VDS を使用した導入

Virtual Desktop Service

NetApp
February 16, 2022

目次

VDS を使用した導入

Azure

Azure Virtual Desktop の 1 つです

AVD 導入ガイド

概要

このガイドでは、 Azure の NetApp Virtual Desktop Service （ VDS ）を利用して Azure Virtual Desktop （ AVD ）を導入する手順を段階的に説明します。

ガイドの内容は次のとおりです。 https://cwasetup.cloudworkspace.com/

このコンセプトの実証（ POC ）ガイドは、お客様が独自の Azure サブスクリプションテストで AVD を迅速に導入して設定できるようにすることを目的としています。このガイドは、クリーンな非本番環境の Azure Active Directory テナントへの環境を構築することを前提としています。

特に既存の AD または Azure AD 環境への本番環境の導入は非常に一般的ですが、この POC ガイドではそのプロセスを考慮していません。複雑な POC や本番環境の導入は、ネットアップ VDS の営業 / サービスチームで開始し、セルフサービスでは実施しないでください。

この POC ドキュメントでは、 AVD の導入全体を説明し、 VDS プラットフォームで利用可能な導入後の構成の主な領域について簡単に説明します。完了すると、完全に展開された機能的な AVD 環境が構築され、ホストプール、アプリケーショングループ、ユーザーが提供されます。オプションで、自動化されたアプリケーション配信、セキュリティグループ、ファイル共有権限、 Azure Cloud Backup 、インテリジェントなコスト最適化を構成できます。VDS では、 GPO 経由で一連のベストプラクティス設定が導入されます。オプションでこれらの制御を無効にする方法についても説明します。 POC では、管理対象外のローカルデバイス環境と同様に、セキュリティ制御を行わない必要があります。

AVD の基本

Azure Virtual Desktop は、クラウドで実行される包括的なデスクトップおよびアプリケーション仮想化サービスです。主な機能の一部を以下に示します。

- ゲートウェイ、ブローカー、ライセンス、ログインなどのプラットフォームサービスが、 Microsoft のサービスとして含まれています。ホストと管理が必要なインフラを最小限に抑えることができます。
- Azure Active Directory をアイデンティティプロバイダとして利用すると、条件付きアクセスなどの追加の Azure セキュリティサービスをレイヤ化できます。
- ユーザーは、 Microsoft サービスのシングルサインオン体験を体験できます。
- ユーザセッションは、独自のリバース接続技術を使用してセッションホストに接続します。つまり、受信ポートをオープンする必要はなく、エージェントが AVD 管理プレーンへの発信接続を作成してエンドユーザデバイスに接続します。
- 逆接続では、パブリックインターネットに公開されることなく仮想マシンを実行できるため、リモート接続を維持しながらもワークロードを分離できます。
- AVD には Windows 10 Multi Session へのアクセスが含まれているため、高密度のユーザセッションの効率性を備えた Windows 10 Enterprise 環境が実現します。

- FSLogix のプロファイルには ' ユーザー・セッションのパフォーマンス ' ストレージ効率の向上 ' 非永続的な環境における Office エクスペリエンスの向上などが含まれます
- AVD では、デスクトップ全体と RemoteApp へのアクセスがサポートされます。永続的または非永続的、および専用とマルチセッションの両方のエクスペリエンス。
- AVD は RDS CAL の必要性に代わる「 Windows 10 Enterprise E3 per User 」を活用し、 Azure でのセッションホスト VM の時間あたりのコストを大幅に削減できるため、組織は Windows ライセンスを節約できます。

ガイドの範囲

このガイドでは、 Azure と VDS の管理者の視点から、ネットアップ VDS テクノロジを使用した AVD の導入手順を説明します。Azure テナントとサブスクリプションは事前構成なしで提供されます。このガイドは、AVD のエンドツーエンドの設定を支援します

このガイドでは、次の手順について説明します。

1. Azure テナント、 Azure サブスクリプション、および Azure 管理者アカウントの権限の前提条件を確認する
2. 必要な検出の詳細を収集します
3. Azure セットアップウィザード専用の VDS を使用して、 Azure 環境を構築します
4. 標準の Windows 10 EVD イメージを使用して、最初のホストプールを作成します
5. Azure AD ユーザへの仮想デスクトップの割り当て
6. ユーザーにデスクトップ環境を提供するために、ユーザーをデフォルトのアプリケーショングループに追加します。 必要に応じて、 RemoteApp サービスを提供するホストプールを追加で作成します
7. クライアントソフトウェアや Web クライアントを介してエンドユーザとして接続します
8. プラットフォームおよびクライアントサービスにローカルおよびドメイン管理者として接続します
9. オプションで 'VDS 管理者および AVD エンド・ユーザーに対して VDS の多要素認証を有効にします
10. オプションで、アプリケーションライブラリ、アプリケーションインストールの自動化、ユーザーやセキュリティグループによるアプリケーションマスキングなど、アプリケーションエンタイトルメントワークフロー全体を順を追って説明します
11. 必要に応じて、 Active Directory セキュリティグループ、フォルダ権限、およびグループごとのアプリケーション使用権を作成および管理します。
12. オプションで、ワークロードのスケジューリングやライブスケーリングなどのコスト最適化テクノロジーを設定できます
13. 必要に応じて、仮想マシンイメージを作成、更新、および Sysprep して、将来の展開に備えます
14. 必要に応じて、 Azure Cloud Backup を設定します
15. 必要に応じて、デフォルトのセキュリティ制御グループポリシーを無効にします

Azure の前提条件

VDS では、ネイティブの Azure セキュリティコンテキストを使用して AVD インスタンスを導入します。VDS セットアップウィザードを開始する前に、いくつかの Azure の前提条件を確立する必要があります。

導入時に、 Azure テナント内から既存の管理者アカウントを認証することで、サービスアカウントと権限が VDS に付与されます。

クイック前提条件チェックリスト

- Azure AD インスタンスを使用する Azure テナント（ Microsoft 365 インスタンスも可）
- Azure サブスクリプション
- Azure 仮想マシンに使用可能な Azure クォータ
- グローバル管理者ロールおよびサブスクリプション所有権ロールを持つ Azure Admin アカウント

詳細な前提条件については、を参照してください "この PDF"

Azure AD の **Azure** 管理者

この既存の Azure 管理者は、ターゲットテナント内の Azure AD アカウントである必要があります。VDS セットアップで Windows Server AD アカウントを導入することはできますが、 Azure AD との同期をセットアップするには追加の手順が必要です（このガイドでは対象外）。

これを確認するには、 Azure Management Portal で「 Users 」 > 「 All Users 」の下にあるユーザアカウントを検索します。[]

グローバル管理者ロール

Azure Administrator には、 Azure テナント内のグローバル管理者ロールが割り当てられている必要があります。

Azure AD での役割を確認するには、次の手順を実行します。

1. Azure ポータルにログインします https://portal.azure.com/
2. Azure Active Directory を検索して選択します
3. 右側の次のペインで、 [管理] セクションの [ユーザー] オプションをクリックします
4. チェックする管理者ユーザの名前をクリックします
5. [ディレクトリの役割] をクリックします。右端のペインに、グローバル管理者ロールが表示されます[]

このユーザにグローバル管理者ロールがない場合は、次の手順を実行して追加できます（ログインしたアカウントはグローバル管理者である必要があります）。

1. 上記のステップ 5 のユーザーディレクトリロール詳細ページで、詳細ページの上部にある割り当ての追加ボタンをクリックします。
2. ロールのリストで [グローバル管理者（ Global administrator ）] をクリックします。[追加] ボタンをクリックします。[]

Azure サブスクリプションの所有権

Azure Administrator は、導入を含むサブスクリプションのサブスクリプション所有者でもある必要があります。

管理者がサブスクリプションオーナーであることを確認するには、次の手順を実行します。

1. Azure ポータルにログインします https://portal.azure.com/
2. を検索し、 [購読] を選択します
3. 右側のペインで、サブスクリプション名をクリックすると、サブスクリプションの詳細が表示されます

4. 左側のペインで、 Access Control （ IAM ）メニュー項目をクリックします
5. [役割の割り当て] タブをクリックします。Azure 管理者は、所有者セクションに記載する必要があります。[]

Azure Administrator が表示されていない場合は、次の手順に従って、アカウントをサブスクリプション所有者として追加できます。

1. ページ上部の [追加] ボタンをクリックし、 [役割の割り当ての追加] オプションを選択します
2. 右側にダイアログが表示されます。ロールのドロップダウンで [Owner] を選択し、 [Select] ボックスに管理者のユーザ名を入力します。Administrator のフルネームが表示されたら、それを選択します
3. ダイアログの下部にある [保存（ Save ）] ボタンをクリックします[]

Azure コンピューティングコアクォータ

CWA セットアップウィザードと VDS ポータルで新しい仮想マシンが作成されます。 Azure サブスクリプションを正常に実行するには、使用可能なクォータが必要です。

クォータを確認するには、次の手順を実行します。

1. [購読] モジュールに移動し '[使用量 + クォータ] をクリックします
2. 「 Providers 」ドロップダウンですべてのプロバイダーを選択し、「 Providers 」ドロップダウンで「 Microsoft.Compute 」を選択します
3. [Locations] ドロップダウンからターゲット領域を選択します
4. 仮想マシンファミリ別の使用可能なクォータのリストが表示されます[]クォータを増やす必要がある場合は、 [Request add] をクリックし、プロンプトに従って容量を追加します。初期導入の場合 ' 特に標準 DSVI 3 ファミリの拡張見積もりを要求します

検出の詳細を収集

CWA セットアップウィザードを使用して作業したら、いくつかの質問に答えてください。NetApp VDS では、導入前にこれらの選択を記録できるリンク PDF が提供されています。アイテムには次のものが

項目	説明
VDS 管理者クレデンシャル	既存の VDS 管理者クレデンシャルがある場合は、それらを収集します。それ以外の場合は、導入時に新しい管理者アカウントが作成されます。
Azure リージョン	サービスのパフォーマンスと可用性に基づいて、対象となる Azure リージョンを特定します。これ "Microsoft ツール" 地域に基づいてエンドユーザーの経験を推定できます。
Active Directory タイプ	VM はドメインに参加する必要がありますが、 Azure AD に直接参加することはできません。VDS 環境では、新しい仮想マシンを作成するか、既存のドメインコントローラを使用できます。

項目	説明
File Management の略	パフォーマンスは、特にユーザプロファイルストレージに関連するディスク速度に大きく依存します。VDS セットアップウィザードでは、シンプルなファイルサーバを導入したり、 Azure NetApp Files （ ANF ）を設定したりできます。ほとんどの本番環境では ANF を推奨しますが、 POC ではファイルサーバオプションで十分なパフォーマンスを実現できます。ストレージオプションについて、 Azure で既存のストレージリソースを使用するなど、導入後に改定することができます。詳細については、 ANF の価格設定を参照してください https://azure.microsoft.com/en-us/pricing/details/netapp/
仮想ネットワークのスコープ	導入には、ルーティング可能な /20 ネットワーク範囲が必要です。VDS セットアップウィザードでは、この範囲を定義できます。この範囲は、Azure またはオンプレミスの既存の VNet と重複しないことが重要です（ 2 つのネットワークが VPN または ExpressRoute 経由で接続される場合）。

VDS セットアップセクション

にログインします https://cwasetup.cloudworkspace.com/ 前提条件のセクションに記載されている Azure 管理者のクレデンシャルを使用してログイン

IaaS とプラットフォーム

[]

Azure AD ドメイン名

Azure AD ドメイン名は、選択したテナントに継承されます。

場所

適切な **Azure** リージョン を選択します。これ "Microsoft ツール" 地域に基づいてエンドユーザーの経験を推定できます。

Active Directory タイプ

VDS は、ドメインコントローラ機能用の 新しい仮想マシン でプロビジョニングすることも、既存のドメインコントローラを利用するようにセットアップすることもできます。このガイドでは、新規 Windows Server Active Directory を選択します。これにより、サブスクリプションの下に 1 つまたは 2 つの VM が作成されます（このプロセスで選択した内容に基づいて）。

既存の AD 展開に関する詳細な記事を参照してください "こちらをご覧ください"。

Active Directory ドメイン名

- ドメイン名 ** を入力してください。Azure AD ドメイン名は上記からミラーリングすることを推奨します。

ファイル管理

VDS では、単純なファイルサーバ仮想マシンをプロビジョニングしたり、 Azure NetApp Files をセットアッ

プおよび設定したりできます。本番環境では、ユーザーごとに 30GB を割り当てることをお勧めします。また、最適なパフォーマンスを得るには、ユーザーごとに 5-15 の IOPS を割り当てる必要があることを確認しました。

POC （非本番環境）では、ファイルサーバは低コストでシンプルな導入オプションですが、 Azure Managed Disks の利用可能なパフォーマンスは、小規模な本番環境でも IOPS 消費に圧倒されることがあります。

たとえば、 Azure 内の 4TB 標準 SSD ディスクは最大 500 IOPS をサポートし、最大 100 ユーザの IOPS を 5 ユーザあたりサポートします。ANF Premium では、同じサイズのストレージセットアップで、 32 倍以上の IOPS 転記で 1 万 6 、 000 IOPS をサポートします。

本番環境の AVD 展開では、 **Microsoft** の推奨事項 として Azure NetApp Files が推奨されています。

> Azure NetApp Files を導入するサブスクリプションで利用できるようにする必要があります。ネットアップアカウント担当者にお問い合わせいただくか、 https://aka.ms/azurenetappfiles にアクセスしてください

また、ネットアップをプロバイダとして登録する必要があります。これを行うには、次の手順を実行します。

- Azure ポータルのサブスクリプションに移動します
  - [リソースプロバイダ] をクリックします
  - ネットアップをフィルタリング
  - プロバイダーを選択して、 [登録] をクリックします

RDS ライセンス番号

NetApp VDS を使用して、 RDS 環境や AVD 環境を導入できます。AVD を展開する場合、このフィールドは空 のままにすることができます。

ThinPrint

NetApp VDS を使用して、 RDS 環境や AVD 環境を導入できます。AVD を展開するときに、この切り替えは **off** （左に切り替え）のままにできます。

通知 **E** メール

VDS では、展開通知と継続的な正常性レポートが、提供された ** メールに送信されます。これはあとで変更できます。

VM およびネットワーク

VDS 環境をサポートするために実行する必要があるさまざまなサービスがあります。これらは総称して「 VDS プラットフォーム」と呼ばれます。これらの設定には、 CWMGR 、 1 つまたは 2 つの RDS ゲートウェイ、 1 つまたは 2 つの HTML5 ゲートウェイ、 FTPS サーバ、および 1 つまたは 2 つの Active Directory VM が含まれます。

ほとんどの AVD 展開では、単一の仮想マシンオプションが使用されています。 Microsoft は AVD ゲートウェイを PaaS サービスとして管理しています。

RDS のユースケースを含む小規模でシンプルな環境では、これらのサービスをすべて 1 つの仮想マシンオプションに集約して、 VM コストを削減できます（拡張性に限りがあります）。100 人以上のユーザが使用する

RDS では、 RDS や HTML5 ゲートウェイの拡張性を高めるために、複数の仮想マシンを選択することを推奨します[]

プラットフォーム **VM** の構成

NetApp VDS を使用して、 RDS 環境や AVD 環境を導入できます。AVD を展開する場合は、シングル仮想マシンの選択を推奨します。RDS 展開では、ブローカーやゲートウェイなどの追加コンポーネントを展開して管理する必要があります。これらのサービスは、本番環境では専用の冗長仮想マシン上で実行する必要があります。AVD の場合、これらのサービスはすべて Azure によってサービスとして提供されるため、 シングル仮想マシン 構成が推奨されます。

単一の仮想マシン

AVD のみを使用する（ RDS または 2 つの組み合わせは使用しない）配置には、このオプションを選択することをお勧めします。単一の仮想マシン環境では、 Azure の単一の VM で次のロールがホストされます。

- CW Manager の略
- HTML5 ゲートウェイ
- RDS ゲートウェイ
- リモートアプリ
- FTPS サーバ（オプション）
- ドメインコントローラの役割

このコンフィグレーションで推奨される RDS 使用事例の最大ユーザー数は 100 ユーザーです。この構成では、ロードバランシングが行われた RDS+ HTML5 ゲートウェイはオプションではないため、冗長性が制限されるだけでなく、将来的に拡張性を高めるためのオプションも制限されます。ここでも、 Microsoft はゲートウェイを PaaS サービスとして管理しているため、 AVD の導入にはこの制限は適用されません。

この環境がマルチテナンシー用に設計されている場合、単一の仮想マシン構成はサポートされません。 AVD も AD Connect もサポートされません。

複数の仮想マシン

VDS プラットフォームを複数の仮想マシンに分割する場合、 Azure の専用 VM で次の役割がホストされます。

- リモートデスクトップゲートウェイ

  VDS セットアップを使用して、 1 つまたは 2 つの RDS ゲートウェイを展開および設定できます。これらのゲートウェイは、オープンインターネットから、導入環境内のセッションホスト VM への RDS ユーザセッションをリレーします。RDS ゲートウェイは重要な機能を処理し、 RDS をオープンインターネットからの直接攻撃から保護し、環境内のすべての RDS トラフィックを暗号化します。2 つのリモートデスクトップゲートウェイが選択されている場合、 VDS セットアップは 2 つの VM を展開し、着信 RDS ユーザーセッションをロードバランシングするように設定します。

- HTML5 ゲートウェイ

  VDS セットアップを使用して、 1 つまたは 2 つの HTML5 ゲートウェイを導入および設定できます。これらのゲートウェイは、 VDS の Server_feature への _ 接続と Web ベースの VDS クライアント（ H5 ポータル）で使用される HTML5 サービスをホストします。2 つの HTML5 ポータルを選択すると、 VDS セッ

トアップによって 2 つの VM が導入され、受信する HTML5 ユーザセッションの負荷を分散するように設定されます。

> 複数サーバオプションを使用する場合（インストールされている VDS クライアントのみを介して接続する場合でも） VDS から Server_Functionality への _ 接続を有効にすることを推奨します。

- 『 Gateway Scalability Notes 』

  RDS のユースケースでは、追加のゲートウェイ VM を使用して環境の最大サイズをスケールアウトでき、 RDS または HTML5 ゲートウェイは約 500 ユーザをサポートします。ゲートウェイの追加は、ネットアッププロフェッショナルサービスによるサポートが最小限で済むため、後で追加できます

この環境がマルチテナンシー用に設計されている場合は、仮想マシンを複数選択する必要があります。

タイムゾーン

エンドユーザのエクスペリエンスにはローカルタイムゾーンが反映されますが、デフォルトのタイムゾーンを選択する必要があります。環境の プライマリ管理 を実行するタイムゾーンを選択します。

仮想ネットワークのスコープ

VM をそれぞれの目的に応じて別のサブネットに分離することを推奨します。まず、ネットワークスコープを定義し、 /20 範囲を追加します。

VDS セットアップは、検出して、成功したことを示す範囲を提案します。ベストプラクティスに従い、サブネット IP アドレスはプライベート IP アドレス範囲にする必要があります。

範囲は次のとおりです。

- 192.168.0.0 ～ 192.168.255.255
- 172.16.0.0 ～ 172.31.255.255
- 10.0.0.0 ～ 10.255.255.255

必要に応じて確認と調整を行い、 [検証] をクリックして、次のそれぞれのサブネットを特定します。

- tenant ：セッションホストサーバとデータベースサーバが配置される範囲です
- サービス： Azure NetApp Files のような PaaS サービスが提供される範囲です
- プラットフォーム : プラットフォームサーバーが存在する範囲です
- ディレクトリ： AD サーバが配置される範囲です

レビュー

最後のページでは、選択内容を確認することができます。レビューが完了したら、 [検証（ Validate ）] ボタンをクリックします。VDS セットアップですべてのエントリが確認され、導入環境が提供された情報を続行できることが確認されます。この検証には 2~10 分かかることがあります。進捗状況を確認するには、ログのロゴ（右上）をクリックして検証アクティビティを確認します。

検証が完了すると、 [Validate] ボタンの代わりに緑色の [Provision （プロビジョニング）] ボタンが表示され

ます。Provision （プロビジョニング）をクリックして、導入のプロビジョニングプロセスを開始します。

ステータス

プロビジョニングプロセスにかかる時間は、 Azure のワークロードと選択内容によって異なり、 2 ～ 4 時間です。ステータスページをクリックするか、導入プロセスが完了したことを示す E メールを待つことで、ログの進捗状況を確認できます。導入環境では、 VDS とリモートデスクトップ、または AVD の両方の実装をサポートするために必要な仮想マシンと Azure コンポーネントが構築されます。これには、リモートデスクトップセッションホストとファイルサーバの両方として機能する単一の仮想マシンが含まれます。AVD 実装では、この仮想マシンはファイルサーバとしてのみ動作します。

AD Connect をインストールして設定します

インストールが正常に完了した直後に、 AD Connect をドメインコントローラにインストールして構成する必要があります。単一プラットフォーム VM のセットアップでは、 CWMGR1 マシンが DC です。AD 内のユーザは、 Azure AD とローカルドメインを同期する必要があります。

AD Connect をインストールして設定するには、次の手順を実行します。

1. ドメイン管理者としてドメインコントローラに接続します。
    a. Azure Key Vault からクレデンシャルを取得します（を参照） "ここに記載されているキー・ボールト"）
2. AD Connect をインストールし、ドメイン admin （ Enterprise Admin ロールの権限を持つ）および Azure AD Global Admin でログインします

AVD サービスをアクティブ化しています

導入が完了したら、次の手順で AVD 機能を有効にします。AVD を有効にするには、 Azure Administrator が Azure AVD サービスを使用して Azure AD ドメインとサブスクリプションを登録し、アクセスできるようにする必要があります。同様に、 Microsoft では、 Azure で自動化アプリケーション用に同じ権限を VDS から要求する必要があります。以下の手順で、そのプロセスを説明します。

AVD ホストプールを作成します

AVD 仮想マシンへのエンドユーザアクセスは、仮想マシンを含むホストプールとアプリケーショングループによって管理され、アプリケーショングループにはユーザとユーザアクセスのタイプが含まれます。

をクリックして、最初のホストプールを作成します

1. AVD ホストプールセクションのヘッダーの右側にある追加ボタンをクリックします。[]
2. ホストプールの名前と概要を入力します。
3. ホストプールタイプを選択します
    a. プール 複数のユーザーが同じアプリケーションがインストールされている仮想マシンの同じプールにアクセスすることを意味します。
    b. パーソナル ユーザに独自のセッションホスト VM が割り当てられるホストプールを作成します。
4. ロードバランサのタイプを選択します
    a. 第 **1** の深さ は、プール内の第 2 の仮想マシンで開始する前に、最初の共有仮想マシンを最大ユーザー数まで満たします
    b. まず、その幅 では、プール内のすべての仮想マシンにユーザーがラウンドロビン方式で配布されます

5. このプールで仮想マシンを作成するための Azure 仮想マシンテンプレートを選択します。VDS では、サブスクリプションで使用可能なすべてのテンプレートが表示されますが、ベストなエクスペリエンスを得るために最新の Windows 10 マルチユーザービルドを選択することをお勧めします。現在のビルドは Windows-10-20h1-EVD です。（必要に応じて、 Provisioning Collection 機能を使用してゴールドイメージを作成し、カスタム仮想マシンイメージからホストを作成）
6. Azure マシンサイズを選択します。評価を実施するためには、 D シリーズ（マルチユーザの場合は標準のマシンタイプ）または E シリーズ（負荷の高いマルチユーザシナリオの場合は拡張メモリ構成）を推奨します。シリーズやサイズを変えて試す場合は、 VDS で後からマシンサイズを変更できます
7. ドロップダウンリストから、仮想マシンの管理対象ディスクインスタンスに対応するストレージタイプを選択します
8. ホストプールの作成プロセスで作成する仮想マシンの数を選択します。あとでプールに仮想マシンを追加できますが、 VDS で要求した仮想マシンの数が構築され、作成後にホストプールに追加されます
9. ホストプールの追加ボタンをクリックして、作成プロセスを開始します。AVD ページで進捗状況を追跡することも、 [タスク] セクションの [展開 / 展開名] ページでプロセスログの詳細を確認することもできます
10. ホストプールが作成されると、 AVD ページのホストプールリストに表示されます。ホストプールの名前をクリックすると、その詳細ページが表示されます。このページには、仮想マシン、アプリケーショングループ、およびアクティブユーザのリストが含まれます

VDS 内の AVD ホストは、ユーザーセッションの接続を許可しない設定で作成されます。これは、ユーザ接続を受け入れる前にカスタマイズできるように設計されています。この設定は、セッションホストの設定を編集することで変更できます。 []

ユーザの **VDS** デスクトップを有効にします

前述したように 'VDS は導入時にエンドユーザーのワークスペースをサポートするために必要なすべての要素を作成します展開が完了したら、次の手順では、 AVD 環境に導入するユーザーごとにワークスペースへのアクセスを有効にします。この手順では、仮想デスクトップのデフォルトであるプロファイル設定とエンドユーザデータレイヤアクセスが作成されます。VDS は、 Azure AD エンドユーザーを AVD アプリケーションプールにリンクするために、この構成を再利用します。

エンドユーザーのワークスペースを有効にするには、次の手順を実行します。

1. VDS にログインします https://manage.cloudworkspace.com プロビジョニング時に作成した VDS プライマリ管理者アカウントを使用する。アカウント情報を覚えていない場合は、 NetApp VDS に問い合わせて情報を取得してください
2. [ワークスペース] メニューアイテムをクリックし、プロビジョニング時に自動的に作成されたワークスペースの名前をクリックします
3. [ユーザーとグループ] タブをクリックします[]
4. 有効にする各ユーザについて、ユーザ名をスクロールし、歯車アイコンをクリックします
5. [Enable Cloud Workspace] オプションを選択します[]
6. 有効化プロセスが完了するまで、 30~90 秒かかります。ユーザのステータスが [保留中] から [使用可能] に変わります

Azure AD ドメインサービスをアクティブ化すると、 Azure で管理ドメインが作成され、作成された AVD 仮想マシンがそのドメインに参加します。仮想マシンへの従来のログインを使用するには、 Azure AD ユーザのパスワードハッシュを同期して、 NTLM 認証と Kerberos 認証をサポートする必要があります。このタスクを実行する最も簡単な方法は、 Office.com または Azure Portal でユーザパスワードを変更することです。これにより、パスワードハッシュの同期が強制的に行われます。ドメインサービスサーバの同期サイクルには、最大 20 分かかることがあります。

ユーザセッションを有効にします

デフォルトでは、セッションホストはユーザ接続を受け入れることができません。この設定は、新しいユーザセッションを防止するために本番環境で使用できる「ドレインモード」と呼ばれ、最終的にホストはすべてのユーザセッションを削除できます。新しいユーザセッションがホストで許可される場合、このアクションは通常、セッションホストを「ローテーションに」配置することと呼ばれます。

本番環境では、新しいホストをドレインモードで開始することを推奨します。ホストが本番環境のワークロードに対応できるようになる前に、通常は設定タスクを実行する必要があるためです。

テストと評価では、ホストのドレインモードをすぐに解除して、ユーザが接続できるようにし、機能を確認できるようにすることができます。セッションホストでユーザーセッションを有効にするには ' 次の手順に従います

1. ワークスペースページの AVD セクションに移動します。
2. [AVD host pools] の下のホストプール名をクリックします。[]
3. セッションホストの名前をクリックし、 [新しいセッションを許可する] チェックボックスをオンにして、 [セッションホストの更新] をクリックします。ローテーションに配置する必要があるすべてのホストについて、この手順を繰り返します。[]
4. 各ホスト行項目の AVD のメインページには、「 Allow New Session 」の現在の統計も表示されます。

デフォルトのアプリケーショングループ

デスクトップアプリケーショングループは、ホストプール作成プロセスの一環としてデフォルトで作成されます。このグループは、すべてのグループメンバーにインタラクティブなデスクトップアクセスを提供します。グループにメンバーを追加するには：

1. アプリケーショングループの名前をクリックします[]
2. 追加したユーザの数を示すリンクをクリックします[]
3. 名前の横にあるチェックボックスをオンにして、アプリケーショングループに追加するユーザーを選択します
4. [ユーザーの選択] ボタンをクリックします
5. アプリグループを更新ボタンをクリックします

追加の **AVD** アプリグループを作成

追加のアプリケーショングループをホストプールに追加できます。これらのアプリケーショングループは、RemoteApp を使用して、ホストプール仮想マシンから App Group ユーザに特定のアプリケーションを公開します。

AVD では、エンドユーザーをデスクトップアプリグループタイプまたは RemoteApp グループタイプにのみ割り当てることができます。ただし、両方を同じホストプールに含めることはできません。そのため、ユーザーを適切に分離するようにしてください。ユーザーがデスクトップおよびストリーミングアプリにアクセスする必要がある場合は、アプリをホストするために 2 番目のホストプールが必要です。

新しいアプリケーショングループを作成するには：

1. アプリケーショングループセクションのヘッダーにある追加ボタンをクリックします[]
2. アプリケーショングループの名前と概要を入力します
3. [Add Users] リンクをクリックして、グループに追加するユーザを選択します。名前の横にあるチェックボックスをクリックして各ユーザを選択し、 [Select Users] ボタンをクリックします[]
4. [Add RemoteApps] リンクをクリックして、このアプリケーショングループにアプリケーションを追加します。AVD は、仮想マシンにインストールされているアプリケーションのリストをスキャンすることで、可能なアプリケーションのリストを自動的に生成します。アプリケーション名の横にあるチェックボックスをクリックしてアプリケーションを選択し、 Select RemoteApps ボタンをクリックします。[]
5. [アプリケーショングループの追加] ボタンをクリックして、アプリケーショングループを作成します

エンドユーザ **AVD** アクセス

エンドユーザは、 Web Client またはさまざまなプラットフォーム上にインストールされたクライアントを使用して AVD 環境にアクセスできます

- Web クライアント： https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-web
- Web クライアントのログイン URL ： http://aka.ms/AVDweb
- Windows クライアント： https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-windows-7-and-10
- Android クライアント： https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-android
- MacOS クライアント : https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-macos
- iOS クライアント： https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-ios
- IGEL シンクライアント： https://www.igel.com/igel-solution-family/windows-virtual-desktop/

エンドユーザのユーザ名とパスワードを使用してログインします。リモートアプリケーションとデスクトップ接続（ RADC ）、リモートデスクトップ接続（ mstsc ）、および CloudWorksapce クライアント for Windows アプリケーションは、現在、 AVD インスタンスへのログイン機能をサポートしていません。

ユーザログインを監視する

また、ホストプールの詳細ページには、 AVD セッションにログインしたときにアクティブなユーザのリストも表示されます。

管理接続オプション

VDS 管理者は、さまざまな方法で環境内の仮想マシンに接続できます。

サーバに接続します

ポータル全体で 'VDS 管理者は [サーバへの接続] オプションを見つけますデフォルトでは、この機能は、ローカル管理者クレデンシャルを動的に生成し、 Web クライアント接続に挿入することによって、管理者を仮想マシンに接続します。接続するために Admin がクレデンシャルを知っている必要はありません（また、で提供されることはありません）。

このデフォルト動作は、次のセクションで説明するように、管理者ごとに無効にすることができます。

.tech/Level 3 管理者アカウント

CWA セットアッププロセスでは、「 Level III 」管理者アカウントが作成されます。ユーザ名の形式は username.tech@domain.xyz です

これらのアカウントは、一般に「 .tech 」アカウントと呼ばれ、ドメインレベルの管理者アカウントという名前が付けられています。VDS 管理者は、 CWMGR1 （プラットフォーム）サーバに接続するとき、および環境内の他のすべての仮想マシンに接続するときに、 .tech アカウントを使用できます。

自動ローカル管理ログイン機能を無効にして、レベル III アカウントを強制的に使用するには、この設定を変更します。VDS > Admins > Admin Name > Check "Tech Account Enabled" と進みます。 このチェックボックスをオンにすると 'VDS 管理者は自動的にローカル管理者として仮想マシンにログインせず ' その .tech 資格情報を入力するように求められます

これらのクレデンシャルおよびその他の関連するクレデンシャルは、自動的に _Azure Key Vault に格納され、 Azure Management Portal のからアクセスできます https://portal.azure.com/。

オプションの導入後の操作

多要素認証（ **MFA** ）

NetApp VDS には、 SMS/E メール MFA が無料で含まれます。この機能を使用して 'VDS 管理者アカウントやエンドユーザーアカウントを保護できます"MFA 記事"

アプリケーション使用権のワークフロー

VDS では、アプリケーションカタログと呼ばれる定義済みのアプリケーションリストから、エンドユーザーにアプリケーションへのアクセスを割り当てるメカニズムが提供されます。アプリケーションカタログは、管理されたすべての展開に適用されます。

自動的に導入された TSD1 サーバーは、アプリケーションのエンタイトルメントをサポートするために現状のままにしておく必要があります。具体的には、この仮想マシンに対して「データへの変換」機能を実行しないでください。

アプリケーション管理の詳細については、次の記事を参照してください。 ""

Azure AD セキュリティグループ

VDS には、 Azure AD セキュリティグループによってサポートされるユーザーグループを作成、入力、および削除する機能が含まれます。これらのグループは 'VDS 以外のセキュリティグループと同様に使用できますVDS では、これらのグループを使用してフォルダ権限とアプリケーション権限を割り当てることができます。

ユーザグループを作成します

ユーザーグループの作成は、ワークスペース内のユーザーとグループタブで実行されます。

フォルダ権限をグループごとに割り当てます

会社の共有内のフォルダを表示および編集する権限は、ユーザーまたはグループに割り当てることができます。

""

グループごとにアプリケーションを割り当てます

アプリケーションをユーザに個別に割り当てるだけでなく、グループにプロビジョニングすることもできます。

1. [ユーザーとグループの詳細] に移動します。[]
2. 新しいグループを追加するか、既存のグループを編集します。[]
3. グループにユーザとアプリケーションを割り当てます。[]

コスト最適化オプションを設定します

ワークスペース管理は、 AVD 実装をサポートする Azure リソースの管理にも拡張されています。VDS では、ワークロードスケジュールとライブスケーリングの両方を設定し、エンドユーザーのアクティビティに基づいて Azure 仮想マシンのオンとオフを切り替えることができます。これらの機能により、 Azure のリソース利用率とエンドユーザの実際の使用パターンに合わせた支出が実現します。さらに、概念実証 AVD 実装を設定している場合は、 VDS インターフェイスから導入全体を切り替えることができます。

ワークロードのスケジュール設定

ワークロードスケジューリングは、管理者が、エンドユーザセッションをサポートするために Workspace 仮想マシンを実行するスケジュールを作成できるようにする機能です。一定の曜日にスケジュールされた期間の終了に達すると、 VDS は 1 時間ごとの課金が停止するように Azure 内の仮想マシンの割り当てを停止または解除します。

ワークロードのスケジュール設定を有効にするには

1. VDS にログインします https://manage.cloudworkspace.com VDS クレデンシャルを使用します。
2. [ワークスペース] メニューアイテムをクリックし、リスト内のワークスペースの名前をクリックします。 []
3. [ワークロードのスケジュール] タブをクリックします。 []
4. [ワークロードスケジュール] ヘッダーの [管理] リンクをクリックします。 []
5. [ステータス] ドロップダウンから、 [常にオン]（デフォルト）、 [常にオフ] 、または [スケジュール済み] のいずれかのデフォルトの状態を選択します。
6. [スケジュール済み] を選択した場合は、次のスケジュールオプションがあります。
   a. 毎日、割り当てられた間隔で実行します。このオプションは、スケジュールを週 7 日すべて同じ開始時間と終了時間に設定します。 []
   b. 指定した日に割り当てられた間隔で実行します。このオプションでは、選択した曜日についてのみ、同じ開始タイおよび終了時間にスケジュールを設定します。曜日を選択しないと、原因 VDS で仮想マ

シンがオンにならないようになります。 []

c. 時間間隔や日数を変更して実行します。このオプションを選択すると、選択した各曜日の開始時刻と終了時刻が異なるスケジュールに設定されます。 []

d. スケジュールの設定が完了したら、 Update schedule （スケジュールの更新）ボタンをクリックします。 []

ライブスケーリング

ライブスケーリングでは、ユーザーの同時負荷に応じて、共有ホストプール内の仮想マシンを自動的にオンまたはオフに切り替えます。各サーバがいっぱいになると、ホストプールのロードバランサがユーザセッション要求を送信するときに使用できるように、追加のサーバがオンになります。ライブスケーリングを効果的に使用するには、ロードバランサータイプとして [深度優先] を選択します。

ライブスケーリングを有効にするには：

1. VDS にログインします https://manage.cloudworkspace.com VDS クレデンシャルを使用します。
2. [ワークスペース] メニューアイテムをクリックし、リスト内のワークスペースの名前をクリックします。 []
3. [ワークロードのスケジュール] タブをクリックします。 []
4. Live Scaling セクションで、 Enabled オプションボタンをクリックします。 []
5. [サーバあたりの最大ユーザ数] をクリックし、最大数を入力します。仮想マシンのサイズに応じて、通常は 4~20 の範囲の値を指定します。 []
6. オプション– [Extra Powered On Servers Enabled] をクリックし、ホストプール用に追加するサーバをいくつか入力します。この設定は、アクティブにいっぱいになっているサーバーに加えて、指定されたサーバー数をアクティブにして、同じ時間内にログオンしている大量のユーザーグループのバッファとして機能します。 []

現在、ライブスケーリングはすべての共有リソースプールを環境で実行しています。近い将来、各プールには独立したライブスケーリングオプションがあります。

導入環境全体の電源をオフにします

評価導入のみを散発的な非本番環境でのみ使用する場合は、使用しない環境ですべての仮想マシンをオフにすることができます。

展開をオンまたはオフにする（展開で仮想マシンをオフにする）には、次の手順を実行します。

1. VDS にログインします https://manage.cloudworkspace.com VDS クレデンシャルを使用します。
2. [展開] メニュー項目をクリックします。 []ターゲット展開の行にカーソルを合わせると、設定ギアアイコンが表示されます。 []
3. ギアをクリックし、「停止」を選択します。 []
4. 再起動または開始するには、手順 1 ～ 3 を実行してから、 [開始] を選択します。 []

導入環境内のすべての仮想マシンが停止または起動するまでに数分かかることがあります。

VM イメージの作成と管理

VDS には、将来の導入に備えて仮想マシンイメージを作成および管理する機能が含まれます。この機能を使用するには、 VDS > Deployments > Deployment Name > Provisioning Collections に移動します。「 VDI イメージコレクション」の機能については、次の URL で説明しています。 ""

Azure Cloud Backup Service を設定

VDS は、 Azure クラウドバックアップをネイティブで構成、管理できます。 Azure PaaS サービスは、仮想マシンをバックアップするためのサービスです。バックアップポリシーは、タイプまたはホストプールに基づいて、個々のマシンまたはマシンのグループに割り当てることができます。詳細については、以下を参照してください。 ""

アプリ管理 / ポリシーモードを選択します

VDS では、デフォルトで多数の Group Policy Object （ GPO ；グループポリシーオブジェクト）が実装され、エンドユーザのワークスペースがロックダウンされます。これらのポリシーにより、コアデータレイヤの場所（例： c ：\）へのアクセスと、エンドユーザとしてのアプリケーションのインストールを実行する機能の両方にアクセスできなくなります。

この評価は、 Window Virtual Desktop の機能を実証することを目的としています。したがって、 GPO を削除して、物理ワークスペースと同じ機能とアクセスを提供する「基本的なワークスペース」を実装できます。これを行うには、「基本ワークスペース」オプションの手順に従います。

また、仮想デスクトップ管理の全機能セットを利用して「管理されたワークスペース」を実装することもできます。これらの手順には、エンドユーザアプリケーションエンタイトルメント用のアプリケーションカタログの作成と管理、およびアプリケーションとデータフォルダへのアクセスを管理するための管理者レベルの権限の使用が含まれます。AVD ホストプールにこのタイプのワークスペースを実装するには、「管理されたワークスペース」セクションの手順に従います。

制御された AVD ワークスペース (デフォルトポリシー)

VDS 導入では、制御されたワークスペースを使用することがデフォルトモードです。ポリシーは自動的に適用されます。このモードでは、 VDS 管理者がアプリケーションをインストールする必要があります。その後、エンドユーザーはセッションデスクトップのショートカットを使用してアプリケーションにアクセスできます。同様に、マッピングされた共有フォルダを作成し、標準のブートドライブやデータドライブではなく、マッピングされたドライブレターのみを表示する権限を設定することで、データフォルダへのアクセスがエンドユーザに割り当てられます。この環境を管理するには、以下の手順に従って、アプリケーションをインストールし、エンドユーザーアクセスを提供します。

基本的な AVD ワークスペースに戻します

基本的なワークスペースを作成するには、デフォルトで作成されたデフォルトの GPO ポリシーを無効にする必要があります。

これを行うには、次の 1 回限りのプロセスを実行します。

1. VDS にログインします https://manage.cloudworkspace.com プライマリ管理者のクレデンシャルを使用する。
2. 左側の [Deployments] メニュー項目をクリックします。 []
3. 展開の名前をクリックします。 []
4. [Platform Servers] セクション（右中央ページ）で、 CWMGR1 の行の右側をスクロールしてギヤを表示し

ます。 []

5. ギアをクリックして、「接続」を選択します。 []
6. プロビジョニング中に作成した「 Tech 」クレデンシャルを入力し、 HTML5 アクセスを使用して CWMGR1 サーバにログオンします。 []
7. スタート（ Windows ）メニューをクリックし、 Windows 管理ツールを選択します。 []
8. [グループポリシーの管理] アイコンをクリックします。 []
9. 左側のペインのリストで AADDC Users 項目をクリックします。 []
10. 右側のペインのリストで [Cloud Workspace Users （クラウドワークスペースユーザー）] ポリシーを右クリックし、 [Link Enabled （リンク有効）] オプションの選択を解除します。[OK] をクリックして、この操作を確定します。 [] []
11. メニューから [アクション] 、 [グループポリシーの更新] を選択し、それらのコンピュータでポリシーの更新を強制することを確認します。 []
12. 手順 9 と 10 を繰り返しますが、リンクを無効にするポリシーとして [AADDC Users] と [Cloud Workspace Companies （クラウドワークスペース企業）] を選択します。この手順の後で、グループポリシーを強制的に更新する必要はありません。 [] []
13. グループポリシー管理エディタおよび管理ツールウィンドウを閉じ、ログオフします。 []ここでは、エンドユーザー向けの基本的なワークスペース環境について説明します。これを確認するには、エンドユーザーアカウントの 1 つとしてログインします。セッション環境には、非表示の [スタート] メニュー、 C ： \ ドライブへのロックダウンアクセス、非表示の [コントロールパネル] など、制御されたワークスペースの制限はありません。

> 導入時に作成された .tech アカウントには 'VDS に関係なく ' アプリケーションをインストールし ' フォルダのセキュリティを変更するためのフルアクセス権がありますただし、 Azure AD ドメインのエンドユーザに同様のフルアクセスを許可する場合は、各仮想マシンのローカル管理者グループに追加する必要があります。

AVD 展開ガイド - 既存の AD 補足

概要

VDS セットアップでは、新しい導入環境を既存の AD 構造に接続できます。これらの手順では、このオプションについて詳しく説明します。この資料はスタンドアロンではなく、で説明している [新しい AD] オプションの代わりとなる詳細な説明です "AVD 導入ガイド"

Active Directory タイプ

次のセクションでは 'VDS 配備の Active Directory 配備タイプを定義しますこのガイドでは、既存の Windows Server Active Directory を選択します。これは、すでに存在する AD 構造を利用します。

既存の AD ネットワーク

VDS セットアップでは、既存の AD 構造と Azure AD の間の接続を表す vNet のリストが表示されます。選択する VNet には、 Azure で設定した Azure ホスト型 DC が必要です。また、 VNet には、 Azure ホスト型 DC で参照されるカスタム DNS 設定があります。

[]

既存の **Active Directory** ドメイン名

使用する既存のドメイン名を入力します。注： Azure Portal の Active Directory モジュールの下にあるドメインは、原因の DNS の問題が原因で使用することはできません。この主な例は、ユーザーがデスクトップ内からその Web サイト（ <yourdomain>.com など）にアクセスできないことです。

既存の **AD** ユーザ名とパスワード

既存の AD 構造を使用した導入を容易にするために必要なクレデンシャルを提供する方法は 3 つあります。

1. Active Directory のドメイン管理者のユーザ名とパスワードを入力します

   これは最も簡単な方法です。導入を容易にするために使用されるドメイン管理者クレデンシャルを提供します。

   

   このアカウントは、 1 回限りの目的で作成でき、導入プロセスが完了すると削除されます。

2. 必要な権限に一致するアカウントを作成します

   この方法では、お客様の管理者が手動で権限構造を作成し、 CloudWorkspaceSVC アカウントのクレデンシャルをここに入力して次に進んでください。

3. 手動での導入プロセス

   権限のあるアカウントプリンシパルが最小の AD アクセスの設定については、 NetApp VDS サポートにお問い合わせください。

次のステップ

この記事では、既存の AD 環境に展開するための固有の手順について説明します。これらの手順が完了したら、標準の導入ガイドに戻ることができます "こちらをご覧ください"。

VDS コンポーネントと権限

AVD および **VDS** セキュリティエンティティとサービス

Azure Virtual Desktop （ AVD ）では、自動化されたアクションを実行するために、 Azure AD とローカル Active Directory の両方にセキュリティアカウントとコンポーネントが必要です。NetApp の Virtual Desktop Service （ VDS ）は、導入プロセス中にコンポーネントとセキュリティ設定を作成し、管理者が AVD 環境を制御できるようにします。このドキュメントでは、両方の環境で関連する VDS アカウント、コンポーネント、およびセキュリティ設定について説明します。

導入の自動化プロセスのコンポーネントと権限は、最終的に導入された環境のコンポーネントとは大きく異なります。このため、この記事は、「導入の自動化」セクションと「導入環境」セクションの 2 つの主要なセクションで構成されています。

[幅 = 75%]

AVD 展開の自動化コンポーネントと権限

VDS 環境では、 Azure とネットアップの複数のコンポーネントとセキュリティ権限を利用して環境とワーク

スペースの両方を実装します。

VDS 導入サービス

エンタープライズアプリケーション

VDS は、テナントの Azure AD ドメインでエンタープライズアプリケーションとアプリケーション登録を利用します。エンタープライズアプリケーションは、 Azure Resource Manager 、 Azure Graph 、および（ AVD Fall Release を使用している場合） AVD API エンドポイントに対する呼び出し用のコンジットであり、 Azure AD インスタンスセキュリティコンテキストから、関連するサービスプリンシパルに付与された委任ロールと権限を使用します。VDS を使用してテナントの AVD サービスの初期化状態に応じて、アプリケーション登録を作成できます。

これらの VM の作成と管理を有効にするために、 VDS は Azure サブスクリプションにいくつかのサポートコンポーネントを作成します。

クラウドワークスペース

これは最初のエンタープライズアプリケーション管理者が同意を得たものであり、 VDS セットアップウィザードの展開プロセスで使用されます。

クラウドワークスペースエンタープライズアプリケーションは、 VDS セットアッププロセスで特定の権限セットを要求します。これらの権限は次のとおりです。

- サインインユーザとしてのアクセスディレクトリ（委任）
- 読み取り / 書き込みディレクトリデータ（委譲）
- サインインしてユーザプロファイルを読み取り（委任）
- サインユーザーイン（委任）
- ユーザの基本プロファイルの表示（委任）
- 組織ユーザとして Azure Service Management にアクセス（委任）

Cloud Workspace API

Azure PaaS 関数の一般的な管理呼び出しを処理します。Azure PaaS の機能には、 Azure コンピューティング、 Azure バックアップ、 Azure ファイルなどがあります。このサービスプリンシパルには、初期導入時にターゲットの Azure サブスクリプションに対する所有者の権限が必要です。継続的な管理を行う貢献者の権限が必要です（注： Azure Files を使用するには、 Azure File オブジェクトに対するユーザ権限ごとに設定するサブスクリプションの所有者権限が必要です）。

クラウドワークスペース API エンタープライズアプリケーションは、 VDS セットアッププロセスで特定の権限セットを要求します。これらの権限は次のとおりです。

- サブスクリプションコントリビュータ（ Azure ファイルを使用する場合はサブスクリプション所有者）
- Azure AD グラフ
  - すべてのアプリケーションの読み取りと書き込み（アプリケーション）
  - このアプリケーションが作成または所有するアプリケーションを管理する（アプリケーション）
  - 読み取り / 書き込みデバイス（アプリケーション）

- サインインユーザとしてディレクトリにアクセスする（委任）
- ディレクトリデータの読み取り（アプリケーション）
- 読み取りディレクトリデータ（委任）
- ディレクトリデータの読み取りと書き込み（アプリケーション）
- 読み取り / 書き込みディレクトリデータ（委譲）
- 読み取りドメインと書き込みドメイン（アプリケーション）
- すべてのグループの読み取り（委任）
- 読み取りおよび書き込みすべてのグループ（委任）
- すべての非表示メンバーシップ（アプリケーション）を読む
- 非表示メンバーシップの読み取り（委任）
- サインインしてユーザプロファイルを読み取り（委任）
- すべてのユーザの全プロファイルの読み取り（委任）
- すべてのユーザの基本プロファイルを読み取る（委任）

- Azure サービス管理
  - 組織ユーザとして Azure Service Management にアクセス（委任）

NetApp VDS

VDS コントロールプレーンを介して NetApp VDS コンポーネントを使用し、 AVD の役割、サービス、リソースの導入と構成を自動化します。

カスタムロール

Automation Contributor ロールは、最小限の権限を持つ方法で展開を容易にするために作成されます。このロールにより、 CWMGR1 VM は Azure オートメーションアカウントにアクセスできます。

自動化アカウント

自動化アカウントは、導入時に作成され、プロビジョニングプロセス中に必要なコンポーネントです。Automation アカウントには、変数、クレデンシャル、モジュール、および目的の State Configuration が含まれており、 Key Vault を参照しています。

目的の状態の設定

これは、 CWMGR1 の設定を作成するために使用される方法です。設定ファイルは VM にダウンロードされ、 VM 上の Local Configuration Manager を介して適用されます。構成要素には次のようなものがあります。

- Windows 機能をインストールしています
- ソフトウェアをインストールしています
- ソフトウェア設定の適用
- 適切な権限セットが適用されていることを確認します
- Let ' s Encrypt 証明書を適用します

- DNS レコードが正しいことを確認しています
- CWMGR1 がドメインに参加していることを確認します

モジュール：

- ActiveDirectoryDsc: Active Directory の展開と設定に必要な状態設定リソース。これらのリソースを使用すると、新しいドメイン、子ドメイン、およびハイアベイラビリティドメインコントローラを設定し、クロスドメイン信頼を確立し、ユーザ、グループ、および OU を管理できます。
- AZ.Accounts ： Microsoft が提供したモジュールで、 Azure モジュールのクレデンシャルと共通の構成要素を管理します
- AZ.Automation ： Microsoft が Azure Automation コマンドレット用のモジュールを提供しました
- Az.Compute:A Microsoft が Azure Compute コマンドレットのモジュールを提供しました
- AZ.KeyVault ： Microsoft が提供する Azure Key Vault コマンドレット用のモジュール
- AZ.Resources ： Microsoft が提供している Azure Resource Manager コマンドレットのモジュール
- CChoco ： chocolatey を使用してパッケージをダウンロードおよびインストールするために必要な状態設定リソース
- cjaz ：ネットアップが開発したこのモジュールは、 Azure 自動化モジュールに自動化ツールを提供します
- cjAzACS ：ネットアップが開発したこのモジュールには、ユーザコンテキスト内から実行される環境自動化機能と PowerShell プロセスが含まれています。
- cjAzBuild ：ネットアップが開発したこのモジュールには、システムコンテキストから実行される、ビルドおよびメンテナンスの自動化と PowerShell プロセスが含まれています。
- cNtfsAccessControl: NTFS アクセス制御管理用に必要な状態構成リソース
- ComputerManagementDsc ：ドメインへの参加やタスクのスケジュール設定などのコンピュータ管理タスク、および仮想メモリ、イベントログ、タイムゾーン、電源設定などの項目の設定を可能にする目的の状態設定リソース。
- cUserRightsAssignment : ログオン権限や特権などのユーザー権限の管理を可能にする必要な状態構成リソース
- NetworkingDsc: ネットワークの必要な状態構成リソース
- xCertificate ： Windows Server での証明書の管理を簡素化する目的の状態設定リソース。
- xDnsServer: Windows Server DNS サーバーの構成と管理に必要な状態構成リソース
- xNetworking: ネットワーク関連の望ましい状態の構成リソース。
- "xRemoteDesktopAdmin": このモジュールは、ローカルまたはリモートマシン上でリモートデスクトップ設定と Windows ファイアウォールを構成するために必要な状態構成リソースを含むリポジトリを使用します。
- xRemoteDesktopSessionHost: Remote Desktop Session Host (RDSH) インスタンスの作成と設定を有効にするための、目的の状態構成リソース (xRDSessionDeployment, xRDSessionCollectionConfiguration, xRDRemoteApp)
- xSmbShare ： SMB 共有の設定と管理に必要な状態の設定リソース
- xSystemSecurity: UAC および IE Esc を管理するための望ましい状態設定リソース

Azure Virtual Desktop は、 Azure Virtual Desktop および Azure Virtual Desktop Client のエンタープライズアプリケーションおよびアプリケーション登録、 AVD テナント、 AVD ホストプール、 AVD アプリケーショングループ、 AVD 登録仮想マシンなどの Azure コンポーネントもインストールします。VDS 自動化コンポーネントはこれらのコンポーネントを管理しますが 'AVD はデフォルトの構成と属性セットを制御します詳細については 'AVD のマニュアルを参照してください

ハイブリッド **AD** コンポーネント

ネットアップのソリューションを導入すると、既存の AD を効率的に、またはパブリッククラウドで運用することができます。そのためには、既存の AD 環境にコンポーネントや権限を追加する必要があります。

Domain Controller の略

既存のドメインコントローラは、 AD Connect またはサイト間 VPN （または Azure ExpressRoute ）を介して AVD 環境に統合できます。

AD 接続

AVD PaaS サービスによるユーザ認証を成功させるために、 AD 接続を使用してドメインコントローラと Azure AD を同期できます。

セキュリティグループ

VDS では、 CW-Infrastructure という Active Directory セキュリティグループを使用して、ドメイン参加や GPO ポリシーの添付など、 Active Directory に依存するタスクを自動化するために必要な権限を含めます。

サービスアカウント

VDS では、 VDS Windows サービスと IIS アプリケーションサービスの ID として使用される CloudworkspaceSVC という Active Directory サービスアカウントが使用されます。このアカウントは非対話型（ RDP ログインを許可しない）であり、 CW インフラストラクチャアカウントの主要メンバーです

VPN または **ExpressRoute**

サイト間 VPN または Azure ExpressRoute を使用して、既存のドメインに Azure VM を直接参加させることができます。これは、プロジェクトの要件から指示があった場合に使用できるオプションの設定です。

ローカルの **AD** 権限の委譲

ネットアップは、ハイブリッド AD プロセスを合理化するオプションのツールを提供しています。ネットアップのオプションツールを使用する場合は、次のことを行う必要があります。

- Workstation OS ではなく、サーバ OS 上で実行します
- ドメインに参加しているサーバ、またはドメインコントローラで実行します
- PowerShell 5.0 以降を、ツールを実行しているサーバ（ドメインコントローラで実行していない場合）とドメインコントローラの両方に配置します
- ドメイン管理者権限を持つユーザーが実行するか、ローカル管理者権限を持つユーザーが実行し、ドメイン管理者資格情報（ RunAs で使用）を提供することができます。

手動で作成するか、ネットアップのツールで適用するかにかかわらず、必要な権限は次のとおりです。

- CW - インフラストラクチャグループ
  - Cloud Workspace Infrastructure （ **CW-Infrastructure** ）セキュリティグループには、 Cloud Workspace OU レベルおよびすべての子孫オブジェクトに対するフルコントロールが付与されています
  - <deployment code>.cloudworkspace.app DNS Zone – CW - インフラストラクチャグループ許可された CreateChild 、 DeleteChild 、 ListChildren 、 ReadProperty 、 DeleteTree 、 ExtendedRight 、 Delete 、 GenericWrite
  - DNS サーバー– CW インフラストラクチャグループに ReadProperty 、 GenericExecute が付与されました
  - 作成された VM のローカル管理者アクセス（ CWMGR1 、 AVD セッション VM ）（管理対象 AVD システムのグループポリシーによって実行）
- CW-MCWMGRAccess グループこのグループは、すべてのテンプレート、単一サーバ、新しいネイティブ Active Directory テンプレートで CWMGR1 にローカル管理権限を与えます。これらのテンプレートは、組み込みグループ Server Operators Remote Desktop Users 、および Network Configuration Operators を利用します。

AVD 環境コンポーネントと権限

導入の自動化プロセスが完了したら、導入とワークスペースの継続的な使用と管理を行い、以下に定義する個別のコンポーネントと権限のセットが必要です。上記のコンポーネントや権限の多くは関連性がありますが、ここでは導入されたの構造を定義することに重点を置いています。

VDS の導入環境とワークスペースのコンポーネントは、いくつかの論理カテゴリに分類できます。

- エンドユーザクライアント
- VDS コントロールプレーンコンポーネント
- Microsoft Azure AVD-PaaS のコンポーネント
- VDS プラットフォームコンポーネント
- VDS ワークスペースコンポーネントを Azure テナントに表示
- ハイブリッド AD コンポーネント

エンドユーザクライアント

ユーザは、 AVD デスクトップやさまざまなエンドポイントタイプから接続できます。Microsoft では、 Windows 、 macOS 、 Android 、および iOS 向けのクライアントアプリケーションを公開しています。さらに、 Web クライアントからクライアントレスアクセスを実行できます。

AVD のエンドポイントクライアントを公開している Linux シンクライアントベンダーもいくつかあります。これらはに記載されています https://docs.microsoft.com/en-us/azure/virtual-desktop/linux-overview

VDS コントロールプレーンコンポーネント

VDS REST API

VDS は、完全にドキュメント化された REST API を基盤としているため、 Web アプリケーションで使用できるすべてのアクションを API でも使用できます。API のドキュメントは次のとおりです。

https://api.cloudworkspace.com/5.4/swagger/ui/index#

VDS Web アプリケーション

VDS 管理者は、 VDS Web アプリを使用して ADS アプリケーションを操作できます。この Web ポータルには次のアドレスがあります。 https://manage.cloudworkspace.com

コントロールプレーンデータベース

VDS のデータと設定は、ネットアップがホストし管理するコントロールプレーンの SQL データベースに格納されます。

VDS 通信

Azure テナントコンポーネント

VDS 導入の自動化では、 1 つの Azure リソースグループが作成され、 VM 、ネットワークサブネット、ネットワークセキュリティグループ、 Azure Files コンテナまたは Azure NetApp Files 容量プールなど、他の AVD コンポーネントが含まれます。注：デフォルトは 1 つのリソースグループですが 'VDS には必要に応じて追加のリソースグループにリソースを作成するツールがあります

Microsoft Azure AVD-PaaS のコンポーネント

AVD REST API

Microsoft AVD は API を使用して管理できます。VDS では、これらの API を広範囲に活用して AVD 環境を自動化および管理しています。ドキュメントは次の場所にあります。 https://docs.microsoft.com/en-us/rest/api/desktopvirtualization/

セッションブローカー

ブローカーは、ユーザーに許可されたリソースを判別し、ユーザーとゲートウェイとの接続をオーケストレーションします。

Azure 診断プログラム

Azure Diagnostics は、 AVD 環境をサポートするように特別に設計されています。

AVD Web クライアント

Microsoft は、ローカルにインストールされたクライアントを使用せずに、ユーザが AVD リソースに接続できる Web クライアントを提供しています。

セッションゲートウェイ

ローカルにインストールされた RD クライアントはゲートウェイに接続し、 AVD 環境に安全に通信します。

VDS プラットフォームコンポーネント

CWMGR1

CMWGR1 は、各導入の VDS 制御 VM です。デフォルトでは、ターゲット Azure サブスクリプションに Windows Server 2019 VM として作成されます。CWMGR1 にインストールされた VDS およびサードパーティコンポーネントのリストについては、「ローカル展開」セクションを参照してください。

AVD では、 AVD VM が Active Directory ドメインに参加している必要があります。このプロセスを容易にし、 VDS 環境を管理するための自動化ツールを提供するために、上記の CWMGR1 VM に複数のコンポーネントがインストールされ、 AD インスタンスに複数のコンポーネントが追加されます。コンポーネントは次のとおりです。

- * Windows サービス *- VDS では、 Windows サービスを使用して、導入環境から自動化と管理のアクションを実行します。
  - *CW オートメーションサービス * は、各 AVD 環境で CWMGR1 に展開されている Windows サービスで、環境内のユーザー向けの自動化タスクの多くを実行します。このサービスは、 * CloudWorkspaceSVC * AD アカウントで実行されます。
  - **CW VM Automation Service** は、仮想マシンの管理機能を実行する各 AVD 展開において CWMGR1 に展開される Windows サービスです。このサービスは、 * CloudWorkspaceSVC * AD アカウントで実行されます。
  - **CW Agent Service** は、 CWMGR1 を含む VDS 管理下の各仮想マシンに展開される Windows サービスです。このサービスは、仮想マシンの * LocalSystem* コンテキストで実行されます。
  - **CWManagerX API** は、各 AVD 展開の CWMGR1 にインストールされている IIS アプリケーションプールベースのリスナーです。これは、グローバルコントロールプレーンからのインバウンド要求を処理し、 * CloudWorkspaceSVC * AD アカウントで実行されます。
- * SQL Server 2017 Express * – VDS は、 CWMGR1 VM 上に SQL Server Express インスタンスを作成し、自動化コンポーネントによって生成されたメタデータを管理します。
- * インターネットインフォメーションサービス（ IIS ） * – CWMGR1 で IIS が有効になっており、 CWManagerX および CWApps IIS アプリケーションをホストします（ RDS RemoteApp 機能が有効になっている場合のみ）。VDS を使用するには、 IIS バージョン 7.5 以降が必要です。
- * HTML5 ポータル（オプション） * – VDS は、 Spark Gateway サービスをインストールして、導入環境内の VM と VDS Web アプリケーションから HTML5 経由でアクセスできるようにします。これは Java ベースのアプリケーションであり、このアクセス方法が不要な場合は無効にして削除できます。
- * RD ゲートウェイ（オプション） * – VDS を使用すると、 CWMGR1 の RD ゲートウェイロールで RDS コレクションベースのリソースプールへの RDP アクセスを提供できます。このロールは、 AVD リバースコネクトアクセスのみが必要な場合は、無効化 / アンインストールできます。
- * RD Web （オプション） * – VDS を使用すると、 RD Web ロールが有効になり、 CWApps IIS Web アプリケーションが作成されます。AVD アクセスのみが必要な場合は、このロールを無効にできます。
- *DC 構成 * –導入と VDS サイト固有の構成と高度な構成タスクを実行するために使用する Windows アプリケーション。
- * テスト VDC ツール * - トラブルシューティングのために API または Web アプリケーションのタスクを変更する必要があるまれなケースで、仮想マシンおよびクライアントレベルの設定変更の直接タスク実行をサポートする Windows アプリケーション。
- * ワイルドカード証明書を暗号化する（オプション） * – VDS によって作成および管理されます。 TLS 経由の HTTPS トラフィックを必要とするすべての VM は、毎晩証明書で更新されます。更新も自動化されたタスクによって処理されます（証明書は 90 日なので、更新はすぐ前から開始されます）。お客様は、必要に応じて独自のワイルドカード証明書を提供できます。VDS では、自動化タスクをサポートするために複数の Active Directory コンポーネントも必要になります。設計上の目的は、最小限の数の AD コンポ

ーネントと権限の追加を利用しながら、環境をサポートして管理を自動化することです。次のコンポーネントが含まれます。

- * クラウドワークスペース組織単位（ OU ） * –この組織単位は、必要な子コンポーネントのプライマリ AD コンテナとして機能します。CW インフラストラクチャおよびクライアント DHP アクセスグループの権限は、このレベルとその子コンポーネントで設定されます。この OU で作成されるサブ OU については、付録 A を参照してください。
- * Cloud Workspace Infrastructure Group （ CW-Infrastructure ） * は、必要な委任された権限を VDS サービスアカウントに割り当てるためにローカル AD で作成されたセキュリティグループです（ * CloudWorkspaceSVC * ）。
- * クライアント DHP アクセスグループ (ClientDHPAccess)* はローカル AD で作成されるセキュリティグループで、企業の共有データ、ユーザーホームデータ、およびプロファイルデータが存在する場所を VDS が管理できるようにします。
- * CloudWorkspaceSVC * サービスアカウント（ Cloud Workspace Infrastructure Group のメンバー）
- * 配置コード > .cloudworkspace.app domain * （このドメインは、セッションホスト VM 用に自動作成された DNS 名を管理します）用の DNS ゾーン– Deploy の構成で作成されます。
- * ネットアップ固有の GPO * は、クラウドワークスペースの組織単位のさまざまな子 OU にリンクされています。次の GPO があります。
  - * Cloud Workspace GPO （ Cloud Workspace OU にリンク） * – CW インフラストラクチャグループのメンバーのアクセスプロトコルと方法を定義します。また、 AVD セッションホスト上のローカル Administrators グループにもグループを追加します。
  - * クラウドワークスペースファイアウォール GPO * （専用の顧客サーバー、リモートデスクトップ、およびステージング OU にリンク） - プラットフォームサーバーからセッションホストへの接続を確実に分離するポリシーを作成します。
  - * Cloud Workspace RDS * （専用顧客サーバー、リモートデスクトップ、およびステージング OU ） - セッション品質、信頼性、切断タイムアウト制限に関するポリシーセットの制限。RDS セッションでは、 TS ライセンスサーバの値が定義される。
  - * Cloud Workspace Companies * （デフォルトではリンクされていません）–オプションの GPO を使用して、管理ツールやエリアへのアクセスを禁止し、ユーザーセッション / ワークスペースを「ロックダウン」します。リンク / 有効にして、アクティビティの制限付きワークスペースを提供できます。

デフォルトのグループポリシー設定は、要求に応じて指定できます。

VDS ワークスペースコンポーネント

データレイヤ

Azure NetApp Files の特長

VDS 設定でデータ層オプションとして Azure NetApp Files を選択した場合は、 Azure NetApp Files 容量プールと関連付けられたボリュームが作成されます。ボリュームは ' ユーザー・プロファイル（ FSLogix コンテナ経由） ' ユーザー個人用フォルダ ' および企業データ共有フォルダの共有ファイル・ストレージをホストします

Azure Files の特長

CWS セットアップで [データレイヤ] オプションとして Azure ファイルを選択した場合は、 Azure ファイル

共有とそれに関連付けられた Azure ストレージアカウントが作成されます。Azure File Share は、（ FSLogix コンテナを介して）ユーザプロファイルの共有ファイルストレージ、ユーザの個人フォルダ、および企業のデータ共有フォルダをホストします。

管理対象ディスクがあるファイルサーバ

VDS セットアップでデータ層オプションとしてファイルサーバーを選択した場合は、管理対象ディスクを使用して Windows Server VM が作成されます。ファイルサーバーは、 FSLogix コンテナを介してユーザープロファイルの共有ファイルストレージ、ユーザー個人フォルダ、および企業データ共有フォルダをホストします。

Azure ネットワーク

Azure Virtual Network の略

VDS では、 Azure Virtual Network とサポートサブネットが作成されます。VDS では、 CWMGR1 、 AVD ホストマシン、および Azure ドメインコントローラ用に個別のサブネットが必要です。また、サブネット間にピアリングが必要です。通常、 AD コントローラサブネットはすでに存在するため、導入した VDS サブネットを既存のサブネットとピアリングする必要があります。

ネットワークセキュリティグループ

CWMGR1 VM へのアクセスを制御するネットワークセキュリティグループが作成されます。

- テナント：セッションホストおよびデータ VM で使用する IP アドレスが含まれます
- サービス： PaaS サービスで使用する IP アドレス（ Azure NetApp Files など）が含まれる
- プラットフォーム： NetApp プラットフォーム VM （ CWMGR1 およびゲートウェイサーバ）として使用する IP アドレスが含まれています。
- ディレクトリ： Active Directory VM として使用する IP アドレスが格納されます

Azure AD

VDS の自動化とオーケストレーションでは、ターゲットの Active Directory インスタンスに仮想マシンを導入してから、指定のホストプールにマシンを追加します。AVD 仮想マシンは、 AD 構造（組織単位、グループポリシー、ローカルコンピュータ管理者権限など）と AVD 構造（ホストプール、ワークスペースアプリケーショングループメンバーシップ）の両方によってコンピュータレベルで管理され、 Azure AD エンティティと権限によって管理されます。VDS では、 AVD アクション用の VDS Enterprise アプリケーション /Azure サービスプリンシパルと、ローカル AD およびローカルコンピュータアクション用のローカル AD サービスアカウント（ CloudWorkspaceSVC ）を使用して、この「デュアルコントロール」環境を処理します。

AVD 仮想マシンを作成して AVD ホストプールに追加するための具体的な手順は、次のとおりです。

- Azure テンプレートから、 AVD に関連付けられた Azure サブスクリプションに表示される仮想マシンを作成する（ Azure サービスプリンシパル権限を使用）
- VDS 導入時に指定した Azure VNet を使用して新しい仮想マシンの DNS アドレスを確認 / 設定します（ローカル AD 権限が必要です（上記の CW インフラストラクチャに委任されたものすべて）。標準 VDS 命名スキーム * _ ｛ companycode ｝ TS ｛ sequenceNumber ｝ _ * を使用して仮想マシン名を設定します。例： XYZTS3（ローカル AD 権限が必要（オンプレミスで作成した OU 構造に配置）（リモートデスクトップ / 企業コード / 共有）（上記と同じ権限 / グループ概要）
- 指定された Active Directory の組織単位（ AD ）に仮想マシンを配置（上記の手動プロセスで指定された

OU 構造への委任された権限が必要）

- 新しいマシン名 /IP アドレスで内部 AD DNS ディレクトリを更新（ローカル AD 権限が必要）
- 新しい仮想マシンをローカル AD ドメインに追加（ローカル AD 権限が必要）
- VDS ローカルデータベースを新しいサーバー情報で更新する (追加の権限は不要)
- 指定された AVD ホストプールに VM を参加させる (AVD サービスプリンシパルの権限が必要)
- chocolatey コンポーネントを新しい仮想マシンにインストールします（ * CloudWorkspaceSVC * アカウントにはローカルコンピュータ管理者権限が必要です）。
- AVD インスタンスの FSLogix コンポーネントをインストールします（ローカル AD の AVD OU に対するローカルコンピュータ管理権限が必要です）
- AD Windows ファイアウォール GPO を更新して、新しい VM へのトラフィックを許可します（ AVD OU とそれに関連付けられた仮想マシンに関連付けられたポリシーに対して AD GPO の作成 / 変更が必要です）。ローカル AD の AVD OU で AD GPO ポリシーの作成 / 変更が必要です。VDS で VM を管理しない場合は、インストール後にオフにすることができます。）
- 新しい仮想マシンに「 Allow New Connections 」フラグを設定します（ Azure Service Principal 権限が必要です）。

VM の **Azure AD** への参加

Azure テナント内の仮想マシンはドメインに参加する必要がありますが、 VM を Azure AD に直接参加させることはできません。このため 'VDS では VDS プラットフォームにドメインコントローラの役割が導入され 'AD Connect を使用してその DC を Azure AD と同期します別の設定オプションとして、 Azure AD ドメインサービス（ AADDS ）の使用、 AD Connect を使用したハイブリッド DC （オンプレミスまたはその他の場所）への同期、サイト間 VPN または Azure ExpressRoute を使用した VM のハイブリッド DC への直接参加があります。

AVD ホストプール

ホストプールは、 Azure Virtual Desktop 環境内の 1 つ以上の同一の仮想マシン（ VM ）の集まりです。各ホストプールには、ユーザが物理デスクトップと同じように操作できるアプリケーショングループを含めることができます。

セッションホスト

任意のホストプール内で、同一の仮想マシンが 1 つ以上存在します。このホストプールに接続するこれらのユーザセッションは、 AVD ロードバランササービスによってロードバランシングされます。

アプリケーショングループ

デフォルトでは、展開時に _Desktop Users_app グループが作成されます。このアプリグループ内のすべてのユーザーには、 Windows デスクトップのフルエクスペリエンスが提供されます。また、アプリグループを作成して、ストリーミングアプリサービスを提供することもできます。

ログ分析ワークスペース

ログ分析ワークスペースは、展開プロセスと DSC プロセスおよび他のサービスからログを保存するために作成されます。これは導入後に削除できますが、他の機能が有効になるため、この操作は推奨されません。ログはデフォルトで 30 日間保持されるため、保持の料金は発生しません。

可用性セット

可用性セットは、障害ドメイン間で共有 VM （ AVD ホストプール、 RDS リソースプール）を分離できるように、導入プロセスの一環として設定されます。必要に応じて導入後に削除することもできますが、共有 VM のフォールトトレランスを強化するオプションは無効にします。

Azure の SnapVault

リカバリサービスボールトは、導入時に VDS 自動化によって作成されます。Azure Backup は、導入プロセス中に CWMGR1 に適用されるため、現在はこの機能がデフォルトでアクティブになっています。この処理は、非アクティブ化して必要に応じて削除することができますが、環境で Azure Backup が有効になっている場合は再作成されます。

Azure キーバックアップ

Azure Key Vault は導入プロセス中に作成され、導入時に Azure Automation アカウントで使用される証明書、 API キー、およびクレデンシャルを格納するために使用されます。

付録 A –クラウドワークスペースのデフォルトの組織単位構造

- クラウドワークスペース
  - クラウドワークスペース企業
  - クラウドワークスペースサーバ
    - 専用の顧客サーバー
    - インフラ
- CWMGR サーバ
- ゲートウェイサーバ
- FTP サーバ
- テンプレート VM
  - リモートデスクトップ
  - ステージング
    - Cloud Workspace サービスアカウント
  - クライアントサービスアカウント
  - インフラストラクチャサービスアカウント
    - Cloud Workspace Tech ユーザ
  - グループ
  - 技術 3 技術者

AVD および VDS v5.4 の前提条件

AVD および VDS の要件と注意事項

本ドキュメントでは、 NetApp Virtual Desktop Service （ VDS ）を使用して Azure Virtual Desktop （ AVD ）を導入するために必要な要素について説明します。「クイックチェックリスト」には、効率的な導入を実現す

るために必要なコンポーネントと導入前の手順の簡単なリストが記載されています。このガイドの残りの部分では、構成の選択内容に応じて、各要素の詳細を説明します。

クイックチェックリスト

Azure の要件

- Azure AD テナント
- AVD をサポートする Microsoft 365 ライセンス
- Azure サブスクリプション
- Azure 仮想マシンに使用可能な Azure クォータ
- グローバル管理者ロールおよびサブスクリプション所有権ロールを持つ Azure Admin アカウント
- AD Connect セットアップ用の「 Enterprise Admin 」ロールを持つドメイン管理者アカウント

導入前の情報

- ユーザの総数を決定します
- Azure リージョンを特定します
- Active Directory タイプを決定します
- ストレージタイプを決定します
- セッションホスト VM のイメージまたは要件を特定します
- 既存の Azure とオンプレミスのネットワーク構成を評価

VDS 環境詳細な要件

エンドユーザの接続要件

Azure Virtual Desktop をサポートするリモートデスクトップクライアントは次のとおりです。

- Windows デスクトップ
- ウェブ：
- MacOS
- iOS
- IGEL Think Client （ Linux ）
- Android （プレビュー）

Azure Virtual Desktop は、 RemoteApp および Desktop Connection （ RADC ）クライアントまたは Remote Desktop Connection （ MSTSC ）クライアントをサポートしていません。

Azure Virtual Desktop は、現在、 Windows ストアからのリモートデスクトップクライアントをサポートしていません。このクライアントのサポートは今後のリリースで追加される予定です。

- リモートデスクトップクライアントは、次の URL にアクセスできる必要があります。 *

住所	アウトバウンド **TCP** ポート	目的	クライアント
* .AVD.microsoft.com	443	サービストラフィック	すべて
* .servicebus.windows.net 443 トラブルシューティングデータ	すべて	go.microsoft.com	443
Microsoft FWLinks	すべて	aak.ms	443
Microsoft URL の短縮	すべて	docs.microsoft.com	443
ドキュメント	すべて	privacy.microsoft.com	443
プライバシーに関する声明	すべて	query.prod.cms.rt.microsoft.com	443

信頼性の高いクライアントエクスペリエンスを実現するには、これらの URL を開くことが不可欠です。これらの URL へのアクセスをブロックすることはサポートされていないため、サービス機能に影響します。これらの URL はクライアントサイトとリソースにのみ対応しており、 Azure Active Directory などの他のサービスの URL は含まれていません。

VDS セットアップウィザードの開始点

VDS セットアップウィザードでは、 AVD 展開を成功させるために必要な前提条件のセットアップの多くを処理できます。セットアップウィザード（""）次の構成要素を作成または使用します。

Azure テナント

- 必須： * Azure テナントと Azure Active Directory

Azure での AVD のアクティブ化は、テナント全体に適用されます。VDS では、テナントごとに 1 つの AVD インスタンスを実行できます。

Azure サブスクリプション

- 必須： * Azure サブスクリプション（使用するサブスクリプション ID をメモしておきます）

導入したすべての Azure リソースを 1 つの専用サブスクリプションでセットアップする必要があります。これにより、 AVD のコスト追跡が大幅に簡素化され、導入プロセスが簡素化されます。注： Azure の無償トライアルは、機能する AVD 環境を導入するための十分なクレジットがないためサポートされていません。

Azure コアクォータ

使用する VM ファミリに十分なクォータ（特に、最初のプラットフォーム導入で使用できるのは DS v3 ファミリの少なくとも 10 コアですが、 10 は初期導入の可能性をすべてカバーしています）。

Azure 管理者アカウント

- 必須： * Azure グローバル管理者アカウント。

VDS セットアップウィザードでは、 Azure 管理者が VDS サービスプリンシパルに委任された権限を付与し、 VDS Azure Enterprise アプリケーションをインストールするように要求します。管理者には、 Azure の

次のロールを割り当てる必要があります。

- テナントのグローバル管理者
- サブスクリプションの所有者ロール

VM イメージ

- 必須： * 複数セッションの Windows 10 をサポートする Azure イメージ。

Azure Marketplace では、最新バージョンの Windows 10 ベースイメージが提供されており、すべての Azure サブスクリプションからこれらのイメージに自動的にアクセスできます。別のイメージまたはカスタムイメージを使用する場合は、 VDS チームに他のイメージの作成や変更に関するアドバイスを提供するか、 Azure イメージに関する一般的な質問をさせていただき、商談のスケジュールを設定してください。

Active Directory

AVD では、ユーザ ID が Azure AD の一部であること、および VM が同じ Azure AD インスタンスと同期されている Active Directory ドメインに参加していることが必要です。VM を Azure AD インスタンスに直接接続することはできないため、ドメインコントローラを設定し、 Azure AD と同期する必要があります。

サポートされるオプションは次のとおりです。

- サブスクリプション内での Active Directory インスタンスの自動ビルド。通常、 AD インスタンスは、このオプションを使用する Azure Virtual Desktop 環境の VDS 制御 VM （ CWMGR1 ）上の VDS によって作成されます。セットアッププロセスの一環として、 AD Connect をセットアップし、 Azure AD と同期するように設定しておく必要があります。

  []

- Azure サブスクリプションからアクセス可能な既存の Active Directory ドメインに統合し（通常は Azure VPN または Express Route 経由で）、 AD Connect またはサードパーティ製品を使用して Azure AD とユーザリストを同期します。

  []

ストレージレイヤ

AVD では、永続的なユーザー / 企業データが AVD セッション VM に存在しないようにストレージ戦略が設計されています。ユーザプロファイル、ユーザファイル、フォルダ、および企業 / アプリケーションデータの永続的データは、独立したデータレイヤでホストされている 1 つ以上のデータボリュームでホストされます。

FSLogix は ' セッション初期化時にユーザー・プロファイル・コンテナ（ VHD または VHDX フォーマット）をセッション・ホストにマウントすることによって ' ユーザー・プロファイルの多くの問題（データのスプロール化やログインの遅延など）を解決する ' プロファイルのコンテナ化テクノロジーです

このアーキテクチャのため、データストレージ機能が必要です。この機能は、ユーザーのログイン / ログオフの大部分が同時に発生したときに、毎朝 / 午後に必要となるデータ転送を処理できる必要があります。中規模の環境であっても、データ転送には大きな要件があります。データストレージレイヤのディスクパフォーマンスは、プライマリエンドユーザのパフォーマンス変数の 1 つです。ストレージ容量だけでなく、このストレージのパフォーマンスを適切にサイジングするには、特に注意が必要です。一般に、ストレージレイヤは、ユーザあたり 5~15 IOPS をサポートするようにサイズを設定します。

VDS セットアップウィザードでは、次の構成がサポートされます。

- Azure NetApp Files （ ANF ）のセットアップと設定（推奨）_ ANF 標準サービスレベルは最大 150 ユーザをサポートしますが、ユーザ数は 150 ～ 500 人までにすることを推奨します。500 人を超えるユーザには ANF Ultra を推奨します。 _

  []

- ファイルサーバ VM のセットアップと構成

  []

ネットワーキング

- 必須： * Azure Express Route または VPN を介して Azure サブスクリプションから参照できるサブネットを含む、既存のすべてのネットワークサブネットのインベントリ。サブネットが重複しないように環境を構成する必要があります。

VDS セットアップウィザードでは、既存のネットワークとの統合計画の一環として、必要な範囲がある場合、または回避する必要がある場合にネットワークの範囲を定義できます。

導入時にユーザが使用する IP 範囲を決定します。Azure のベストプラクティスに従って、プライベート範囲の IP アドレスのみがサポートされます。

サポートされる選択肢は次のとおりですが、デフォルトは **/20** 範囲です。

- 192.168.0.0 ～ 192.168.255.255
- 172.16.0.0 ～ 172.31.255.255
- 10.0.0.0 ～ 10.255.255.255

CWMGR1

コスト削減ワークロードのスケジューリング機能やライブスケーリング機能など、 VDS 固有の機能の一部では、テナントとサブスクリプション内に管理者の存在が必要です。したがって、 VDS セットアップウィザードの自動化の一環として、 CWMGR1 という管理 VM が導入されます。VDS の自動化タスクに加えて、この VM は、 SQL Express データベース、ローカルログファイル、および DCConfig という高度な設定ユーティリティで VDS の設定も保持します。

VDS セットアップウィザードで選択した内容に応じて、この **VM** を使用して次の追加機能をホストできます。

- RDS ゲートウェイ（ RDS 配置でのみ使用）
- HTML 5 ゲートウェイ（ RDS 配置でのみ使用）
- RDS ライセンスサーバー（ RDS 展開でのみ使用）
- ドメインコントローラ（選択した場合）

Deployment Wizard の **Decision Tree** を参照してください

初期導入の一環として、新しい環境の設定をカスタマイズするための一連の質問に回答します。以下に、主要な決定事項の概要を示します。

Azure リージョン

AVD 仮想マシンをホストする Azure リージョンを決定します。Azure NetApp Files と特定の VM ファミリー

（ GPU 対応 VM など）には Azure リージョンのサポートリストが定義されており、 AVD はほとんどのリージョンで使用できます。

- このリンクを使用して、を識別できます "Azure 製品は地域ごとに提供されています"

Active Directory タイプ

使用する Active Directory の種類を決定します。

- 既存のオンプレミス Active Directory
- を参照してください "AVD VDS コンポーネントとアクセス権" Azure 環境とローカルの Active Directory 環境で必要な権限とコンポーネントの説明を文書化します
- 新しい Azure サブスクリプションベースの Active Directory インスタンス
- Azure Active Directory ドメインサービス

データストレージ

ユーザプロファイル、個々のファイル、および企業共有のデータをどこに配置するかを決定します。次の選択肢があります。

- Azure NetApp Files の特長
- Azure Files の特長
- 従来のファイルサーバ（ Azure VM と管理対象ディスク）

ネットアップ **VDS** 導入の要件 **-** 既存のコンポーネント

既存の **Active Directory** ドメインコントローラを使用した **NetApp VDS** の導入

この構成タイプは、既存の Active Directory ドメインを拡張して AVD インスタンスをサポートします。この場合 'VDS では 'AVD コンポーネントの自動プロビジョニングと管理タスクをサポートするために ' 限定されたコンポーネントセットがドメインに導入されます

この構成には、次のものが

- Azure VNet 上の VM からアクセス可能な既存の Active Directory ドメインコントローラ。通常は Azure VPN または Express Route 、または Azure で作成されたドメインコントローラを使用します。
- AVD ホストプールとデータボリュームをドメインに参加させる際の VDS 管理に必要な VDS コンポーネントとアクセス許可の追加。『 AVD VDS Components and Permissions 』ガイドでは、必要なコンポーネントと権限を定義しています。また、展開プロセスでは、必要な要素を作成するスクリプトを実行するためにドメイン権限を持つドメインユーザーが必要です。
- VDS 環境では、 VDS で作成された VM に対してデフォルトで VNet が作成されます。VNet は、既存の Azure ネットワーク VNet または CWMGR1 VM との間で、必要なサブネットが事前に定義されている既存の VNet に移動できます。

クレデンシャルとドメイン準備ツール

管理者は、導入プロセスのある時点でドメイン管理者の資格情報を提供する必要があります。ドメイン管理者の一時的な資格情報は、後で作成、使用、および削除できます（展開プロセスが完了した後）。また、前提条件の構築にサポートが必要なお客様は、ドメイン準備ツールを利用できます。

ネットアップ **VDS** 環境に既存のファイルシステムがある場合

VDS では、ユーザプロファイル、個人フォルダ、および企業データに AVD セッション VM からアクセスできるようにする Windows 共有が作成されます。VDS では、デフォルトでファイルサーバまたは Azure NetApp ファイルオプションのいずれかが導入されますが、 VDS の導入が完了した時点で既存のファイルストレージコンポーネント VDS がそのコンポーネントを指すことがあります。

と既存のストレージコンポーネントを使用するための要件は次のとおりです。

- コンポーネントが SMB v3 をサポートしている必要があります
- コンポーネントは、 AVD セッションホストと同じ Active Directory ドメインに参加する必要があります
- VDS 構成で使用する UNC パスをコンポーネントで公開できる必要があります。 3 つの共有すべてに 1 つのパスを使用することも、それぞれに別々のパスを指定することもできます。VDS ではこれらの共有にユーザーレベルのアクセス権が設定されるので 'VDS AVD コンポーネントとアクセス権ドキュメントを参照して 'VDS Automation Services に適切なアクセス権が付与されていることを確認してください

既存の **Azure AD** ドメインサービスを使用した **NetApp VDS** の導入

この構成では、既存の Azure Active Directory ドメインサービスインスタンスの属性を特定するプロセスが必要です。アカウントマネージャに連絡して、このタイプの導入を依頼してください。既存の AVD 環境での NetApp VDS の導入この構成タイプは、必要な Azure VNet 、 Active Directory 、および AVD コンポーネントがすでに存在することを前提としています。VDS の導入は、「既存の AD を使用した NetApp VDS の導入」構成と同じ方法で実行されますが、次の要件が追加されます。

- AVD テナントに対する RD オーナーの役割は、 Azure の VDS エンタープライズアプリケーションに付与する必要があります
- VDS Web App の VDS インポート機能を使用して、 AVD ホストプールと AVD ホストプール VM を VDS にインポートする必要がありますこのプロセスでは、 AVD ホストプールとセッション VM メタデータを収集し、 VDS に保存して、これらの要素を VDS で管理できるようにします
- CRA ツールを使用して、 AVD ユーザデータを VDS ユーザセクションにインポートする必要があります。このプロセスは 'VDS コントロールプレーンに各ユーザーのメタデータを挿入し 'AVD アプリケーショングループのメンバーシップとセッション情報を VDS で管理できるようにします

付録 **A** ： **VDS** コントロールプレーンの **URL** と **IP** アドレス

Azure サブスクリプション内の VDS コンポーネントは、 VDS Web アプリケーションや VDS API エンドポイントなどの VDS グローバルコントロールプレーンコンポーネントと通信します。アクセスするには、次のベース URI アドレスを、ポート 443 で双方向アクセスのためにセーフリストに登録する必要があります。

""

https://cjdownload3.file.core.windows.net/media

アクセス制御デバイスが IP アドレスによるセーフリストのみを許可する場合、次の IP アドレスリストはセーフリストに登録する必要があります。VDS は Azure Traffic Manager サービスを使用するため、このリストは時間の経過とともに変更される場合があります。

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230
13.67.227.67.227.9227.227.9227.92.239.1519.157
40.78.132.16.2.132.132.132.132.112.142.142.118.114.82.118.118.114.82.148.114.82.113.142.132.132.132.1
32.132.132.132.132.132.132.132.132.142.142.132.142.142.142.132.132.132.142.132.132.132.142.142.1
42.142.142.132.142.132.132.132.132.142.142.

この「 Microsoft AVD の要件」セクションでは、 Microsoft の AVD 要件の概要を説明します。完全な AVD 要件と最新の AVD 要件については、次のサイトを参照してください。

https://docs.microsoft.com/en-us/azure/virtual-desktop/overview#requirements

Azure Virtual Desktop セッションホストライセンス

Azure Virtual Desktop では次のオペレーティングシステムがサポートされているため、導入予定のデスクトップとアプリケーションに基づいて、ユーザに適したライセンスがあることを確認してください。

OS	必要なライセンス
Windows 10 Enterprise マルチセッションまたは Windows 10 Enterprise	Microsoft 365 E3 、 E5 、 A3 、 A5 、 F3 、 Business Premium Windows E3 、 E5 、 A3 、 A5
Windows 7 Enterprise の場合	Microsoft 365 E3 、 E5 、 A3 、 A5 、 F3 、 Business Premium Windows E3 、 E5 、 A3 、 A5
Windows Server 2012 R2 、 2016 、 2019	ソフトウェアアシュアランスを備えた RDS クライアントアクセスライセンス（ CAL ）

AVD マシンの URL アクセス

Azure Virtual Desktop 用に作成する Azure 仮想マシンには、次の URL へのアクセス権が必要です。

住所	アウトバウンド TCP ポート	目的	サービスタグ
* .AVD.microsoft.com	443	サービストラフィック	WindowsVirtualDesktop
mrsglobalsteus2prod.blob.core.windows.net	443	エージェントおよび SXS スタックの更新	AzureCloud
* .core.windows.net	443	エージェントトラフィック	AzureCloud
* .servicebus.windows.net	443	エージェントトラフィック	AzureCloud
prod.warmpath.msftcloudes.com	443	エージェントトラフィック	AzureCloud
catalogartifact.azureedge.net	443	Azure Marketplace で入手できます	AzureCloud
kms.core.windows.net	1688 年	Windows のライセンス認証	インターネット
AVDportalstorageblob.blob.core.windows.net	443	Azure ポータルサポート	AzureCloud

次の表に、 Azure 仮想マシンがアクセスできるオプションの URL を示します。

住所	アウトバウンド **TCP** ポート	目的	サービスタグ
* .microsoftonline.com	443	MS Online Services への認証	なし
* .events.data.microsoft.com	443	テレメータサービス	なし
www.msftconnecttest.com	443	OS がインターネットに接続されているかどうかを検出します	なし
* .prod.do.dsp.mp.microsoft.com	443	Windows Update を実行します	なし
login.windows.net	443	Microsoft Online Services 、 Office 365 にログインします	なし
* 。 SFX.ms	443	OneDrive クライアントソフトウェアを更新しました	なし
* .digicert.com	443	証明書失効チェック	なし

最適なパフォーマンス要因

最適なパフォーマンスを得るには、ネットワークが次の要件を満たしていることを確認します。

- クライアントのネットワークから、ホストプールが導入されている Azure リージョンへのラウンドトリップ（ RTT ）レイテンシが 150 ミリ秒未満である必要があります。
- デスクトップやアプリケーションをホストする VM が管理サービスに接続されている場合、ネットワークトラフィックが国や地域の境界を越えて流れることがあります。
- ネットワークパフォーマンスを最適化するために、セッションホストの VM を管理サービスと同じ Azure リージョンに配置することを推奨します。

サポートされる仮想マシンの **OS** イメージ

Azure Virtual Desktop でサポートされている x64 オペレーティングシステムイメージは次のとおりです。

- Windows 10 Enterprise マルチセッション、バージョン 1809 以降
- Windows 10 Enterprise バージョン 1809 以降
- Windows 7 Enterprise の場合
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Azure Virtual Desktop は、 x86 （ 32 ビット）、 Windows 10 Enterprise N 、または Windows 10 Enterprise KN オペレーティングシステムイメージをサポートしていません。Windows 7 では、セクターサイズの制限により、管理対象 Azure ストレージでホストされる VHD または VHDX ベースのプロファイルソリューション

もサポートされません。

使用可能な自動化と導入のオプションは、次の表に示すように、選択する OS とバージョンによって異なります。

オペレーティングシステム	**Azure** イメージギャラリー	**VM** の手動導入	**ARM** テンプレート統合	**Azure Marketplace** でホストプールをプロビジョニング
Windows 10 マルチセッション、バージョン 1903	はい。	はい。	はい。	はい。
Windows 10 マルチセッション、バージョン 1809	はい。	はい。	いいえ	いいえ
Windows 10 Enterprise バージョン 1903	はい。	はい。	はい。	はい。
Windows 10 Enterprise バージョン 1809	はい。	はい。	いいえ	いいえ
Windows 7 Enterprise の場合	はい。	はい。	いいえ	いいえ
Windows Server 2019	はい。	はい。	いいえ	いいえ
Windows Server 2016	はい。	はい。	はい。	はい。
Windows Server 2012 R2	はい。	はい。	いいえ	いいえ

AVD および **VDS v6.0** の前提条件

AVD および **VDS** の要件と注意事項

本ドキュメントでは、 NetApp Virtual Desktop Service （ VDS ）を使用して Azure Virtual Desktop （ AVD ）を導入するために必要な要素について説明します。「クイックチェックリスト」には、効率的な導入を実現するために必要なコンポーネントと導入前の手順の簡単なリストが記載されています。このガイドの残りの部分では、構成の選択内容に応じて、各要素の詳細を説明します。

クイックチェックリスト

Azure の要件

- Azure AD テナント
- AVD をサポートする Microsoft 365 ライセンス
- Azure サブスクリプション
- Azure 仮想マシンに使用可能な Azure クォータ
- グローバル管理者ロールおよびサブスクリプション所有権ロールを持つ Azure Admin アカウント
- AD Connect セットアップ用の「 Enterprise Admin 」ロールを持つドメイン管理者アカウント

導入前の情報

- ユーザの総数を決定します
- Azure リージョンを特定します

- Active Directory タイプを決定します
- ストレージタイプを決定します
- セッションホスト VM のイメージまたは要件を特定します
- 既存の Azure とオンプレミスのネットワーク構成を評価

VDS 環境詳細な要件

エンドユーザの接続要件

Azure Virtual Desktop をサポートするリモートデスクトップクライアントは次のとおりです。

- Windows デスクトップ
- ウェブ：
- MacOS
- iOS
- IGEL Think Client （ Linux ）
- Android （プレビュー）

Azure Virtual Desktop は、 RemoteApp および Desktop Connection （ RADC ）クライアントまたは Remote Desktop Connection （ MSTSC ）クライアントをサポートしていません。

Azure Virtual Desktop は、現在、 Windows ストアからのリモートデスクトップクライアントをサポートしていません。このクライアントのサポートは今後のリリースで追加される予定です。

- リモートデスクトップクライアントは、次の URL にアクセスできる必要があります。 *

住所	アウトバウンド **TCP** ポート	目的	クライアント
* .wvd.microsoft.com	443	サービストラフィック	すべて
* .servicebus.windows.net	443	トラブルシューティングデータ	すべて
go.microsoft.com	443	Microsoft FWLinks	すべて
aak.ms	443	Microsoft URL の短縮	すべて
docs.microsoft.com	443	ドキュメント	すべて
privacy.microsoft.com	443	プライバシーに関する声明	すべて
query.prod.cms.rt.microsoft.com	443	クライアントの更新	Windows デスクトップ

信頼性の高いクライアントエクスペリエンスを実現するには、これらの URL を開くことが不可欠です。これらの URL へのアクセスをブロックすることはサポートされていないため、サービス機能に影響します。これらの URL はクライアントサイトとリソースにのみ対応しており、 Azure Active Directory などの他のサービスの URL は含まれていません。

VDS セットアップウィザードの開始点

VDS セットアップウィザードでは、 AVD 展開を成功させるために必要な前提条件のセットアップの多くを処理できます。セットアップウィザード（""）次の構成要素を作成または使用します。

Azure テナント

- 必須： * Azure テナントと Azure Active Directory

Azure での AVD のアクティブ化は、テナント全体に適用されます。VDS では、テナントごとに 1 つの AVD インスタンスを実行できます。

Azure サブスクリプション

- 必須： * Azure サブスクリプション（使用するサブスクリプション ID をメモしておきます）

導入したすべての Azure リソースを 1 つの専用サブスクリプションでセットアップする必要があります。これにより、 AVD のコスト追跡が大幅に簡素化され、導入プロセスが簡素化されます。注： Azure の無償トライアルは、機能する AVD 環境を導入するための十分なクレジットがないためサポートされていません。

Azure コアクォータ

使用する VM ファミリに十分なクォータ（特に、最初のプラットフォーム導入で使用できるのは DS v3 ファミリの少なくとも 10 コアですが、 10 は初期導入の可能性をすべてカバーしています）。

Azure 管理者アカウント

- 必須： * Azure グローバル管理者アカウント。

VDS セットアップウィザードでは、 Azure 管理者が VDS サービスプリンシパルに委任された権限を付与し、 VDS Azure Enterprise アプリケーションをインストールするように要求します。管理者には、 Azure の次のロールを割り当てる必要があります。

- テナントのグローバル管理者
- サブスクリプションの所有者ロール

VM イメージ

- 必須： * 複数セッションの Windows 10 をサポートする Azure イメージ。

Azure Marketplace では、最新バージョンの Windows 10 ベースイメージが提供されており、すべての Azure サブスクリプションからこれらのイメージに自動的にアクセスできます。別のイメージまたはカスタムイメージを使用する場合は、 VDS チームに他のイメージの作成や変更に関するアドバイスを提供するか、 Azure イメージに関する一般的な質問をさせていただき、商談のスケジュールを設定してください。

Active Directory

AVD では、ユーザ ID が Azure AD の一部であること、および VM が同じ Azure AD インスタンスと同期されている Active Directory ドメインに参加していることが必要です。VM を Azure AD インスタンスに直接接続することはできないため、ドメインコントローラを設定し、 Azure AD と同期する必要があります。

サポートされるオプションは次のとおりです。

- サブスクリプション内での Active Directory インスタンスの自動ビルド。通常、 AD インスタンスは、このオプションを使用する Azure Virtual Desktop 環境の VDS 制御 VM （ CWMGR1 ）上の VDS によって作成されます。セットアッププロセスの一環として、 AD Connect をセットアップし、 Azure AD と同期するように設定しておく必要があります。

  []

- Azure サブスクリプションからアクセス可能な既存の Active Directory ドメインに統合し（通常は Azure VPN または Express Route 経由で）、 AD Connect またはサードパーティ製品を使用して Azure AD とユーザリストを同期します。

  []

ストレージレイヤ

AVD では、永続的なユーザー / 企業データが AVD セッション VM に存在しないようにストレージ戦略が設計されています。ユーザプロファイル、ユーザファイル、フォルダ、および企業 / アプリケーションデータの永続的データは、独立したデータレイヤでホストされている 1 つ以上のデータボリュームでホストされます。

FSLogix は ' セッション初期化時にユーザー・プロファイル・コンテナ（ VHD または VHDX フォーマット）をセッション・ホストにマウントすることによって ' ユーザー・プロファイルの多くの問題（データのスプロール化やログインの遅延など）を解決する ' プロファイルのコンテナ化テクノロジーです

このアーキテクチャのため、データストレージ機能が必要です。この機能は、ユーザーのログイン / ログオフの大部分が同時に発生したときに、毎朝 / 午後に必要となるデータ転送を処理できる必要があります。中規模の環境であっても、データ転送には大きな要件があります。データストレージレイヤのディスクパフォーマンスは、プライマリエンドユーザのパフォーマンス変数の 1 つです。ストレージ容量だけでなく、このストレージのパフォーマンスを適切にサイジングするには、特に注意が必要です。一般に、ストレージレイヤは、ユーザあたり 5~15 IOPS をサポートするようにサイズを設定します。

VDS セットアップウィザードでは、次の構成がサポートされます。

- Azure NetApp Files （ ANF ）のセットアップと設定（推奨）_ ANF 標準サービスレベルは最大 150 ユーザをサポートしますが、ユーザ数は 150 ～ 500 人までにすることを推奨します。500 人を超えるユーザには ANF Ultra を推奨します。 _

  []

- ファイルサーバ VM のセットアップと構成

  []

ネットワーキング

- 必須： * Azure Express Route または VPN を介して Azure サブスクリプションから参照できるサブネットを含む、既存のすべてのネットワークサブネットのインベントリ。サブネットが重複しないように環境を構成する必要があります。

VDS セットアップウィザードでは、既存のネットワークとの統合計画の一環として、必要な範囲がある場合、または回避する必要がある場合にネットワークの範囲を定義できます。

導入時にユーザが使用する IP 範囲を決定します。Azure のベストプラクティスに従って、プライベート範囲の IP アドレスのみがサポートされます。

サポートされる選択肢は次のとおりですが、デフォルトは **/20** 範囲です。

- 192.168.0.0 ～ 192.168.255.255
- 172.16.0.0 ～ 172.31.255.255
- 10.0.0.0 ～ 10.255.255.255

CWMGR1

コスト削減ワークロードのスケジューリング機能やライブスケーリング機能など、 VDS 固有の機能の一部では、テナントとサブスクリプション内に管理者の存在が必要です。したがって、 VDS セットアップウィザードの自動化の一環として、 CWMGR1 という管理 VM が導入されます。VDS の自動化タスクに加えて、この VM は、 SQL Express データベース、ローカルログファイル、および DCConfig という高度な設定ユーティリティで VDS の設定も保持します。

VDS セットアップウィザードで選択した内容に応じて、この **VM** を使用して次の追加機能をホストできます。

- RDS ゲートウェイ（ RDS 配置でのみ使用）
- HTML 5 ゲートウェイ（ RDS 配置でのみ使用）
- RDS ライセンスサーバー（ RDS 展開でのみ使用）
- ドメインコントローラ（選択した場合）

Deployment Wizard の **Decision Tree** を参照してください

初期導入の一環として、新しい環境の設定をカスタマイズするための一連の質問に回答します。以下に、主要な決定事項の概要を示します。

Azure リージョン

AVD 仮想マシンをホストする Azure リージョンを決定します。Azure NetApp Files と特定の VM ファミリー（ GPU 対応 VM など）には Azure リージョンのサポートリストが定義されており、 AVD はほとんどのリージョンで使用できます。

- このリンクを使用して、を識別できます "Azure 製品は地域ごとに提供されています"

Active Directory タイプ

使用する Active Directory の種類を決定します。

- 既存のオンプレミス Active Directory
- を参照してください "AVD VDS コンポーネントとアクセス権" Azure 環境とローカルの Active Directory 環境で必要な権限とコンポーネントの説明を文書化します
- 新しい Azure サブスクリプションベースの Active Directory インスタンス
- Azure Active Directory ドメインサービス

データストレージ

ユーザプロファイル、個々のファイル、および企業共有のデータをどこに配置するかを決定します。次の選択肢があります。

- Azure NetApp Files の特長
- Azure Files の特長
- 従来のファイルサーバ（ Azure VM と管理対象ディスク）

ネットアップ **VDS** 導入の要件 **-** 既存のコンポーネント

既存の **Active Directory** ドメインコントローラを使用した **NetApp VDS** の導入

この構成タイプは、既存の Active Directory ドメインを拡張して AVD インスタンスをサポートします。この場合 'VDS では 'AVD コンポーネントの自動プロビジョニングと管理タスクをサポートするために ' 限定されたコンポーネントセットがドメインに導入されます

この構成には、次のものが

- Azure VNet 上の VM からアクセス可能な既存の Active Directory ドメインコントローラ。通常は Azure VPN または Express Route 、または Azure で作成されたドメインコントローラを使用します。
- AVD ホストプールとデータボリュームをドメインに参加させる際の VDS 管理に必要な VDS コンポーネントとアクセス許可の追加。『 AVD VDS Components and Permissions 』ガイドでは、必要なコンポーネントと権限を定義しています。また、展開プロセスでは、必要な要素を作成するスクリプトを実行するためにドメイン権限を持つドメインユーザーが必要です。
- VDS 環境では、 VDS で作成された VM に対してデフォルトで VNet が作成されます。VNet は、既存の Azure ネットワーク VNet または CWMGR1 VM との間で、必要なサブネットが事前に定義されている既存の VNet に移動できます。

クレデンシャルとドメイン準備ツール

管理者は、導入プロセスのある時点でドメイン管理者の資格情報を提供する必要があります。ドメイン管理者の一時的な資格情報は、後で作成、使用、および削除できます（展開プロセスが完了した後）。また、前提条件の構築にサポートが必要なお客様は、ドメイン準備ツールを利用できます。

ネットアップ **VDS** 環境に既存のファイルシステムがある場合

VDS では、ユーザプロファイル、個人フォルダ、および企業データに AVD セッション VM からアクセスできるようにする Windows 共有が作成されます。VDS では、デフォルトでファイルサーバまたは Azure NetApp ファイルオプションのいずれかが導入されますが、 VDS の導入が完了した時点で既存のファイルストレージコンポーネント VDS がそのコンポーネントを指すことがあります。

と既存のストレージコンポーネントを使用するための要件は次のとおりです。

- コンポーネントが SMB v3 をサポートしている必要があります
- コンポーネントは、 AVD セッションホストと同じ Active Directory ドメインに参加する必要があります
- VDS 構成で使用する UNC パスをコンポーネントで公開できる必要があります。 3 つの共有すべてに 1 つのパスを使用することも、それぞれに別々のパスを指定することもできます。VDS ではこれらの共有にユーザーレベルのアクセス権が設定されるので 'VDS AVD コンポーネントとアクセス権ドキュメントを参照して 'VDS Automation Services に適切なアクセス権が付与されていることを確認してください

既存の **Azure AD** ドメインサービスを使用した **NetApp VDS** の導入

この構成では、既存の Azure Active Directory ドメインサービスインスタンスの属性を特定するプロセスが必要です。アカウントマネージャに連絡して、このタイプの導入を依頼してください。既存の AVD 環境での NetApp VDS の導入この構成タイプは、必要な Azure VNet 、 Active Directory 、および AVD コンポーネント

がすでに存在することを前提としています。VDS の導入は、「既存の AD を使用した NetApp VDS の導入」構成と同じ方法で実行されますが、次の要件が追加されます。

- AVD テナントに対する RD オーナーの役割は、 Azure の VDS エンタープライズアプリケーションに付与する必要があります
- VDS Web App の VDS インポート機能を使用して、 AVD ホストプールと AVD ホストプール VM を VDS にインポートする必要がありますこのプロセスでは、 AVD ホストプールとセッション VM メタデータを収集し、 VDS に保存して、これらの要素を VDS で管理できるようにします
- CRA ツールを使用して、 AVD ユーザデータを VDS ユーザセクションにインポートする必要があります。このプロセスは 'VDS コントロールプレーンに各ユーザーのメタデータを挿入し 'AVD アプリケーショングループのメンバーシップとセッション情報を VDS で管理できるようにします

付録 **A** ： **VDS** コントロールプレーンの **URL** と **IP** アドレス

Azure サブスクリプション内の VDS コンポーネントは、 VDS Web アプリケーションや VDS API エンドポイントなどの VDS グローバルコントロールプレーンコンポーネントと通信します。アクセスするには、次のベース URI アドレスを、ポート 443 で双方向アクセスのためにセーフリストに登録する必要があります。

""

https://cjdownload3.file.core.windows.net/media

アクセス制御デバイスが IP アドレスによるセーフリストのみを許可する場合、次の IP アドレスリストはセーフリストに登録する必要があります。VDS は Azure Traffic Manager サービスを使用するため、このリストは時間の経過とともに変更される場合があります。

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230
13.67.227.67.227.9227.227.9227.92.239.1519.157
40.78.132.16.2.132.132.132.132.112.142.142.118.114.82.118.118.114.82.148.114.82.113.142.132.132.132.1
32.132.132.132.132.132.132.132.132.142.142.132.142.142.142.132.132.132.142.132.132.132.142.142.1
42.142.142.132.142.132.132.132.132.142.142.

付録 **B** ： **Microsoft AVD** の要件

この「 Microsoft AVD の要件」セクションでは、 Microsoft の AVD 要件の概要を説明します。完全な AVD 要件と最新の AVD 要件については、次のサイトを参照してください。

https://docs.microsoft.com/en-us/azure/virtual-desktop/overview#requirements

Azure Virtual Desktop セッションホストライセンス

Azure Virtual Desktop では次のオペレーティングシステムがサポートされているため、導入予定のデスクトップとアプリケーションに基づいて、ユーザに適したライセンスがあることを確認してください。

OS	必要なライセンス
Windows 10 Enterprise マルチセッションまたは Windows 10 Enterprise	Microsoft 365 E3 、 E5 、 A3 、 A5 、 F3 、 Business Premium Windows E3 、 E5 、 A3 、 A5
Windows 7 Enterprise の場合	Microsoft 365 E3 、 E5 、 A3 、 A5 、 F3 、 Business Premium Windows E3 、 E5 、 A3 、 A5

OS	必要なライセンス
Windows Server 2012 R2 、 2016 、 2019	ソフトウェアアシュアランスを備えた RDS クライアントアクセスライセンス（ CAL ）

AVD マシンの **URL** アクセス

Azure Virtual Desktop 用に作成する Azure 仮想マシンには、次の URL へのアクセス権が必要です。

住所	アウトバウンド **TCP** ポート	目的	サービスタグ
* .AVD.microsoft.com	443	サービストラフィック	WindowsVirtualDesktop
mrsglobalsteus2prod.blob.core.windows.net	443	エージェントおよび SXS スタックの更新	AzureCloud
* .core.windows.net	443	エージェントトラフィック	AzureCloud
* .servicebus.windows.net	443	エージェントトラフィック	AzureCloud
prod.warmpath.msftcloudes.com	443	エージェントトラフィック	AzureCloud
catalogartifact.azureedge.net	443	Azure Marketplace で入手できます	AzureCloud
kms.core.windows.net	1688 年	Windows のライセンス認証	インターネット
AVDportalstorageblob.blob.core.windows.net	443	Azure ポータルサポート	AzureCloud

次の表に、 Azure 仮想マシンがアクセスできるオプションの URL を示します。

住所	アウトバウンド **TCP** ポート	目的	サービスタグ
* .microsoftonline.com	443	MS Online Services への認証	なし
* .events.data.microsoft.com	443	テレメータサービス	なし
www.msftconnecttest.com	443	OS がインターネットに接続されているかどうかを検出します	なし
* .prod.do.dsp.mp.microsoft.com	443	Windows Update を実行します	なし
login.windows.net	443	Microsoft Online Services 、 Office 365 にログインします	なし

住所	アウトバウンド **TCP** ポート	目的	サービスタグ
* 。 SFX.ms	443	OneDrive クライアントソフトウェアを更新しました	なし
* .digicert.com	443	証明書失効チェック	なし

最適なパフォーマンス要因

最適なパフォーマンスを得るには、ネットワークが次の要件を満たしていることを確認します。

- クライアントのネットワークから、ホストプールが導入されている Azure リージョンへのラウンドトリップ（ RTT ）レイテンシが 150 ミリ秒未満である必要があります。
- デスクトップやアプリケーションをホストする VM が管理サービスに接続されている場合、ネットワークトラフィックが国や地域の境界を越えて流れることがあります。
- ネットワークパフォーマンスを最適化するために、セッションホストの VM を管理サービスと同じ Azure リージョンに配置することを推奨します。

サポートされる仮想マシンの **OS** イメージ

Azure Virtual Desktop でサポートされている x64 オペレーティングシステムイメージは次のとおりです。

- Windows 10 Enterprise マルチセッション、バージョン 1809 以降
- Windows 10 Enterprise バージョン 1809 以降
- Windows 7 Enterprise の場合
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Azure Virtual Desktop は、 x86 （ 32 ビット）、 Windows 10 Enterprise N 、または Windows 10 Enterprise KN オペレーティングシステムイメージをサポートしていません。Windows 7 では、セクターサイズの制限により、管理対象 Azure ストレージでホストされる VHD または VHDX ベースのプロファイルソリューションもサポートされません。

使用可能な自動化と導入のオプションは、次の表に示すように、選択する OS とバージョンによって異なります。

オペレーティングシステム	**Azure** イメージギャラリー	**VM** の手動導入	**ARM** テンプレート統合	**Azure Marketplace** でホストプールをプロビジョニング
Windows 10 マルチセッション、バージョン 1903	はい。	はい。	はい。	はい。
Windows 10 マルチセッション、バージョン 1809	はい。	はい。	いいえ	いいえ
Windows 10 Enterprise バージョン 1903	はい。	はい。	はい。	はい。

オペレーティングシステム	**Azure** イメージギャラリー	**VM** の手動導入	**ARM** テンプレート統合	**Azure Marketplace** でホストプールをプロビジョニング
Windows 10 Enterprise バージョン 1809	はい。	はい。	いいえ	いいえ
Windows 7 Enterprise の場合	はい。	はい。	いいえ	いいえ
Windows Server 2019	はい。	はい。	いいえ	いいえ
Windows Server 2016	はい。	はい。	はい。	はい。
Windows Server 2012 R2	はい。	はい。	いいえ	いいえ

Google

Google Cloud （ GCP ）向け RDS 導入ガイド

概要

本書では、 Google Cloud の NetApp Virtual Desktop Service （ VDS ）を利用してリモートデスクトップサービス（ RDS ）を導入する手順を、順を追って説明します。

このコンセプトの実証（ POC ）ガイドは、独自のテスト GCP プロジェクトで RDS の導入と構成を迅速に行えるように設計されています。

本番環境の導入、特に既存の AD 環境への導入は非常に一般的ですが、この POC ガイドではプロセスについては考慮していません。複雑な POC や本番環境の導入は、ネットアップ VDS の営業 / サービスチームで開始し、セルフサービスでは実施しないでください。

この POC ドキュメントでは、 RDS 導入全体を説明し、 VDS プラットフォームで利用できる導入後の構成の主な領域について簡単に説明します。完了すると、セッションホスト、アプリケーション、ユーザーを含む、完全に展開された機能的な RDS 環境が実現します。オプションで、自動化されたアプリケーション配信、セキュリティグループ、ファイル共有権限、 Cloud Backup 、インテリジェントなコスト最適化を構成できます。VDS では、 GPO 経由で一連のベストプラクティス設定が導入されます。オプションでこれらの制御を無効にする方法についても説明します。 POC では、管理対象外のローカルデバイス環境と同様に、セキュリティ制御を行わない必要があります。

導入アーキテクチャ

[幅 = 75%]

RDS の基礎

VDS では、フル機能の RDS 環境が導入され、必要なサポートサービスがすべてゼロから提供されます。この機能には次のものがあります。

- RDS ゲートウェイサーバ
- Web クライアントアクセスサーバ
- ドメインコントローラサーバ

- RDS ライセンスサービス
- ThinPrint ライセンスサービス
- Filezilla FTPS サーバサービス

ガイドの範囲

このガイドでは、 GCP と VDS の管理者の視点から、 NetApp VDS テクノロジを使用した RDS の導入方法を順を追って説明します。GCP プロジェクトを初期構成にする場合、このガイドは RDS のエンドツーエンドの設定に役立ちます

サービスアカウントを作成します

1. GCP で、 _iam & Admin > Service Accounts _ に移動します（または検索します）

   []

2. [+] サービスアカウントの作成 _ をクリックします

   []

3. 一意のサービスアカウント名を入力し、 _CREATE _ をクリックします。後の手順で使用するサービスアカウントのメールアドレスをメモしておきます。

   []

4. サービスアカウントの _Owner_role を選択し、 _CONTINUE _ をクリックします

   []

5. 次のページで変更する必要はありません (_ このサービスアカウントへのアクセスをユーザーに許可する (オプション)_) 。 _done をクリックします

   []

6. _ サービスアカウント _ ページで ' アクションメニューをクリックして _ キーの作成 _ を選択します

   []

7. P12_ を選択し、 _CREATE _ をクリックします

   []

8. .P12 ファイルをダウンロードし、コンピュータに保存します。_Private キーの PASSWORD_Unchanged を実行します。

   []

   []

Google コンピューティング **API** を有効にします

1. GCP で、 *APIs & Services* > *Library* に移動（または検索）します

[]

2. GCP API ライブラリで、 *Compute Engine API* に移動（または検索）し、 _enable_を クリックします

[]

新しい **VDS** 導入を作成します

1. VDS で、 *Deployments*] に移動し、 [+] New Deployment_ をクリックします

[]

2. 導入環境の名前を入力します

[]

3. Google Cloud Platform _ を選択します

[]

インフラプラットフォーム

1. _ プロジェクト ID_ および OAuth 電子メールアドレスを入力します。このガイドの前半の .p12 ファイルをアップロードし、この配置に適したゾーンを選択します。[*Test*] をクリックして、エントリが正しいことと、適切な権限が設定されていることを確認します。

OAuth メールは、このガイドで先に作成したサービスアカウントのアドレスです。

[]

2. 確認したら、 *Continue* をクリックします

[]

アカウント

ローカル **VM** アカウント

1. ローカル管理者アカウントのパスワードを指定します。このパスワードは後で使用するために文書化しておいて
2. SQL SA アカウントのパスワードを入力します。このパスワードは後で使用するために文書化しておいて

パスワードを複雑にするには、大文字、小文字、数字、特殊文字の 4 種類のうち 3 種類が必要です

SMTP アカウント

VDS では、カスタム SMTP 設定で E メール通知を送信することも、 *Automatic* を選択して組み込みの SMTP サービスを使用することもできます。

1. VDS から E メール通知を送信する場合に、送信元アドレスとして使用する E メールアドレスを入力します。_no-reply@<your-domain>.com は一般的な形式です。
2. 成功レポートを送信する E メールアドレスを入力します。
3. 障害レポートの送信先となる E メールアドレスを入力します。

[]

レベル **3** の技術者

レベル 3 の技術者アカウント（別名、は 'VDS 環境で VM の管理タスクを実行するときに 'VDS 管理者が使用するドメイン・レベルのアカウントですこの手順以降では、追加のアカウントを作成できます。

1. レベル 3 管理者アカウントのユーザ名とパスワードを入力します。入力したユーザ名に「 .tech 」が追加され、エンドユーザと技術アカウントを区別できるようになります。これらのクレデンシャルは、あとで使用できるように記録

> 環境に対するドメインレベルのクレデンシャルを持つすべての VDS 管理者に対して名前付きアカウントを定義することを推奨します。このタイプのアカウントを持たない VDS 管理者は 'VDS に組み込まれた server_functionality への _Connect 経由で VM レベルの管理者アクセス権を持つことができます

[]

ドメイン

Active Directory

目的の AD ドメイン名を入力します。

パブリックドメイン

外部アクセスは SSL 証明書を使用して保護されます。独自のドメインと自己管理 SSL 証明書を使用してカスタマイズできます。また、 *Automatic_* を選択すると、証明書の 90 日の自動更新を含む SSL 証明書を管理することができます。自動を使用する場合は、各導入環境で固有のサブドメイン _cloudworkspace.app_を 使用します。

[]

仮想マシン

RDS の導入では、ドメインコントローラ、 RDS ブローカー、 RDS ゲートウェイなどの必要なコンポーネントをプラットフォームサーバにインストールする必要があります。本番環境では、これらのサービスを専用の冗長仮想マシンで実行する必要があります。コンセプトの実証環境では、 1 台の VM でこれらすべてのサービスをホストできます。

プラットフォーム **VM** の構成

単一の仮想マシン

これは、 POC 環境で推奨される選択です。シングル仮想マシン環境では、次の役割がすべて 1 つの VM でホストされます。

- CW Manager の略
- HTML5 ゲートウェイ
- RDS ゲートウェイ
- リモートアプリ
- FTPS サーバ（オプション）
- Domain Controller の略

このコンフィグレーションで推奨される RDS 使用事例の最大ユーザー数は 100 ユーザーです。この構成では、ロードバランシングが行われた RDS+ HTML5 ゲートウェイはオプションではないため、冗長性が制限されるだけでなく、将来的に拡張性を高めるためのオプションも制限されます。

この環境がマルチテナンシー用に設計されている場合、シングル仮想マシン構成はサポートされません。

複数のサーバ

VDS プラットフォームを複数の仮想マシンに分割する場合は、次の役割が専用 VM でホストされます。

- リモートデスクトップゲートウェイ

  VDS セットアップを使用して、 1 つまたは 2 つの RDS ゲートウェイを展開および設定できます。これらのゲートウェイは、オープンインターネットから、導入環境内のセッションホスト VM への RDS ユーザセッションをリレーします。RDS ゲートウェイは重要な機能を処理し、 RDS をオープンインターネットからの直接攻撃から保護し、環境内のすべての RDS トラフィックを暗号化します。2 つのリモートデスクトップゲートウェイが選択されている場合、 VDS セットアップは 2 つの VM を展開し、着信 RDS ユーザーセッションをロードバランシングするように設定します。

- HTML5 ゲートウェイ

  VDS セットアップを使用して、 1 つまたは 2 つの HTML5 ゲートウェイを導入および設定できます。これらのゲートウェイは、 VDS の Server_feature への _ 接続と Web ベースの VDS クライアント（ H5 ポータル）で使用される HTML5 サービスをホストします。2 つの HTML5 ポータルを選択すると、 VDS セットアップによって 2 つの VM が導入され、受信する HTML5 ユーザセッションの負荷を分散するように設定されます。

  複数サーバオプションを使用する場合（インストールされている VDS クライアントのみを介して接続する場合でも） VDS から Server_Functionality への _ 接続を有効にすることを推奨します。

- 『 Gateway Scalability Notes 』

  RDS のユースケースでは、追加のゲートウェイ VM を使用して環境の最大サイズをスケールアウトでき、 RDS または HTML5 ゲートウェイは約 500 ユーザをサポートします。ゲートウェイの追加は、ネットアッププロフェッショナルサービスによるサポートが最小限で済むため、後で追加できます

この環境がマルチテナンシー用に設計されている場合は、 _multiple servers _ selection を指定する必要があります。

サービスの役割

- Cwmgr1

  この VM はネットアップ VDS 管理 VM です。SQL Express データベース、ヘルパーユーティリティ、およびその他の管理サービスを実行します。a_single server_deployment では、この VM は他のサービスもホストできますが、 _multiple server_configuration では、これらのサービスは別の VM に移動されます。

- CWPortal1(2)

  最初の HTML5 ゲートウェイの名前は *CWPortal1*'2 番目は _CWPortal2_です導入時に 1 つまたは 2 つ作成できます。導入後にサーバを追加して容量を増やすことができます（サーバあたり最大 500 接続）。

- CWRDSGateway1 （ 2 ）

  最初の RDS ゲートウェイの名前は *CWRDSGateway1*、 2 番目は _CWRDSGateway2_です 。導入時に 1 つまたは 2 つ作成できます。導入後にサーバを追加して容量を増やすことができます（サーバあたり最大 500 接続）。

- リモートアプリ

  App Service は、 RemotApp アプリケーションをホストするための専用コレクションですが、 RDS ゲートウェイとその RDWeb ロールを使用して、エンドユーザセッション要求をルーティングし、 RDWeb アプリケーションサブスクリプションリストをホストします。このサービスロールには VM 専用 VM が導入されていません。

- ドメインコントローラ

  導入時に 'VDS と連携するように 1 つまたは 2 つのドメインコントローラを自動的に構築および構成できます

[]

オペレーティングシステム

プラットフォームサーバーに展開するサーバーオペレーティングシステムを選択します。

タイムゾーン

希望するタイムゾーンを選択します。プラットフォームサーバがこの時間に設定され、ログファイルにこのタイムゾーンが反映されます。この設定に関係なく、エンドユーザセッションには、自身のタイムゾーンが反映されます。

その他のサービス

FTP

VDS では、オプションで Filezilla をインストールして設定し、 FTPS サーバで環境との間でデータを移動することができます。このテクノロジーは古く、より最新のデータ転送方法（ Google ドライブなど）を推奨します。

[]

ネットワーク

VM をそれぞれの目的に応じて別のサブネットに分離することを推奨します。

ネットワークスコープを定義し、 /20 範囲を追加します。

VDS セットアップは、検出して、成功したことを示す範囲を提案します。ベストプラクティスに従い、サブネット IP アドレスはプライベート IP アドレス範囲にする必要があります。

範囲は次のとおりです。

- 192.168.0.0 ～ 192.168.255.255
- 172.16.0.0 ～ 172.31.255.255
- 10.0.0.0 ～ 10.255.255.255

必要に応じて確認と調整を行い、 [検証] をクリックして、次のそれぞれのサブネットを特定します。

- テナント：セッションホストサーバとデータベースサーバが配置される範囲です
- サービス： Cloud Volumes Service などの PaaS サービスが提供される範囲です
- プラットフォーム : プラットフォームサーバーが存在する範囲です
- Directory ： AD サーバが配置される範囲です

[]

ライセンス

SPLA#

VDS で RDS ライセンスサービスを構成して SPLA RDS CAL レポートを簡単に作成できるように、 SPLA 番号を入力します。POC 導入では一時的な番号（ 12345 など）を入力できますが、試用期間（ 120 日以内）後、 RDS セッションの接続は停止します。

SPLA 製品

SPLA でライセンスされた Office 製品の MAK ライセンスコードを入力して 'VDS レポートから SPLA レポートを簡単に作成できるようにします

ThinPrint

同梱の ThinPrint ライセンスサーバとライセンスをインストールして、エンドユーザーのプリンタのリダイレクトを簡素化します。

[]

レビューとプロビジョニング

すべての手順が完了したら、選択内容を確認し、環境を検証してプロビジョニングします。[]

次のステップ

導入の自動化プロセスでは、導入ウィザードで選択したオプションを使用して、新しい RDS 環境が導入されるようになりました。

導入が完了すると、複数の E メールが送信されます。完了すると、最初のワークスペースに対応できる環境が整います。ワークスペースには、エンドユーザーをサポートするために必要なセッションホストとデータサーバーが含まれます。このガイドに戻って、導入の自動化が 1~2 時間で完了したら次の手順に進みます。

新しいプロビジョニングコレクションを作成します

コレクションのプロビジョニングは、 VM イメージの作成、カスタマイズ、 Sysprep を可能にする VDS の機能です。ワークプレースの導入に入ると、導入するイメージが必要になり、次の手順で VM イメージを作成します。

導入の基本イメージを作成するには、次の手順を実行します。

1. [*Deployments] > [Provisioning Collections]* に移動し、 *[_Add*] をクリックします

   []

2. 名前と概要を入力します。[Type] に [Shared_] を選択します。

   > 共有または VDI を選択できます。Shared は、セッションサーバと、データベースなどのアプリケーション用のビジネスサーバ（オプション）をサポートします。VDI は VM 用の単一の VM イメージで、個々のユーザ専用になります。

3. [追加] をクリックして、ビルドするサーバーイメージのタイプを定義します。

   []

4. 「 TSData 」を「 *server role*」 、適切な VM イメージ（この場合は「 Server 2016 」）、および必要なストレージタイプとして選択します。サーバーの追加 _ をクリックします

   []

5. 必要に応じて、このイメージにインストールするアプリケーションを選択します。

   a. 使用可能なアプリケーションのリストは、 App Library から読み込まれます。 App Library にアクセスするには、右上にある _ 設定 > App Catalog_page の下にある管理者名メニューをクリックします。

      []

6. [コレクションの追加] をクリックし、 VM が作成されるまで待ちます。VDS は、アクセスおよびカスタマイズ可能な VM を構築します。
7. VM のビルドが完了したら、サーバに接続し、必要な変更を行います。

   a. ステータスに「 *Collection Validation*」 と表示されたら、コレクション名をクリックします。

      []

   b. 次に、 _ サーバテンプレート名 _ をクリックします

      []

c. 最後に、 *Connect to Server* ボタンをクリックします。接続され、ローカル管理者資格情報を使用して VM に自動的にログインします。

[]

[]

8. すべてのカスタマイズが完了したら、 _Validate Collection_so VDS を使用して sysprep を実行し、イメージをファイナライズできます。完了すると VM が削除され、 VDS 導入ウィザードで導入フォームを使用できるようになります。

[]5.

新しいワークスペースを作成します

ワークスペースは、ユーザーのグループをサポートするセッションホストとデータサーバーの集合です。導入環境には、単一のワークスペース（シングルテナント）または複数のワークスペース（マルチテナント）を含めることができます。

ワークスペースは、特定のグループの RDS サーバーコレクションを定義します。この例では、仮想デスクトップ機能をデモンストレーションするために単一のコレクションを導入します。ただし、モデルを複数のワークスペース /RDS コレクションに拡張して、同じ Active Directory ドメイン領域内の異なるグループと異なる場所をサポートすることもできます。管理者は、必要に応じて、ワークスペースやコレクション間のアクセスを制限して、アプリケーションやデータへのアクセスを制限するなどのユースケースに対応できます。

クライアント設定（ **&S** ）

1. NetApp VDS で、 _ ワークスペース _ に移動し、 _ + 新規ワークスペース _ をクリックします

[]

2. *Add* をクリックして ' 新しいクライアントを作成しますクライアントの詳細は、通常、会社情報または特定の場所 / 部門の情報のいずれかを表します。

[]

a. 会社の詳細を入力し、このワークスペースを配置する展開を選択します。

b. * データドライブ： * 会社の共有マップドライブに使用するドライブ文字を定義します。

c. * ユーザー・ホーム・ドライブ：マップされたドライブに使用するドライブ文字を定義します

d. * 追加設定 *

以下の設定は、導入時または導入後に定義できます。

i. _ リモートアプリを有効にする： _ リモートアプリは、完全なリモートデスクトップセッションを表示するのではなく、ストリーミングアプリケーションとしてアプリケーションを表示します。

ii. _App Locker を有効にする： _VDS にはアプリケーションの展開とエンタイトルメント機能が含まれています。デフォルトでは、システムはエンドユーザーに対してアプリケーションを表示 / 非表示にします。App Locker を有効にすると、 GPO セーフリストを介したアプリケーションアクセスが強制されます。

iii. ワークスペースユーザーデータストレージを有効にする：エンドユーザーが仮想デスクトップで

データストレージアクセスを行う必要があるかどうかを判断します。RDS 環境では、ユーザプロファイルのデータアクセスを有効にするには、この設定を常にチェックする必要があります。

iv. _ プリンタアクセスを無効にする： _VDS はローカルプリンタへのアクセスをブロックできます。

v. _ タスクマネージャへのアクセスを許可する :_VDS は、 Windows のタスクマネージャへのエンドユーザーアクセスを有効または無効にすることができます。

vi. 複雑なユーザーパスワードを要求する :_ 複雑なパスワードを要求すると、ネイティブの Windows Server の複雑なパスワードルールが有効になります。また、ロックされたユーザアカウントの自動ロック解除の遅延時間も無効になります。このため、有効にすると、エンドユーザが複数回失敗したパスワードを使用してアカウントをロックする場合に、管理者の介入が必要になります。

vii. すべてのユーザーに対して MFA を有効にする :_VDS には無料の電子メール /SMS MFA サービスが含まれており、エンドユーザーや VDS 管理者アカウントへのアクセスを保護するために使用できます。これを有効にすると、このワークスペースのすべてのエンドユーザーが MFA を使用して認証し、デスクトップやアプリケーションにアクセスする必要があります。

アプリケーションを選択します

このガイドで前の手順で作成した Windows OS バージョンと Provisioning コレクションを選択します。

この時点でアプリケーションを追加することもできますが、この POC では、導入後にアプリケーションの使用権に対処します。

[]

ユーザを追加します

ユーザを追加するには、既存の AD セキュリティグループを選択するか、個々のユーザを選択します。この POC ガイドでは、導入後にユーザを追加します。

[]

レビューとプロビジョニング

最後のページで、選択したオプションを確認し、 _Provision _ をクリックして、 RDS リソースの自動ビルドを開始します。

[]

展開プロセス中にログが作成され、展開詳細ページの下部にある _ タスク履歴 _ でアクセスできます。アクセスするには、 _VDS > 配置 > 配置名 _ に移動します

次のステップ

ワークプレース自動化プロセスでは、導入ウィザードで選択したオプションを使用して、新しい RDS リソースを配置できるようになりました。

完了すると、一般的な RDS 配置をカスタマイズするためのいくつかの一般的なワークフローを実行できます。

- "ユーザを追加します"

- "エンドユーザアクセス"
- "アプリケーションエンタイトルメント"
- "コストの最適化"

Google Compute Platform （ GCP ）と VDS の前提条件

GCP と VDS の要件と注意事項

本ドキュメントでは、 NetApp Virtual Desktop Service （ VDS ）を使用して Remote Desktop Services （ RDS ）を導入するために必要な要素について説明します。「クイックチェックリスト」には、効率的な導入を実現するために必要なコンポーネントと導入前の手順の簡単なリストが記載されています。このガイドの残りの部分では、構成の選択内容に応じて、各要素の詳細を説明します。

[幅 = 75%]

クイックチェックリスト

GCP の要件

- GCP テナント
- GCP プロジェクト
- オーナーロールが割り当てられたサービスアカウント

導入前の情報

- ユーザの総数を決定します
- GCP のリージョンとゾーンを特定します
- Active Directory のタイプを決定します
- ストレージの種類を確認します
- セッションホスト VM のイメージまたは要件を特定します
- 既存の GCP とオンプレミスのネットワーク構成を評価します

VDS 環境詳細な要件

エンドユーザの接続要件

GCP で RDS をサポートするリモートデスクトップクライアントは次のとおりです。

- "Windows 用の NetApp VDS クライアント"
  - NetApp VDS Client for Windows アウトバウンド URL セーフリスト要件
    - api.cloudworkspace.com
    - vdsclient.app
    - api.vdsclient.app
    - bin.vdsclient.app
  - 拡張機能：

        - VDS Wake On Demand
        - ThinPrint クライアントおよびスライスの使用
        - セルフサービスパスワードがリセットされました
        - サーバおよびゲートウェイアドレスの自動ネゴシエーション
        - デスクトップおよびストリーミング・アプリケーションの完全サポート
        - カスタムブランディングが可能です
        - 導入と設定を自動化するためのインストーラスイッチ
        - トラブルシューティングツールが組み込まれています
- "NetApp VDS Web クライアント"
- "Microsoft RD Client"
    - Windows の場合
    - MacOS
    - .iso
    - Android
- サードパーティ製ソフトウェアまたはシンクライアント
    - 要件： RD ゲートウェイ設定をサポートします

ストレージレイヤ

VDS で導入された RDS では、永続的なユーザ / 企業データが AVD セッション VM に存在しないようにストレージ戦略が設計されています。ユーザプロファイル、ユーザファイル、フォルダ、および企業 / アプリケーションデータの永続的データは、独立したデータレイヤでホストされている 1 つ以上のデータボリュームでホストされます。

FSLogix は ' セッション初期化時にユーザー・プロファイル・コンテナ（ VHD または VHDX フォーマット）をセッション・ホストにマウントすることによって ' ユーザー・プロファイルの多くの問題（データのスプロール化やログインの遅延など）を解決する ' プロファイルのコンテナ化テクノロジーです

このアーキテクチャのため、データストレージ機能が必要です。この機能は、ユーザーのログイン / ログオフの大部分が同時に発生したときに、毎朝 / 午後に必要となるデータ転送を処理できる必要があります。中規模の環境であっても、データ転送には大きな要件があります。データストレージレイヤのディスクパフォーマンスは、プライマリエンドユーザのパフォーマンス変数の 1 つです。ストレージ容量だけでなく、このストレージのパフォーマンスを適切にサイジングするには、特に注意が必要です。一般に、ストレージレイヤは、ユーザあたり 5~15 IOPS をサポートするようにサイズを設定します。

ネットワーキング

- 必須： * VPN 経由で GCP プロジェクトから認識できるサブネットを含む、既存のすべてのネットワークサブネットのインベントリ。サブネットが重複しないように環境を構成する必要があります。

VDS セットアップウィザードでは、既存のネットワークとの統合計画の一環として、必要な範囲がある場合、または回避する必要がある場合にネットワークの範囲を定義できます。

導入時にユーザが使用する IP 範囲を決定します。ベストプラクティスに従い、プライベートレンジの IP アドレスのみがサポートされます。

サポートされる選択肢は次のとおりですが、デフォルトは **/20** 範囲です。

- 192.168.0.0 ～ 192.168.255.255
- 172.16.0.0 ～ 172.31.255.255
- 10.0.0.0 ～ 10.255.255.255

CWMGR1

コスト削減ワークロードスケジューリング機能やライブスケーリング機能など、 VDS 固有の機能の一部では、組織およびプロジェクト内に管理者としての存在が必要です。したがって、 VDS セットアップウィザードの自動化の一環として、 CWMGR1 という管理 VM が導入されます。VDS の自動化タスクに加えて、この VM は、 SQL Express データベース、ローカルログファイル、および DCConfig という高度な設定ユーティリティで VDS の設定も保持します。

VDS セットアップウィザードで選択した内容に応じて、この **VM** を使用して次の追加機能をホストできます。

- RDS ゲートウェイ
- HTML 5 ゲートウェイ
- RDS ライセンスサーバー
- ドメインコントローラ

Deployment Wizard の **Decision Tree** を参照してください

初期導入の一環として、新しい環境の設定をカスタマイズするための一連の質問に回答します。以下に、主要な決定事項の概要を示します。

GCP リージョン

VDS 仮想マシンをホストする GCP リージョンを決定します。エンドユーザと利用可能なサービスに基づいてリージョンを選択する必要があります。

データストレージ

ユーザプロファイル、個々のファイル、および企業共有のデータをどこに配置するかを決定します。次の選択肢があります。

- Cloud Volumes Service for GCP
- 従来のファイルサーバ

ネットアップ **VDS** 導入の要件 **-** 既存のコンポーネント

既存の **Active Directory** ドメインコントローラを使用した **NetApp VDS** の導入

この設定タイプは、 RDS インスタンスをサポートするために既存の Active Directory ドメインを拡張します。この場合 'VDS は限定されたコンポーネントセットをドメインに展開し 'RDS コンポーネントの自動プロビジョニングと管理タスクをサポートします

この構成には、次のものが

- GCP VPC ネットワーク上の VM からアクセスできる既存の Active Directory ドメインコントローラ。通常は、 VPN または GCP で作成されたドメインコントローラを介してアクセスできます。

- ドメインに参加する際の RDS ホストとデータボリュームの VDS 管理に必要な VDS コンポーネントと権限の追加。配置プロセスでは、必要な要素を作成するスクリプトを実行するために、ドメイン権限を持つドメインユーザーが必要です。
- VDS 環境では、作成された VM について、デフォルトで VPC ネットワークが作成されます。VPC ネットワークは、既存の VPC ネットワークとピア関係に設定することも、 CWMGR1 VM は、必要なサブネットが事前定義されている既存の VPC ネットワークに移動することもできます。

クレデンシャルとドメイン準備ツール

管理者は、導入プロセスのある時点でドメイン管理者の資格情報を提供する必要があります。ドメイン管理者の一時的な資格情報は、後で作成、使用、および削除できます（展開プロセスが完了した後）。また、前提条件の構築にサポートが必要なお客様は、ドメイン準備ツールを利用できます。

ネットアップ **VDS** 環境に既存のファイルシステムがある場合

VDS では、ユーザープロファイル、個人フォルダ、および企業データに RDS セッションホストからアクセスできるようにする Windows 共有が作成されます。VDS はデフォルトでファイルサーバーを配備しますが ' 既存のファイルストレージコンポーネント VDS がある場合 'VDS の配備が完了したらそのコンポーネントを指すことができます

と既存のストレージコンポーネントを使用するための要件は次のとおりです。

- コンポーネントが SMB v3 をサポートしている必要があります
- このコンポーネントは、 RDS セッションホストと同じ Active Directory ドメインに参加している必要があります。
- VDS 構成で使用する UNC パスをコンポーネントで公開できる必要があります。 3 つの共有すべてに 1 つのパスを使用することも、それぞれに別々のパスを指定することもできます。VDS ではこれらの共有に対するユーザレベルの権限が設定されることに注意してください。 VDS Automation Services に適切な権限が付与されていることを確認してください。

付録 **A** ： **VDS** コントロールプレーンの **URL** と **IP** アドレス

GCP プロジェクトの VDS コンポーネントは、 VDS Web アプリケーションや VDS API エンドポイントなど、 Azure でホストされる VDS グローバルコントロールプレーンコンポーネントと通信します。アクセスするには、次のベース URI アドレスを、ポート 443 で双方向アクセスのためにセーフリストに登録する必要があります。

""

アクセス制御デバイスが IP アドレスによるセーフリストのみを許可する場合、次の IP アドレスリストはセーフリストに登録する必要があります。VDS では冗長パブリック IP アドレスを持つロードバランサが使用されるため、このリストは時間の経過とともに変更される可能性があります。

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230
13.67.227.67.227.9227.227.9227.92.239.1519.157
40.78.132.16.2.132.132.132.132.112.142.142.118.114.82.118.118.114.82.148.114.82.113.142.132.132.132.1
32.132.132.132.132.132.132.132.132.142.142.132.142.142.142.132.132.132.142.132.132.132.142.142.1
42.142.142.132.142.132.132.132.132.142.142.

最適なパフォーマンス要因

最適なパフォーマンスを得るには、ネットワークが次の要件を満たしていることを確認します。

- クライアントのネットワークから、セッションホストが配置されている GCP リージョンへのラウンドトリップ（ RTT ）レイテンシは 150 ミリ秒未満である必要があります。
- デスクトップやアプリケーションをホストする VM が管理サービスに接続されている場合、ネットワークトラフィックが国や地域の境界を越えて流れることがあります。
- ネットワークパフォーマンスを最適化するには、セッションホストの VM を管理サービスと同じリージョンに配置することを推奨します。

サポートされる仮想マシンの **OS** イメージ

VDS によって配備された RDS セッションの動作は、次の x64 オペレーティングシステムイメージをサポートします。

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2