを確認します。

外部データベースへの接続

内部 PostgreSQL データベースは、Workspace アプライアンスに組み込まれています。Workspace で外部データベースを使用するには、Workspace データベースに接続する前に、データベース管理者は Oracle または PostgreSQL の空の外部データベースとスキーマを準備する必要があります。

外部データベースには、Workspace セットアップ ウィザードを実行する際に接続できます。Appliance Configurator の [データベース接続] ページに移動して外部データベースへの接続を構成することもできます。

ライセンスを保有するユーザーは、外部の vPostgres 仮想アプライアンスまたは Oracle データベースを使用して高可用性環境を設定できます。

注意　内部データベースの高可用性を構成する場合は、「KB 2094258, Using embedded vPostgres database for VMware Workspace Portal 2.1（VMware Workspace Portal 2.1 用の組み込み vPostgres データベースの使用）」を参照してください。

Oracle データベースの構成

Oracle のインストール時に、Workspace とのパフォーマンスを最適化するため、特定の Oracle 構成を指定する必要があります。

開始する前に

Workspace では、ユーザー名とスキーマに Oracle 引用識別子が必要です。したがって、Oracle **saas** ユーザー名とスキーマを作成する際には、二重引用符を使用する必要があります。

手順

1 Oracle データベースの作成時に次の設定を指定します。

   a [General Purpose/Transaction Processing Database] 構成オプションを選択します。

   b [Unicode を使用] - [UTF8] をクリックします。

   c National Character Set を使用します。

2 インストール完了後に Oracle データベースに接続します。

3 Oracle データベースに sys ユーザーとしてログインします。

4 プロセス接続を増やします。Workspace で機能するように、それぞれの追加 workspace-va 仮想マシンに最大 300 プロセスの接続が必要です。 たとえば、環境に 2 台の workspace-va 仮想マシンがある場合は、sys またはシステム ユーザーとして `alter` コマンドを実行します。

a `alter` コマンドを使用して、プロセス接続を増やします。

```
alter system set processes=600 scope=spfile
```

b データベースを再起動します。

5 すべてのユーザーが使用できるデータベース トリガーを作成します。

データベース トリガを作成するためのサンプル SQL

```
CREATE OR REPLACE
TRIGGER CASE_INSENSITIVE_ONLOGON
AFTER LOGON ON DATABASE
DECLARE
username VARCHAR2(30);
BEGIN
username:=SYS_CONTEXT('USERENV','SESSION_USER');
IF username = 'saas' THEN
execute immediate 'alter session set NLS_SORT=BINARY_CI';
execute immediate 'alter session set NLS_COMP=LINGUISTIC';
END IF;
EXCEPTION
WHEN OTHERS THEN
NULL;
END;
```

6 Oracle コマンドを実行して新しいユーザー スキーマを作成します。

新しいユーザーを作成するためのサンプル SQL

```
CREATE USER "saas"
IDENTIFIED BY <password>
DEFAULT TABLESPACE USERS
TEMPORARY TABLESPACE TEMP
PROFILE DEFAULT
ACCOUNT UNLOCK;
GRANT RESOURCE TO "saas" ;
GRANT CONNECT TO "saas" ;
ALTER USER "saas" DEFAULT ROLE ALL;
GRANT UNLIMITED TABLESPACE TO "saas";
```

クラスタ化されている Oracle データベースを使用している場合、RAC セットアップに関する VMware のドキュメントを参照してください。

PostgreSQL データベースの構成

PostgreSQL のインストール時に、Workspace とのパフォーマンスを最適化するため、特定の PostgreSQL 構成を指定する必要があります。

注意 Workspace は現在、汎用 PostgreSQL をサポートしていません。

開始する前に

- インストールした citext モジュールのいずれかのインストール パッケージ（OVA、OVF、または RPM）から、VMware vFabric PostgreSQL のサポート対象バージョンを外部データベース サーバとしてインストールし、構成します。citext モジュールは、大文字と小文字を区別しないテキスト タイプである CITEXT データ タイプをサポートします。使用している VMware vFabric PostgreSQL のバージョンが Workspace のバージョンと互換性があることを確認します。サポートされる VMware vFabric PostgreSQL バージョンの詳細については、「VMware 製品の相互運用性マトリックス」（http://www.vmware.com/resources/compatibility/sim/interop_matrix.php）を参照してください。
- ロード バランス機能の実装をインストールし、構成します。
- 環境が次の要件を満たしていることを確認します。
  - 使用しているデータベース サーバが PostgreSQL である。
  - データベース管理者のユーザー名とパスワードが使用可能である。
  - ユーザー名とパスワードを入力して、**saas** スキーマに対する権限を持つユーザーを作成する必要があります。このユーザーは、workspace-va 仮想マシン インスタンスをデータベースに接続する際に必要です。

    注意　workspace-va 仮想マシンは、データベース名 **saas** を使用します。初期化プロセス時に、**saas** という既存のデータベースを削除して作成し直します。

手順

1 root ユーザーとしてログインします。

2 **postgresql.conf** ファイルを編集します。

  たとえば、VMware vFabric PostgreSQL データベースの場所は **/var/vmware/vpostgres/current/pgdata/** です。

3 **max_connections** パラメータを大きくします。Workspace で正しく機能するには、追加の workspace-va 仮想マシンごとに少なくとも **300** の接続が必要です。

4 2 つの workspace-va 仮想マシンの **max_connections** パラメータ値を **600** に設定します。

5 データベースを再起動します。

6 新しい行を **postgresql.conf.auto** ファイルに追加して、**search_path='saas'** パラメータを記述します。

7 PostgresSQL コマンドを実行して新しい PostgreSQL データベース スキーマを作成します。

表 4-2. 新しいデータベース スキーマ SQL を作成する

新しいデータベース スキーマを作成するためのサンプル SQL
CREATE ROLE horizon LOGIN PASSWORD **yourpassword** NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE NOREPLICATION; ALTER ROLE horizon SET search_path = saas; CREATE DATABASE saas WITH OWNER = postgres ENCODING = 'UTF8' TABLESPACE = pg_default CONNECTION LIMIT = -1; GRANT CONNECT, TEMPORARY ON DATABASE saas TO public; GRANT ALL ON DATABASE saas TO postgres; GRANT ALL ON DATABASE saas TO horizon; \connect saas; CREATE SCHEMA saas AUTHORIZATION horizon; CREATE EXTENSION citext SCHEMA saas;

内部データベースのデータの転送

展開時に内部データベースを使用し、外部データベースに切り替える予定がある場合は、データベースから既存のデータを抽出し、新しい外部データベースに追加できます。

開始する前に

外部データベース サーバを準備します。「PostgreSQL データベースの構成 (P. 23)」を参照してください。

手順

1 root ユーザーとしてログインします。

2 **/opt/vmware/vpostgres/current/bin** ディレクトリに移動します。

3 **./pg_dump –U postgres –w ––clean –f /tmp/db_dump.data saas** コマンドを実行します。

4 **db_dump.data** ファイルを新たに準備した外部データベース サーバにコピーします。

```
scp /tmp/db_dump.data
```

5 外部データベース サーバで root ユーザーとしてログインします。

6 **/opt/vmware/vpostgres/current/bin** ディレクトリに移動します。

7 **db_dump.data** コマンドを実行します。

```
./psql –U postgres –w –d saas –f /tmp/db_dump.data
```

db_dump.data コマンドの実行中に **DROP** コマンドや **ALTER** コマンドが表示される場合があります。

Workspace アプライアンスへの外部データベースの追加

Workspace セットアップ ウィザードを実行した後に、別のデータベースを使用するように Workspace を構成できます。

Workspace が、初期化された設定済みのデータベースを参照している必要があります。たとえば、Workspace [セットアップ] ウィザードが正常に実行された結果構成されたデータベース、バックアップからのデータベース、またはリカバリされたスナップショットからの既存のデータベースを使用できます。

開始する前に

- VMware vFabric PostgreSQL または Oracle を外部データベース サーバとしてインストールして構成します。Workspace のための PostgreSQL データベースの構成については、「PostgreSQL データベースの構成 (P. 23)」を参照してください。Workspace でサポートされている個々の Oracle バージョンの詳細については、「VMware 製品の相互運用性マトリックス」（http://www.vmware.com/resources/compatibility/sim/interop_matrix.php）を参照してください。
- 内部データベースを使用していた場合は、内部データベースからデータを転送します。

手順

1 Workspace 管理コンソール で [設定] をクリックし、[VA 構成] を選択します。

2 [構成の管理] をクリックします。

3 Workspace 管理者パスワードを使用して Appliance Configurator にログインします。

4 [データベース接続のセットアップ] ページで、データベース タイプに [外部データベース] を選択します。

5 データベース接続に関する情報を入力します。

a データベース サーバの JDBC URL を入力します。

PostgreSQL	`jdbc:postgresql://<IP_address>/saas?stringtype=unspecified`
Oracle	`jdbc:oracle:thin:@//<IP_address>:<port>/<sid>`

b データベースの読み取りと書き込みの権限があるユーザーの名前を入力します。

PostgreSQL	`horizon`
Oracle	`“saas”`

c Oracle または PostgreSQL データベースの構成時に作成したユーザーのパスワードを入力します。

6 [接続をテスト] をクリックして情報を検証し、保存します。

Syslog サーバの有効化

Workspace は、アプリケーション レベルのイベントを外部の syslog サーバにエクスポートします。オペレーティング システムのイベントはエクスポートされません。

ほとんどの企業でディスク容量に限りがあるため、Workspace は各仮想マシンのログ履歴を完全には保存しません。より多くの履歴を保存したり、ログ履歴を一元管理する場所を作成したりする場合は、外部の syslog サーバを設定できます。

初回構成時に syslog サーバを構成しない場合は、後で Appliance Configurator の [Syslog 構成] ページで構成できます。

開始する前に

外部の syslog サーバをセットアップします。利用可能な任意の標準 syslog サーバを使用できます。いくつかの syslog サーバには、詳細検索機能が備わっています。

手順

1 Workspace 管理コンソール で [設定] をクリックし、[VA 構成] を選択します。

2 [構成の管理] をクリックします。

3 Appliance Configurator にログインします。

4 左側のナビゲーション ペインで [Syslog の構成] をクリックします。

5 [有効化] をクリックします。

6 ログを保存するサーバの IP アドレスまたは FQDN を入力します。

7 [保存] をクリックします。

Workspace が、ログのコピーを syslog サーバに送信します。

Workspace での SSL 証明書の使用

Workspace アプライアンスのインストール時に、デフォルトの SSL 証明書が自動的にインストールされます。Workspace をテストするために、自己署名証明書を使用できます。Workspace を本番環境で使用する場合には、商用 SSL 証明書の生成とインストールをお勧めします。

機関証明書 (CA) は信頼できるエンティティで、証明書および作成者の ID を保証します。証明書が信頼できる CA によって署名されていれば、ユーザーは証明書の検証を要求するメッセージを受け取ることはなくなります。

Workspace を自己署名の SSL 証明書を使用して展開する場合は、Workspace にアクセスするすべてのクライアントが Workspace のルート CA 証明書を信頼できる CA として使用できるようにする必要があります。この場合のクライアントには、エンド ユーザーのマシン、ロード バランサ、プロキシなどが含まれます。Workspace ルート CA は、https://<workspacehostname.com>/horizon_workspace_rootca.pem からダウンロードできます。

Workspace の機関証明書は、[Appliance Configurator] > [証明書のインストール] ページでインストールできます。このページでは、ロード バランサのルート CA 証明書も同じように追加できます。「ロード バランサへの Workspace ルート証明書の適用 (P. 41)」を参照してください。

Workspace へのパブリック証明機関の適用

一部の企業は、自社または他の証明機関が生成した証明書を使用しています。このような証明書は、信頼できる証明機関リストに含まれていません。

Workspace に新しい証明書を追加できます。

注意 Workspace FQDN がロード バランサを参照している場合は、SSL 証明書はロード バランサに適用されます。

開始する前に

証明書の署名要求 (CSR) を生成し、CA から有効な署名証明書を取得します。組織が CA によって署名された SSL 証明書を提供している場合には、これらの証明書を使用できます。

手順

1 Workspace に証明書を適用するには、Workspace 管理コンソールで、[設定] をクリックし、[VA 構成] を選択します。

2 [構成の管理] をクリックします。

3 Workspace 管理者パスワードを使用して Appliance Configurator にログインします。

4 [証明書のインストール] を選択します。

5 [Workspace アプライアンス] タブの [SSL の終了] で、完全な証明書チェーンとプライベート キーを貼り付けます。証明書に Workspace FQDN ホスト名が含まれていることを確認します。

6 SSL 証明書を保存します。

次に進む前に

ユーザーがログインできることを確認します。

ログ ファイル情報

Workspace ログ ファイルは、デバッグとトラブルシューティングに役立ちます。下記にリストしたログ ファイルの開始点は共通です。その他のログは `/opt/vmware/horizon/workspace/logs` ディレクトリにあります。

表 4-3. ログ ファイル情報

コンポーネント	ログ ファイルの場所	説明
Workspace サービス ログ	`/opt/vmware/horizon/workspace/logs/horizon.log`	資格、ユーザー、およびグループなどの、Workspace アプリケーションのアクティビティに関する情報。
Configurator ログ	`/opt/vmware/horizon/workspace/logs/configurator.log`	Configurator が REST クライアントと Web インターフェイスから受け取る要求。
Connector ログ	`/opt/vmware/horizon/workspace/logs/connector.log`	Web インターフェイスから受信された各要求の記録。各ログ エントリには要求 URL、タイムスタンプ、例外が含まれています。同期アクションは記録されません。
Update ログ	`/opt/vmware/var/log/update.log` `/opt/vmware/var/log/vami`	Workspace アップグレード中の更新要求に関連する出力メッセージの記録。 `/opt/vmware/var/log/vami` ディレクトリのファイルはトラブルシューティングに役立ちます。これらのファイルは、アップグレード後のすべての仮想マシンにあります.
Apache Tomcat ログ	`/opt/vmware/horizon/workspace/logs/catalina.log`	他のログ ファイルで記録されないメッセージの Apache Tomcat レコード。

ログ情報の収集

テスト時やトラブルシューティング時にログを参照すると、仮想アプライアンスのアクティビティやパフォーマンスに関するフィードバックや、発生した問題に関する情報を確認できます。

環境にインストールされている各 workspace-va アプライアンスのログを収集します。

手順

1 Appliance Configurator にログインします。

2 [ログ ファイルの場所] ページを開いて [ログ バンドルの準備] をクリックします。

情報は、ダウンロード可能な tar.gz ファイルに収集されます。

3 準備ができたバンドルをダウンロードします。

次に進む前に

すべてのログを収集するには、各 workspace-va アプライアンスでこの操作を実行します。

Connector Services Admin ページでの Workspace 設定の更新

5

Workspace を構成したら、Connector Services Admin ページで Workspace ディレクトリの管理、認証アダプタの有効化または無効化、Active Directory ユーザー属性の変更、Active Directory グループの管理、ディレクトリの手動での同期、Workspace で使用する View プール、Citrix ベースのリソース、ThinApp パッケージなどのリソースのセットアップを行うことができます。

表 5-1. Connector Services Admin ページで管理する設定

ページ名	設定
バージョン情報	[バージョン情報] ページには、バージョン番号などの Workspace に関する全般的な情報が表示されます。
構成	現時点では、Workspace アプライアンスに [構成] ページは適用されません。
ドメインに参加	[ドメインに参加] を有効にし、このページで情報を入力することで、Workspace の View リソースや ThinApp リソースを使用したり、Windows の Kerberos 認証を使用して Web インターフェイスにシングル サインオンでアクセスできるようにします。リソースが使用する Active Directory と同じ Active Directory に参加する必要があります。 このページで入力する Active Directory の情報は、Active Directory ドメインにマシンを参加させる権限があるユーザーに対するものです。 これらのリソースの構成については、 『VMware Workspace Portal ガイド』の「リソースのセットアップ」の該当する章を参照してください。
ディレクトリ認証方法	Windows 認証を有効にして、Workspace でマルチドメイン、シングル フォレストまたは信頼できるマルチフォレスト Active Directory 環境を構成します。「マルチドメインまたは信頼できるマルチフォレスト Active Directory のための Windows 認証の構成 (P. 34)」を参照してください。
ID プロバイダ	[ID プロバイダ] ページには、企業ネットワーク内の Active Directory でユーザーの認証に使用する ID プロバイダ インスタンスが表示されます。
認証アダプタ	[認証アダプタ] ページには、パスワード認証、Kerberos 認証、SecureID など、Workspace で使用できる認証方法が表示されます。認証情報を有効化して構成できます。第 8 章「ユーザー認証の設定 (P. 45)」を参照してください。
ディレクトリ	このページで、Active Directory 接続情報を表示および管理できます。「Active Directory への接続の確立 (P. 32)」を参照してください。
ユーザー属性をマップ	このページには、Active Directory 属性から Workspace ディレクトリ属性へのマッピングが表示されます。View リソースを構成する場合は、このページで userPrincipalName 属性を選択する必要があります。
ディレクトリ同期	同期スケジュールを変更します。Workspace をインストールしたときに、1 日に 1 回午後 11 時 55 分にディレクトリを同期するスケジュールがデフォルトで設定されています。ディレクトリの同期ルールを編集して Active Directory のユーザーやグループを選択することもできます。
同期のセーフガード	ディレクトリ同期の結果として Workspace に追加されるユーザーおよびグループに対する意図せぬ変更を防止するために、同期のセーフガードを設定します。たとえば、一度に削除可能なユーザーの最大割合に制限を設定することができます。トリガー条件のいずれかが満たされると、ディレクトリ同期は実行されず、手動での介入が必要になります。デフォルト条件が有効になりますが、保護の程度の強弱を調整することができます。[トラブルシューティング] タブでセーフガード アラートを表示できます。

表 5-1. Connector Services Admin ページで管理する設定 (続き)

ページ名	設定
Horizon DaaS リソース	リソースとして Horizon DaaS を有効にして構成します。[ユーザー属性をマップ] ページで、distinguishedName 属性を有効にする必要があります。
View プール	Workspace でリソースとして View プールを有効にして構成します。そのためにはまず、[ドメインに参加] ページでドメインの接続を構成し、[ユーザー属性をマップ] ページで userPrincipalName 属性を有効にします。 このリソースの構成については、 『VMware Workspace Portal ガイド』の「リソースのセットアップ」 の該当する章を参照してください。
公開アプリケーション - Citrix	Workspace でリソースとして Citrix ベースのアプリケーションを有効にして構成します。 このリソースの構成については、 『VMware Workspace Portal ガイド』の「リソースのセットアップ」 の該当する章を参照してください。
パッケージ化されたアプリ - ThinApps	Workspace でリソースとして ThinApp パッケージを有効にして構成します。そのためにはまず、[ドメインに参加] 接続ページでドメインを構成する必要があります。 このリソースの構成については、 『VMware Workspace Portal ガイド』の「リソースのセットアップ」 の該当する章を参照してください。

手順

1 https://<Workspace_FQDN>.com:8443 にアクセスします。

2 Workspace 管理者パスワードを使用して Connector Services Admin にログインします。

3 左側のナビゲーション ペインを使用して、表示するページを選択します。

次に進む前に

新しい設定または更新が使用できることを確認します。

Active Directory と Workspace との接続の管理 6

Active Directory 環境は単一 Active Directory ドメイン、単一 Active Directory フォレストの複数のドメイン、または複数の Active Directory フォレスト全体の複数のドメインから成ります。Active Directory をカスタマイズしたら、Workspace で構成情報を更新します。

- Workspace と Active Directory の統合 (P. 31)

  Workspace は、単一の Active Directory ドメイン、単一の Active Directory フォレスト内の複数のドメイン、または複数の Active Directory フォレストにわたる複数のドメインを持つ Active Directory 環境と統合できます。

- Active Directory への接続の確立 (P. 32)

  Workspace は、ユーザーの認証や管理に既存の Active Directory インフラストラクチャを使用します。Workspace をインストールしてセットアップするときに、Active Directory の情報を構成します。

- Active Directory のマルチドメインまたは信頼できるマルチフォレスト ドメインへの接続の確立 (P. 34)

  Workspace をインストールすると単一の Active Directory ドメインが構成され、Workspace に同期されます。Windows 認証を有効にしてマルチドメイン、シングル フォレスト、または信頼できるマルチフォレストの Active Directory 環境を Workspace で構成する必要があります。

Workspace と Active Directory の統合

Workspace は、単一の Active Directory ドメイン、単一の Active Directory フォレスト内の複数のドメイン、または複数の Active Directory フォレストにわたる複数のドメインを持つ Active Directory 環境と統合できます。

Workspace をインストールしたら、単一の Active Directory ドメインに Workspace を接続します。複数のドメインがある場合は、Workspace のインストール後に Connector Services Admin ページで Workspace を既存の Active Directory 環境に統合できます。

単一の Active Directory ドメイン環境

単一の Active Directory 展開環境では、単一の Active Directory ドメインからユーザーとグループを同期できます。単一の Active Directory ドメイン環境に Workspace をインストールするには、「Active Directory への接続の確立 (P. 32)」を参照してください。

マルチ ドメイン、シングル フォレストの Active Directory 環境

マルチドメイン、シングル フォレストの Active Directory の展開では、シングル フォレスト内の複数の Active Directory ドメインからユーザーとグループを同期できます。

ディレクトリ認証方法として Windows 認証を有効にして、Workspace のマルチドメイン、シングル フォレストの Active Directory 環境を構成します。

マルチ ドメイン、シングル フォレストの Active Directory 環境に Workspace をインストールするには、「マルチドメインまたは信頼できるマルチフォレスト Active Directory のための Windows 認証の構成 (P. 34)」を参照してください。

信頼関係があるマルチフォレスト Active Directory 環境

信頼関係があるマルチフォレスト Active Directory の展開では、ドメイン間に双方向の信頼が存在するフォレスト全体で複数の Active Directory ドメインのユーザーとグループを同期できます。

ディレクトリ認証方法として Windows 認証を有効にして、Workspace のマルチフォレスト Active Directory 環境を構成します。

信頼できるマルチフォレスト Active Directory 環境に Workspace をインストールするには、「マルチドメインまたは信頼できるマルチフォレスト Active Directory のための Windows 認証の構成 (P. 34)」を参照してください。

信頼関係がないマルチフォレスト Active Directory 環境

信頼関係がないマルチフォレスト Active Directory の展開では、ドメイン間に信頼関係がないフォレスト全体で複数の Active Directory ドメインのユーザーとグループを同期できます。この展開では、Workspace ユーザー ストア テクノロジを使用する必要があります。

信頼関係がないマルチフォレスト Active Directory の展開の詳細については、VMware Professional Services にお問い合わせください。

Active Directory への接続の確立

Workspace は、ユーザーの認証や管理に既存の Active Directory インフラストラクチャを使用します。Workspace をインストールしてセットアップするときに、Active Directory の情報を構成します。

必要な Active Directory 情報

エンド ユーザーがログインすると、Workspace は次の Active Directory 情報を使用してエンド ユーザーの認証情報を検証します。Workspace をインストールするときにこの情報を構成します。

サーバ ホスト	Active Directory のホスト アドレス。
SSL を使用する	ディレクトリの接続に SSL を使用する場合は、この設定を構成して [証明書] フィールドに証明書を追加します。
DNS サービスの場所の使用	サーバ ホスト名とポート番号が分からない場合は、[DNS サービスの場所の使用] を選択します。Workspace は DNS サービスの場所レコードを使用して Active Directory ドメインを検索します。
サーバ ポート	Active Directory ホストのポート番号。LDAP のデフォルト ポートは 389 番です。SSL を使用する LDAP のデフォルト ポートは 636 番です。
検索属性	ユーザー名を含む Active Directory アカウント属性。ほとんどの Active Directory ドメイン サービスの展開で **sAMAccountName** を使用します。
ベース識別名 (DN)	ディレクトリ サーバの検索の開始点であるベース DN。 たとえば、DC=mycompany,DC=com というように指定します。Connector によって、この DN から開始してマスター リストが作成され、後で、このリストから個々のユーザーを除外し、グループを追加できます。

バインド DN	ユーザーを検索する権限がある Active Directory ユーザー アカウントのバインド DN。Active Directory 内のバインド DN アカウント ユーザー レコードには、ユーザー名、名前、姓、メール アドレス、必須拡張属性、および Active Directory に定義されている DN 属性が含まれている必要があります。 このユーザーは、Workspace 展開の管理者になります。Workspace 管理コンソールを使用して、他の Active Directory ユーザーを管理者ロールに昇格することができます。 注意　マルチフォレスト Active Directory が構成され、ドメイン ローカル グループに異なるフォレストのドメインのメンバが含まれる場合、Workspace ディレクトリ ページで使用されるバインド DN ユーザーをドメイン ローカル グループが存在するドメインの管理者グループに追加する必要があります。これを行わなければ、これらのメンバはドメイン ローカル グループに含まれなくなります。 次の例は、ベース DN とバインド DN を選択する場合のベスト プラクティスです。 ■ ベース DN : dc=example, dc=com（すべてのユーザーおよびグループを含めるため、最上位レベルのベース DN を使用します。） ■ バインド DN : cn=admin user, ou=users, dc=example, dc=com（選択したベース DN にバインド DN が含まれていることを確認します。）
バインド パスワード	バインド DN アカウントの Active Directory パスワード。

Workspace と同期する Active Directory ユーザーとグループの選択

Workspace で Active Directory の接続を構成する場合は、ユーザーの検索場所としてベース DN をセットアップします。この検索にはすべてのユーザーが含まれます。Workspace と同期するユーザー数を制限する場合は、ユーザー属性ベースの検索フィルタを作成して特定のタイプのユーザーを除外します。

セットアップしたベース DN がユーザーの検索に使用されます。検索にグループを加える場合は、フィルタを作成して Workspace ディレクトリに特定のタイプのグループを追加します。

Workspace でフィルタの作成およびグループの追加を行うには、まず Active Directory の構造を把握して同期するユーザーとグループを適切に選択するために、Active Directory 管理者とともに作業します。

フィルタを使用したユーザーとグループの追加

Workspace と同期するユーザーとグループを選択します。Workspace の初回セットアップ時に、最初の同期が発生します。Connector Services Admin ページからいつでも変更できます。

手順

1 Connector Services Admin にログインします。

2 [ディレクトリ同期] ページを選択し、[ディレクトリ同期ルールを編集] をクリックします。

3 [ユーザーを選択] ページの [ユーザーのベース DN] テキスト ボックスに、既存のベース DN が表示されます。別のベース DN を追加するには、[さらに追加] をクリックします。

4 [ユーザーを除外するフィルタの適用] ドロップダウン メニューで、特定のユーザー タイプの除外、フィルタ基準にするユーザー属性の選択、クエリ ルールの選択、および値の追加を選択します。

5 [さらに追加] をクリックして、フィルタを追加します。

6 [次へ] をクリックして、グループを追加します。

7 [選択したグループ] リストで特定のグループを見つけるには、[グループ名のフィルタ] テキスト ボックスに、追加するグループ名を入力します。

8 追加するグループ名の横にある [追加] をクリックします。

9 [次へ] をクリックします。

[Workspace にプッシュ] ページに、Workspace に追加するユーザーとグループの数が表示されます。

10 [保存して続行] をクリックします。

Active Directory は Workspace と同期されます。

Active Directory のマルチドメインまたは信頼できるマルチフォレスト ドメインへの接続の確立

Workspace をインストールすると単一の Active Directory ドメインが構成され、Workspace に同期されます。Windows 認証を有効にしてマルチドメイン、シングル フォレスト、または信頼できるマルチフォレストの Active Directory 環境を Workspace で構成する必要があります。

注意　Windows 認証を有効にすると、[ディレクトリ] の構成は [DNS サービスの場所] フィールドを有効にするように変更されます。組み込み SRV 参照をオーバーライドする場合は、「ドメイン ホスト参照ファイルを作成して DNS Service Location (SRV) 参照をオーバーライドする (P. 37)」を参照してください。

ユーザー インタラクティブな Windows 認証の指定を Workspace で構成するには、Workspace を Active Directory ドメインに参加させて Workspace で Windows 認証を有効にし、ユーザーとグループを Workspace と同期する必要があります。

マルチドメインまたは信頼できるマルチフォレスト Active Directory のための Windows 認証の構成

マルチドメインまたは信頼できるマルチフォレスト Active Directory ドメインへのインタラクティブな Windows 認証の指定を Workspace で構成するには、Workspace を Active Directory ドメインに参加させて Windows 認証を有効にし、ユーザーとグループを Workspace と同期する必要があります。

手順

1 マルチドメインまたは信頼できるマルチフォレスト ドメインの Active Directory ドメインへの Workspace の参加 (P. 35)

インタラクティブな Windows 認証方法を使用するマルチドメイン、シングル フォレスト、または信頼できるマルチフォレストの Active Directory を構成するには、Workspace アプライアンスを Active Directory ドメインに参加させる必要があります。

2 信頼されたマルチフォレスト Active Directory ドメインの Windows 認証へのアクセスを有効にする (P. 35)

ユーザー インタラクティブな Windows 認証の指定を Workspace で構成するには、Workspace を信頼できるマルチフォレスト Active Directory ドメインに参加させた後に、Workspace で Windows 認証を有効にする必要があります。

3 Workspace と同期するユーザーとグループの選択 (P. 36)

Active Directory ドメインのユーザーとグループを Workspace と同期するには、まず Workspace に追加するユーザーのタイプを制限し、異なるドメインから追加する必要があるグループを選択します。

4 ログイン ページへの複数のドメイン名の追加 (P. 37)

複数の Active Directory ドメインに Windows 認証を構成したら、パスワード アダプタを有効にしてユーザー サインイン ページにドメインを追加します。Workspace にサインインすると、ユーザーは各自のドメインをドロップダウン リストから選択できます。

5 ドメイン ホスト参照ファイルを作成して DNS Service Location (SRV) 参照をオーバーライドする (P. 37)

Windows 認証を有効にすると、[ディレクトリ] の構成は [DNS サービスの場所] フィールドを有効にするように変更されます。組み込み SRV 参照をオーバーライドするには、`domain_krb.properties` というファイルを作成し、SRV 参照より優先されるホスト値にドメインを追加できます。

マルチドメインまたは信頼できるマルチフォレスト ドメインの Active Directory ドメインへの Workspace の参加

インタラクティブな Windows 認証方法を使用するマルチドメイン、シングル フォレスト、または信頼できるマルチフォレストの Active Directory を構成するには、Workspace アプライアンスを Active Directory ドメインに参加させる必要があります。

開始する前に

- Active Directory ドメイン名と、そのドメインに参加する権限を持つ Active Directory 内のアカウントのユーザー名とパスワードがあることを確認します。

手順

1 Connector Services Admin にログインします。

2 [[ドメインに参加]] ページを選択します。

3 [AD ドメイン] テキスト ボックスに、Active Directory の完全修飾ドメイン名を入力します。

4 [AD ユーザー名] テキスト ボックスに、Active Directory ドメインにシステムを参加させる権限がある Active Directory のアカウントのユーザー名を入力します。

5 [AD パスワード] テキスト ボックスに、AD ユーザー名に関連付けられたパスワードを入力します。このパスワードは Workspace に保存されません。

6 [ドメインに参加] をクリックします。

[ドメインに参加] ページを更新すると、現在ドメインに参加していることを示すメッセージが表示されます。

次に進む前に

Windows 認証を有効にして、マルチドメイン、シングル フォレスト、または信頼できるマルチフォレスト Active Directory ドメインにアクセスします。

信頼されたマルチフォレスト Active Directory ドメインの Windows 認証へのアクセスを有効にする

ユーザー インタラクティブな Windows 認証の指定を Workspace で構成するには、Workspace を信頼できるマルチフォレスト Active Directory ドメインに参加させた後に、Workspace で Windows 認証を有効にする必要があります。

開始する前に

Workspace を Active Directory ドメインに参加させていることを確認します。

手順

1 Connector Services Admin にログインします。

2 [ディレクトリ認証方法] ページを選択します。

3 [Windows 認証を有効にする] をクリックします。

4 [保存] をクリックします。

Windows 認証方法が有効になります。Workspace は [ディレクトリ] ページおよび認証アダプタの [PasswordIdpAdapter] ページを更新し、[DNS サービスの場所の使用] フィールドにチェック マークを追加してバインド DN アカウント形式を sAMAccountName に変更します。

Active Directory がドメインを Workspace と同期すると、[ディレクトリ認証方法] ページにドメインのリストが追加されます。認証アダプタの [PasswordIdpAdapter] ページでパスワード アダプタ認証を有効にすると、ユーザー サインイン ページにドメイン名が追加されます。

次に進む前に

マルチフォレスト Active Directory が構成され、ドメイン ローカル グループに異なるフォレストのドメインのメンバが含まれる場合、[Workspace ディレクトリ] ページで使用されるバインド DN ユーザーをドメイン ローカル グループが存在するドメインの管理者グループに追加する必要があります。これを行わなければ、これらのメンバはドメイン ローカル グループに含まれなくなります。

Active Directory ドメインからユーザーとグループを選択して、Active Directory を Workspace に同期します。

Workspace と同期するユーザーとグループの選択

Active Directory ドメインのユーザーとグループを Workspace と同期するには、まず Workspace に追加するユーザーのタイプを制限し、異なるドメインから追加する必要があるグループを選択します。

開始する前に

フィルタとして使用する Active Directory ユーザー属性のリスト、および Workspace に追加するグループのリストを作成します。

手順

1 Connector Services Admin にログインします。

2 [ディレクトリ同期] ページを選択します。[ディレクトリ同期ルールを編集] をクリックします。

3 [ユーザーを選択] ページの [ユーザーのベース DN] テキスト ボックスに、既存のベース DN 構成が表示されます。別のベース DN を追加するには、[さらに追加] をクリックします。

4 特定のユーザー タイプを除外するには、[フィルタを適用してユーザーを除外] ドロップダウン メニューでフィルタ基準 にするユーザー属性を選択し、クエリ ルールを選択して値を追加します。

5 [さらに追加] をクリックしてフィルタを追加します。

6 [次へ] をクリックして、グループを追加します。

7 Active Directory で作成されたグループが、[選択したグループ] ページに一覧表示されます。特定のグループを見つけるには、[グループ名のフィルタ] テキスト フィールドで、追加するグループ名を入力します。

8 追加するグループ名の横にある [追加] をクリックします。

9 [次へ] をクリックします。

   [Workspace にプッシュ] ページに、Workspace に追加するユーザーとグループの数が表示されます。

10 [保存して続行] をクリックします。

Active Directory ドメインのユーザーとグループは、Workspace と同期されます。ドメイン名が Workspace と同期されると、[ディレクトリ認証方法] ページに追加されます。

次に進む前に

Active Directory ドメイン名がユーザー サインイン ページに追加されるように、パスワード アダプタ機能を有効にします。ユーザーは、サインインするときに各自のドメインを選択します。

ログイン ページへの複数のドメイン名の追加

複数の Active Directory ドメインに Windows 認証を構成したら、パスワード アダプタを有効にしてユーザー サインイン ページにドメインを追加します。Workspace にサインインすると、ユーザーは各自のドメインをドロップダウン リストから選択できます。

開始する前に

マルチドメインまたは信頼できるマルチフォレスト ドメインに接続を確立するには、Workspace で Windows 認証方法を有効にする必要があります。

Active Directory ドメインは、Workspace に同期されます。

手順

1 Connector Services Admin にログインします。

2 [認証アダプタ] ページを開いて PasswordldpAdapter 行で [編集] をクリックします。

3 [パスワード アダプタを有効にする] を選択します。

4 [保存] をクリックします。

ドメイン名が、ユーザー サインイン ページのドロップダウン リストに追加されます。

ドメイン ホスト参照ファイルを作成して DNS Service Location (SRV) 参照をオーバーライドする

Windows 認証を有効にすると、[ディレクトリ] の構成は [DNS サービスの場所] フィールドを有効にするように変更されます。組み込み SRV 参照をオーバーライドするには、`domain_krb.properties` というファイルを作成し、SRV 参照より優先されるホスト値にドメインを追加できます。

手順

1 workspace-va コマンド ラインで、ルート権限を保有するユーザーとしてログインします。

2 `/usr/local/horizon/conf` ディレクトリに移動し、`domain_krb.properties` というファイルを作成します。

3 domain_krb.properties ファイルを編集して、ホスト値にドメインのリストを追加します。この情報は、 `<AD Domain>=<host:port>, <host2:port2>, <host2:port2>` のように追加します。

   たとえば、リストを `example.com=examplehost.com:636, examplehost2.example.com:389` のように入力します。

4 domain_krb.properties ファイルの所有者を horizon に変更し、グループを www に変更します。
`chown horizon:www /usr/local/horizon/conf/domain_krb.properties` と入力します。

5 Workspace を再起動します。**`service horizon-workspace restart`** と入力します。

VMware Workspace Portal アプライアンスの詳細構成 7

基本的な Workspace のインストールが完了したら、Workspace への外部アクセスの有効化や仮想マシンのクローン作成などの他の構成タスクを完了する必要がある場合もあります。

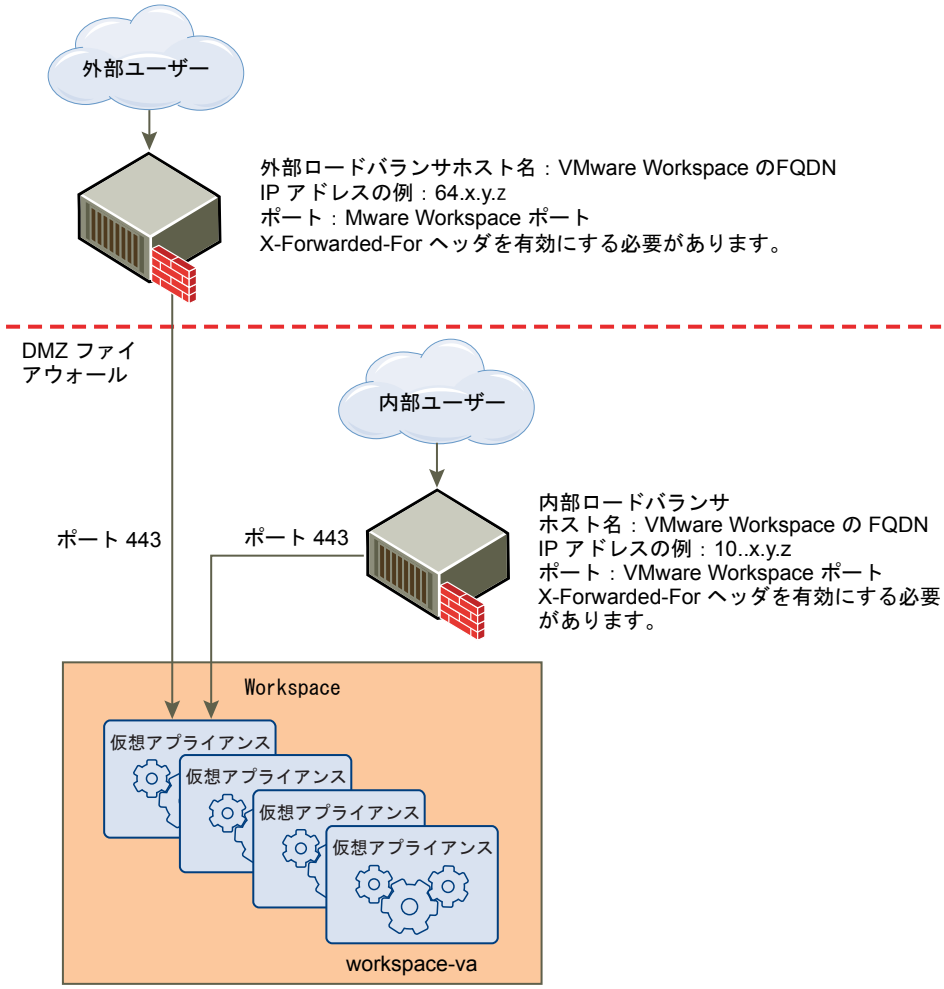
Workspace アーキテクチャの図に、Workspace 環境内の構築例を示します。標準的な展開については、第 2 章「VMware Workspace Portal のインストールの準備 (P. 7)」を参照してください。

ロード バランサを使用した Workspace への外部アクセスの有効化

展開時に、内部ネットワーク内に Workspace が設定されます。ネットワークの外側から接続するユーザーが Workspace にアクセスできるようにする場合は、Apache、nginx、F5 などのロード バランサを DMZ にインストールする必要があります。

ロード バランサを使用しない場合、Workspace 仮想マシンの数を後で拡張することはできません。冗長性やロード バランスを実現するために、Workspace 仮想マシンをさらに追加しなければならなくなる可能性があります。下記の図に、外部アクセスを有効するために使用できる、基本展開アーキテクチャを示します。

図 7-1. 外部ロード バランサ プロキシと仮想マシン



展開時の Workspace FQDN の指定

Workspace 仮想マシンの展開時に、Workspace FQDN と Workspace のポート番号を入力する必要があります。これらの値は、エンド ユーザーがアクセスするホスト名を指定する必要があります。

Workspace 仮想マシンは、常にポート 443 で実行されます。ロード バランサには、異なるポート番号を使用できます。ロード バランサには、異なるポート番号を使用できます。異なるポート番号を使用する場合は、展開時に指定する必要があります。

Workspace を構成するロード バランサの設定

X-Forwarded-For ヘッダの有効化、ロード バランサのタイムアウトの正確な設定、およびスティッキー セッションの有効化など、Workspace を構成するロード バランサ設定。さらに、Workspace とロード バランサ間に SSL トラストを構成する必要があります。

- X-Forwarded-For ヘッダ。ロード バランサで X-Forwarded-For ヘッダーを有効にする必要があります。これによって、認証方法が決定します。詳細については、ロード バランサのベンダーから提供されるドキュメントを参照してください。
- ロード バランサのタイムアウト。Workspace が正しく機能するように、ロード バランサの要求のタイムアウトをデフォルトの値から増やす必要がある場合があります。この値は、分単位で設定します。タイムアウト設定が短すぎると、“502 error: The service is currently unavailable.” というエラーが発生することがあります。

- Workspace に対するロード バランサのスティッキー セッションの有効化。展開で複数のワークスペース サーバを使用する場合は、workspace-va サーバに対してロード バランサのスティッキー セッションを有効にします。スティッキー セッションによって、Web インターフェイスのパフォーマンスが向上します。スティッキー セッションが有効でないと、一部の機能が失敗することがあります。

ロード バランサへの Workspace ルート証明書の適用

ロード バランサで Workspace が構成されている場合は、ロード バランサと Workspace 間の SSL トラストを確立する必要があります。Workspace ルート証明書をロード バランサにコピーする必要があります。証明書は、[Appliance Configurator]、[証明書のインストール] ページからダウンロードできます。

Workspace FQDN がロード バランサを参照している場合は、SSL をロード バランサのみに適用できます。ロード バランサは Workspace 仮想マシンと通信するため、Workspace ルート CA 証明書を信頼できる証明書としてロード バランサにコピーする必要があります。

手順

1 Workspace 管理コンソール で [設定] をクリックし、[VA 構成] を選択します。

2 [構成の管理] をクリックします。

3 Workspace 管理者パスワードを使用して Appliance Configurator にログインします。

4 [証明書のインストール] を選択します。

5 [ロード バランサ] タブで [SSL の終了] を選択し、[アプライアンスの root CA 証明書] フィールドでリンク `https://<workspacehostname>/horizon_workspace_rootca.pem` をクリックします。

Workspace ルート証明書が表示されます。

6 各ロード バランサの正しい場所にルート証明書をコピーして貼り付けます。ロード バランサのベンダーが提供するドキュメントを参照してください。

次に進む前に

[ロード バランサ] ページの [Workspace Appliance Configurator]、[証明書のインストール]、[SSL の終了] で、ロード バランサのルート証明書をコピーして貼り付けます。

Workspace 仮想アプライアンスの冗長性/フェイルオーバーの構成

Workspace を使用すると、企業は Workspace クラスタに複数の workspace-va 仮想アプライアンスを追加してフェイルオーバーおよび冗長性を実現できます。何らかの理由で仮想アプライアンスのいずれかがシャットダウンした場合、Workspace を引き続き使用できます。

Workspace でフェイルオーバーをセットアップするには、workspace-va 仮想アプライアンスのクローンを作成します。仮想アプライアンスのクローン作成では、クローン元と同じ構成でアプライアンスの複製を作成します。クローン作成された仮想アプライアンスの仮想アプライアンス名、ネットワーク設定、およびその他のプロパティを必要に応じて変更し、カスタマイズできます。

クローン作成された仮想アプライアンスの IP アドレスは、元の仮想アプライアンスの IP アドレスと同じガイドラインに従う必要があります。IP アドレスは、正引きと逆引きの DNS を使用して有効なホスト名に解決する必要があります。

クラスタのすべてのノードは同一で、お互いにほぼステートレスなコピーです。Active Directory と、Workspace に構成されている View や ThinApp などのリソースとの同期は、クローン作成された仮想アプライアンスでは無効です。

複数の Workspace 仮想アプライアンスの作成

フェイルオーバーの場合、企業は workspace-va 仮想アプライアンスのクローンを作成して同じタイプの複数の仮想アプライアンスを作成し、トラフィックを分散して潜在的なダウンタイムを解消できます。

複数の workspace-va 仮想アプライアンスを使用することによって、可用性を高め、Workspace への要求を負荷分散して、エンド ユーザーへの応答時間を短縮できます。

開始する前に

- 仮想アプライアンスは、ロード バランサの背後に構成する必要があります。ロード バランサ ポートが 443 番であることを確認します。ポート番号 8443 は Workspace 管理ポートで、各仮想アプライアンスに一意であるため、これはポート番号として使用しないでください。
- workspace-va 仮想アプライアンスを追加するには、「外部データベースへの接続 (P. 22)」の説明に従って構成された外部データベースまたは「KB 2094258, Using embedded vPostgres database for VMware Workspace Portal 2.1（VMware Workspace Portal 2.1 用の組み込み vPostgres データベースの使用）」の説明に従って構成された内部データベースのいずれかが設定されている必要があります。
- VMware vSphere Client または vSphere Web Client で 仮想アプライアンスのクローンを作成し、クローン作成された仮想アプライアンスにアクセスしてネットワークを構成する必要があります。
- クローン作成された仮想アプライアンス プロパティへの IP アドレスの追加 (P. 43)

  クローン作成された仮想アプライアンスをパワーオンするには、まず新しい IP アドレスを割り当てる必要があります。IP アドレスは、DNS で解決できる必要があります。逆引き DNS でアドレスを参照できない場合は、ホスト名も割り当てる必要があります。
- SecurID 認証の有効化 (P. 43)

  企業においては、さまざまな状況で、外部ネットワークから接続する自社のエンド ユーザーに対して、RSA SecurID ベースの認証を有効にします。workspace-va 仮想アプライアンスのクローン作成後に、RSA SecureID 認証を使用する場合は、クローン作成された Workspace のホスト名と IP アドレスを RSA サーバに追加して、クローン作成された仮想アプライアンスに新しいエージェントを作成する必要があります。
- Kerberos 認証の有効化 (P. 43)

  企業は、社内の Windows マシンから接続する自社のエンド ユーザーに対して、Kerberos 認証を有効にできます。Kerberos 認証を使用すると、エンド ユーザーは、ユーザー名とパスワードを入力せずに Workspace にログインできます。Workspace 仮想アプライアンスのクローンの作成後、Kerberos 認証を使用する場合は、クローン作成された仮想マシンでドメインの参加と Kerberos 認証を再び有効にする必要があります。

手順

1 クローン作成されている workspace-va 仮想アプライアンスをパワーオフします。

2 クローン作成されている仮想アプライアンスを右クリックして、[次へ] をクリックします。

3 このクローン作成された仮想アプライアンスを識別するために使用する名前を入力しますこの名前は、仮想アプライアンス フォルダ内で一意である必要があります。

4 クローン作成された仮想アプライアンスを実行するホストまたはクラスタを選択します。

5 仮想アプライアンスを実行するリソース プールを選択して [次へ] をクリックします。

6 仮想アプライアンスのファイルを格納するデータストアの場所を選択します。

7 仮想アプライアンスのディスクの形式を選択します。この形式は、ソースと同じ形式にする必要があります。[次へ] をクリックします。

8 ゲスト OS のオプションとして [カスタマイズしない] を選択します。

9 選択したオプションを確認します。内容が正しければ、[終了] をクリックします。

クローン作成された仮想アプライアンスが展開されます。クローン作成が完了するまで、仮想アプライアンスは使用することも編集することもできません。

次に進む前に

クローン workspace-va に IP アドレスを割り当ててから、マシンの電源を入れて新しい仮想アプライアンスをロード バランサに追加します。

クローン作成された仮想アプライアンス プロパティへの IP アドレスの追加

クローン作成された仮想アプライアンスをパワーオンするには、まず新しい IP アドレスを割り当てる必要があります。IP アドレスは、DNS で解決できる必要があります。逆引き DNS でアドレスを参照できない場合は、ホスト名も割り当てる必要があります。

手順

1 vSphere Client または vSphere Web Client で、クローン作成した仮想アプライアンスを選択します。

2 [概要] - [コマンド] を選択して、[編集] をクリックします。

3 [オプション] を選択し、[オプションの設定] リストで [プロパティ] を選択します。

4 [IP アドレス] フィールドの IP アドレスを変更します。

5 逆引き DNS で IP アドレスを参照できない場合は、[ホスト名] テキスト ボックスにホスト名を追加します。

6 [OK] をクリックします。

7 クローン マシンをパワーオンします。

次に進む前に

クローン作成された仮想アプライアンスそれぞれで Workspace に構成した認証方法を有効にします。

SecurID 認証の有効化

企業においては、さまざまな状況で、外部ネットワークから接続する自社のエンド ユーザーに対して、RSA SecurID ベースの認証を有効にします。workspace-va 仮想アプライアンスのクローン作成後に、RSA SecureID 認証を使用する場合は、クローン作成された Workspace のホスト名と IP アドレスを RSA サーバに追加して、クローン作成された仮想アプライアンスに新しいエージェントを作成する必要があります。

開始する前に

クローン作成された Workspace アプライアンスのホスト名と IP アドレスを使用して、新しい RSA サーバ認証エージェントを作成します。「Connector Services Admin のための RSA SecurID サーバの準備 (P. 46)」を参照してください。

手順

1 Connector Services Admin にログインします。

2 [認証アダプタ] をクリックします。

3 Secure ID 行で、[編集] をクリックします。

4 新しい Workspace IP アドレスを追加して、[SecureID 認証アダプタ] ページを再構成します。「Workspace での RSA SecurID 認証の構成 (P. 46)」を参照してください。

Kerberos 認証の有効化

企業は、社内の Windows マシンから接続する自社のエンド ユーザーに対して、Kerberos 認証を有効にできます。Kerberos 認証を使用すると、エンド ユーザーは、ユーザー名とパスワードを入力せずに Workspace にログインできます。Workspace 仮想アプライアンスのクローンの作成後、Kerberos 認証を使用する場合は、クローン作成された仮想マシンでドメインの参加と Kerberos 認証を再び有効にする必要があります。

手順

◆ Connector Services Admin にログインします。

a [[ドメインに参加]] ページを選択します。

b [AD パスワード] テキスト ボックスに、ドメインを参加させる権限がある Active Directory ユーザーのパスワードを入力します。

c [ドメインに参加] をクリックします。

d [認証アダプタ] をクリックします。

e KerberosldAdapter を選択し、開いたページで [Windows 認証を有効にする] を選択します。

f [保存] をクリックします。

View が複数コネクタを備えた Workspace 展開環境と統合されている場合は、View デスクトップをサポートするすべての Connector で View プールを有効にし、構成していることを確認します。View プールが有効でないと、Connector からデスクトップに接続できません。[View Pool Sync] 処理をいずれかの Connector からスケジュールすると、この処理によって、Connector が View 構成と同期されます。

ユーザー認証の設定

8

Workspace は、Active Directory パスワード、Kerberos、および RSA SecureID の各認証方法をサポートします。

デフォルトでサポートされる Workspace 認証タイプ	説明
パスワード	まったく構成を行わないと、Workspace は Active Directory パスワード認証をサポートします。この方法では、Active Directory に対して直接、ユーザーを認証します。
Kerberos	Kerberos 認証によりドメイン ユーザーがシングル サインオンで Workspace にアクセスできるため、ドメイン ユーザーがエンタープライズ ネットワークへのログイン後に Workspace にログインする必要がなくなります。ID プロバイダ インスタンスは、キー配布センター（KDC）が配布する Kerberos チケットを使用して、ユーザー デスクトップ資格情報を検証します。
RSA SecurID	RSA SecurID 認証では、ユーザーがトークン ベースの認証システムを使用する必要があります。RSA SecurID は、エンタープライズ ネットワークの外部から Workspace にアクセスするユーザーに対して推奨される認証方法です。

Workspace ユーザー認証の構成の詳細については、Workspace 管理者ガイド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。

Workspace のための SecurID の構成

RSA SecurID サーバを構成する場合は、RSA SecurID サーバの認証エージェントとして Workspace アプライアンスの情報を追加し、Workspace で RSA SecureID サーバの情報を構成します。

Workspace の展開後に、SecurID を構成して、セキュリティを強化できます。ネットワークが Workspace の導入環境用に正しく構成されていることを確認する必要があります。SecurID については特に、正しいポートが開いていて、SecurID がエンタープライズ ネットワーク外部のユーザーを認証できることを確認する必要があります。

Workspace [セットアップ] ウィザードの実行後に、RSA SecurID サーバの準備に必要な情報を入手できます。Workspace アプライアンスの RSA SecurID サーバの準備ができたら、WorkspaceConnector Services Admin の [認証アダプタ] ページに移動して SecurID を有効にします。

Connector Services Admin のための RSA SecurID サーバの準備

RSA SecurID サーバは Workspace アプライアンスを認証エージェントとした情報で構成される必要があります。必須の情報は、ネットワーク インターフェイスのホスト名と IP アドレスです。

開始する前に

Workspace

- RSA Authentication Manager のバージョン 6.1.2、7.1 SP2 以上、または 8.0 以上がエンタープライズ ネットワークにインストールされ、動作しており、Connector Services Admin と通信できることを確認します。Workspace は、AuthSDK_Java_v8.1.1.312.06_03_11_03_16_51（Agent API 8.1 SP1）を使用しますが、このバージョンは、RSA Authentication Manager（RSA SecurID サーバ）の以前のバージョンのみをサポートしています。RSA Authentication Manager（RSA SecurID サーバ）のインストールと構成の詳細については、RSA のドキュメントを参照してください。

手順

1 RSA SecurID サーバのサポート対象バージョンで、Workspace アプライアンスを認証エージェントとして追加します。以下の情報を入力します。

オプション	説明
ホスト名	Workspace アプライアンスのホスト名
IP アドレス	Workspace アプライアンスの IP アドレス
代替 IP アドレス	RSA SecurID サーバに到達するために、トラフィックが Workspace アプライアンスからネットワーク アドレス変換（NAT）デバイスにパススルーする場合は、Workspace アプライアンスのプライベート IP アドレスを入力します。

2 圧縮された構成ファイルをダウンロードし、`sdconf.rec` ファイルを解凍します。

Workspace で RSA SecurID を構成するときにこのファイルを後でアップロードできるようにしておきます。

次に進む前に

Connector Services Admin の [詳細] タブに移動し、[認証アダプタ] ページで SecurID を構成します。

Workspace での RSA SecurID 認証の構成

Workspace アプライアンスを RSA SecurID サーバの認証エージェントとして構成したら、Workspace に RSA SecureID 構成情報を追加する必要があります。

開始する前に

- RSA Authentication Manager（RSA SecurID サーバ）がインストールされ、正しく構成されていることを確認します。
- 圧縮ファイルを RSA SecurID サーバからダウンロードし、サーバ構成ファイルを展開します。

手順

1 Connector Services Admin の [認証アダプタ] ページの SecurIDldpAdapter 行で [編集] をクリックします。

2 [SecurID を有効にする] チェック ボックスをクリックします。

3 [SecurID 認証アダプタ] ページで構成します。

RSA SecurID サーバで使用される情報と生成されるファイルは、[SecurID] ページを構成する際に必要です。

オプション	操作
名前	名前は必須です。デフォルトの名前は、SecurIDldpAdapter です。この名前は、 いつでも変更できます。
SecurID を有効化	このボックスを選択して securID 認証を有効化します。
許可される認証の試行回数	RSA SecurID トークンを使用したログインの失敗が許可される最大回数。デフォルトは、5 回です。
コネクタのアドレス	Workspace ローカル ホスト名または IP アドレスを入力します。入力する値は、認証エージェントとして Workspace アプライアンスを RSA SecurID サーバに追加するときに使用した値と一致する必要があります。別の IP アドレスのプロンプトに割り当てた値が RSA SecurID サーバにある場合は、その値を Workspace IP アドレスとして入力します。別の IP アドレスが割り当てられていない場合は、認証エージェントとして Workspace アプライアンスを RSA SecurID サーバに追加するときに使用した値を IP アドレスのプロンプトに入力します。
エージェント IP アドレス	RSA SecurID サーバの [IP アドレス] プロンプトに割り当てられている値を入力します。
サーバ構成	RSA SecureID サーバ構成ファイルをアップロードします。 最初に、RSA SecurID サーバから圧縮ファイルをダウンロードしてサーバ構成ファイル（デフォルトの名前は `sdconf.rec`）を解凍する必要があります。
ノード シークレット	[ノード シークレット] フィールドを空白のままにしておくと、ノード シークレットを自動生成できます。RSA SecurID サーバのノード シークレット ファイルをクリアすることをお勧めします。このファイルを意図的にアップロードしないでください。RSA SecurID サーバや Workspace アプライアンスのノード シークレット ファイルは常に一致する必要があります。どちらかでノード シークレットを変更する場合は、もう一方でも同じように変更します。たとえば、RSA SecurID サーバでノード シークレットをクリアまたは生成した場合は、Workspace アプライアンスのノード シークレット ファイルもクリアまたはアップロードします。

4 SecurID の設定を保存します。

Workspace 用 Kerberos の構成

Kerberos 認証を使用すると、ユーザーは Workspace にシングル サインオンでアクセスできます。Windows 認証を有効にすると、Kerberos プロトコルによってユーザーのブラウザと Workspace 間の通信が安全になります。Kerberos が Workspace の展開環境で機能するようにするために、Active Directory を直接構成する必要はありません。

Connector Services Admin ページに移動して Kerberos 認証を有効にします。Connector Services Admin の [ドメインに参加] ページでドメインを参加させて、[認証アダプタ] ページで Kerberos を有効にする必要があります。

Kerberos 認証オペレーティング システムのサポート

現在、ユーザーのブラウザと Workspace の間のやり取りは、Windows オペレーティング システムでのみ、Kerberos によって認証されます。それ以外のオペレーティング システムからの Workspace へのアクセスでは、Kerberos 認証を利用できません。

ブラウザの構成

Windows を実行しているコンピュータの Workspace に Kerberos 認証情報を送信するように、Web ブラウザ（Firefox、Internet Explorer、および Chrome）を構成できます。すべてのブラウザで、追加構成が必要です。

Kerberos が有効な場合は、ユーザーがログインするときに Web ブラウザを構成して Kerberos 認証情報を Workspace に送信する必要があります。

- Workspace での Kerberos の構成 (P. 48)

  Workspace を構成して Kerberos 認証を使用するには、ドメインに参加して Workspace で Kerberos 認証を有効にする必要があります。。

- Web インターフェイスにアクセスするための Internet Explorer の構成 (P. 48)

  Workspace の展開環境に Kerberos が構成されていたり、Internet Explorer ブラウザを使用してユーザーが Web インターフェイスにアクセスできるようにしたりするには、Internet Explorer ブラウザを構成する必要があります。

- Web インターフェイスにアクセスするための Firefox の構成 (P. 50)

  Workspace の展開環境に Kerberos が構成されていたり、Firefox ブラウザを使用してユーザーが Web インターフェイスにアクセスできるようにしたりするには、Firefox ブラウザを構成する必要があります。

- Web インターフェイスにアクセスするための Chrome ブラウザの構成 (P. 50)

  Workspace の展開環境に Kerberos が構成されていたり、Chrome ブラウザを使用してユーザーが Web インターフェイスにアクセスできるようにしたりするには、Chrome ブラウザを構成する必要があります。

Workspace での Kerberos の構成

Workspace を構成して Kerberos 認証を使用するには、ドメインに参加して Workspace で Kerberos 認証を有効にする必要があります。。

手順

1 Connector Services Admin にアクセスして [ドメインへの参加] を選択します。

2 [ドメインに参加] ページで、Active Directory ドメインの情報を入力します。

   a [AD ドメイン] テキスト ボックスに、Active Directory の完全修飾ドメイン名を入力します。入力するドメイン名は、Workspace アプライアンスが常駐する Windows ドメインと同じにする必要があります。

   b [AD ユーザー名] テキスト ボックスに、Active Directory ドメインにシステムを参加させる権限がある Active Directory のアカウントのユーザー名を入力します。

   c [AD パスワード] テキスト ボックスに、AD ユーザー名に関連付けられたパスワードを入力します。このパスワードは Workspace に保存されません。

   d [ドメインに参加] をクリックします。

   [ドメインに参加] ページを更新すると、現在ドメインに参加していることを示すメッセージが表示されます。

3 Connector Services Admin ページで [認証アダプタ] を選択し、KerberosIdpAdapter 行で [編集] をクリックします。

   a [名前] フィールドに、名前として KerberosIdpAdapter が表示されます。このタイプは変更できます。

   b [ディレクトリの UID 属性] テキスト ボックスに、ユーザー名を含むアカウント属性を入力します。

   c [Windows 認証を有効にする] を選択して、ユーザーのブラウザと Workspace 間の認証相互作用を拡張します。

   d [NTLM を有効にする] を選択し、NTLM (NT LAN Manager) プロトコルベースの認証を有効にします。

   e ラウンド ロビン DNS やロード バランサが Kerberos でサポートされない場合は、[リダイレクトの有効化] を選択します。認証要求は、リダイレクト ホスト名にリダイレクトされます。これを選択した場合は、[リダイレクト ホスト名] テキスト ボックスにリダイレクト ホスト名を入力します。

   f [保存] をクリックします。

Web インターフェイスにアクセスするための Internet Explorer の構成

Workspace の展開環境に Kerberos が構成されていたり、Internet Explorer ブラウザを使用してユーザーが Web インターフェイスにアクセスできるようにしたりするには、Internet Explorer ブラウザを構成する必要があります。

Kerberos 認証は、Windows オペレーティング システム上の Workspace と連携して動作します。

注意　ここに記載する Kerberos 関連の手順を、他のオペレーティング システムに適用しないでください。

開始する前に

Kerberos を構成した後に、Internet Explorer ブラウザをユーザーごとに構成するか、ユーザーに手順を指示します。

手順

1 Windows にドメイン内のユーザーとしてログインしていることを確認します。

2 Internet Explorer で、自動ログオンを有効にします。

   a [ツール] - [インターネット オプション] - [セキュリティ] を選択します。

   b [レベルのカスタマイズ] を選択します。

   c [イントラネットゾーンでのみ自動的にログオンする] を選択します。

   d [OK] をクリックします。

3 Workspace アプライアンスのこのインスタンスがローカル イントラネット ゾーンの一部であることを確認します。

   a Internet Explorer を使用して、https://workspaceHostname.DomainName/authenticate/ の Workspace ログイン URL にアクセスします。

   b ブラウザ ウィンドウのステータス バーの右下に表示されているゾーンを確認します。

   ゾーンがローカル イントラネットであれば、Internet Explorer の構成は完了です。

4 ゾーンがローカル イントラネットでない場合は、Workspace をイントラネット ゾーンに追加します。

   a [ツール] - [インターネット オプション] - [セキュリティ] - [ローカル イントラネット] - [サイト] を選択します。

   b [イントラネットのネットワークを自動的に検出する] を選択します。

   このオプションが選択されていなかった場合は、選択するだけで、Workspace をイントラネット ゾーンに追加できる場合があります。

   c （オプション）[イントラネットのネットワークを自動的に検出する] を選択した場合は、[OK] をクリックして、すべてのダイアログ ボックスを閉じます。

   d [ローカル イントラネット] ダイアログ ボックスで、[詳細設定] をクリックします。

   2 つ目の [ローカル イントラネット] という名前のダイアログ ボックスが表示されます。

   e Workspace URL を [次の Web サイトをゾーンに追加する] テキスト ボックスに入力します。

   https://workspaceHostname.DomainName/authenticate/

   f [追加 > 閉じる > OK] をクリックします。

5 Internet Explorer が信頼済みサイトとして Windows 認証をパスするよう許可されていることを確認します。

   a [インターネット オプション] ダイアログ ボックスで、[詳細設定] タブをクリックします。

   b [統合 Windows 認証を使用する] を選択します。

   このオプションは、Internet Explorer の再起動後に初めて有効になります。

   c [OK] をクリックします。

6 https://workspaceHostname.DomainName/authenticate/ の Workspace Web インターフェイスにログインし、アクセスできることを確認します。

   Kerberos 認証が成功すると、テストの URL が Web インターフェイスに接続されます。

Kerberos プロトコルによって、この Internet Explorer ブラウザ インスタンスと Workspace の間のすべてのやり取りのセキュリティが保証されます。これで、ユーザーが Workspace へのシングル サインオン アクセスを使用できるようになりました。

Web インターフェイスにアクセスするための Firefox の構成

Workspace の展開環境に Kerberos が構成されていたり、Firefox ブラウザを使用してユーザーが Web インターフェイスにアクセスできるようにしたりするには、Firefox ブラウザを構成する必要があります。

Kerberos 認証は、Windows オペレーティング システム上の Workspace と連携して動作します。

注意　ここに記載する Kerberos 関連の手順を、他のオペレーティング システムに適用しないでください。

開始する前に

Kerberos を構成した後に、Firefox ブラウザをユーザーごとに構成するか、ユーザーに手順を指示します。

手順

1 Firefox ブラウザの [URL] テキスト ボックスに **`about:config`** と入力して、詳細設定にアクセスします。

2 [細心の注意を払って使用する] をクリックします。

3 [設定名] 列の [network.negotiate-auth.trusted-uris] をダブルクリックします。

4 Workspace URL をテキスト ボックスに入力します。

https://<workspaceHostname>

5 [OK] をクリックします。

6 [設定名] 列の [network.negotiate-auth.delegation-uris] をダブルクリックします。

7 Workspace URL をテキスト ボックスに入力します。

https://<workspaceHostname>

8 [OK] をクリックします。

9 Firefox ブラウザを使用して https://<workspaceHostname> の Workspace にログインし、Kerberos 機能をテストします。

Kerberos 認証が成功すると、テスト URL が Web インターフェイスに接続されます。

Kerberos プロトコルによって、この Firefox ブラウザ インスタンスと Workspace の間のすべてのやり取りのセキュリティが保証されます。これで、ユーザーが Workspace へのシングル サインオン アクセスを使用できるようになりました。

Web インターフェイスにアクセスするための Chrome ブラウザの構成

Workspace の展開環境に Kerberos が構成されていたり、Chrome ブラウザを使用してユーザーが Web インターフェイスにアクセスできるようにしたりするには、Chrome ブラウザを構成する必要があります。

Kerberos 認証は、Windows オペレーティング システム上の Workspace と連携して動作します。

注意　ここに記載する Kerberos 関連の手順を、他のオペレーティング システムに適用しないでください。

開始する前に

- Kerberos を構成します。
- Chrome は Internet Explorer の構成を使用して Kerberos 認証を有効にするため、Internet Explorer を構成して、Chrome が Internet Explorer の構成を使用できるようにする必要があります。Chrome の Kerberos 認証の構成方法については、Google のドキュメントを参照してください。

手順

1 Chrome ブラウザを使用して、Kerberos の機能をテストします。

2 https://<Workspace FQDN> の Workspace にログインします。

Kerberos 認証が成功すると、テストの URL が Web インターフェイスに接続されます。

関連するすべての Kerberos 構成が正しければ、関連プロトコル（Kerberos）によって、この Chrome ブラウザ インスタンスと Workspace の間のすべてのやり取りのセキュリティが確保されます。ユーザーは Workspace へのシングル サインオン アクセスを使用できます。

9 デモ ユーザー ストアのカスタマイズ

組み込み OpenLDAP サービスは一般的に、デモやテストの構成に使用されます。組み込み OpenLDAP サービスは、新規ユーザーの追加、既存ユーザーの削除、ユーザー パスワードの変更などの一般的な LDAP 処理を実行するために使用されます。

これらの情報は、標準の LDAP の処理やコマンドに精通しているシステム管理者向けのものです。

組み込み OpenLDAP サーバは TCP ポート 389 で動作します。OpenLDAP サーバにアクセスできるのは、ローカルの workspace-va 仮想アプライアンスの Linux コンソールだけです。標準の LDAP コマンドを使用して、組み込み OpenLDAP サーバで処理を実行できます。必要なバイナリ（**ldapadd**、**ldapsearch**、**ldapdelete**、および **ldapmodify**）は、仮想アプライアンスにインストールされます。

Appliance Configurator および Connector Services Admin のページで OpenLDAP を構成する場合は、特定のパラメータを使用する必要があります。

表 9-1. OpenLDAP 構成情報

属性	値
ホスト名	<ConnectorFullyQualifiedDomainName> または <localhost>
検索属性	**sAMAccountName**
サーバ ポート	389
ベース DN	ou=users、dc=test、dc=example、dc=com
バインド DN	cn=test user1、ou=users、dc=test、dc=example、dc=com
バインド パスワード	パスワード

デモ ユーザー ストアには、デモに使用できる 10 のサンプル ユーザーと 1 つのグループが含まれます。

デモ ユーザー ストアには特定のサンプル データが含まれています。展開中に、このデータがサンプル データベースにロードされます。

ユーザーまたはグループを追加するには、新しいファイルを作成して、**ldapusers.ldif** および **ldapgroups.ldif** という名前を付けます。オリジナルのファイルである **users.ldif** と **groups.ldif** を、テンプレートとして使用します。「「デモ ユーザー ストアへのユーザーの追加 (P. 54)」」と「「デモ ユーザー ストアにおけるグループの追加とユーザーのグループへの割り当て (P. 56)」」を参照してください。

表 9-2. デモ ユーザー ストアに含まれるサンプル情報

サンプル名	値
サンプル ファイル	**users.ldif** **groups.ldif**
ディレクトリ パス	**/etc/openldap**
サンプル ユーザー名	testuser1 ～ testuser10

表 9-2. デモ ユーザー ストアに含まれるサンプル情報 (続き)

サンプル名	値
すべてのユーザーのパスワード	パスワード
サンプル グループ サンプル グループの testgroup1 には、10 のサンプル ユーザーが含まれます。	testgroup1

- デモ ユーザー ストアへのユーザーの追加 (P. 54)

  デモ ユーザー ストアをセットアップする場合は、本番環境に基いて、追加するユーザーの数を決定します。十分な数のユーザーを追加して、本番環境と同等のテスト結果が得られるようにする必要があります。

- デモ ユーザー ストアにおけるグループの追加とユーザーのグループへの割り当て (P. 56)

  デモ ユーザー ストアをセットアップする場合は、本番環境のサイズに基づいて、追加するグループとユーザーの数を決定します。本番環境に近い環境を作成するのに十分なグループとユーザーを追加します。

デモ ユーザー ストアへのユーザーの追加

デモ ユーザー ストアをセットアップする場合は、本番環境に基いて、追加するユーザーの数を決定します。十分な数のユーザーを追加して、本番環境と同等のテスト結果が得られるようにする必要があります。

デモ ユーザー ストアにユーザーを追加するには、workspace-va 仮想マシンで `ldapusers.ldif` ファイルを変更して `ldapadd` コマンドを実行します。

開始する前に

`sAMAccountName` をデモ ユーザー ストアの [検索属性] として使用する必要があります。デモ ユーザー ストアを使用する場合、Workspace は、`userPrincipalName` をサポートしません。

手順

1 `ldapusers.ldif` ファイルの <value> タグは、自分の情報に置き換えます。サンプルの `ldapusers.ldif` テーブルを参照してください。

2 workspace-va 仮想マシンに `ldif` ファイルをコピーします。

3 `ldapadd` コマンドを実行してデモ ユーザー ストアに新しいユーザーを追加します。

```
/usr/bin/ldapadd -h 127.0.0.1 -D <cn=Manager,dc=test,dc=example,dc=com> -w H0rizon! -x -f <ldif file path>
```

`ldif` ファイルで異なる値を使用すると、複数のユーザーを追加できます。

4 LDAP サービスを再起動します。

```
/sbin/service ldap restart
```

表 9-3. サンプル `ldapusers.ldif` ファイル

サンプル `ldapusers.ldif`
パラメータごとに一意の <value> を使用します。 dn:cn=<値>,ou=users,dc=test,dc=example,dc=com objectClass: user objectCategory: person cn:<値> sn:<値> sAMAccountName:<値> canonicalName:<値> mail:<値> givenName:<値> distinguishedName:cn=<value>,ou=users,dc=test,dc=example,dc=com objectGUID:<値>（たとえば、cd0ff02b-f9d6-4fac-a5bc-6380d1867999） userPassword:<値>（たとえば、{SSHA}WbipwJh13Jdy2tltppdkFMzzNVSfkqsZ）

次に進む前に

デモ ユーザー ストアのユーザーによって使用される暗号化されたパスワードを生成します。「SSHA 暗号化パスワードの生成 (P. 55)」を参照してください。

SSHA 暗号化パスワードの生成

SSHA（Salted Secure Hash Algorithm）は、SHA アルゴリズムの改良版で、ハッシュをランダムに生成し、ハッシュが暗号化されない可能性を低くします。

SSHA 暗号化パスワードを生成する必要があります。すべてのデモ ユーザー アクセスに同じパスワードを使用できます。ユーザーごとに異なるパスワードが必要な場合は、それぞれのパスワードを 1 つずつ暗号化します。

開始する前に

「デモ ユーザー ストアへのユーザーの追加 (P. 54)」.

手順

1 workspace-va 仮想アプライアンスを開きます。

2 `slappasswd` コマンドを実行します。

3 新しいパスワードを入力し、確認のために再入力します。

SSHA で暗号化された値が表示されます。

4 この値を `ldif` ファイルに追加して、ユーザー パスワードを設定します。

次に進む前に

グループを追加し、ユーザーをデモ ユーザー ストアに割り当てます。

デモ ユーザー ストアにおけるグループの追加とユーザーのグループへの割り当て

デモ ユーザー ストアをセットアップする場合は、本番環境のサイズに基づいて、追加するグループとユーザーの数を決定します。本番環境に近い環境を作成するのに十分なグループとユーザーを追加します。

`ldapgroups.ldif` ファイルを変更し、workspace-va 仮想マシンで `ldapadd` コマンドを実行して、グループをデモ ユーザー ストアに追加します。

手順

1 `ldapgroups.ldif` ファイルの <value> タグと <user DN> タグを置換します。

ユーザー DN は、LDAP の既存のユーザーの識別名である必要があります。<value> タグを置換することでグループを作成し、<User DN> タグを置換することで作成する新しいグループにユーザーを割り当てます。

2 `ldif` ファイルを workspace-va 仮想マシンにコピーします。

3 `ldapadd` コマンドを実行して、グループをデモ ユーザー ストアに追加します。

```
/usr/bin/ldapadd –h 127.0.0.1 –D <cn=Manager,dc=test,dc=example,dc=com> –w H0rizon!
–x –f<ldif file path>
```

`ldif` ファイルで異なる値を使用すると、複数のグループを追加できます。

4 LDAP サービスを再起動します。

```
/sbin/service ldap restart
```

表 9-4. `ldapgroups.ldif` ファイルの例

サンプル パラメータ
パラメータごとに一意の <value> を使用します。
dn:cn=<value>,ou=users,dc=test,dc=example,dc=com
objectClass: group
objectCategory: group
sAMAccountName:<値>
canonicalName:<値>
mail:<値>
distinguishedName:cn=<value>,ou=users,dc=test,dc=example,dc=com
objectGUID:<value>（たとえば、cd0ff02b-f9d6-4fac-a5bc-6380d1867899）
member:<User DN1>（たとえば、cn=user1,ou=users,dc=test,dc=example,dc=com）
member:<User DN2>
member:<User DN3>
member:<User DN4>

次に進む前に

本番環境の Workspace に移行する準備が整うまで、テストにデモ ユーザー ストアを使用します。

インデックス