AWS ホワイトペーパー

デプロイのベストプラクティス WorkSpaces

デプロイのベストプラクティス WorkSpaces: AWS ホワイトペーパー

Table of Contents

Amazon をデプロイするためのベストプラクティス WorkSpaces

発行日: 2022 年 6 月 1 日 (ドキュメントの改訂)

要約

このホワイトペーパーでは、 のデプロイに関する一連のベストプラクティスの概要を説明します WorkSpaces。このホワイトペーパーでは、ネットワークに関する考慮事項、ディレクトリサービスとユーザー認証、セキュリティ、モニタリングとログ記録について説明します。

このホワイトペーパーでは、関連情報にすばやくアクセスでき、ネットワークエンジニア、ディレクトリエンジニア、またはセキュリティエンジニアを対象としています。

序章

Amazon WorkSpaces はクラウド内のマネージドデスクトップコンピューティングサービスです。Amazon は、ハードウェアの調達やデプロイ、または複雑なソフトウェアのインストールの負担 WorkSpaces を取り除き、Amazon Web Services (AWS) コマンドラインインターフェイス (CLI)、またはアプリケーションプログラミングインターフェイス (API) を使用してAWS Management Console、 を数回クリックするだけでデスクトップエクスペリエンスを提供します。Amazon を使用すると WorkSpaces、Microsoft Windows または Amazon Linux デスクトップを数分で起動できます。これにより、オンプレミスまたは外部ネットワークからデスクトップソフトウェアに安全かつ確実に、すばやく接続してアクセスできます。次のようにできます。

- AWS Directory Service : Active Directory Connector (AD Connector) を使用して、既存のオンプレミス Microsoft Active Directory (AD) を活用します。
- ディレクトリを AWS クラウドに拡張します。
- AWS Directory Service Microsoft AD または Simple AD を使用してマネージドディレクトリを構築し、ユーザーと を管理します WorkSpaces。
- AD Connector でオンプレミスまたはクラウドホスト型 RADIUS サーバーを活用して、 に多要素認証 (MFA) を提供します WorkSpaces。

CLI または API WorkSpaces を使用して Amazon のプロビジョニングを自動化できます。これにより、Amazon を既存のプロビジョニングワークフロー WorkSpaces に統合できます。

セキュリティ上の理由から、Amazon WorkSpaces のサービスが提供する統合ネットワーク暗号化に加えて、 の保管時の暗号化を有効にすることもできます WorkSpaces。このドキュメントの「暗号化 WorkSpaces」セクションを参照してください。

Microsoft System Center Configuration Manager (SCCM)、Puppet Enterprise、Ansible などの WorkSpaces 既存のオンプレミスツールを使用して、アプリケーションを にデプロイできます。

以下のセクションでは WorkSpaces、Amazon の詳細、サービスの仕組み、サービスの起動に必要な内容、使用できるオプションと機能について説明します。

WorkSpaces の要件

Amazon WorkSpaces サービスが正常にデプロイするには、次の 3 つのコンポーネントが必要です。

- WorkSpaces クライアントアプリケーション — Amazon WorkSpacesがサポートするクライアントデバイス。「 の開始方法 WorkSpace」を参照してください。

  また、Personal Computer over Internet Protocol (PCoIP) ゼロクライアントを使用して に接続することもできます WorkSpaces。使用可能なデバイスのリストについては、「Amazon の PCoIP ゼロクライアント WorkSpaces」を参照してください。
- ユーザーを認証し、そのユーザーへのアクセスを提供するディレクトリサービス WorkSpace — Amazon WorkSpaces は現在、AWS Directory Service と Microsoft AD で動作しています。 AWS Directory Service でオンプレミス AD サーバーを使用して、Amazon で既存のエンタープライズユーザー認証情報をサポートできます WorkSpaces。
- Amazon を実行する Amazon Virtual Private Cloud (Amazon VPC) WorkSpaces — 各 AWS Directory Service コンストラクトにはマルチ AZ 配置に 2 つのサブネットが必要なため、Amazon WorkSpaces デプロイには最低 2 つのサブネットが必要です。

ネットワークに関する考慮事項

各 WorkSpace は、作成に使用した特定の Amazon VPC および AWS Directory Service コンストラクトに関連付けられます。すべての AWS Directory Service コンストラクト (Simple AD、AD Connector、および Microsoft AD) では、それぞれ異なるアベイラビリティーゾーン (AZs) で動作する 2 つのサブネットが必要です。サブネットは Directory Service コンストラクトに永続的に関連付けられており、作成後に変更することはできません。このため、Directory Services コンストラクトを作成する前に、適切なサブネットサイズを決定することが不可欠です。サブネットを作成する前に、次の点を慎重に検討してください。

- 時間の経過とともに必要 WorkSpaces になる はいくつありますか？
- 予想される増加はどのくらいですか？
- どのタイプのユーザーに対応する必要がありますか？
- 接続する AD ドメインの数はいくつですか？
- エンタープライズアカウントの場所

Amazon では、計画プロセスの一環として必要なアクセスのタイプとユーザー認証に基づいて、ユーザーグループまたはペルソナを定義することを推奨しています。これらの質問への回答は、特定のアプリケーションまたはリソースへのアクセスを制限する必要がある場合に役立ちます。定義されたユーザーペルソナは、 AWS Directory Service、ネットワークアクセスコントロールリスト、ルーティングテーブル、VPC セキュリティグループを使用してアクセスをセグメント化および制限するのに役立ちます。各 AWS Directory Service コンストラクトは 2 つのサブネットを使用し、そのコンストラクトから起動 WorkSpaces するすべての に同じ設定を適用します。例えば、AD Connector にア WorkSpaces タッチされているすべての に適用されるセキュリティグループを使用して、MFA が必要かどうか、またはエンドユーザーが でローカル管理者アクセス権を持つかどうかを指定できます WorkSpace。

> **Note**
>
> 各 AD Connector は、既存の Enterprise Microsoft AD に接続します。この機能を利用して組織単位 (OU) を指定するには、ユーザーのペルソナを考慮するように Directory Service を構築する必要があります。

VPC の設計

このセクションでは、VPC とサブネットのサイズ設定、トラフィックフロー、ディレクトリサービス設計への影響に関するベストプラクティスについて説明します。

ここでは、Amazon の VPC、サブネット、セキュリティグループ、ルーティングポリシー、ネットワークアクセスコントロールリスト (ACLsを設計する際に考慮すべき点をいくつか紹介 WorkSpaces し、スケール、セキュリティ、管理のしやすさのための WorkSpaces 環境を構築できるようにします。

- VPC — WorkSpaces デプロイ専用の別の VPC を使用することをお勧めします。別の VPC を使用すると、トラフィックを分離 WorkSpaces することで、 に必要なガバナンスとセキュリティガードレールを指定できます。
- ディレクトリサービス — 各 AWS Directory Service コンストラクトには、AZs 間で可用性の高いディレクトリサービス分割を提供するサブネットのペアが必要です。
- サブネットサイズ — WorkSpaces デプロイはディレクトリコンストラクトに関連付けられ、選択した と同じ VPC に存在しますが AWS Directory Service、異なる VPC サブネットに配置できます。いくつかの考慮事項：
  - サブネットサイズは永続的であり、変更できません。将来の成長に備えて十分なスペースを確保する必要があります。
  - 選択した にデフォルトのセキュリティグループを指定できます AWS Directory Service。セキュリティグループは、特定の AWS Directory Service コンストラクトに関連付けられているすべての WorkSpaces に適用されます。
  - 複数の インスタンスで同じサブネット AWS Directory Service を使用できます。

VPC を設計するときは、将来の計画を検討してください。例えば、ウイルス対策サーバー、パッチ管理サーバー、AD または RADIUS MFA サーバーなどの管理コンポーネントを追加したい場合があります。このような要件を満たすために、VPC 設計で使用可能な IP アドレスを追加で計画する価値があります。

VPC 設計とサブネットのサイズ設定に関する詳細なガイダンスと考慮事項については、re:Invent プレゼンテーション「Amazon.com が Amazon に移行する WorkSpaces方法」を参照してください。

ネットワークインターフェイス

各 WorkSpaces には 2 つの Elastic Network Interface (ENIs管理ネットワークインターフェイス (eth0) 、プライマリネットワークインターフェイス () がありますeth1。 は管理ネットワークインターフェイス AWS を使用して WorkSpace を管理します。これはクライアント接続が終了するインターフェイスです。このインターフェイスのプライベート IP アドレス範囲 AWS を使用します。ネットワークルーティングが正しく機能するためには、 WorkSpaces VPC と通信できるネットワークでこのプライベートアドレス空間を使用することはできません。

リージョンごとに使用されるプライベート IP 範囲のリストについては、「Amazon WorkSpaces の詳細」を参照してください。

> **Note**
>
> Amazon WorkSpaces および関連する管理ネットワークインターフェイスは VPC 内に存在せず、 で管理ネットワークインターフェイスまたは Amazon Elastic Compute Cloud (Amazon EC2) インスタンス ID を表示することはできません AWS Management Console （ Figure 5、Figure 6、および を参照Figure 7 ）。ただし、コンソールでプライマリネットワークインターフェイス (eth1) のセキュリティグループ設定を表示および変更できます。それぞれのプライマリネットワークインターフェイス WorkSpace は、ENI Amazon EC2 リソースクォータにカウントされます。Amazon の大規模なデプロイでは WorkSpaces、 経由でサポートチケットを開いて ENI クォータ AWS Management Console を増やす必要があります。

トラフィックフロー

Amazon WorkSpaces トラフィックを 2 つの主要コンポーネントに分割できます。

- クライアントデバイスと Amazon WorkSpaces サービス間のトラフィック。
- Amazon WorkSpaces サービスとカスタマーネットワークトラフィック間のトラフィック。

次のセクションでは、これらのコンポーネントの両方について説明します。

クライアントデバイスから WorkSpace

場所 (オンプレミスまたはリモート) に関係なく、Amazon WorkSpaces クライアントを実行しているデバイスは、Amazon WorkSpaces サービスへの接続に同じ 2 つのポートを使用します。クライアントは、すべての認証およびセッション関連の情報にポート 443 (HTTPS ポート) を使用し、特定の WorkSpace およびネットワークヘルスチェックへのピクセルストリーミングに Transmission Control Protocol (TCP) と User Datagram Protocol (UDP) の両方にポート 4172 (PCoIP ポート) を使用します。両方のポートのトラフィックは暗号化されます。ポート 443 トラフィックは認証およびセッション情報に使用され、トラフィックの暗号化に TLS を使用します。ピクセルストリーミングトラフィックは、ストリーミングゲートウェイを介したクライアントと `eth0` の通信に WorkSpaceAES-256-bit暗号化を使用します。詳細については、このドキュメントのセキュリティ「」セクションを参照してください。

PCoIP ストリーミングゲートウェイとネットワークヘルスチェックエンドポイントのリージョンごとの IP 範囲を公開しています。Amazon を使用している特定の AWS リージョンへのポート 4172 のアウトバウンドトラフィックのみを許可することで、企業ネットワークから AWS ストリーミングゲートウェイおよびネットワークヘルスチェックエンドポイントへのポート 4172 のアウトバウンドトラフィックを制限できます WorkSpaces。IP 範囲とネットワークヘルスチェックエンドポイントについては、「Amazon WorkSpaces PCoIP Gateway IP 範囲」を参照してください。

Amazon WorkSpaces クライアントには、ネットワークステータスチェックが組み込まれています。このユーティリティは、アプリケーションの右下のステータスインジケータを使用して、ネットワークが接続をサポートできるかどうかを示します。次の図は、クライアントの右上にあるネットワークを選択して、ネットワークステータスのより詳細なビューにアクセスできることを示しています。

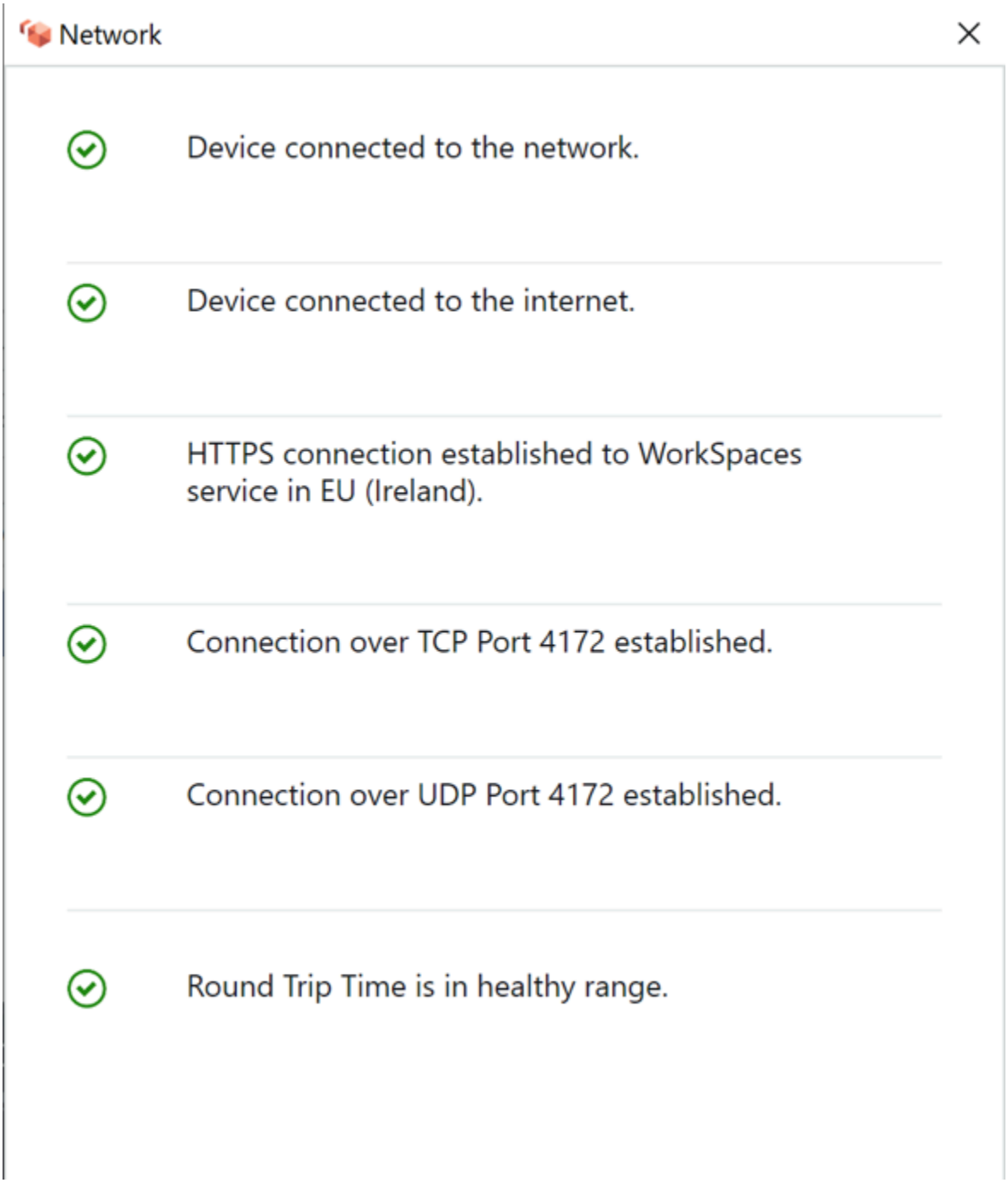

図 1: WorkSpaces クライアント: ネットワークチェック

ユーザーは、Directory Service コンストラクトで使用されるディレクトリ、通常は社内ディレクトリのログイン情報を指定して、クライアントから Amazon WorkSpaces サービスへの接続を開始します。ログイン情報は、 が配置されているリージョンの Amazon WorkSpaces サービスの認証ゲートウェイに HTTPS 経由で送信 WorkSpace されます。Amazon WorkSpaces サービスの認証ゲート

ウェイは、 に関連付けられた特定の AWS Directory Service コンストラクトにトラフィックを転送します WorkSpace。

例えば、AD Connector を使用する場合、AD Connector は認証リクエストを AD サービスに直接転送します。AD サービスはオンプレミスでも AWS VPC でもかまいません。詳細については、このドキュメントの「AD DS デプロイシナリオ」セクションを参照してください。AD Connector は認証情報を保存せず、ステートレスプロキシとして機能します。そのため、AD Connector は AD サーバーに接続することが不可欠です。AD Connector は、AD Connector の作成時に定義した DNS サーバーを使用して、接続先の AD サーバーを決定します。

AD Connector を使用していて、 ディレクトリで MFA が有効になっている場合、MFA トークンはディレクトリサービス認証の前にチェックされます。MFA 検証が失敗した場合、ユーザーのログイン情報は AWS Directory Service に転送されません。

ユーザーが認証されると、ストリーミングトラフィックは、 AWS ストリーミングゲートウェイ経由で へのポート 4172 (PCoIP ポート) を使用して開始されます WorkSpace。セッション関連の情報は、セッション全体で引き続き HTTPS 経由で交換されます。ストリーミングトラフィックは、VPC に接続されていない WorkSpace （ `eth0` の WorkSpace) で最初の ENI を使用します。ストリーミングゲートウェイから ENI へのネットワーク接続は、 によって管理されます AWS。ストリーミングゲートウェイから WorkSpaces ストリーミング ENI への接続に障害が発生した場合は、CloudWatch イベントが生成されます。詳細については、このドキュメントの「Amazon を使用したモニタリングまたはログ記録 CloudWatch」セクションを参照してください。

Amazon WorkSpaces サービスとクライアントの間で送信されるデータ量は、ピクセルアクティビティのレベルによって異なります。ユーザーに最適なエクスペリエンスを得るには、 WorkSpaces クライアントと が WorkSpaces 配置されている AWS リージョン間のラウンドトリップタイム (RTT) を 100 ミリ秒 (ms) 未満にすることをお勧めします。通常、これは WorkSpaces クライアントが、 がホスト WorkSpace されているリージョンから 2,000 マイル未満にあることを意味します。Connection Health Check ウェブページは、Amazon WorkSpaces サービスに接続するための最適な AWS リージョンを決定するのに役立ちます。

Amazon WorkSpaces サービスから VPC へ

クライアントから への接続が認証 WorkSpace され、ストリーミングトラフィックが開始されると、 WorkSpaces クライアントには仮想プライベートクラウド (VPC WorkSpace) に接続されている Windows または Linux デスクトップ (Amazon) のいずれかが表示され、その接続が確立されたことがネットワークに示されます。として識別される WorkSpaceのプライマリ Elastic Network Interface (ENI) には`eth1`、VPC が提供する Dynamic Host Configuration Protocol (DHCP) サービス

から、通常は AWS Directory Service と同じサブネットから IP アドレスが割り当てられます。IP アドレスは、 WorkSpaceの存続期間中、 に残ります WorkSpace。VPC 内の ENI は、VPC 内の任意のリソース、および VPC に接続した任意のネットワーク (VPC ピアリング、 AWS Direct Connect 接続、または VPN 接続経由) にアクセスできます。

ネットワークリソースへの ENI アクセスは、Directory AWS Service が各 に設定するサブネットのルートテーブルとデフォルトのセキュリティグループ WorkSpace、および ENI に割り当てる追加のセキュリティグループによって決まります。 AWS Management Console または を使用して、VPC に向ける ENI にセキュリティグループをいつでも追加できます AWS CLI。 (セキュリティグループの詳細については、「 のセキュリティグループ WorkSpaces」を参照してください。) セキュリティグループに加えて、特定の で任意のホストベースのファイアウォールを使用して WorkSpace 、VPC 内のリソースへのネットワークアクセスを制限できます。

ご使用の環境に固有の Active Directory の権限を持つ DNS サーバー IP (複数可) と完全修飾ドメイン名を使用して DHCP オプションセットを作成し、それらのカスタム作成 DHCP オプションセットを Amazon が使用する Amazon VPC に割り当てることをお勧めします WorkSpaces。デフォルトでは、Amazon Virtual Private Cloud (Amazon VPC) はディレクトリサービスの AWS DNS の代わりに DNS を使用します。DHCP オプションセットを使用すると、 だけでなく WorkSpaces、デプロイのために計画したサポートワークロード (複数可) またはインスタンス (複数可) に対しても、内部 DNS ネームサーバーの適切な DNS 名解決と一貫した設定が保証されます。

DHCP オプションを適用する場合、従来の EC2 インスタンスでどのように適用されるか WorkSpaces とは対照的に、それらがどのように に適用されるかには 2 つの重要な違いがあります。 EC2

- 最初の違いは、DHCP オプション DNS サフィックスがどのように適用されるかです。各 WorkSpace には、プライマリ DNS サフィックスと接続固有の DNS サフィックスを追加し、プライマリ DNS サフィックスオプションの親サフィックスを追加できるネットワークアダプター用に設定された DNS 設定があります。設定は、登録して に WorkSpace デフォルトで関連付けた Directory Service AWS 内で設定された DNS サフィックスで更新されます。また、使用する DHCP オプションセット内で設定された DNS サフィックスが異なる場合は、関連付けられた に追加されて適用されます WorkSpaces。
- 2 つ目の違いは、Amazon WorkSpaces サービスが設定済みディレクトリのドメインコントローラー IPs アドレスに優先順位を付ける WorkSpace ため、設定済み DHCP オプション DNS IP は に適用されないことです。

または、ハイブリッドまたは分割された DNS 環境をサポートし、Amazon WorkSpaces 環境に適した DNS 解決を取得するように Route 53 プライベートホストゾーンを設定することもできます。詳

細については、「VPC のハイブリッドクラウド DNS オプション」およびAWS 「アクティブディレクトリ のハイブリッド DNS」を参照してください。

> **Note**
>
> 新しい DHCP オプションセットまたは異なる DHCP オプションセットを VPC に適用するときは、それぞれ IP テーブルを更新 WorkSpace する必要があります。更新するには、更新された DHCP オプションセットで設定された VPC で ipconfig /renew を実行するか、 WorkSpace(s) を再起動できます。AD Connector を使用していて、接続されている IP アドレス/ドメインコントローラーの IP アドレスを更新する場合は、 の Skylight `DomainJoinDNS`レジストリキーを更新する必要があります WorkSpaces。GPO 経由でこれを行うことをお勧めします。このレジストリキーへのパスは ですHKLM:\SOFTWARE\Amazon\Skylight。AD Connector の DNS 設定が変更されても、この値は更新`REG_SZ`されず、VPC DHCP オプションセットもこのキーを更新しません。

このホワイトペーパーの AD DS デプロイシナリオセクションの図は、説明されているトラフィックフローを示しています。

前述のように、Amazon WorkSpaces サービスは DNS 解決のために設定済みディレクトリのドメインコントローラー IP アドレスを優先し、DHCP オプションセットで設定されている DNS サーバーを無視します。Amazon の DNS サーバー設定をより細かく制御する必要がある場合は WorkSpaces、「Amazon 管理ガイド」の「Amazon の DNS サーバーの更新」ガイド WorkSpaces にある手順を使用して、Amazon の DNS サーバー WorkSpacesを更新できます。 WorkSpaces

で他のサービスを解決 WorkSpaces する必要がある場合 AWS、VPC で設定されたデフォルトの DHCP オプションを使用している場合、この VPC 内のドメインコントローラー DNS サービスは、VPC CIDR のベースに IP アドレスに 2 を加えた https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#AmazonDNSDNS 転送を使用するように設定する必要があります。つまり、VPC CIDR が 10.0.0.0/24 の場合は、標準の Route 53 DNS リゾルバー 10.0.0.2 を使用するように DNS 転送を設定する必要があります。

でオンプレミスネットワーク上のリソースの DNS 解決 WorkSpaces が必要な場合は、Route 53 Resolver アウトバウンドエンドポイント を使用し、Route 53 転送ルールを作成して、この DNS 解決を必要とする VPCs にこのルールを関連付けます。前の段落で説明したように、ドメインコントローラー DNS サービスで転送を VPC のデフォルトの Route 53 DNS リゾルバーに設定した場合、DNS 解決プロセスは、Amazon Route 53 デベロッパーガイドの「VPC とVPCs」に記載されています。

デフォルトの DHCP オプションセットを使用していて、Active Directory ドメインに含まれていない VPCs 内の他のホストが Active Directory 名前空間内のホスト名を解決できるようにする場合は、この Route 53 Resolver アウトバウンドエンドポイントを使用し、Active Directory ドメインの DNS クエリを Active Directory DNS サーバーに転送する別の Route 53 転送ルールを追加できます。この Route 53 転送ルールは、Active Directory DNS サービスに到達できる Route 53 Resolver アウトバウンドエンドポイント、および WorkSpaces Active Directory ドメイン内の DNS レコードの解決を有効にするすべての VPCs に関連付ける必要があります。

同様に、Route 53 Resolver インバウンドエンドポイントを使用して、オンプレミスネットワークから Active Directory ドメインの WorkSpaces DNS レコードの DNS 解決を許可できます。

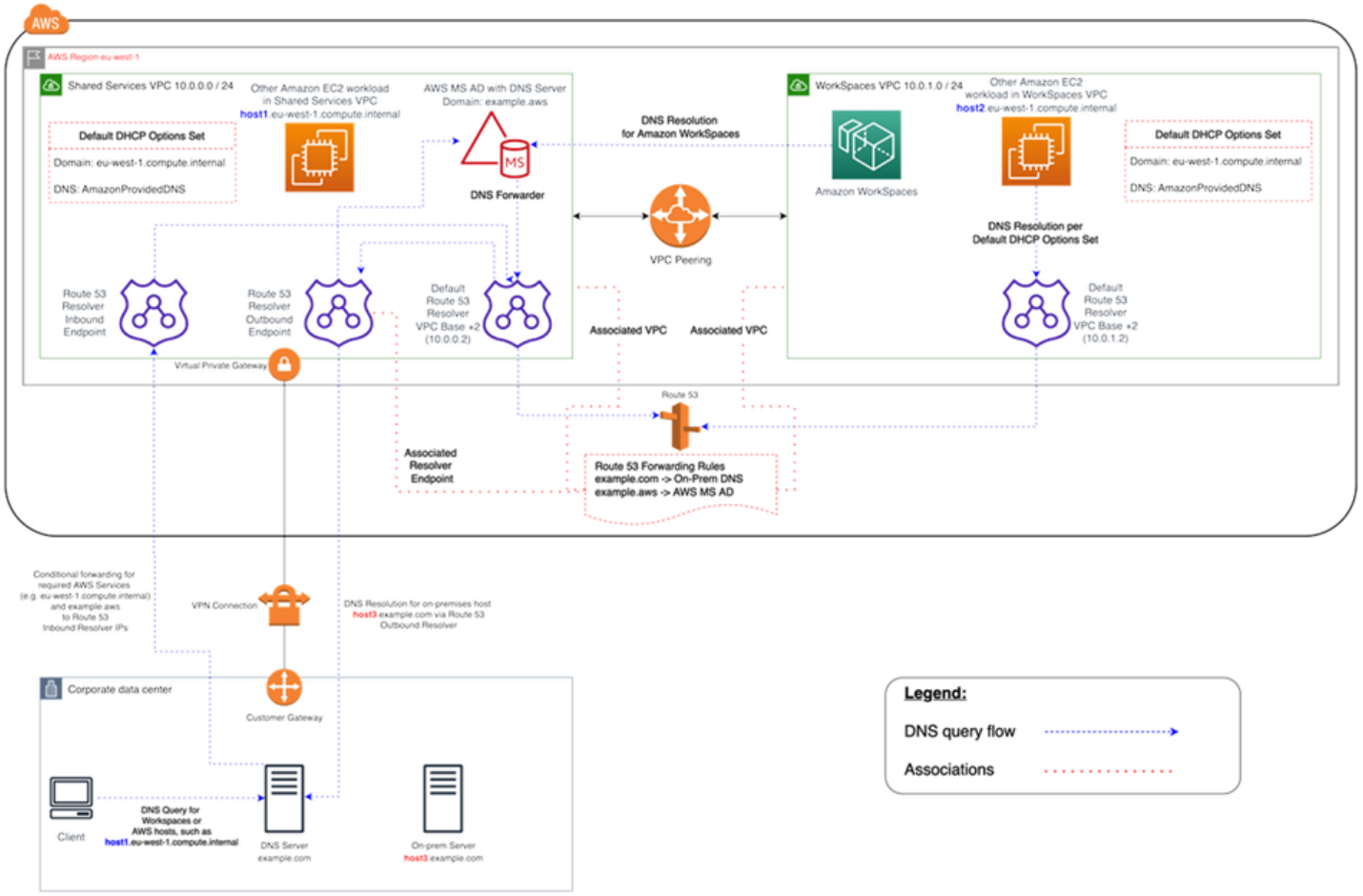

図 2: Route 53 エンドポイントを使用した WorkSpaces DNS 解決の例

- Amazon WorkSpaces は DNS 解決に AWS Directory Service for Microsoft Active Directory （ AWS Managed Microsoft AD) DNS サービスを使用します。 AWS Managed Microsoft AD DNS サービスは`example.aws`ドメインを解決し、他のすべての DNS クエリを VPC CIDR ベース IP アドレス +2 のデフォルトの Route 53 DNS Resolver に転送して DNS 解決を有効にします。

共有サービス VPC には、2 つの Route 53 転送ルールに関連付けられた Route 53 アウトバウンドリゾルバーエンドポイントが含まれています。これらのルールの 1 つが、example.comドメインの DNS クエリをオンプレミスの DNS サーバーに転送します。2 番目のルールは、 AWS Managed Microsoft AD ドメインの DNS クエリexample.awsを共有サービス VPC の Active Directory DNS サービスに転送します。

このアーキテクチャでは、Amazon WorkSpaces は次の DNS クエリを解決できます。

- AWS Managed Microsoft AD ドメイン example.aws。
- デフォルトの DHCP オプションセット (などhost1.eu-west-1.compute.internal) と、他の AWS サービスまたはエンドポイントで設定されたドメイン内の EC2 インスタンス。
- などのオンプレミスドメインのホストとサービスhost3.example.com。

- • 共有サービス VPC (host1.eu-west-1.compute.internal) および WorkSpaces VPC (host2.eu-west-1.compute.internal) 内の他の EC2 ワークロードは、Route 53 転送ルールが両方の VPCs に関連付けられている限り WorkSpaces、 と同じ DNS 解決を実行できます。この場合、example.awsドメインの DNS 解決は、VPC CIDR ベース IP アドレス +2 のデフォルトの Route 53 DNS リゾルバーを通過します。この IP アドレスは、設定および関連する Route 53 転送ルールごとに Route 53 Resolver アウトバウンドエンドポイント WorkSpacesを介してアクティブディレクトリ DNS サービスに転送されます。
- • 最後に、オンプレミスのクライアントは同じ DNS 解決を実行することもできます。オンプレミスの DNS サーバーは example.awsおよび eu-west-1.compute.internalドメインの条件付きフォワーダーで構成され、これらのドメインの DNS クエリを Route 53 Resolver インバウンドエンドポイント IP アドレスに転送するためです。

一般的な設定の例

2 種類のユーザーがあり、 AWS Directory Service がユーザー認証に一元化された AD を使用するシナリオを考えてみましょう。

- どこからでもフルアクセスを必要とするワーカー (フルタイム従業員など) — これらのユーザーはインターネットと内部ネットワークへのフルアクセスを持ち、VPC からオンプレミスネットワークにファイアウォールを通過します。
- 社内ネットワーク内からのアクセスのみを制限するワーカー (請負業者やコンサルタントなど) — これらのユーザーは、プロキシサーバー経由で VPC 内の特定のウェブサイトへのインターネットアクセスを制限され、VPC 内およびオンプレミスネットワークへのネットワークアクセスが制限されます。

フルタイムの従業員にソフトウェアをインストール WorkSpace するためのローカル管理者アクセス権を付与し、MFA による 2 要素認証を実施したい場合。また、フルタイムの従業員が、 の制限なしにインターネットにアクセスできるようにしたいと考えています WorkSpace。

請負業者の場合、特定のプリインストールされたアプリケーションのみを使用できるように、ローカル管理者アクセスをブロックする必要があります。これらの のセキュリティグループを使用して、制限的なネットワークアクセスコントロールを適用したい場合 WorkSpaces。特定の内部ウェブサイトに対してのみポート 80 と 443 を開く必要があり、そのウェブサイトからのインターネットへのアクセスを完全にブロックする必要があります。

このシナリオでは、ネットワークアクセスとデスクトップアクセスの要件が異なる 2 種類のユーザーペルソナがあります。管理と設定 WorkSpaces 方法はベストプラクティスです。ユーザーペルソナごとに 1 つずつ、合計 2 つの AD Connector を作成する必要があります。各 AD Connector には、使用量の増加の見積りを満たす WorkSpacesのに十分な IP アドレスを持つ 2 つのサブネットが必要です。

> **Note**
>
> 各 AWS VPC サブネットは、管理目的で 5 つの IP アドレス (最初の 4 つ目と最後の IP アドレス) を消費し、各 AD Connector は、それが保持される各サブネットで 1 つの IP アドレスを消費します。

このシナリオのその他の考慮事項は次のとおりです。

- AWS VPC サブネットはプライベートサブネットにする必要があります。これにより、インターネットアクセスなどのトラフィックは、ネットワークアドレス変換 (NAT) ゲートウェイ、クラウド内のプロキシ NAT サーバー、またはオンプレミスのトラフィック管理システムを介してルーティングし直すことができます。
- ファイアウォールは、オンプレミスネットワークに向かうすべての VPC トラフィックに設定されます。
- Microsoft AD サーバーと MFA RADIUS サーバーは、オンプレミス (このドキュメントの「シナリオ 1: AD Connector を使用してオンプレミス AD DS をプロキシ認証する」を参照) または クラウド実装の一部 (このドキュメントの「シナリオ 2」と「シナリオ 3、AD DS デプロイシナリオ」を参照) です。 AWS ???

すべての には何らかのインターネットアクセス WorkSpaces が付与され、プライベートサブネットでホストされている場合、インターネットゲートウェイを介してインターネットにアクセスできるパ

ブリックサブネットも作成する必要があります。フルタイム従業員には、インターネットへのアクセスを許可する NAT ゲートウェイが必要です。また、コンサルタントと請負業者には Proxy-NAT サーバーを使用して、特定の社内ウェブサイトへのアクセスを制限する必要があります。障害の計画、高可用性の設計、AZ 間のトラフィック料金の制限を行うには、マルチ AZ 配置の 2 つの異なるサブネットに 2 つの NAT ゲートウェイと NAT サーバーまたはプロキシサーバーが必要です。パブリックサブネットとして選択した 2 つの AZs は、3 つ以上のゾーンを持つリージョンで、 WorkSpaces サブネットに使用する 2 つの AZs と一致します。各 WorkSpaces AZ から対応するパブリックサブネットにすべてのトラフィックをルーティングして、AZ 間のトラフィック料金を制限し、管理を容易にすることができます。次の図は、VPC 設定を示しています。

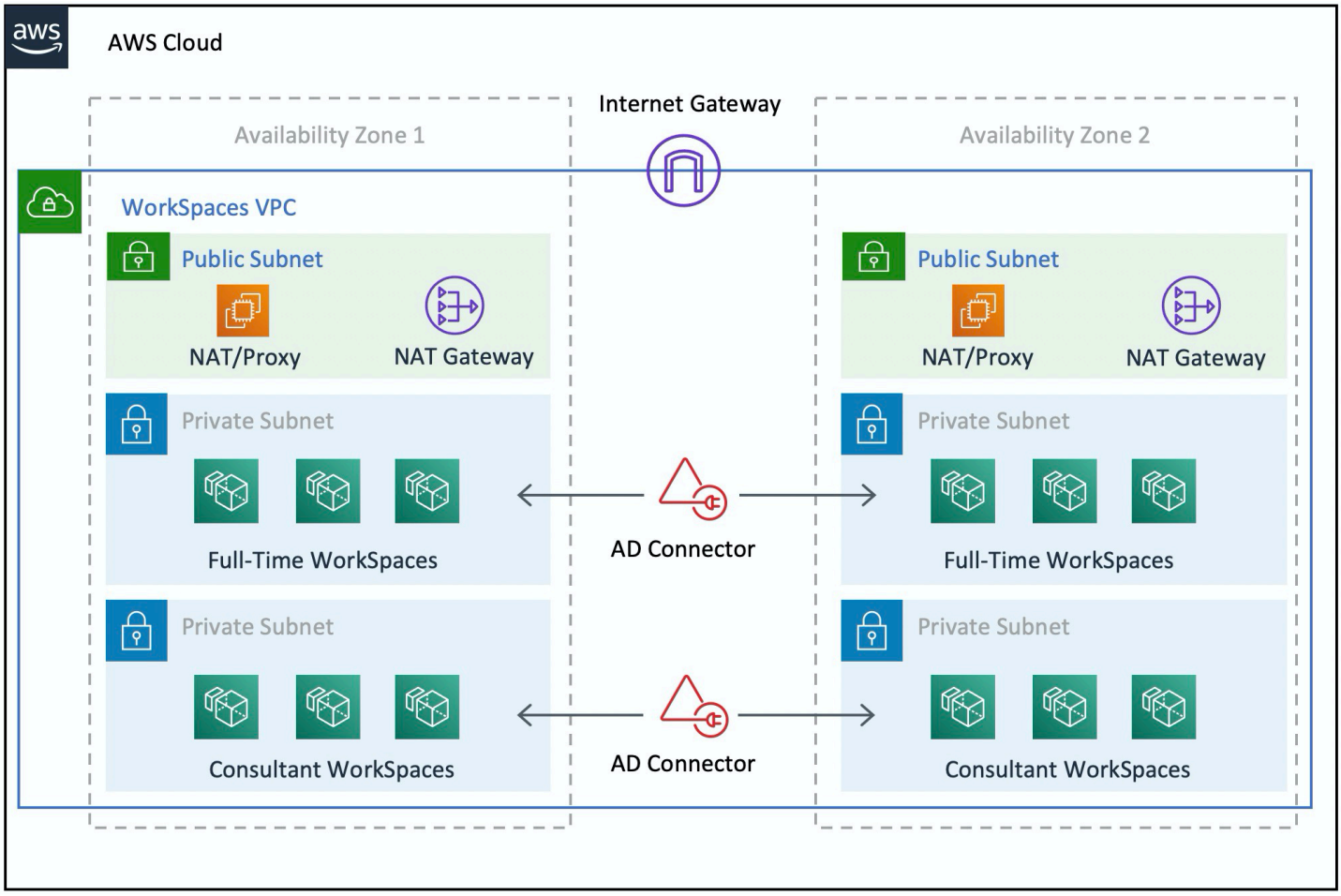

図 3: 高レベルの VPC 設計

次の情報では、2 つの異なる WorkSpaces タイプを設定する方法について説明します。

フルタイム従業員 WorkSpaces を設定するには：

1. Amazon WorkSpaces マネジメントコンソールで、メニューバーのディレクトリオプションを選択します。

2. フルタイム従業員をホストするディレクトリを選択します。
3. ローカル管理者設定を選択します。

このオプションを有効にすると、新しく作成されたすべての にローカル管理者権限が付与 WorkSpace されます。インターネットアクセスを許可するには、VPC からのアウトバウンドインターネットアクセス用に NAT を設定します。MFA を有効にするには、RADIUS サーバー、サーバー IPs、ポート、事前共有キーを指定する必要があります。

フルタイム従業員の場合 WorkSpaces、AD Connector 設定を介してデフォルトのセキュリティグループを適用することで、 へのインバウンドトラフィックを、 ヘルプスクサブネットからのリモートデスクトッププロトコル (RDP) に制限 WorkSpace できます。

を請負業者とコンサルタント WorkSpaces 用に設定するには：

1. Amazon WorkSpaces マネジメントコンソールで、インターネットアクセスとローカル管理者設定を無効にします。
2. セキュリティグループ設定セクションにセキュリティグループを追加して、そのディレクトリの下に作成されるすべての新しい WorkSpaces にセキュリティグループを適用します。

コンサルタントの場合は WorkSpaces、AD Connector 設定を介してデフォルトのセキュリティグループを AD Connector WorkSpaces に関連付けられているすべての に適用 WorkSpaces することで、 へのアウトバウンドトラフィックとインバウンドトラフィックを制限します。セキュリティグループは、 から HTTP および HTTPS 以外のトラフィック WorkSpaces へのアウトバウンドアクセス、およびオンプレミスネットワークの Helpdesk サブネットから RDP へのインバウンドトラフィックを防止します。

> **Note**
>
> セキュリティグループは、VPC 内の ENI (`eth1` の WorkSpace) にのみ適用され、セキュリティグループの結果として WorkSpaces クライアント WorkSpace からの へのアクセスは制限されません。次の図は、最終的な WorkSpaces VPC 設計を示しています。

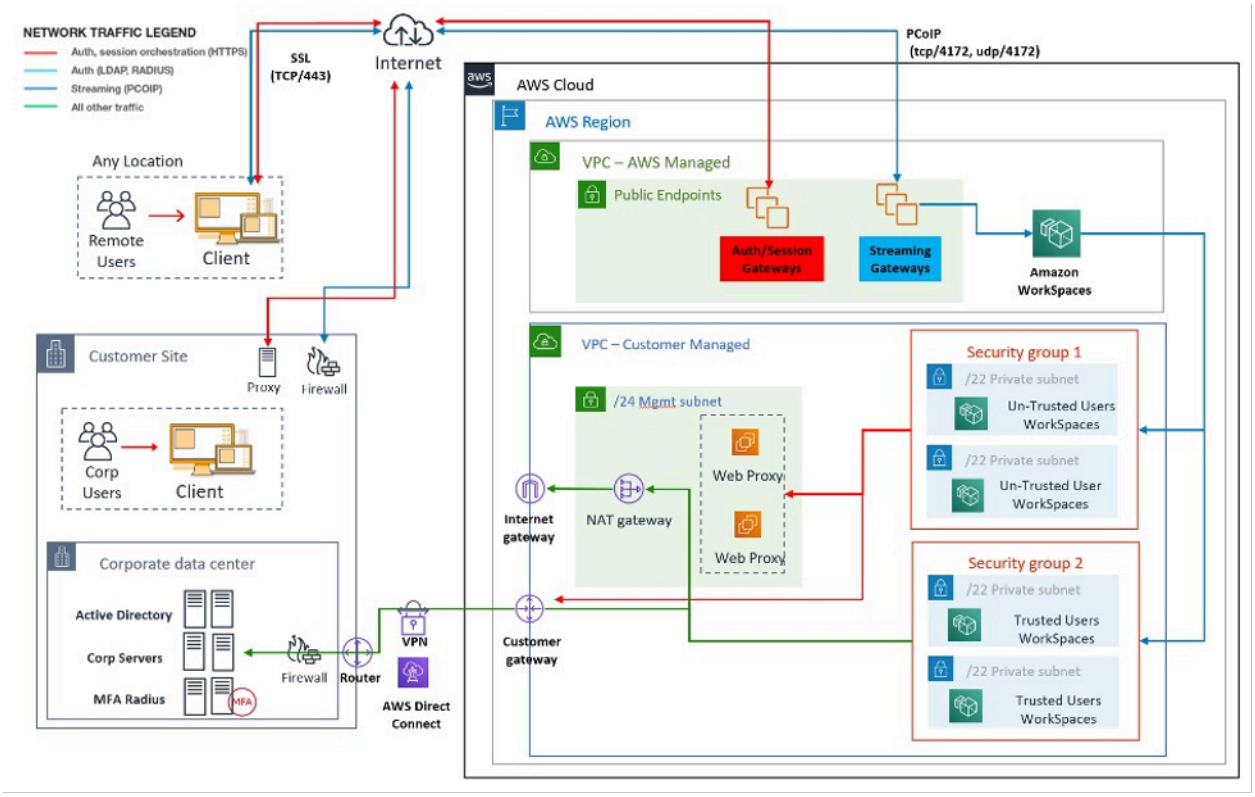

図 4: ユーザーペルソナを使用して WorkSpaces 設計する

AWS ディレクトリサービス

紹介で説明したように、 AWS Directory Service は Amazon のコアコンポーネントです WorkSpaces。 AWS Directory Service では、Amazon で 3 種類のディレクトリを作成できます WorkSpaces。

- AWS Managed Microsoft AD は、Windows Server 2012 R2. AWS Managed Microsoft AD を搭載したマネージド Microsoft AD で、Standard Edition または Enterprise Edition で利用できます。
- Simple AD は、スタンドアロンの Microsoft AD 互換の、Samba 4 を搭載したマネージドディレクトリサービスです。
- AD Connector は、認証リクエストとユーザーまたはグループ検索を既存のオンプレミス Microsoft AD にリダイレクトするためのディレクトリプロキシです。

次のセクションでは、Amazon WorkSpaces ブローカーage サービスと AWS Directory Service 間の認証の通信フロー、 AWS Directory Service による実装 WorkSpacesのベストプラクティス、および MFA などの高度な概念について説明します。また、オンプレミスの Microsoft AD ドメインサービス

(AD DS) との統合など、Amazon WorkSpaces の大規模なインフラストラクチャアーキテクチャの概念、Amazon VPC の要件、および AWS Directory Service についても説明します。

AD DS デプロイシナリオ

Amazon のバックアップ WorkSpaces は AWS Directory Service であり、ディレクトリサービスの適切な設計とデプロイが不可欠です。以下の 6 つのシナリオは、 AWS クイックスタートガイドの Active Directory ドメインサービスに基づいて構築され、Amazon で使用する AD DS のベストプラクティスのデプロイオプションについて説明します WorkSpaces。このドキュメントの「設計上の考慮事項」セクションでは、AD Connector for を使用する際の具体的な要件とベストプラクティスについて詳しく説明しています。これは WorkSpaces、設計概念全体 WorkSpacesにおいて不可欠なものです。

- シナリオ 1: AD Connector を使用してオンプレミス AD DS に認証をプロキシする — このシナリオでは、ネットワーク接続 (VPN/Direct Connect) がお客様に導入され、すべての認証が Directory Service (AD Connector) を介して AWS オンプレミス AD DS にプロキシされます。
- シナリオ 2: オンプレミス AD DS を AWS （ レプリカ) に拡張する — このシナリオはシナリオ 1 と似ていますが、ここではカスタマー AD DS のレプリカが AD Connector と組み合わせて AWS にデプロイされるため、AD DS および AD DS グローバルカタログへの認証/クエリリクエストのレイテンシーが軽減されます。
- シナリオ 3: AWS クラウドの AWS Directory Service を使用したスタンドアロンの分離されたデプロイ — これは分離されたシナリオであり、認証のために顧客への接続は含まれません。このアプローチでは、 AWS Directory Service (Microsoft AD) と AD Connector を使用します。このシナリオでは、顧客への接続を認証に依存しませんが、VPN または Direct Connect 経由で必要な場合、アプリケーショントラフィックをプロビジョニングします。
- シナリオ 4: AWS Microsoft AD とオンプレミスへの双方向の推移的信頼 — このシナリオには、オンプレミスの Microsoft AD フォレストへの双方向の推移的信頼を持つ AWS Managed Microsoft AD Service (MAD) が含まれます。
- シナリオ 5: 共有サービス VPC を使用する AWS Microsoft AD — このシナリオでは、共有サービス VPC 内の AWS Managed Microsoft AD を複数の AWS サービス (Amazon EC2、Amazon など) のアイデンティティドメインとして使用し WorkSpaces、AD Connector を使用して Lightweight Directory Access Protocol (LDAP) ユーザー認証リクエストを AD ドメインコントローラーにプロキシします。
- シナリオ 6: AWS Microsoft AD、共有サービス VPC、オンプレミス AD への 1 方向の信頼 — このシナリオはシナリオ 5 と似ていますが、オンプレミスへの一方向の信頼を使用して異なる ID ドメインとリソースドメインが含まれています。

Active Directory Domain Services (ADDS) のデプロイシナリオを選択する際には、いくつかの考慮事項を行う必要があります。このセクションでは、Amazon での AD Connector の役割について説明し WorkSpaces、ADDS デプロイシナリオを選択する際の重要な考慮事項をいくつか説明します。での ADDS の設計と計画に関する詳細なガイダンスについては AWS、AWS 「設計と計画に関する Active Directory ドメインサービス」ガイドを参照してください。

Amazon での AWS AD Connector のロール WorkSpaces

AWS AD Connector は、Active AWS Directory のプロキシサービスとして機能する Directory Service です。ユーザーの認証情報は保存またはキャッシュされませんが、認証またはルックアップリクエストをオンプレミスまたは 上の Active Directory に転送します AWS。を使用していない限り AWS Managed Microsoft AD、Amazon () で使用するために Active Directory (オンプレミスまたは に拡張 AWS) を登録する唯一の方法でもあります WorkSpaces WorkSpaces。

AD Connector は、オンプレミスの Active Directory、 AWS (Amazon EC2 の AD ドメインコントローラー) に拡張された Active Directory、または を指すことができます AWS Managed Microsoft AD。

AD Connector は、以下のセクションで説明するほとんどのデプロイシナリオで重要な役割を果たします。で AD Connector を使用すると、次のような多くの利点 WorkSpaces があります。

- 会社の Active Directory を指すと、ユーザーは既存の会社の認証情報を使用して、 WorkSpaces や Amazon WorkDocs などの他の サービスにログオンできます。
- 既存のセキュリティポリシー (パスワードの有効期限、アカウントロックアウトなど) は、ユーザーがオンプレミスインフラストラクチャや などの のリソースにアクセスするかどうかにかかわらず AWS クラウド、一貫して適用できます WorkSpaces。
- AD Connector を使用すると、既存の RADIUS ベースの MFA インフラストラクチャと簡単に統合して、セキュリティをさらに強化できます。
- これにより、ユーザーの分離が可能になります。例えば、複数の AD Connector がユーザー認証のために Active Directory の同じドメインコントローラー (DNS サーバー) を指す可能性があるため、ビジネスユニットまたはペルソナごとに多数の WorkSpaces オプションを設定できます。
  - Active Directory グループポリシーオブジェクト (GPOsのターゲットアプリケーション用のターゲットドメインまたは組織単位
  - との間のトラフィックフローを制御するさまざまなセキュリティグループ WorkSpaces
  - さまざまなアクセスコントロールオプション (許可されたクライアントデバイス) と IP アクセスコントロールグループ (IP 範囲へのアクセスの制限)
  - ローカル管理者権限の選択的な有効化

- さまざまなセルフサービスアクセス許可
- Multi-Factor Authentication (MFA)の選択的な強制
- 分離のための異なる VPCs またはサブネットへの WorkSpaces Elastic Network Interface (ENI) の配置

複数の AD Connector では、単一の小規模または大規模な AD Connector のパフォーマンス制限に達した場合、より多くのユーザーをサポートすることもできます。詳細については、のサイジング AWS Managed Microsoft AD「」セクションを参照してください。

で AD Connector を使用すること WorkSpaces は、小規模な AD Connector に 1 人以上のアクティブ WorkSpaces ユーザーがあり、大規模な AD Connector に 100 人以上のアクティブ WorkSpaces ユーザーがいれば、料金はかかりません。詳細については、AWS 「ディレクトリサービスの料金」ページを参照してください。

オンプレミスのアクティブディレクトリ AWS を使用した へのネットワークリンクの重要性

WorkSpaces は Active Directory への接続に依存しています。したがって、Active Directory へのネットワークリンクの可用性が最も重要です。例えば、シナリオ 1 のネットワークリンクがダウンしている場合、ユーザーは認証できず、その結果 を使用できなくなります WorkSpaces。

シナリオの一部としてオンプレミスの Active Directory を使用する場合は、 へのネットワークリンクの耐障害性、レイテンシー、トラフィックコストを考慮する必要があります AWS。マルチリージョン WorkSpaces デプロイでは、異なる AWS リージョンに複数のネットワークリンクがある場合や、オンプレミス AD に接続 AWS Transit Gatewayして AD トラフィックを VPC にルーティングするために、リージョン間でピアリングが確立されている複数の が含まれる場合があります。これらのネットワークリンクに関する考慮事項は、次のセクションで説明するほとんどのシナリオに適用されますが、AD Connector からの AD トラフィックと がオンプレミスの Active Directory に到達するためにネットワークリンクを経由 WorkSpaces する必要があるシナリオでは特に重要です。 シナリオ 1 では、いくつかの注意点に焦点を当てています。

での多要素認証の使用 WorkSpaces

でMulti-Factor Authentication (MFA) を使用する場合は WorkSpaces、AD Connector または を使用する必要があります AWS 。これらのサービスでのみ AWS Managed Microsoft AD、RADIUS WorkSpaces と RADIUS の設定で使用するディレクトリの登録が許可されるためです。RADIUS サーバーの配置については、オンプレミスのアクティブディレクトリ AWS を使用した へのネット

ワークリンクの重要性「」セクションで説明されているネットワークリンクに関する考慮事項が適用されます。

アカウントとリソースドメインの分離

セキュリティ上の理由から、または管理しやすくするために、アカウントドメインをリソースドメインから分離することをお勧めします。例えば、 WorkSpaces コンピュータオブジェクトを別のリソースドメインに配置し、ユーザーはアカウントドメインの一部になります。このような実装を使用すると、パートナー組織はリソースドメイン内の AD グループポリシーを使用して を管理 WorkSpacesできますが、コントロールを放棄したり、アカウントドメインへのアクセスを許可したりする必要はありません。これは、Active Directory Trust が設定された 2 つの Active Directory を使用することで実現できます。以下のセクションでこれについて詳しく説明します。

- シナリオ 4: AWS Microsoft AD とオンプレミスへの双方向の推移的信頼
- シナリオ 6: AWS Microsoft AD、共有サービス VPC、オンプレミスへの一方向の信頼

大規模な Active Directory デプロイ

Active Directory サイトとサービスが適切に設定されていることを確認する必要があります。これは、Active Directory が地理的に異なる場所にある多数のドメインコントローラーで構成されている場合に特に重要です。Windows WorkSpaces は、標準の Microsoft メカニズムを使用して、割り当てられている Active Directory サイトのドメインコントローラーを検出します。この DC Locator プロセスは DNS に依存しており、DC Locator プロセスの早い段階で特定の優先度と重みの異なるドメインコントローラーの長いリストが返された場合、大幅に長くなる可能性があります。さらに重要なのは、最適でないドメインコントローラーに WorkSpaces 「ピン留め」された場合、このドメインコントローラーとのそれ以降の通信はすべて、広域ネットワークリンクを通過するときに、ネットワークレイテンシーが増加し、帯域幅が減るのに悩む可能性があります。これにより、多数のグループポリシーオブジェクト (GPOsの処理やドメインコントローラーからのファイル転送など、ドメインコントローラーとの通信が遅くなります。ネットワークトポロジによっては、 WorkSpaces とドメインコントローラー間で交換されるデータが不必要にコストがかかるネットワークパスを通過する可能性があるため、ネットワークコストが増加する可能性があります。VPC 設計の DHCP と DNS、VPC の設計および Active Directory サイトとサービスに関するガイダンスについては、「」と設計上の考慮事項「」セクションを参照してください。

での Microsoft Azure Active Directory または Active Directory ドメインサービスの使用 WorkSpaces

で Microsoft Azure Active Directory を使用する場合は WorkSpaces、Azure AD Connect を使用して、オンプレミスの Active Directory または の Active Directory AWS (Amazon EC2 または のドメインコントローラー) と ID を同期できます AWS Managed Microsoft AD。ただし、これにより Azure Active Directory WorkSpaces に参加することはできません。詳細については、Microsoft Azure ドキュメントの「Microsoft Hybrid Identity Documentation」を参照してください。

を Azure Active Directory に結合する場合は、Microsoft Azure Active Directory Domain Services (Azure AD DS) WorkSpaces をデプロイし、 AWS と Azure 間の接続を確立し、Azure AWS AD DS ドメインコントローラーを指す AD Connector を使用する必要があります。これを設定する方法の詳細については、「Azure Active Directory Domain Services を使用して Azure AD WorkSpaces に を追加する」ブログ記事を参照してください。

AWS Directory Serviceで を使用する場合は WorkSpaces、 AWS Directory Service を適切にサイズ設定するために、デプロイのサイズ WorkSpacesと予想される増加を考慮する必要があります。このセクションでは、 AWS Directory Service で使用する のサイズ設定に関するガイダンスを提供します WorkSpaces。AD Connector のベストプラクティスと、 AWS Directory Service 管理ガイドの「 のベストプラクティス AWS Managed Microsoft AD」セクションも確認することをお勧めします。

を使用した AD Connector のサイズ設定 WorkSpaces

Active Directory Connector (AD Connector) には、Small と Large の 2 つのサイズがあります。ユーザーまたは接続の制限は適用されませんが、最大 500 WorkSpaces 人の権限を持つユーザーには小さな AD Connector を使用し、最大 5000 人の WorkSpaces 権限を持つユーザーには大きな AD Connector を使用することをお勧めします。アプリケーションの負荷を複数の AD Connector に分散して、パフォーマンスのニーズに合わせてスケールできます。例えば、1500 人の WorkSpaces ユーザーをサポートする必要がある場合は、それぞれ 500 人のユーザーをサポートする 3 つの小さな AD Connector に を WorkSpaces 均等に分散できます。すべてのユーザーが同じドメインに存在する場合、AD Connector はすべて Active Directory ドメインを解決する同じ DNS サーバーのセットを指すことができます。

小規模な AD Connector で開始し、時間の経過とともに WorkSpaces デプロイが増大する場合は、サポートチケットを引き上げて、 WorkSpaces AD Connector のサイズを小規模から大規模に変更して、資格のあるユーザーの数を増やすことができます。

のサイジング AWS Managed Microsoft AD

AWS Managed Microsoft AD では、Microsoft Active Directory をマネージドサービスとして実行できます。サービスの起動時に、Standard Edition と Enterprise Edition のいずれかを選択できます。Standard Edition は、最大 5,000 人のユーザーを持つ小規模および中規模のビジネスに推奨され、ユーザー、グループ、コンピュータなど、最大 30,000 個のディレクトリオブジェクトをサポートします。Enterprise Edition は、最大 500,000 個のディレクトリオブジェクトをサポートするように設計されており、マルチリージョンレプリケーション などの追加機能も提供します。

500,000 を超えるディレクトリオブジェクトをサポートする必要がある場合は、Amazon EC2 に Microsoft Active Directory ドメインコントローラーをデプロイすることを検討してください。これらのドメインコントローラーのサイズ設定については、Microsoft の「Active Directory Domain Services の容量計画」ドキュメントを参照してください。

シナリオ 1: AD コネクタを使用してオンプレミスの Active Directory Service に認証をプロキシする

このシナリオは、オンプレミス AD サービスを に拡張したくない場合や AWS、AD DS の新しいデプロイがオプションでないお客様を対象としています。次の図は、高レベル、各コンポーネント、およびユーザー認証フローを示しています。

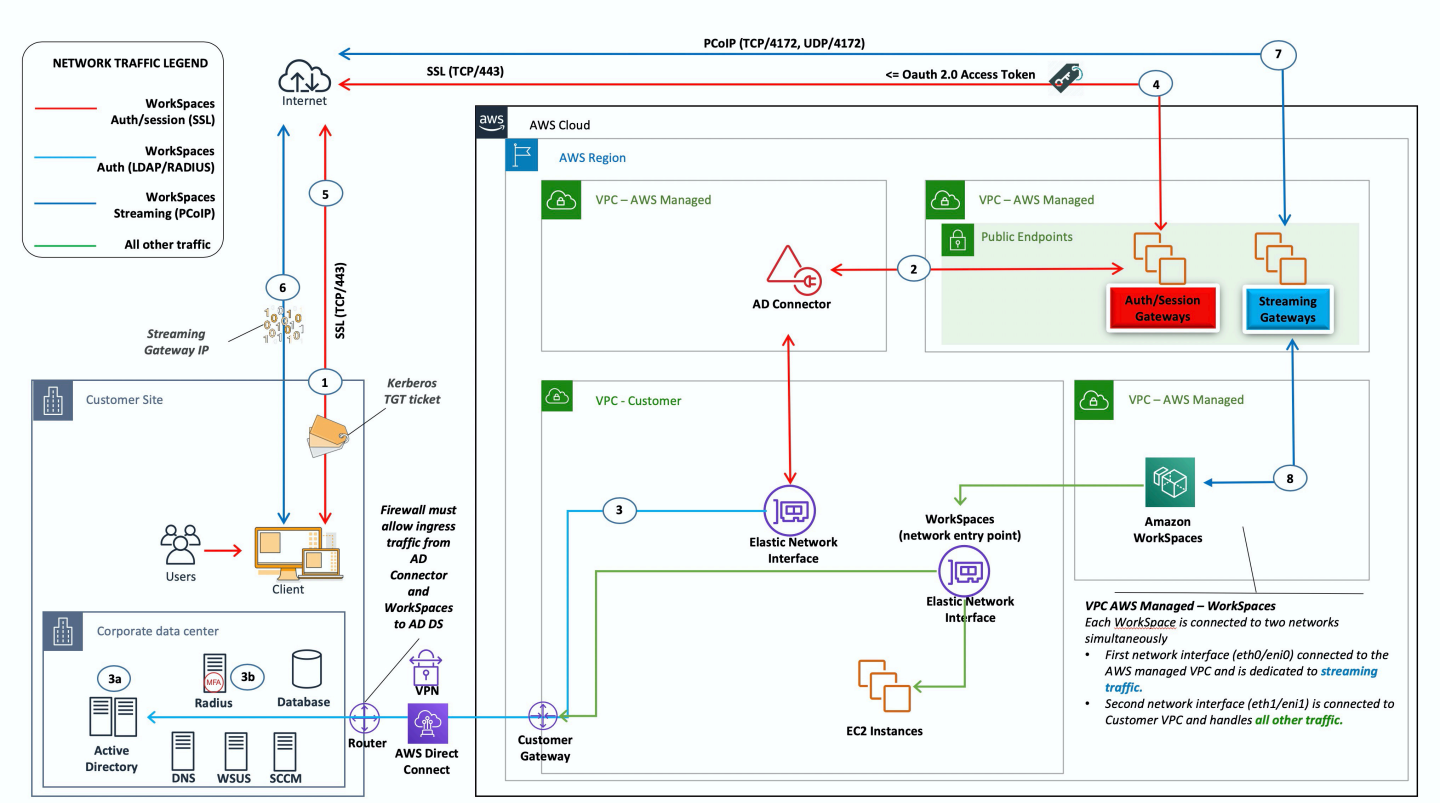

図 5: AD Connector からオンプレミスの Active Directory へ

このシナリオでは、AD Connector を介して顧客のオンプレミス AD DS (次の図を参照) にプロキシされるすべてのユーザーまたは MFA 認証に AWS ディレクトリサービス (AD Connector) が使用されます。認証プロセスに使用されるプロトコルまたは暗号化の詳細については、このドキュメントのセキュリティ「」セクションを参照してください。

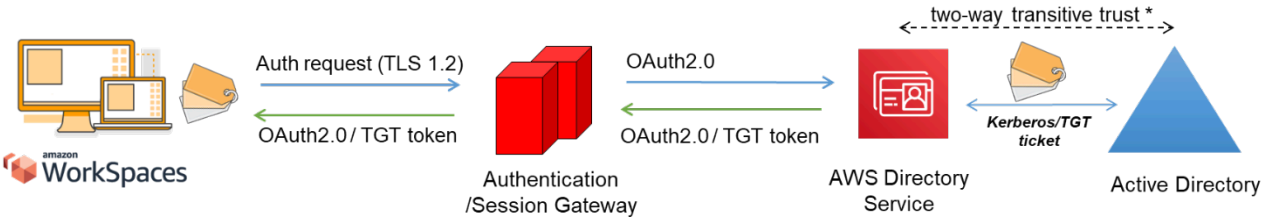

図 6: Authentication Gateway によるユーザー認証

シナリオ 1 は、顧客が既に にリソースを持っている可能性があるハイブリッドアーキテクチャと AWS、Amazon 経由でアクセスできるオンプレミスデータセンターのリソースを示しています WorkSpaces。ユーザーは、既存のオンプレミス AD DS サーバーと RADIUS サーバーを利用して、ユーザーと MFA 認証を行うことができます。

このアーキテクチャでは、次のコンポーネントまたはコンストラクトを使用します。

AWS

- Amazon VPC — 2 つの AZs にまたがる少なくとも 2 つのプライベートサブネットを持つ Amazon VPC の作成。
- DHCP オプションセット — Amazon VPC DHCP オプションセットの作成。これにより、お客様が指定したドメイン名とドメインネームサーバー (DNS) (オンプレミスサービス) を定義できます。詳細については、「DHCP オプションセット」を参照してください。
- Amazon Virtual Private Gateway — IPsec VPN トンネルまたは AWS Direct Connect 接続を介した独自のネットワークとの通信を有効にします。
- AWS Directory Service — AD Connector は Amazon VPC プライベートサブネットのペアにデプロイされます。
- Amazon WorkSpaces — AD Connector と同じプライベートサブネットにデプロイ WorkSpaces されます。詳細については、このドキュメントの「Active Directory: サイトとサービス」セクションを参照してください。

カスタマー

- ネットワーク接続 — 企業 VPN または Direct Connect エンドポイント。
- AD DS — 企業 AD DS。
- MFA (オプション) — 企業 RADIUS サーバー。
- エンドユーザーデバイス — Amazon WorkSpaces サービスへのアクセスに使用される企業または Bring Your Own License (BYOL) エンドユーザーデバイス (Windows、Mac、iPads、Android タブレット、ゼロクライアント、Chromebooks など)。サポートされているデバイスおよびウェブブラウザについては、このクライアントアプリケーションのリストを参照してください。

このソリューションは、AD DS をクラウドにデプロイしたくないお客様に最適ですが、いくつかの注意点があります。

- 接続への依存 — データセンターへの接続が失われた場合、ユーザーはそれぞれの にログインできず WorkSpaces、既存の接続は Kerberos/Ticket-Granting チケット (TGT) の存続期間中も有効です。

- レイテンシー — 接続を介してレイテンシーが存在する場合 (これは Direct Connect よりも VPN の場合が多い)、 WorkSpaces 認証とグループポリシー (GPO) の適用などの AD DS 関連のアクティビティには時間がかかります。
- トラフィックコスト — すべての認証は VPN または Direct Connect リンクを経由する必要があるため、接続タイプによって異なります。これは、Amazon EC2 からインターネットへのデータ転送出力、またはデータ転送出力 (Direct Connect) のいずれかです。

> **Note**
>
> AD Connector はプロキシサービスです。ユーザー認証情報は保存またはキャッシュされません。代わりに、すべての認証、ルックアップ、および管理リクエストは AD によって処理されます。ディレクトリサービスには、すべてのユーザー情報を読み取り、コンピュータをドメインに参加させる権限を持つ委任権限を持つアカウントが必要です。

一般に、 WorkSpaces エクスペリエンスは前の図に示されている Active Directory 認証プロセスに大きく依存します。このシナリオでは、 WorkSpaces 認証エクスペリエンスはカスタマー AD と WorkSpaces VPC 間のネットワークリンクに大きく依存します。お客様は、リンクの可用性が高いことを確認する必要があります。

シナリオ 2: オンプレミス AD DS を に拡張する AWS （ レプリカ ）

このシナリオはシナリオ 1 に似ています。ただし、このシナリオでは、カスタマー AD DS のレプリカが AD Connector と組み合わせて AWS にデプロイされます。これにより、Amazon Elastic Compute Cloud (Amazon EC2) で実行されている AD DS への認証またはクエリリクエストのレイテンシーが短縮されます。次の図は、各コンポーネントとユーザー認証フローの概要を示しています。

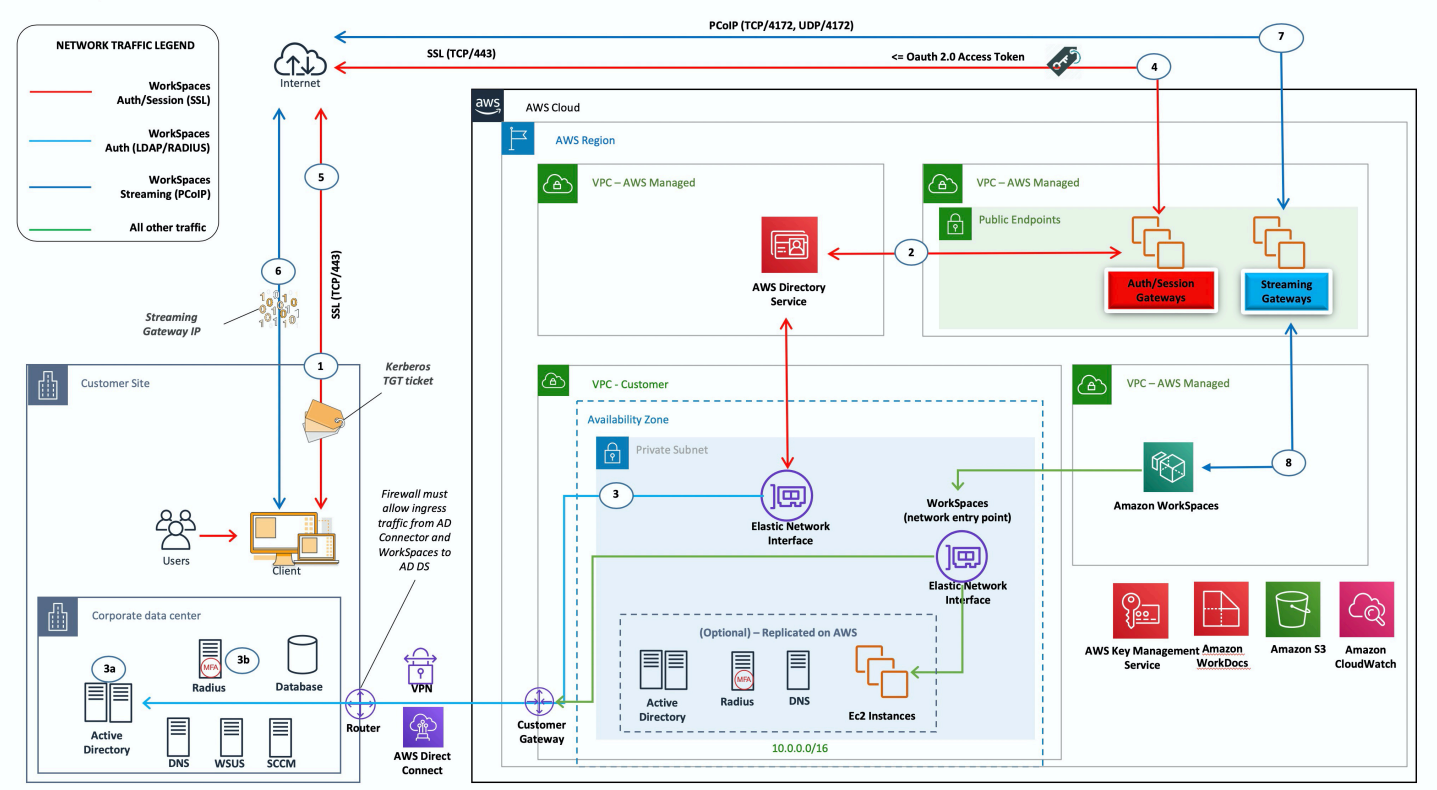

図 7: お客様の Active Directory ドメインをクラウドに拡張する

シナリオ 1 と同様に、AD Connector はすべてのユーザーまたは MFA 認証に使用され、これが顧客の AD DS にプロキシされます (前の図を参照)。このシナリオでは、カスタマー AD DS は、 AWS クラウドで実行されているカスタマーのオンプレミス AD フォレスト のドメインコントローラーとして昇格された Amazon EC2 インスタンス上の AZs にデプロイされます。各ドメインコントローラーは VPC プライベートサブネットにデプロイされ、 AWS クラウドで AD DS を高可用性にします。AD DS を にデプロイするためのベストプラクティスについては AWS、このドキュメントの設計上の考慮事項セクションを参照してください。

WorkSpaces インスタンスがデプロイされると、クラウドベースのドメインコントローラーにアクセスして、安全で低レイテンシーのディレクトリサービスと DNS にアクセスできます。AD DS 通信、認証リクエスト、AD レプリケーションを含むすべてのネットワークトラフィックは、プライベートサブネット内、またはカスタマー VPN トンネルまたは Direct Connect 経由で保護されます。

このアーキテクチャでは、次のコンポーネントまたはコンストラクトを使用します。

AWS

- Amazon VPC — 2 つの AZs にまたがる少なくとも 4 つのプライベートサブネットを持つ Amazon VPC の作成。2 つはカスタマー AD DS 用、2 つは AD Connector または Amazon 用です WorkSpaces。
- DHCP オプションセット — Amazon VPC DHCP オプションセットの作成。これにより、お客様は指定されたドメイン名と DNSs (AD DS local) を定義できます。詳細については、「DHCP オプションセット」を参照してください。
- Amazon Virtual Private Gateway — IPsec VPN トンネルまたは AWS Direct Connect 接続を介した顧客所有のネットワークとの通信を有効にします。
- 「Amazon EC2」
  - 専用プライベート VPC サブネットの Amazon EC2 インスタンスにデプロイされたカスタマー企業の AD DS ドメインコントローラー。
  - 専用プライベート VPC サブネットの Amazon EC2 インスタンス上の MFA 用のカスタマー (オプション) RADIUS サーバー。
- AWS ディレクトリサービス — AD Connector は Amazon VPC プライベートサブネットのペアにデプロイされます。
- Amazon WorkSpaces — AD Connector と同じプライベートサブネットに WorkSpaces デプロイされます。詳細については、このドキュメントの「Active Directory: サイトとサービス」セクションを参照してください。

カスタマー

- ネットワーク接続 — 企業 VPN または AWS Direct Connect エンドポイント。
- AD DS — 企業 AD DS (レプリケーションに必要) 。
- MFA (オプション) — 企業 RADIUS サーバー。
- エンドユーザーデバイス — Amazon WorkSpaces サービスへのアクセスに使用される企業デバイスまたは BYOL エンドユーザーデバイス (Windows、Mac、iPadsAndroid タブレット、ゼロクライアント、Chromebook など) 。サポートされているデバイスおよびウェブブラウザのクライアントアプリケーションのリストを参照してください。このソリューションには、シナリオ 1 と同じ注意点はありません。Amazon WorkSpaces と AWS Directory Service は、接続に依存することはありません。

- 接続への依存 — お客様のデータセンターへの接続が失われた場合、認証とオプションの MFA がローカルで処理されるため、エンドユーザーは引き続き作業できます。
- レイテンシー — レプリケーショントラフィックを除き、すべての認証はローカルで低レイテンシーです。このドキュメントの「Active Directory: サイトとサービス」セクションを参照してください。
- トラフィックコスト — このシナリオでは、認証はローカルで、AD DS レプリケーションのみが VPN または Direct Connect リンクを通過するため、データ転送が減少します。

一般に、前の図に示すように、 WorkSpaces エクスペリエンスは強化されており、オンプレミスのドメインコントローラーへの接続に大きく依存しません。これは、特に AD DS グローバルカタログのクエリに関連して、顧客が何千ものデスクトップ WorkSpaces にスケーリングしたい場合にも当てはまります。このトラフィックは WorkSpaces 環境に対してローカルのままです。

シナリオ 3: AWS クラウドの AWS Directory Service を使用したスタンドアロンの独立したデプロイ

次の図に示すこのシナリオでは、AD DS をスタンドアロンの分離環境で AWS クラウドにデプロイしています。 AWS Directory Service はこのシナリオでのみ使用されます。AD DS を完全に管理する代わりに、可用性の高いディレクトリトポロジの構築、ドメインコントローラーのモニタリング、バックアップとスナップショットの設定などのタスクに AWS Directory Service を使用できます。

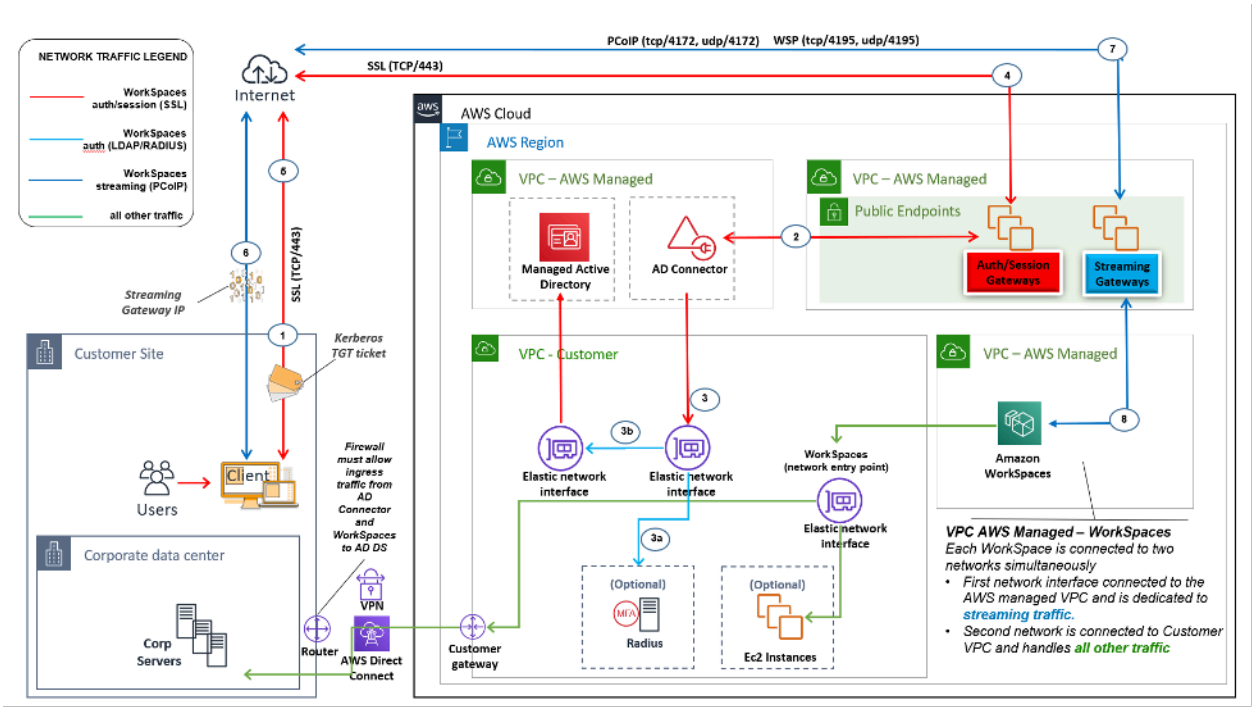

図 8: クラウドのみ： AWS ディレクトリサービス (Microsoft AD)

シナリオ 2 と同様に、AD DS (Microsoft AD) は 2 つの AZs にまたがる専用サブネットにデプロイされるため、AD DS は AWS クラウドで高可用性を実現できます。Microsoft AD に加えて、AD Connector (3 つのシナリオすべて) は WorkSpaces 認証または MFA 用にデプロイされます。これにより、Amazon VPC 内のロールまたは関数が分離されます。これは標準的なベストプラクティスです。詳細については、このドキュメントの「設計上の考慮事項」セクションを参照してください。

シナリオ 3 は、 AWS Directory Service のデプロイ、パッチ適用、高可用性、モニタリング AWS を管理したいお客様に適した標準オールイン設定です。このシナリオは、分離モードのため、概念、ラボ、本番環境の証明にも適しています。

AWS Directory Service の配置に加えて、この図は、ユーザーからワークスペースへのトラフィックのフローと、ワークスペースが AD サーバーおよび MFA サーバーとやり取りする方法を示しています。

このアーキテクチャでは、次のコンポーネントまたはコンストラクトを使用します。

AWS

- Amazon VPC — 2 つの AZs にまたがる少なくとも 4 つのプライベートサブネットを持つ Amazon VPC の作成。2 つは AD DS Microsoft AD 用、2 つは AD Connector または 用です WorkSpaces。
- DHCP オプションセット — Amazon VPC DHCP オプションセットの作成。これにより、お客様は指定されたドメイン名と DNS (Microsoft AD) を定義できます。詳細については、「DHCP オプションセット」を参照してください。
- オプション: Amazon Virtual Private Gateway — IPsec VPN トンネル (VPN) または AWS Direct Connect 接続を介した顧客所有のネットワークとの通信を有効にします。を使用して、オンプレミスのバックエンドシステムにアクセスします。
- AWS Directory Service — VPC サブネットの専用ペア (AD DS Managed Service) にデプロイされた Microsoft AD。
- Amazon EC2 — MFA 用の「オプション」RADIUS サーバーのお客様。
- AWS ディレクトリサービス — AD Connector は Amazon VPC プライベートサブネットのペアにデプロイされます。
- Amazon WorkSpaces — AD Connector と同じプライベートサブネットに WorkSpaces デプロイされます。詳細については、このドキュメントの「Active Directory: サイトとサービス」セクションを参照してください。

カスタマー

- オプション: ネットワーク接続 — 企業 VPN または AWS Direct Connect エンドポイント。
- エンドユーザーデバイス — Amazon WorkSpaces サービスへのアクセスに使用される企業デバイスまたは BYOL エンドユーザーデバイス (Windows、Mac、iPadsAndroid タブレット、ゼロクライアント、Chromebook など) 。サポートされているデバイスおよびウェブブラウザについては、このクライアントアプリケーションのリストを参照してください。

シナリオ 2 と同様に、このシナリオでは、お客様のオンプレミスデータセンターへの接続、レイテンシー、データ転送コスト (VPC WorkSpaces 内でインターネットアクセスが有効になっている場合を除く) に依存しません。これは設計上、分離されたシナリオまたはクラウドのみのシナリオであるためです。

シナリオ 4: AWS Microsoft AD とオンプレミスへの双方向の推移的信頼

このシナリオは、次の図に示すように、 AWS マネージド AD が AWS クラウドにデプロイされています。このクラウドは、オンプレミス AD に対して双方向の推移的な信頼を持っています。ユーザーと WorkSpaces は Managed AD に作成され、AD の信頼により、オンプレミス環境でリソースにアクセスできるようになります。

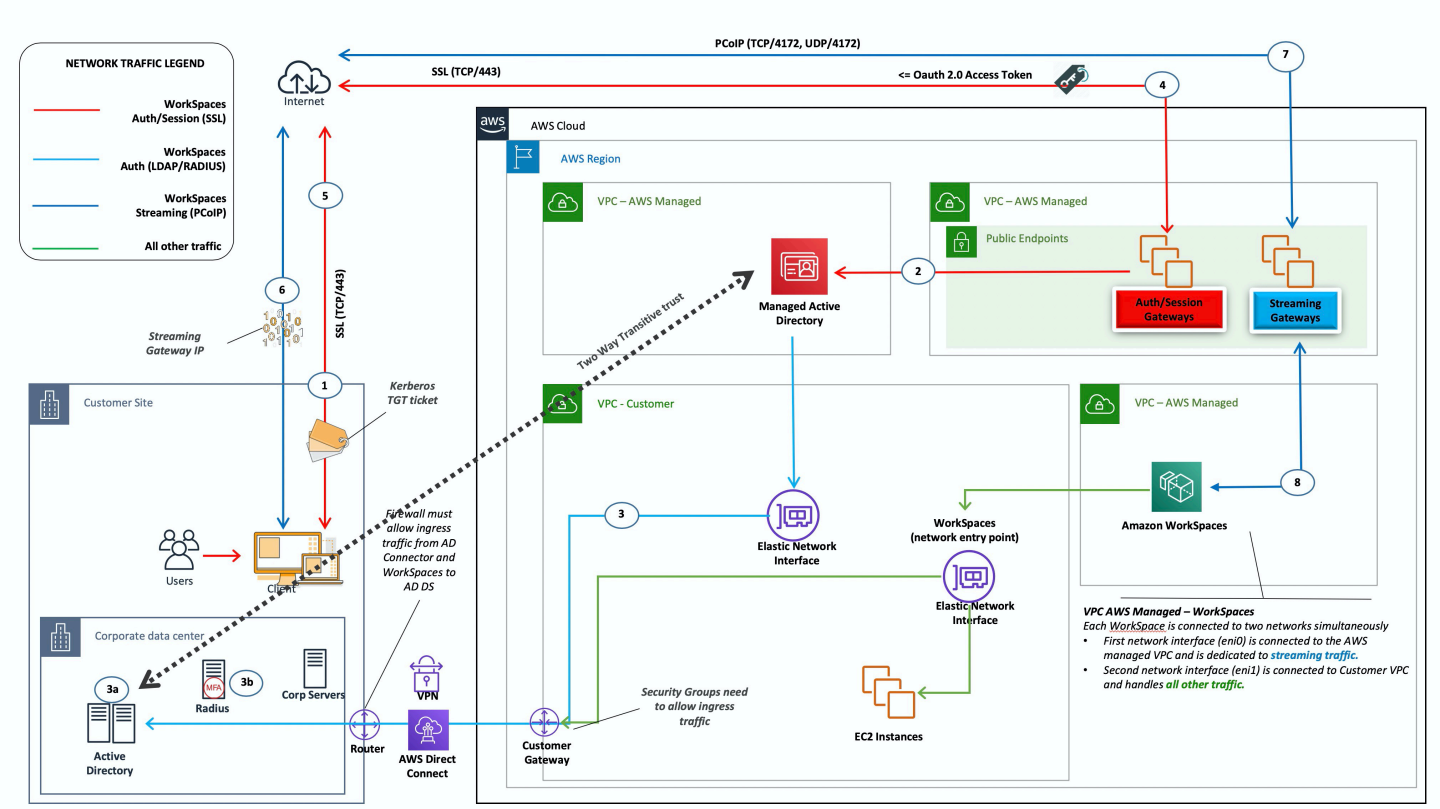

図 9: AWS Microsoft AD とオンプレミスへの双方向の推移的信頼

シナリオ 3 と同様に、AD DS (Microsoft AD) は 2 つの AZs にまたがる専用サブネットにデプロイされるため、AD DS は AWS クラウドで高可用性を実現できます。

このシナリオは、 AWS クラウドのデプロイ、パッチ適用、高可用性、モニタリングなど、フルマネージド型の AWS Directory Service を希望するお客様に適しています。このシナリオでは、WorkSpaces ユーザーは既存のネットワーク上の AD 結合リソースにアクセスすることもできます。このシナリオでは、ドメインの信頼を確立する必要があります。セキュリティグループとファイアウォールルールは、2 つのアクティブディレクトリ間の通信を許可する必要があります。

AWS Directory Service の配置に加えて、前の図は、ユーザーからワークスペースへのトラフィックの流れと、ワークスペースが AD サーバーおよび MFA サーバーとどのようにやり取りするかをまとめたものです。

このアーキテクチャでは、次のコンポーネントまたはコンストラクトを使用します。

AWS

- Amazon VPC — 2 つの AZs にまたがる少なくとも 4 つのプライベートサブネットを持つ Amazon VPC の作成。2 つは AD DS Microsoft AD 用、2 つは AD Connector または 用です WorkSpaces。

- DHCP オプションセット — Amazon VPC DHCP オプションセットの作成。これにより、お客様は指定されたドメイン名と DNS (Microsoft AD) を定義できます。詳細については、「DHCP オプションセット」を参照してください。
- オプション: Amazon Virtual Private Gateway — IPsec VPN トンネル (VPN) または AWS Direct Connect 接続を介した顧客所有のネットワークとの通信を有効にします。を使用して、オンプレミスのバックエンドシステムにアクセスします。
- AWS Directory Service — VPC サブネットの専用ペア (AD DS Managed Service) にデプロイされた Microsoft AD。

- Amazon EC2 — MFA 用のオプションの RADIUS サーバー。
- Amazon WorkSpaces — AD Connector と同じプライベートサブネットに WorkSpaces デプロイされます。詳細については、このドキュメントの「Active Directory: サイトとサービス」セクションを参照してください。

カスタマー

- ネットワーク接続 — 企業 VPN または AWS Direct Connect エンドポイント。
- エンドユーザーデバイス — Amazon WorkSpaces サービスへのアクセスに使用される企業デバイスまたは BYOL エンドユーザーデバイス (Windows、Mac、iPadsAndroid タブレット、ゼロクライアント、Chromebook など) 。サポートされているデバイスおよびウェブブラウザのクライアントアプリケーションのリストを参照してください。

このソリューションでは、信頼プロセスの運用を可能にするために、お客様のオンプレミスデータセンターへの接続が必要です。 WorkSpaces ユーザーがオンプレミスネットワーク上のリソースを使用している場合は、レイテンシーとアウトバウンドのデータ転送コストを考慮する必要があります。

シナリオ 5: 共有サービス Virtual Private Cloud (VPC) を使用する AWS Microsoft AD

次の図に示すこのシナリオでは、 AWS クラウドに AWS Managed AD をデプロイし、 で既にホストされているワークロード、 AWS またはより広範な移行の一環として予定されているワークロードに認証サービスを提供します。ベストプラクティスとして、Amazon を専用 VPC WorkSpaces に配置することをお勧めします。また、 WorkSpaces コンピュータオブジェクトを整理するために、特定の AD OU を作成する必要があります。

Managed AD をホストする共有サービス VPC WorkSpaces を使用してデプロイするには、Managed AD で作成された TAK サービスアカウントを使用して AD Connector (TAK) をデプロイします。サービスアカウントには、共有サービス Managed AD の WorkSpaces指定された OU にコンピュータオブジェクトを作成するためのアクセス許可が必要です。

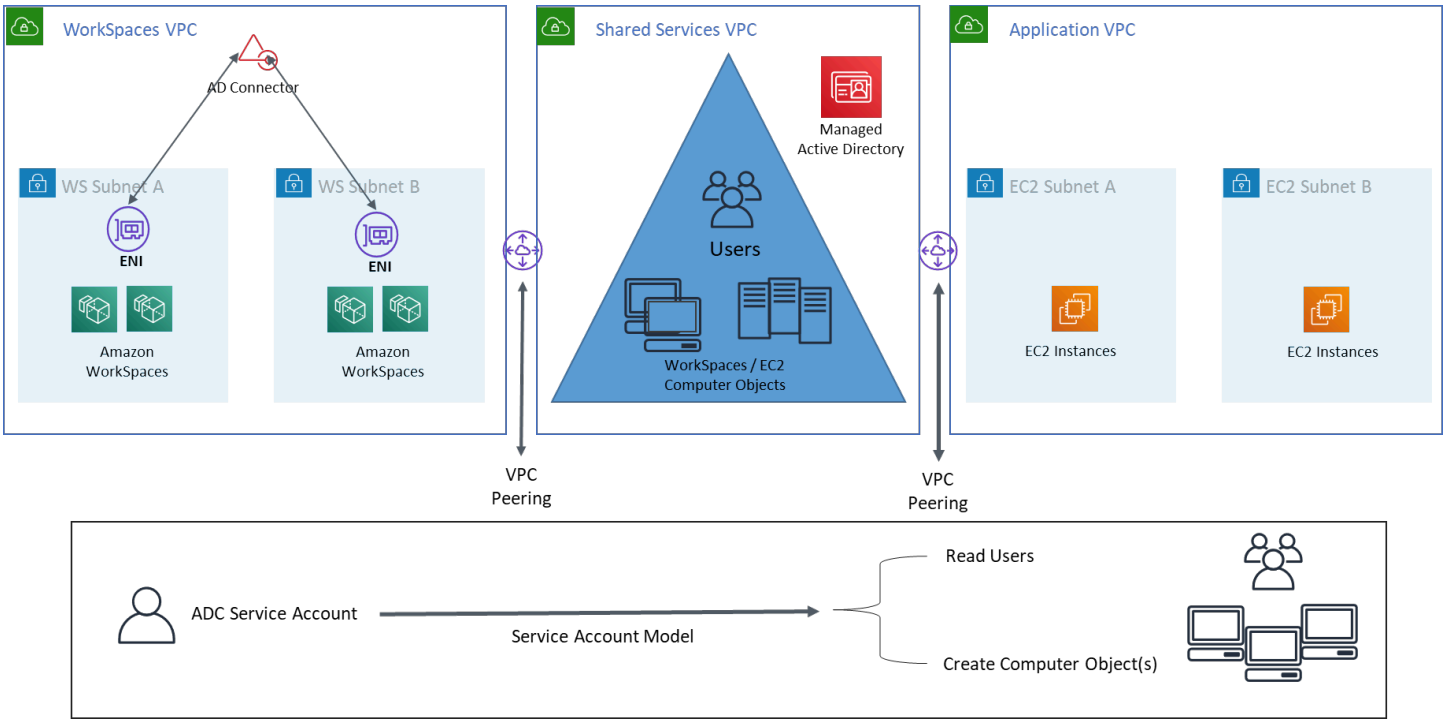

図 10: 共有サービス VPC を使用した AWS Microsoft AD

このアーキテクチャでは、次のコンポーネントまたはコンストラクトを使用します。

AWS

- Amazon VPC — 2 つの AZs にまたがる少なくとも 2 つのプライベートサブネットを持つ Amazon VPC の作成 (AD Connector と では 2 つ WorkSpaces) 。
- DHCP オプションセット — Amazon VPC DHCP オプションセットの作成。これにより、お客様は指定されたドメイン名と DNS (Microsoft AD) を定義できます。詳細については、「DHCP オプションセット」を参照してください。
- オプション: Amazon Virtual Private Gateway — IPsec VPN トンネル (VPN) または AWS Direct Connect 接続を介した顧客所有のネットワークとの通信を有効にします。を使用して、オンプレミスのバックエンドシステムにアクセスします。
- AWS Directory Service — VPC サブネットの専用ペア (AD DS Managed Service)、AD Connector にデプロイされた Microsoft AD

- AWS トランジットゲートウェイ/VPC ピアリング — Workspaces VPC と共有サービス VPC 間の接続を有効にする
- Amazon EC2 — MFA 用のオプションの RADIUS サーバー。
- Amazon WorkSpaces — AD Connector と同じプライベートサブネットに WorkSpaces デプロイされます。詳細については、このドキュメントの「Active Directory: サイトとサービス」セクションを参照してください。

カスタマー

- ネットワーク接続 — 企業 VPN または AWS Direct Connect エンドポイント。
- エンドユーザーデバイス — Amazon WorkSpaces サービスへのアクセスに使用される企業デバイスまたは BYOL エンドユーザーデバイス (Windows、Mac、iPadsAndroid タブレット、ゼロクライアント、Chromebook など) 。サポートされているデバイスおよびウェブブラウザのクライアントアプリケーションのリストを参照してください。

シナリオ 6: AWS Microsoft AD、共有サービス VPC、オンプレミスへの一方向の信頼

このシナリオでは、次の図に示すように、 は既存のオンプレミスの Active Directory をユーザーとして使用し、 AWS クラウドに別の Managed Active Directory を導入して、 に関連付けられたコンピュータオブジェクトをホストします WorkSpaces。このシナリオでは、コンピュータオブジェクトと Active Directory グループポリシーを企業の Active Directory とは別に管理できます。

このシナリオは、サードパーティーがお客様に代わって Windows WorkSpaces を管理したい場合に便利です。これは、サードパーティーにカスタマー AD へのアクセスを許可することなく、関連付けられた WorkSpaces および ポリシーを定義および制御することを許可するためです。このシナリオでは、共有サービス AD の WorkSpaces コンピュータオブジェクトを整理するための特定の Active Directory 組織単位 (OU) が作成されます。

> **Note**
>
> Amazon Linux WorkSpaces では、作成するために双方向の信頼を確立する必要があります。

カスタマー ID ドメインのユーザーを使用して Managed Active Directory をホストする共有サービス VPC で作成されたコンピュータオブジェクト WorkSpaces を使用して Windows をデプロイするには、企業の AD を参照する Active Directory Connector (TAK) をデプロイします。企業 AD (ID ドメイン) で作成された TAK サービスアカウントを使用します。このアカウントには、共有サービスマネージド AD の Windows 用に設定され、企業の Active Directory (ID ドメイン) に対する読み取り権限を持つ組織単位 (OU) WorkSpaces にコンピュータオブジェクトを作成するためのアクセス許可が委任されています。

Domain Locator 関数が ID ドメインの目的の AD サイトの WorkSpaces ユーザーを認証できるようにするには、Microsoft のドキュメント に従って、Amazon WorkSpaces サブネットの両方のドメインの AD サイトに同じ名前を付けます。 https://techcommunity.microsoft.com/t5/ask-the-directory-services-team/domain-locator-across-a-forest-trust/ba-p/395689ID ドメインと共有サービスドメイン AD ドメインコントローラーの両方を Amazon と同じ AWS リージョンに配置することがベストプラクティスです WorkSpaces。

このシナリオを設定する詳細な手順については、「 実装ガイド」を参照して、Amazon WorkSpaces と AWS Directory Services の双方向の信頼を設定します。

このシナリオでは、共有サービス VPC AWS Managed Microsoft AD 内の とオンプレミス AD の間に一方向の推移的信頼を確立します。図 11 は、信頼とアクセスの方向と、 AWS AD Connector が AD Connector サービスアカウントを使用してリソースドメインにコンピュータオブジェクトを作成する方法を示しています。

可能な限り Kerberos 認証が使用されるように、Microsoft の推奨事項に従ってフォレストの信頼が使用されます。のリソースドメインからグループポリシーオブジェクト (GPOs) WorkSpaces を受け取ります AWS Managed Microsoft AD。さらに、 は ID ドメインで Kerberos 認証 WorkSpaces を実行します。これを確実に機能させるには、前述の AWS ように ID ドメインを に拡張するのがベストプラクティスです。詳細については、「実装ガイドによる一方向信頼リソースドメイン WorkSpaces を使用した Amazon のデプロイ AWS Directory Service」を確認することをお勧めします。

AD Connector と の両方が WorkSpaces、ID ドメインとリソースドメインのドメインコントローラーと通信できる必要があります。詳細については、「Amazon WorkSpaces 管理ガイド」の「 の IP アドレスとポートの要件 WorkSpaces」を参照してください。

複数の AD Connector を使用する場合は、各 AD Connector で独自の AD Connector サービスアカウントを使用するのがベストプラクティスです。

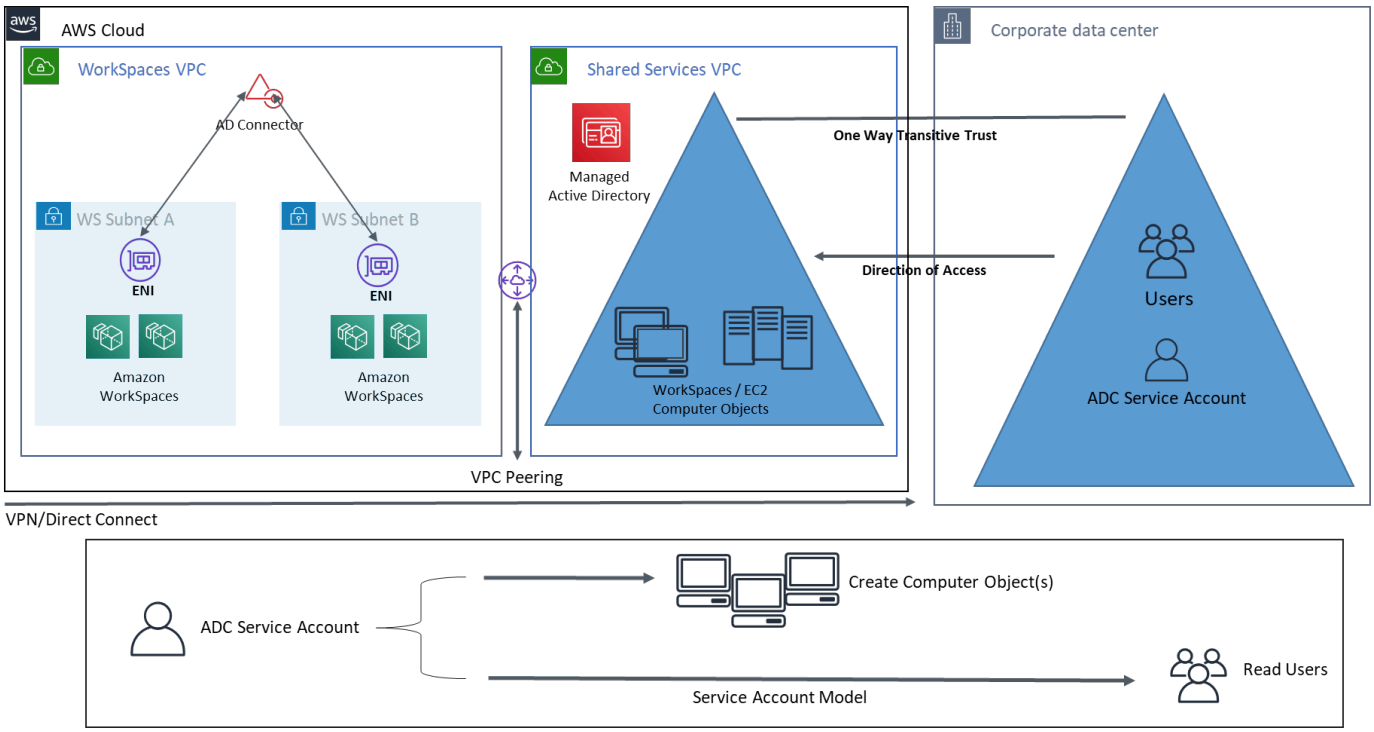

図 11: AWS Microsoft、共有サービス VPC、および AD オンプレミスへの一方向の信頼

このアーキテクチャでは、次のコンポーネントまたはコンストラクトを使用します。

AWS

- Amazon VPC — 2 つの AZs にまたがる少なくとも 2 つのプライベートサブネットを持つ Amazon VPC の作成 — AD Connector と 用の 2 つです WorkSpaces。
- DHCP オプションセット — Amazon VPC DHCP オプションセットの作成。これにより、お客様は指定されたドメイン名と DNS (Microsoft AD) を定義できます。詳細については、「DHCP オプションセット」を参照してください。
- オプション: Amazon Virtual Private Gateway — IPsec VPN トンネル (VPN) または AWS Direct Connect 接続を介した顧客所有のネットワークとの通信を有効にします。を使用して、オンプレミスのバックエンドシステムにアクセスします。
- AWS ディレクトリサービス — Microsoft AD は、VPC サブネットの専用ペア (AD DS Managed Service)、AD Connector にデプロイされます。
- トランジットゲートウェイ/VPC ピアリング — Workspaces VPC と共有サービス VPC 間の接続を有効にします。
- Amazon EC2 — MFA 用のカスタマー「オプション」RADIUS サーバー。

- Amazon WorkSpaces — AD Connector と同じプライベートサブネットに WorkSpaces デプロイされます。詳細については、このドキュメントの「Active Directory: サイトとサービス」セクションを参照してください。

カスタマー

- ネットワーク接続 — 企業 VPN または AWS Direct Connect エンドポイント。
- エンドユーザーデバイス — Amazon WorkSpaces サービスへのアクセスに使用される企業デバイスまたは BYOL エンドユーザーデバイス (Windows、Mac、iPadsAndroid タブレット、ゼロクライアント、Chromebook など) 。サポートされているデバイスおよびウェブブラウザについては、このクライアントアプリケーションのリストを参照してください。

Amazon でのマルチリージョン AWS マネージド Active Directory の使用 WorkSpaces

AWS Directory Service for Microsoft Active Directory (MAD) は、Amazon と組み合わせることができるフルマネージド型の Microsoft Active Directory (AD) です WorkSpaces。お客様は、高可用性、モニタリング、バックアップが組み込まれているため、 AWS Managed Microsoft AD を選択します。AWS Managed Microsoft AD Enterprise Edition では、マルチリージョンレプリケーション を設定する機能が追加されています。この機能は、リージョン間のネットワーク接続を自動的に設定し、ドメインコントローラーをデプロイし、すべての Active Directory データを複数のリージョンにレプリケートします。これにより、それらのリージョンに存在する Windows および Linux ワークロードが、低レイテンシーと高パフォーマンスで AWS MAD に接続して使用できるようになります。レプリケートされた MAD リージョンを に直接登録 WorkSpacesすることはできませんが、レプリケートされたドメインコントローラーを指すように AD Connector (TAK) を設定 WorkSpaces することで、レプリケートされた MAD ディレクトリを に登録できます。

MAD で AD Connector をデプロイする際のベストプラクティスは、 WorkSpaces 環境内の各ビジネスユニットに AD Connector を作成することです。これにより、各ビジネスユニットを Active Directory 内の特定の組織単位に合わせることができます。その後、問題のビジネスユニットと直接一致する組織単位レベルで AD グループポリシーオブジェクトを割り当てることができます。

アーキテクチャ

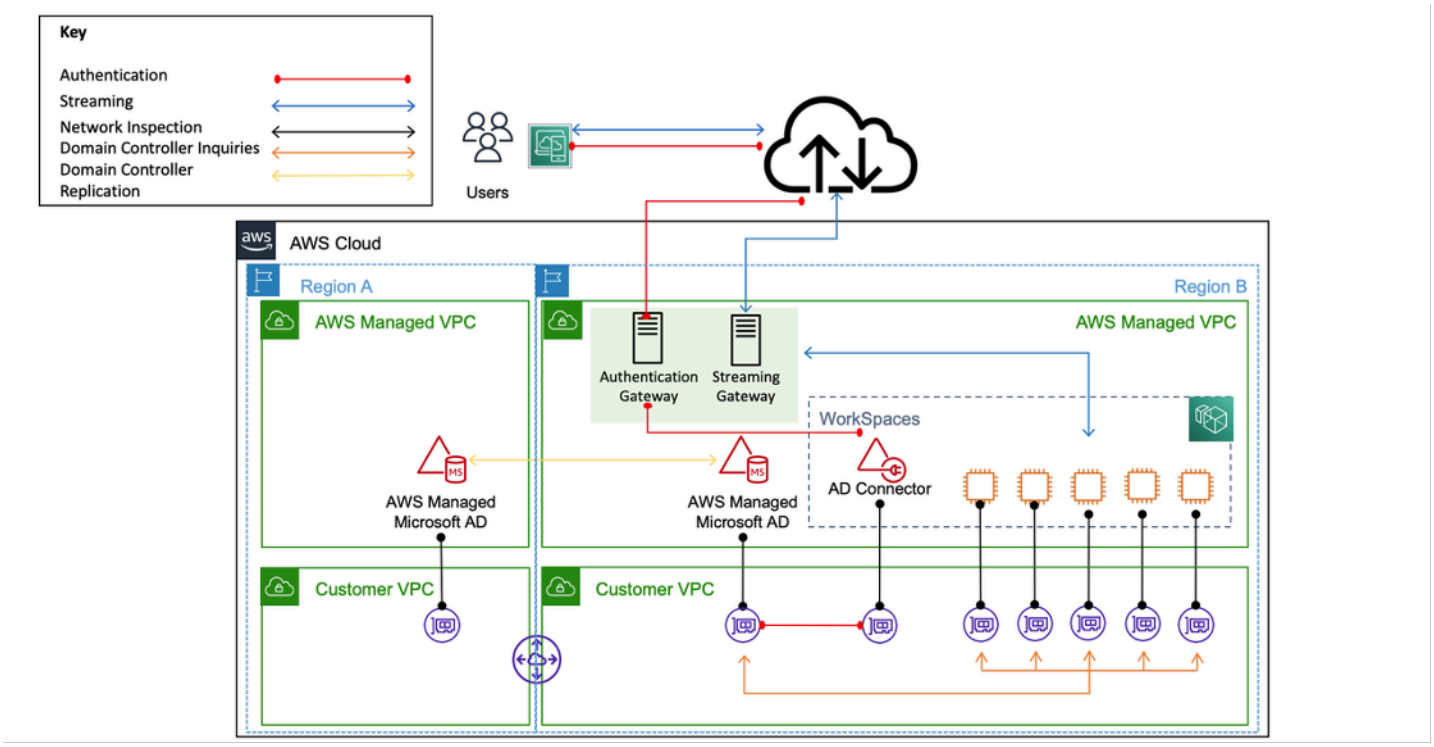

図 12: レプリケートされた MAD リージョンを に登録するためのサンプルアーキテクチャ WorkSpace

実装

レプリケートされた MAD リージョンを に登録するには WorkSpaces、MAD ドメインコントローラー IPs を指す AD Connector を作成する必要があります。MAD ドメインコントローラーの IP アドレスは、AWS ディレクトリサービスコンソールのナビゲーションペインに移動し、ディレクトリを選択してから、正しいディレクトリ ID を選択することで確認できます。これらの AD Connector を作成するには、このガイド に従ってください。作成したら、 に登録 WorkSpacesできます。新しいリージョン WorkSpaces にデプロイする前に、VPCs DHCP オプションセットが更新されていることを確認してください。

設計上の考慮事項

AWS クラウドでの AD DS の機能的なデプロイには、Active Directory の概念と特定の AWS サービスの両方を十分に理解する必要があります。このセクションでは、AD DS for Amazon WorkSpaces、Directory Service の AWS VPC ベストプラクティス、DHCP と DNS の要件、AD Connector の詳細、AD サイトとサービスをデプロイする際の重要な設計上の考慮事項について説明します。

VPC の設計

このドキュメントの「ネットワークに関する考慮事項」セクションで前述し、シナリオ 2 と 3 で説明したように、お客様は AD DS を AWS クラウド内の専用プライベートサブネットのペアにデプロイし、2 つの AZs にまたがって AD Connector または WorkSpaces サブネットから分離する必要があります。このコンストラクトは、 の AD DS サービスへの可用性が高く、低レイテンシーのアクセスを提供しながら WorkSpaces、Amazon VPC 内のロールまたは機能の分離に関する標準的なベストプラクティスを維持します。

次の図は、AD DS と AD Connector を専用のプライベートサブネット (シナリオ 3) に分離する方法を示しています。この例では、すべてのサービスが同じ Amazon VPC に存在します。

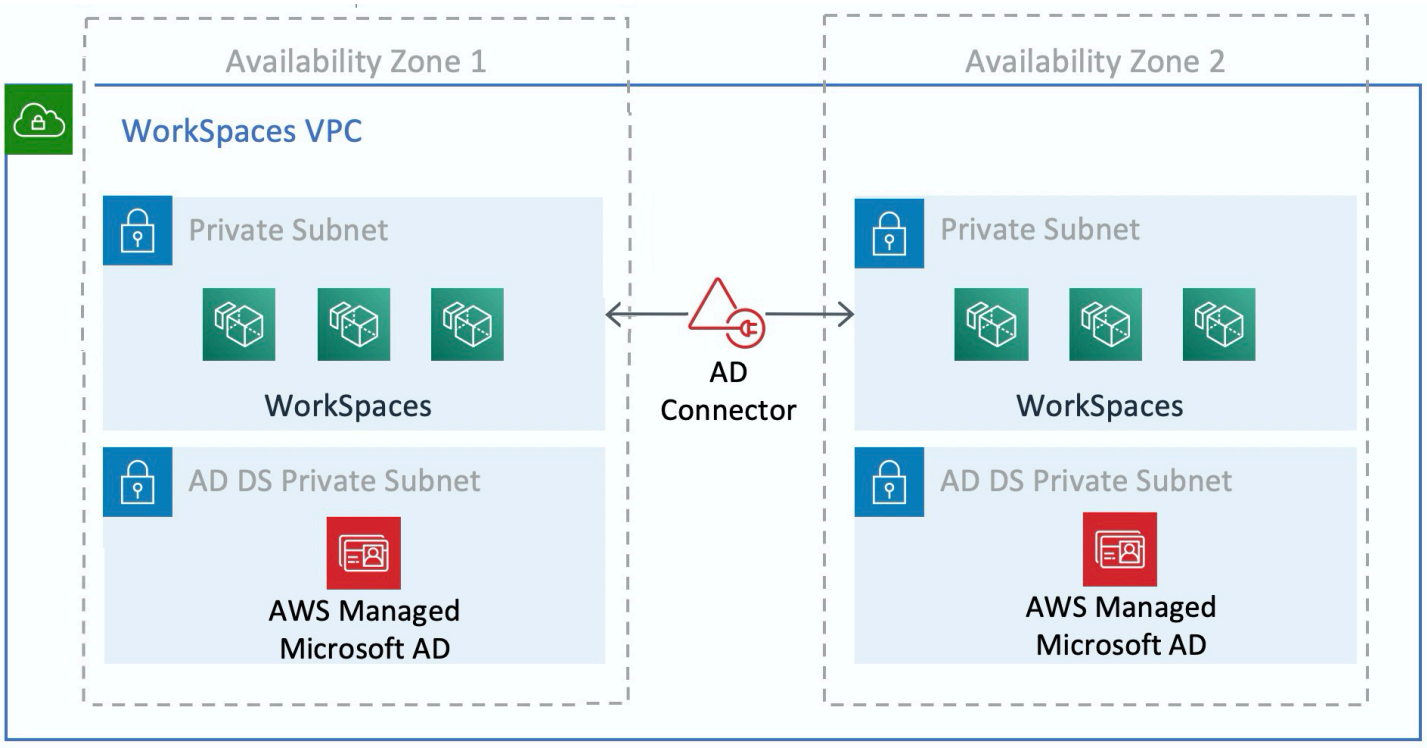

図 13: AD DS ネットワーク分離

次の図は、シナリオ 1 と同様の設計を示していますが、このシナリオでは、オンプレミス部分は専用の Amazon VPC にあります。

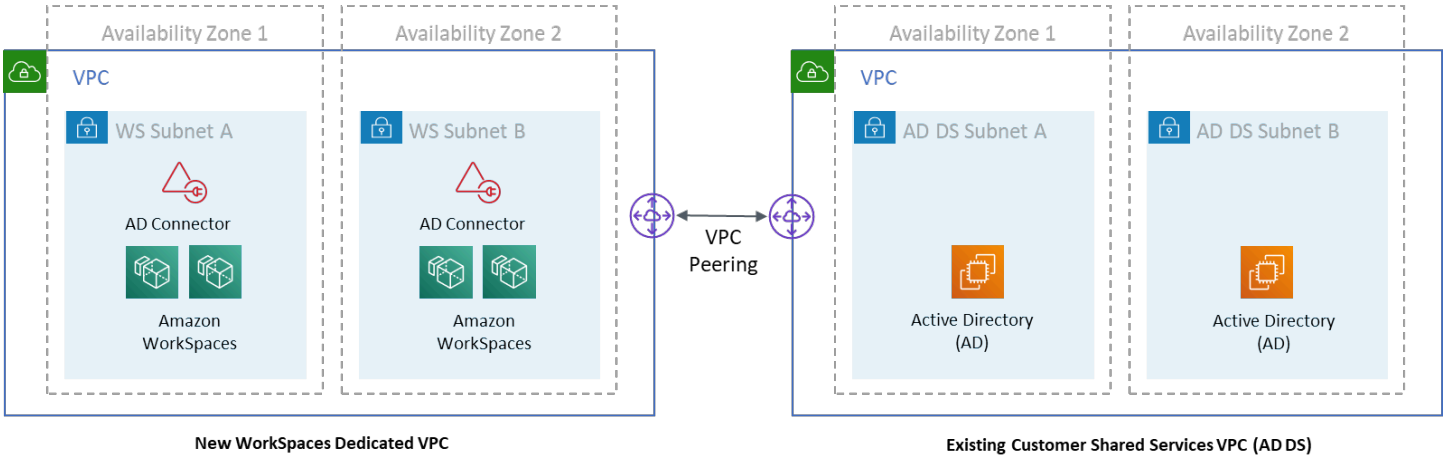

図 14: 専用 WorkSpaces VPC

> **Note**
>
> AD DS が使用されている既存の AWS デプロイメントをご利用のお客様は、 を WorkSpaces 専用 VPC に配置し、AD DS 通信に VPC ピアリングを使用することをお勧めします。

AD DS の専用プライベートサブネットの作成に加えて、ドメインコントローラーとメンバーサーバーには、AD DS レプリケーション、ユーザー認証、Windows Time サービス、分散ファイルシステム (DFS) などのサービスのトラフィックを許可するための複数のセキュリティグループルールが必要です。

> **Note**
>
> ベストプラクティスは、必要なセキュリティグループルールを WorkSpacesプライベートサブネットに制限し、シナリオ 2 の場合、次の表に示すように、 AWS クラウドとの間でオンプレミスの双方向 AD DS 通信を許可することです。

表 1 — AWS クラウドとの間の双方向 AD DS 通信

プロトコル	ポート	使用アイテム	デスティネーション
TCP	53、88、135、139、389、445、464、636	認証 (プライマリ)	Active Directory (プライベートデータセンターまたは Amazon EC2) *
TCP	49152 ~ 65535	RPC ハイポート	Active Directory (プライベートデータセンターまたは Amazon EC2) **
TCP	3268-3269	信頼	Active Directory (プライベートデータセンターまたは Amazon EC2) *
TCP	9389	リモート Microsoft Windows PowerShell (オプション)	Active Directory (プライベートデータセンターまたは Amazon EC2) *
UDP	53、88、123、137、138、389、445、464	認証 (プライマリ)	Active Directory (プライベートデータセンターまたは Amazon EC2) *
UDP	1812	Auth (MFA) (オプション)	RADIUS (プライベートデータセンターまたは Amazon EC2) *

詳細については、「Active Directory および Active Directory ドメインサービスポート要件」および「Windows のサービス概要とネットワークポート要件」を参照してください。

ルールの実装に関する step-by-step ガイダンスについては、「Amazon Elastic Compute Cloud ユーザーガイド」の「セキュリティグループへのルールの追加」を参照してください。

VPC 設計: DHCP と DNS

Amazon VPC では、インスタンスに Dynamic Host Configuration Protocol (DHCP) サービスがデフォルトで提供されます。デフォルトでは、すべての VPC は、Classless Inter-Domain Routing (CIDR) +2 アドレス空間を介してアクセス可能な内部ドメインネームシステム (DNS) サーバーを提供し、デフォルトの DHCP オプションセットを介してすべてのインスタンスに割り当てられます。

DHCP オプションセットは Amazon VPC 内で使用され、DHCP 経由でカスタマーインスタンスに渡す必要のあるドメイン名やネームサーバーなどのスコープオプションを定義します。カスタマー VPC 内の Windows サービスの正しい機能は、この DHCP スコープオプションによって異なります。前に定義した各シナリオでは、お客様はドメイン名とネームサーバーを定義する独自のスコープを作成して割り当てます。これにより、ドメインに参加している Windows インスタンスまたは WorkSpaces が AD DNS を使用するように設定されます。

次の表は、Amazon WorkSpaces と AWS Directory Services が正しく機能するために作成する必要がある DHCP スコープオプションのカスタムセットの例です。

表 2 — DHCP スコープオプションのカスタムセット

パラメータ	値
名前タグ	key = name と value を特定の文字列に設定したタグを作成します。 例: example.com
ドメイン名	example.com
ドメインネームサーバー	DNS サーバーアドレス、カンマ区切り 例: 192.0.2.10、192.0.2.21
NTP サーバー	このフィールドは空白のままにしておきます。
NetBIOS ネームサーバー	ドメインネームサーバーごとに同じカンマ区切り IPsを入力する 例: 192.0.2.10、192.0.2.21
NetBIOS ノードタイプ	2

カスタム DHCP オプションセットの作成と Amazon VPC との関連付けの詳細については、Amazon Virtual Private Cloud ユーザーガイドの「DHCP オプションセットの使用」を参照してください。

シナリオ 1 では、DHCP スコープはオンプレミス DNS または AD DS になります。ただし、シナリオ 2 または 3 では、これはローカルにデプロイされたディレクトリサービス (Amazon EC2 の AD DS または AWS Directory Services: Microsoft AD) になります。 AWS クラウドに存在する各ドメインコントローラーは、グローバルカタログとディレクトリ統合 DNS サーバーにすることをお勧めします。

Active Directory: サイトとサービス

シナリオ 2 では、サイトとサービスは AD DS の正しい機能にとって重要なコンポーネントです。サイトトポロジは、同じサイト内およびサイト境界を越えるドメインコントローラー間の AD レプリケーションを制御します。シナリオ 2 では、オンプレミスとクラウドの Amazon の 2 WorkSpaces つ以上のサイトがあります。

正しいサイトトポロジを定義すると、クライアントのアフィニティが保証されます。つまり、クライアント (この場合は WorkSpaces) は希望するローカルドメインコントローラーを使用します。

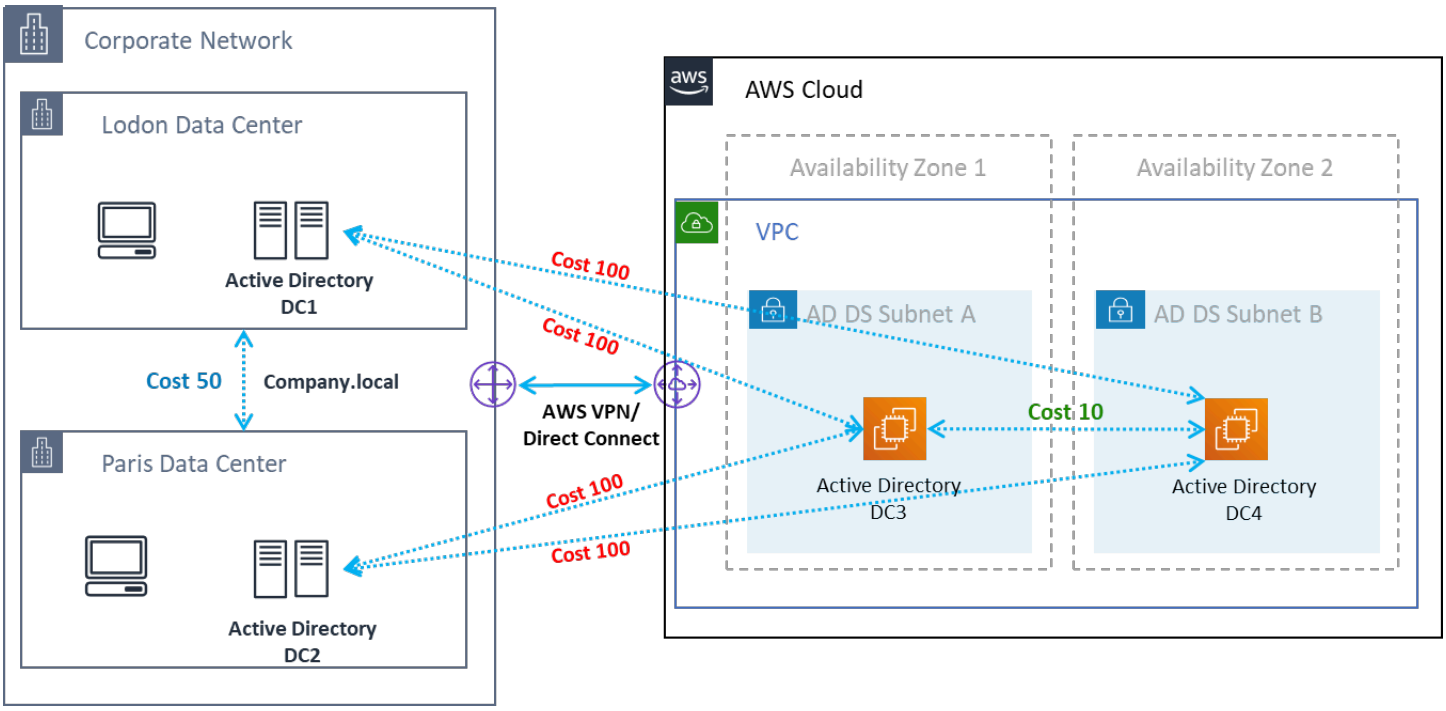

図 15: Active Directory サイトとサービス: クライアントアフィニティ

ベストプラクティス： オンプレミス AD DS と AWS クラウド間のサイトリンクのコストが高いことを定義します。次の図は、サイトに依存しないクライアントアフィニティを確保するためにサイトリンクに割り当てるコスト (コスト 100) の例です。

これらの関連付けにより、AD DS レプリケーションやクライアント認証などのトラフィックがドメインコントローラーへの最も効率的なパスを使用するようになります。シナリオ 2 と 3 の場合、これによりレイテンシーとクロスリンクトラフィックを確実に削減できます。

プロトコル

Amazon WorkSpaces Streaming Protocol (WSP) はクラウドネイティブなストリーミングプロトコルで、世界中の距離や信頼性の低いネットワークにわたって一貫したユーザーエクスペリエンスを実現します。WSP は、メトリクス分析、エンコーディング、コーデックの使用状況と選択をオフロード WorkSpaces することで、プロトコルを からデカップリングします。WSP はポート TCP/UDP 4195 を使用します。WSP プロトコルを使用するかどうかを決定するときは、デプロイ前に回答する必要がある重要な質問がいくつかあります。以下の決定マトリックスを参照してください。

質問	WSP	PCoIP
識別された WorkSpaces ユーザーには双方向のオーディオ/ビデオが必要ですか？	•	
ゼロクライアントはリモートエンドポイント (ローカルデバイス) として使用されますか？		•
Windows または macOS はリモートエンドポイントに使用されますか？	•	•
Ubuntu 18.04 はリモートエンドポイントに使用されますか？		•
ユーザーはウェブアクセス WorkSpaces 経由で Amazon にアクセスしますか？		•

質問	WSP	PCoIP
セッション前またはセッション内のスマートカードサポート (PIC/CAC) は必要ですか？	•	
中国 (寧夏) リージョンで WorkSpaces 使用されますか？		•
スマートカードの事前認証またはセッション内のサポートが必要ですか？	•	
エンドユーザーが信頼できない、高レイテンシー、低帯域幅の接続を使用しているか？	•	

前の質問は、使用するプロトコルを決定する上で重要です。推奨されるプロトコルのユースケースに関する追加情報は、ここで確認できます。使用するプロトコルは、Amazon WorkSpaces 移行機能を使用して後で変更することもできます。この機能の使用の詳細については、「」を参照してください。

WSP WorkSpaces を使用してデプロイする場合、サービスへの接続を確保するために、WSP ゲートウェイを許可リストに追加する必要があります。さらに、WSP WorkSpaces を使用して に接続するユーザーは、最高のパフォーマンスを得るには、ラウンドトリップタイム (RTT) が 250 ミリ秒未満である必要があります。RTT が 250 ミリ秒から 400 ミリ秒までの接続は低下します。ユーザーの接続が一貫して低下する場合は、可能であれば、エンドユーザーに最も近いサービスがサポートされているリージョン WorkSpaces に Amazon をデプロイすることをお勧めします。

Multi-Factor Authentication (MFA)

MFA を実装するには WorkSpaces 、Amazon を Active Directory Connector (AD Connector) または AWS Managed Microsoft AD (MAD) のいずれかを Directory Service として設定し、Directory Service がネットワークにアクセスできる RADIUS サーバーが必要です。Simple Active Directory は MFA をサポートしていません。

AD の Active Directory と Directory Services のデプロイに関する考慮事項、および各シナリオ内の RADIUS 設計オプションについては、前のセクションを参照してください。

MFA - 2 要素認証

MFA を有効にすると、ユーザーはそれぞれの WorkSpaces デスクトップへの認証のためにユーザー名、パスワード、および MFA コードを WorkSpaces クライアントに提供する必要があります。

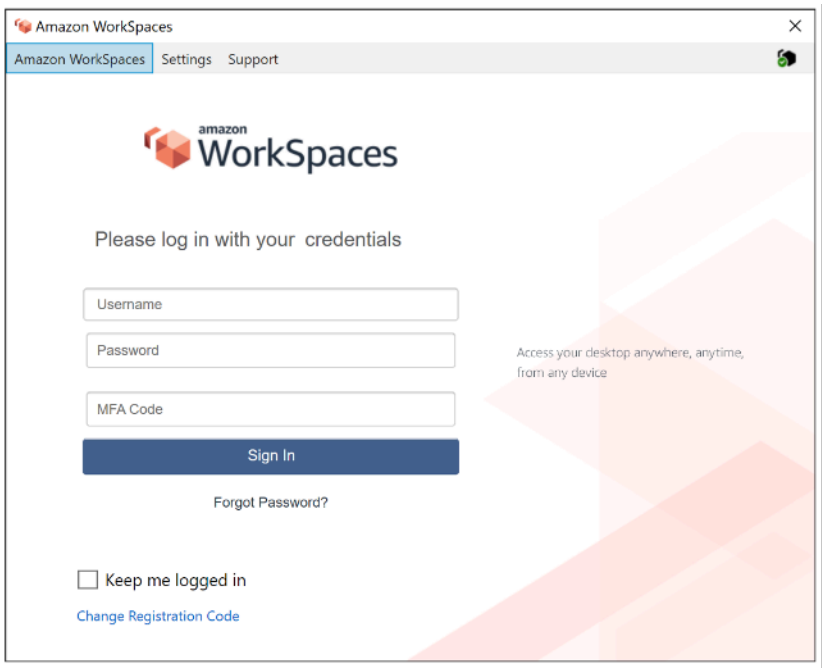

図 16: MFA が有効になっている WorkSpaces クライアント

> **Note**
>
> AWS Directory Service は、ユーザーごとの選択的な またはコンテキスト MFA をサポートしていません。これはディレクトリごとのグローバル設定です。選択的な「ユーザーごと」MFA が必要な場合は、同じソース Active Directory を指す AD Connector でユーザーを区切る必要があります。

WorkSpaces MFA には 1 つ以上の RADIUS サーバーが必要です。通常、これらは RSA や Gemalto など、すでにデプロイしている既存のソリューションです。または、RADIUS サーバーを EC2 インスタンスの VPC 内にデプロイすることもできます (アーキテクチャオプションについては、このドキュメントの「AD DS デプロイシナリオ」セクションを参照してください)。新しい RADIUS ソリューションをデプロイする場合、FreeRADIUS などのいくつかの実装と、 Security や Okta MFA などの SaaS サービスが存在します。

複数の RADIUS サーバーを活用して、ソリューションが障害に対して回復力を持つようにするのがベストプラクティスです。Directory Service を MFA 用に設定する場合、複数の IP アドレスをカンマで区切って入力できます (192.0.0.0,192.0.0.12 など)。Directory Services MFA 機能は、指定された最初の IP アドレスを試行し、イベントネットワーク接続の 2 番目の IP アドレスに移動して、最初の IP アドレスで確立することはできません。高可用性アーキテクチャの RADIUS の設定はソリューションセットごとに異なりますが、包括的な推奨事項は、RADIUS 機能の基盤となるインスタンスを異なるアベイラビリティーゾーンに配置することです。設定例の 1 つとして、セキュリティと Okta MFA では、同じ方法で複数の Okta RADIUS サーバーエージェントをデプロイできます。

AWS Directory Service for MFA を有効にする詳細な手順については、「AD Connector」およびAWS「 Managed Microsoft AD」を参照してください。

ディザスタリカバリ/ビジネス継続性

WorkSpaces クロスリージョンリダイレクト

Amazon WorkSpaces は、顧客にリモートデスクトップアクセスを提供するリージョンレベルのサービスです。ビジネス継続性とディザスタリカバリ要件 (BC/DR) によっては、この WorkSpaces サービスを利用できる別のリージョンにシームレスにフェイルオーバーする必要がある場合もあります。この BC/DR 要件は、 WorkSpaces クロスリージョンリダイレクトオプションを使用して実現できます。これにより、お客様は WorkSpaces 登録コードとして完全修飾ドメイン名 (FQDN) を使用できます。

重要な考慮事項は、フェイルオーバーリージョンへのリダイレクトがどの時点で行われるかを決定することです。この決定の基準は会社のポリシーに基づいて決定する必要がありますが、目標復旧時間 (RTO) と目標復旧時点 (RPO) を含める必要があります。Well-Architected WorkSpaces アーキテクチャ設計には、サービス障害の可能性を含める必要があります。通常の事業運営の回復の許容時間は、決定事項にも影響します。

エンドユーザー WorkSpaces が FQDN WorkSpaces を登録コードとして にログインすると、DNS TXT レコードが解決されます。このレコードには、ユーザーが誘導される登録済みディレクトリを決定する接続識別子が含まれます。 WorkSpaces クライアントのログオンランディングページは、返された接続識別子に関連付けられた登録済みディレクトリに基づいて表示されます。これにより、管理者は FQDN の DNS ポリシーに基づいてエンドユーザーを異なる WorkSpacesディレクトリに誘導できます。このオプションは、プライベートゾーンをクライアントマシンから解決できると仮定して、パブリックまたはプライベート DNS ゾーンで使用できます。クロスリージョンリダイレクト

は、手動または自動で行うことができます。これらのフェイルオーバーはどちらも、目的のディレクトリを指す接続識別子を含む TXT レコードを変更することで実現できます。

BC/DR 戦略を策定する際には、 WorkSpaces クロスリージョンリダイレクトオプションではユーザーデータが同期されず、 WorkSpaces イメージも同期されないため、ユーザーデータを考慮することが重要です。異なる AWS リージョンでの WorkSpaces デプロイは、独立したエンティティです。したがって、セカンダリリージョンへのリダイレクトが発生したときに WorkSpaces ユーザーがデータにアクセスできるように、追加の対策を実行する必要があります。、Windows FSx (DFS 共有) WorkSpaces、またはサードパーティユーティリティなど、ユーザーデータレプリケーションには、リージョン間でデータボリュームを同期するためのオプションが多数あります。同様に、必要な WorkSpaces イメージにセカンダリリージョンが確実にアクセスできることを確認する必要があります。たとえば、リージョン間でイメージをコピーします。詳細については、「Amazon 管理ガイド」の「Amazon のクロスリージョンリダイレクト WorkSpaces」と、図の例を参照してください。
WorkSpaces

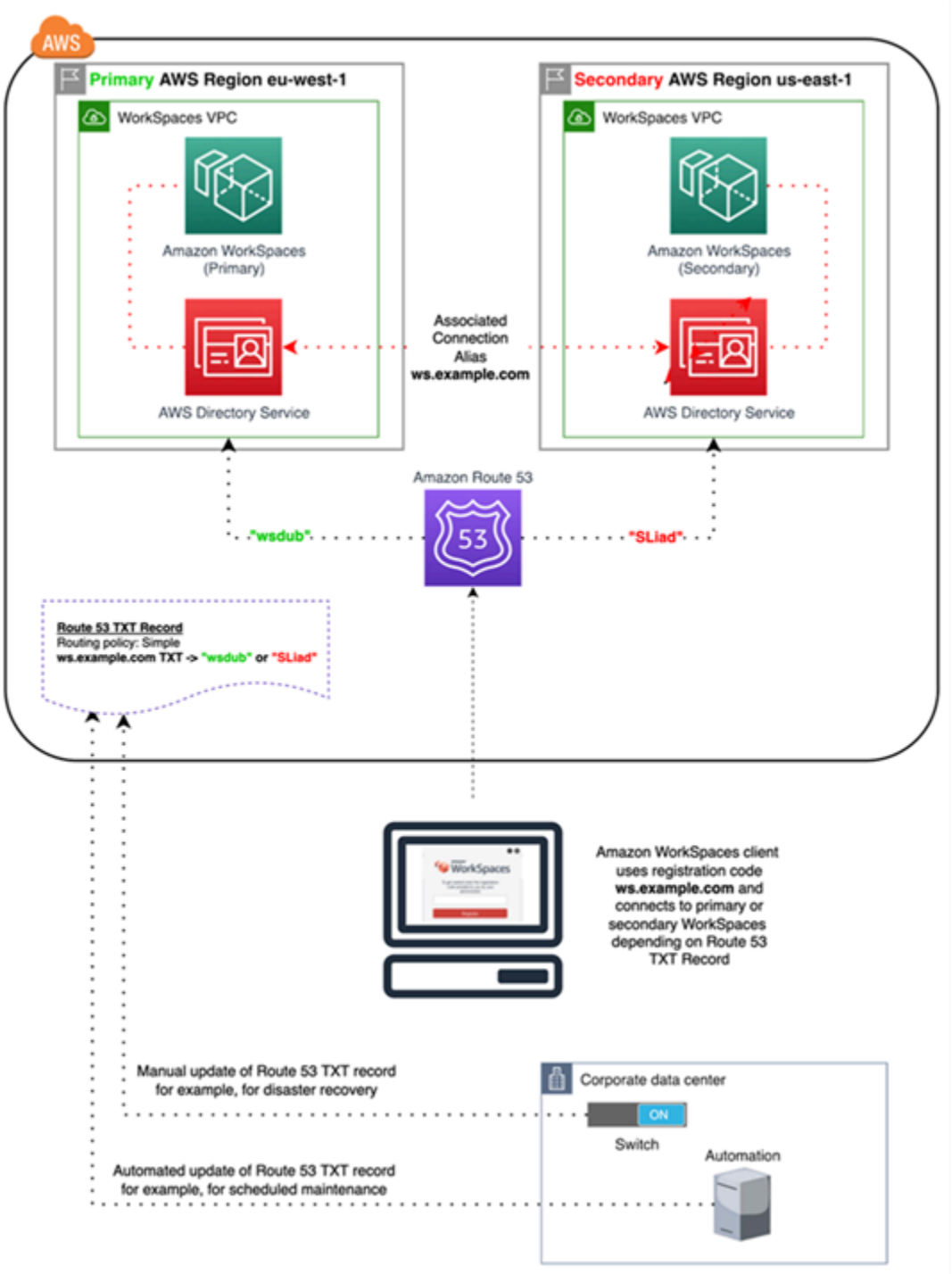

図 17: Amazon Route 53 を使用した WorkSpaces クロスリージョンリダイレクトの例

WorkSpaces インターフェイス VPC エンドポイント (AWS PrivateLink) – API コール

Amazon WorkSpaces パブリック APIs は、 でサポートされていますAWS PrivateLink。 は、パブリックインターネットへのデータの露出を減らすことにより、クラウドベースのアプリケーションと共有されるデータのセキュリティ AWS PrivateLink を強化します。 WorkSpaces API トラフィックは、インターフェイスエンドポイント を使用して VPC 内で保護できます。インターフェイスエンドポイント は、サポートされているサービスを宛先とするトラフィックのエントリポイントとして機能するサブネットの IP アドレス範囲からのプライベート IP アドレスを持つ Elastic Network Interface です。これにより、プライベート IP アドレスを使用して WorkSpaces API サービスにプライベートにアクセスできます。

Public APIs WorkSpaces PrivateLink で を使用すると、VPC 内のリソースのみ、または 経由でデータセンターに接続されているリソースに REST APIs を安全に公開することもできます AWS Direct Connect。

選択した Amazon VPCs と VPC エンドポイントへのアクセスを制限し、リソース固有のポリシーを使用してクロスアカウントアクセスを有効にすることができます。

エンドポイントネットワークインターフェイスに関連付けられているセキュリティグループが、エンドポイントネットワークインターフェイスと、サービスと通信する VPC 内のリソース間の通信を許可していることを確認します。セキュリティグループが VPC 内のリソースからのインバウンド HTTPS トラフィック (ポート 443) を制限している場合、エンドポイントネットワークインターフェイスを介してトラフィックを送信できないことがあります。インターフェイスエンドポイントは TCP トラフィックのみをサポートします。

- エンドポイントは IPv4 トラフィックのみをサポートします。
- エンドポイントを作成するときは、接続先のサービスへのアクセスを制御するエンドポイントポリシーを、エンドポイントにアタッチできます。
- VPC あたりに作成できるエンドポイントの数にはクォータがあります。
- エンドポイントは同じリージョン内でのみサポートされます。VPC と別のリージョンのサービスの間にエンドポイントを作成することはできません。

通知を作成して、インターフェイスエンドポイントイベントに関するアラートを受け取る — 通知を作成して、インターフェイスエンドポイントで発生した特定のイベントに関するアラートを受け取ることができます。通知を作成するには、Amazon SNS トピックを通知に関連付ける必要がありま

す。この SNS トピックへの受信登録を行い、エンドポイントイベントの発生時に E メール通知を受信できます。

Amazon の VPC エンドポイントポリシーを作成する WorkSpaces — Amazon の Amazon VPC エンドポイントのポリシーを作成して WorkSpaces 、以下を指定できます。

- アクションを実行できるプリンシパル。
- 実行可能なアクション。
- このアクションを実行できるリソース。

プライベートネットワークを VPC に接続する — VPC 経由で Amazon WorkSpaces API を呼び出すには、VPC 内にあるインスタンスから接続するか、Amazon Virtual Private Network (VPN) または を使用してプライベートネットワークを VPC に接続する必要があります AWS Direct Connect。Amazon VPN の詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「VPN 接続」を参照してください。の詳細については AWS Direct Connect、「 ユーザーガイド」の「接続の作成AWS Direct Connect 」を参照してください。

VPC インターフェイスエンドポイントを介した Amazon WorkSpaces API の使用の詳細については、「Amazon のインフラストラクチャセキュリティ WorkSpaces」を参照してください。

スマートカードのサポート

スマートカードのサポートは、Microsoft Windows と Amazon Linux の両方で利用できます WorkSpaces。Common Access Card (CAC) および Personal Identity Verification (PIV) によるスマートカードのサポートは、Amazon でのみ WorkSpaces ストリーミングプロトコル (WSP) WorkSpaces を使用して利用できます。WSP でのスマートカードのサポート WorkSpaces により、組織で承認された接続エンドポイントで、スマートカードリーダー形式で特定のハードウェアを使用してユーザーを認証するためのセキュリティ体制が強化されます。まず、スマートカード で利用できるサポートの範囲に慣れ、既存および将来の WorkSpaces デプロイでスマートカードがどのように機能するかを判断することが重要です。

セッション前認証またはセッション内認証のどのタイプのスマートカードサポートが必要かを判断するのがベストプラクティスです。セッション前認証は、この記事の (AWS GovCloud 米国西部)、米国東部 (バージニア北部)、米国西部 (オレゴン)、欧州 (アイルランド)、アジアパシフィック (東京)、アジアパシフィック (シドニー) でのみ利用できます。セッション内のスマートカード認証は、一般的に次のような考慮事項を考慮して利用できます。

- 組織には、Windows Active Directory と統合されたスマートカードインフラストラクチャがありますか？
- オンライン証明書ステータスプロトコル (OCSP) 応答者パブリックインターネットはアクセス可能ですか？
- サブジェクト代替名 (SAN) フィールドのユーザープリンシパル名 (UPN) でユーザー証明書が発行されていますか？
- セッション中セクションとセッション前セクションに関するその他の考慮事項については、詳しく説明します。

スマートカードのサポートは、グループポリシーを通じて有効になります。WSP の Amazon WorkSpaces グループポリシー管理用テンプレートを、Amazon Directory (ies) で使用される Active Directory ドメインのセントラルストアに追加することがベストプラクティスです。 WorkSpaces このポリシーを既存の Amazon WorkSpaces デプロイに適用する場合、すべての WorkSpaces では、コンピュータベースのポリシーであるため、グループポリシーの更新と、変更がすべてのユーザーに対して有効にするための再起動が必要になります。

ルート CA

Amazon WorkSpaces クライアントとユーザーの移植性の性質上、ユーザーが Amazon への接続に使用する各デバイスの信頼されたルート証明書ストアにサードパーティーのルート CA 証明書をリモートで配信する必要があります WorkSpaces。AD ドメインコントローラーとスマートカードを持つユーザーデバイスは、ルート CAsを信頼する必要があります。正確な要件の詳細については、Microsoft が提供するサードパーティー CA の有効化に関するガイドラインを参照してください。 CAs

AD ドメイン参加環境では、これらのデバイスはルート CA 証明書を配布するグループポリシーを通じてこの要件を満たします。Amazon WorkSpaces Client が non-domain-joined デバイスから使用されるシナリオでは、Intune などのサードパーティーのルート CAs の代替配信方法を決定する必要があります。 https://docs.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure

セッション内

セッション内認証は、Amazon WorkSpaces ユーザーセッションがすでに開始された後に、アプリケーション認証を簡素化および保護します。前述のように、Amazon のデフォルトの動作ではスマートカード WorkSpaces が無効になるため、グループポリシーを使用して有効にする必要があります。Amazon WorkSpaces の管理の観点から見ると、認証をパススルーするアプリケーション (ウェ

ブブラウザなど) には特に設定が必要です。AD Connector と Directory(ies) に変更を加える必要はありません。

セッション内認証のサポートを必要とする一般的なアプリケーションは、Mozilla Firefox や Google Chrome などのウェブブラウザ経由です。Mozilla Firefox では、セッション内のスマートカードサポートに対して制限された設定が必要です。Amazon Linux WSP では、Mozilla Firefox と Google Chrome の両方でセッション内スマートカードをサポートするには、追加の設定 WorkSpaces が必要です。

Amazon WorkSpaces Client にはローカルコンピュータへのアクセス許可がない可能性があるため、トラブルシューティングの前にルート CAs がユーザーの個人証明書ストアにロードされていることを確認するのがベストプラクティスです。さらに、スマートカードを使用したセッション内認証の問題のトラブルシューティングを行う場合は、OpenSC を使用してスマートカードデバイスを識別します。最後に、オンライン証明書ステータスプロトコル (OCSP) レスポンダーは、証明書失効チェックを通じてアプリケーション認証のセキュリティ体制を改善するために推奨されます。

セッション前

セッション前認証をサポートするには、Windows WorkSpaces クライアントバージョン 3.1.1 以降、または macOS WorkSpaces クライアントバージョン 3.1.5 以降が必要です。スマートカードによるセッション前認証は、標準認証と根本的に異なるため、ユーザーはスマートカードの挿入と PIN コードの入力の両方を組み合わせて認証する必要があります。この認証タイプでは、ユーザーのセッションの期間は Kerberos チケットの有効期間によって制限されます。完全なインストールガイドは、 にあります。

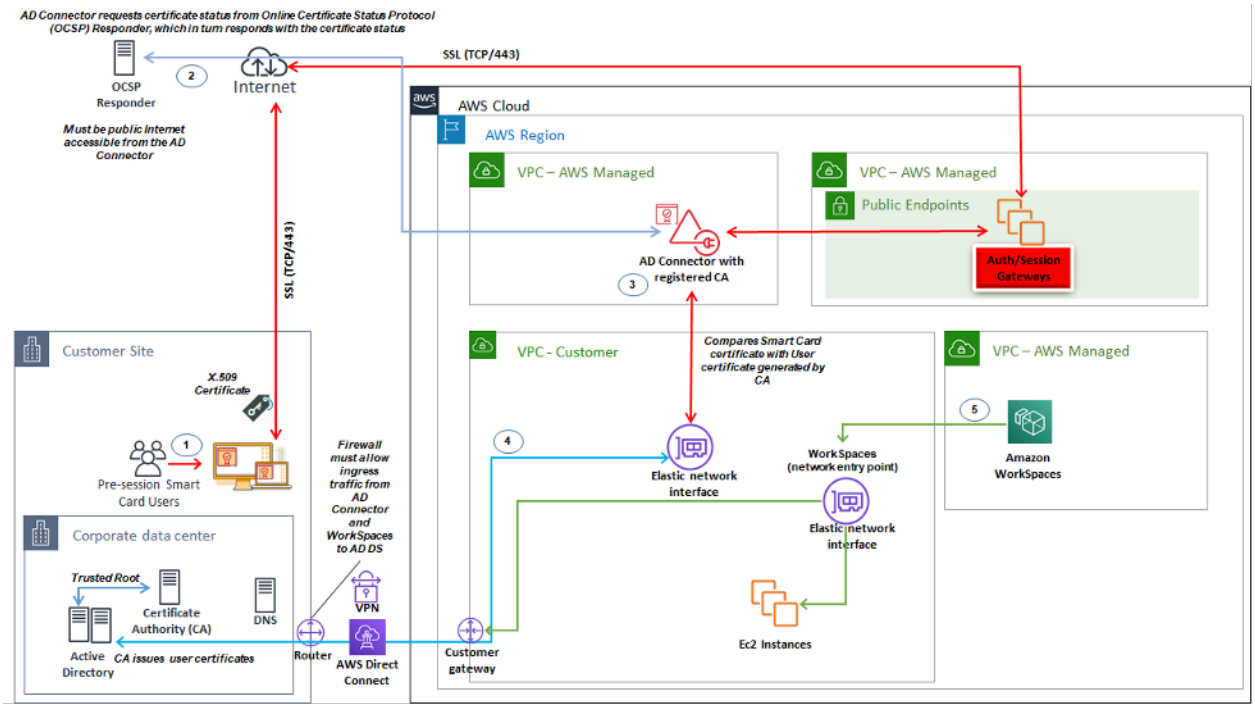

図 18: セッション前認証の概要

1. ユーザーが Amazon WorkSpaces Client を開き、スマートカードを挿入して、PIN を入力します。PIN は、Amazon WorkSpaces Client が X.509 証明書を復号するために使用されます。これは、Authentication Gateway を介して AD Connector にプロキシされる です。
2. AD Connector は、ディレクトリ設定で指定されたパブリックにアクセス可能な OCSP レスポンダー URL に対して X.509 証明書を検証し、証明書が取り消されていないことを確認します。
3. 証明書が有効な場合、Amazon WorkSpaces Client は、X.509 証明書とプロキシを AD Connector に復号化するための PIN を 2 回入力するようにユーザーに求めることで認証プロセスを続行します。その後、検証のために AD Connector のルート証明書と中間証明書と照合されます。
4. 証明書の検証が正常に一致すると、AD Connector が Active Directory を使用してユーザーを認証し、Kerberos チケットが作成されます。
5. Kerberos チケットはユーザーの Amazon に渡 WorkSpace され、WSP セッションを認証して開始します。

OCSP レスポンダーは、カスタマー AWS マネージドネットワークではなくマネージドネットワークを介して接続が実行されるため、このステップではプライベートネットワークへのルーティングは行われないため、パブリックにアクセス可能である必要があります。

AD Connector に提示されるユーザー証明書には、証明書の userPrincipalName (SAN) フィールドにユーザーの subjectAltName (UPN) が含まれているため、ユーザー名を入力する必要はありません。スマートカードによるセッション前認証を必要とするすべてのユーザーを自動化して、Microsoft マネジメントコンソールで個別に実行するのではなく PowerShell、 を使用して証明書で予想される UPN で認証するように AD ユーザーオブジェクトを更新することをお勧めします。

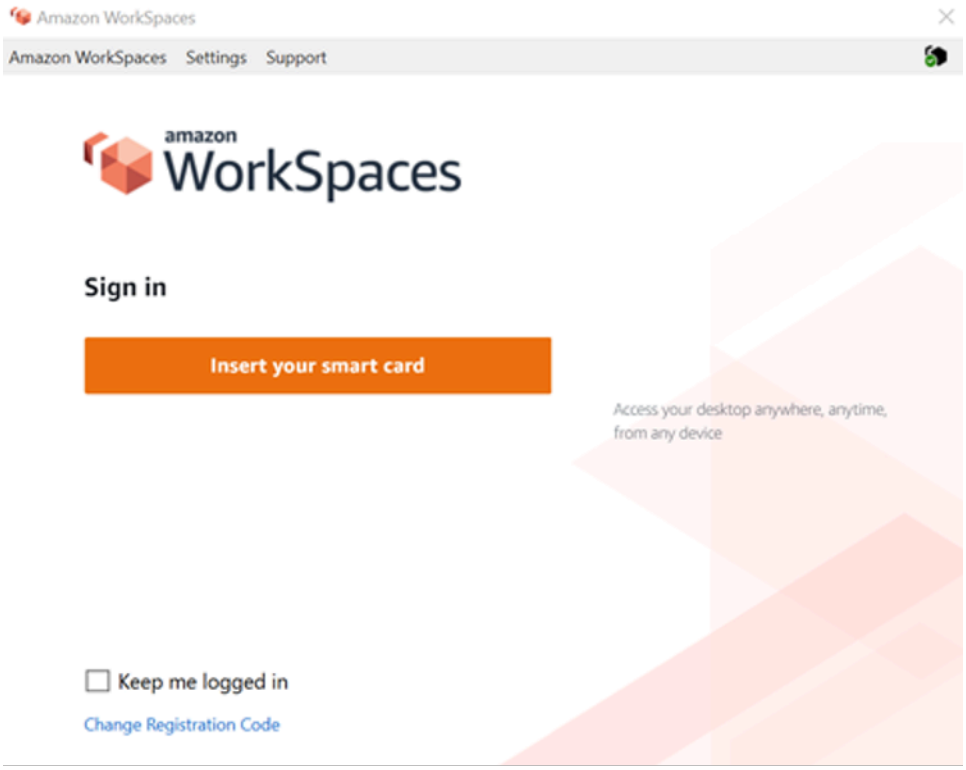

図 19: コンソールに WorkSpaces サインインする

クライアントのデプロイ

Amazon WorkSpaces Client (バージョン 3.X 以降) は、管理者がユーザーの WorkSpaces クライアントを事前設定するために使用できる標準化された設定ファイルを使用します。2 つのメイン設定ファイルのパスは、次の場所にあります。

OS	設定ファイルパス
Windows	C:\Users\USERNAME\AppData\Local\Amazon Web Services\Amazon WorkSpaces

OS	設定ファイルパス
macOS	/Users/USERNAME/Library/Application Support/Amazon Web Services/Amazon WorkSpaces
Linux (Ubuntu 18.04)	/home/ubuntu/.local/share/Amazon Web Services/Amazon WorkSpaces/

これらのパス内には、2 つの設定ファイルがあります。最初の設定ファイルは UserSettings.json で、現在の登録、プロキシ設定、ログ記録レベル、登録リストを保存する機能などを設定します。2 番目の設定ファイルは RegistrationList.json です。このファイルには、クライアントが正しい WorkSpaces ディレクトリにマッピングするために使用するすべての WorkSpaces ディレクトリ情報が含まれます。 RegistrationList.json を事前設定すると、ユーザーのクライアント内のすべての登録コードが入力されます。

> **Note**
>
> ユーザーが WorkSpaces クライアントバージョン 2.5.11 を実行している場合は、クライアントプロキシ設定に proxy.cfg が使用され、client_settings.ini はログレベルを設定し、登録リストを保存する機能も設定します。デフォルトのプロキシ設定では、OS 内で設定されているものが使用されます。

これらのファイルは標準化されているため、管理者はWorkSpaces クライアント をダウンロードし、適用可能な設定をすべて設定してから、同じ設定ファイルをすべてのエンドユーザーにプッシュアウトできます。設定を有効にするには、新しい設定が設定された後にクライアントを起動する必要があります。クライアントの実行中に設定を変更した場合、クライアント内では変更は設定されません。

WorkSpaces ユーザーに対して設定できる最後の設定は、Windows クライアントの自動更新です。これは設定ファイルでは制御されず、代わりに Windows レジストリによって制御されます。クライアントの新しいバージョンがリリースされたら、レジストリキーを作成してそのバージョンをスキップできます。これは、次のパスで完全なバージョン番号の値 SkipThisVersion を持つ文字列レジストリエントリ名を作成することで設定できません: Computer\HKEY_CURRENT_USER\Software\Amazon Web Services。RL\Amazon WorkSpaces\WinSparkle このオプションは macOS でも利用できます。ただし、設定は plist ファイル内であり、編集するには特別なソフトウェアが必要で

す。それでもこのアクションを実行したい場合は、/Users/USERNAME/Library/Preferences にある com.amazon.workspaces ドメイン内に SUSkippedVersion エントリを追加することで実行できます。

Amazon WorkSpaces エンドポイントの選択

のエンドポイントの選択 WorkSpaces

Amazon WorkSpaces は、Windows デスクトップから iPads、Chromebooks まで、複数のエンドポイントデバイスをサポートしています。利用可能な Amazon WorkSpaces クライアントは、Amazon Workspaces ウェブサイト からダウンロードできます。ユーザーに適したエンドポイントを選択することは、重要な決定事項です。ユーザーが双方向のオーディオ/ビデオの使用を必要とし、ストリーミングプロトコルを利用する WorkSpaces場合は、Windows または macOS クライアントを使用する必要があります。すべてのクライアントについて、「Amazon の IP アドレスとポートの要件」に記載されている IP アドレスとポート WorkSpacesが、クライアントがサービスに接続できるように明示的に設定されていることを確認します。エンドポイントデバイスの選択に役立つその他の考慮事項を次に示します。

- Windows — Windows Amazon WorkSpaces クライアントを利用するには、4.x クライアントで 64 ビット Microsoft Windows 8.1、Windows 10 デスクトップが必要です。ユーザーは、ローカルマシンの管理権限なしで、ユーザープロファイルのみにクライアントをインストールできます。システム管理者は、グループポリシー、Microsoft Endpoint Manager Configuration Manager (MEMCM)、または環境で使用されているその他のアプリケーションデプロイツールを使用して、クライアントをマネージドエンドポイントにデプロイできます。Windows クライアントは、最大 4 台のディスプレイと最大解像度 3840 x 2160 をサポートします。
- macOS — 最新の macOS Amazon WorkSpaces クライアントをデプロイするには、macOS デバイスで macOS 10.12 (Sierra) 以降を実行する必要があります。エンドポイントが OSX 10.8.1 以降を実行 WorkSpaces している場合は、古いバージョンの WorkSpaces クライアントをデプロイして PCoIP に接続できます。macOS クライアントは、最大 2 台の 4K 解像度モニターまたは 4 台の WDCRGA (1920 x 1200) 解像度モニターをサポートします。
- Linux — Amazon WorkSpaces Linux クライアントを実行するには、64 ビット Ubuntu 18.04 (AMD64) が必要です。Linux エンドポイントがこの OS バージョンを実行しない場合、Linux クライアントはサポートされません。Linux クライアントをデプロイしたり、登録コードをユーザーに提供する前に、Linux クライアントへのアクセスをディレクトリレベルで有効にしてください。これはデフォルトでは無効になっており、有効にするまで Linux クライアントから接続できないためです。 WorkSpaces Linux クライアントは、最大 2 台の 4K 解像度モニターまたは 4 台の WDCRGA (1920 x 1200) 解像度モニターをサポートします。

- iPad — Amazon WorkSpaces iPad クライアントアプリケーションは PCoIP をサポートしています WorkSpaces。サポートされている iPads は、iOS 8.0 以降の iPad2 以降、iOS 8.0 以降の iPad Retina、iOS 8.0 以降の iPad mini、iOS 9.0 以降の iPad Pro です。ユーザーが接続するデバイスがこれらの基準を満たしていることを確認します。iPad クライアントアプリケーションは、さまざまなジェスチャをサポートしています。（サポートされているジェスチャの完全なリストを参照してください）。Amazon WorkSpaces iPad クライアントアプリケーションは Swiftpoint GT ProPoint、マウスもサポートしています PadPoint 。Swiftpoint TRACPOINT、 PenPoint GoPoint マウスはサポートされていません。
- Android / Chromebook — Android デバイスまたは Chromebook をエンドユーザーのエンドポイントとしてデプロイする場合は、いくつかの考慮事項を考慮する必要があります。このクライアントは PCoIP WorkSpaces のみをサポートしているため、接続先の WorkSpaces ユーザーが PCoIP WorkSpaces であることを確認します。このクライアントは 1 つのディスプレイのみをサポートします。ユーザーがマルチモニターのサポートを必要とする場合は、別のエンドポイントを使用します。Chromebook をデプロイする場合は、デプロイするモデルが Android アプリケーションのインストールをサポートしていることを確認してください。フル機能のサポートは Android クライアントでのみサポートされ、従来の Chromebook クライアントではサポートされません。これは通常、2019 年より前に作成された Chromebook に関する考慮事項にすぎません。Android は、Android が OS 4.4 以降を実行している限り、タブレットと携帯電話の両方に対応しています。ただし、最新の Android クライアントを利用するには、 WorkSpace Android デバイスが OS 9 以降を実行することをお勧めします。Chromebook が WorkSpaces クライアントバージョン 3.0.1 以降を実行している場合、ユーザーはセルフサービスWorkSpaces 機能を利用できるようになりました。さらに、管理者として、信頼できるデバイス証明書を利用して、有効な証明書を持つ信頼できるデバイス WorkSpaces へのアクセスを制限できます。
- ウェブアクセス — ユーザーは、ウェブブラウザを使用して任意の場所 WorkSpaces から Windows にアクセスできます。これは、ロックされたデバイスまたは制限のあるネットワークを使用する必要があるユーザーに最適です。従来のリモートアクセスソリューションを使用して適切なクライアントアプリケーションをインストールする代わりに、ユーザーはウェブサイトを経由して職場のリソースにアクセスできます。ユーザーは WorkSpaces Web Access を利用して、デスクトップエクスペリエンスで Windows 10 または Windows Server 2016 を実行している Windows PCoIP WorkSpaces に接続 non-graphics-basedできます。ユーザーは Chrome 53 以降または Firefox 49 以降を使用して接続する必要があります。WSP ベースの の場合 WorkSpaces、ユーザーは WorkSpaces Web Access を使用して、非グラフィックの Windows ベースの に接続できます WorkSpaces。これらのユーザーは、Microsoft Edge 91 以降または Google Chrome 91 以降を使用して接続する必要があります。サポートされる最小画面解像度は 960 x 720 で、サポートされる最大解像度は 2560 x 1600 です。マルチモニターはサポートされていません。可能な限

り、最適なユーザーエクスペリエンスを得るには、ユーザーが OS バージョンのクライアントを使用することをお勧めします。

- PCoIP ゼロクライアント — PCoIP ゼロクライアントは、PCoIP が割り当てられているエンドユーザー、または PCoIP WorkSpaces が割り当てられているエンドユーザーにデプロイできます。に直接接続するには、Tera2 ゼロクライアントにファームウェアバージョン 6.0.0 以降が必要です WorkSpace。Amazon で多要素認証を使用するには WorkSpaces、Tera2 ゼロクライアントデバイスがファームウェアバージョン 6.0.0 以降を実行する必要があります。ゼロクライアントハードウェアのサポートとトラブルシューティングは、製造元に依頼する必要があります。
- IGEL OS — ファームウェアバージョンが 11.04.280 以上 WorkSpaces であれば、エンドポイントデバイスで IGEL OS を使用して PCoIP ベースに接続できます。サポートされている機能は、現在の既存の Linux クライアントの機能と一致します。IGEL OS クライアントをデプロイしたり、登録コードをユーザーに提供する前に、Linux クライアントアクセスを WorkSpaces ディレクトリレベルで有効にしてください。これはデフォルトで無効になっているため、ユーザーは有効にするまで IGEL OS クライアントから接続できなくなります。IGEL OS クライアントは、最大 2 台の 4K 解像度モニターまたは 4 台の WDCRGA (1920 x 1200) 解像度モニターをサポートします。

ウェブアクセスクライアント

ロックダウンされたデバイス向けに設計された Web Access クライアントは、クライアントソフトウェアをデプロイ WorkSpaces することなく Amazon へのアクセスを提供します。Web Access クライアントは、Amazon が Windows オペレーティングシステム (OS) WorkSpaces で、マウス環境などの限定されたユーザーワークフローに使用される設定でのみ推奨されます。ほとんどのユースケースは、Amazon WorkSpaces クライアントから利用できる機能セットの恩恵を受けます。Web Access クライアントは、デバイスとネットワークの制限に代替の接続方法が必要な特定のユースケースでのみ推奨されます。

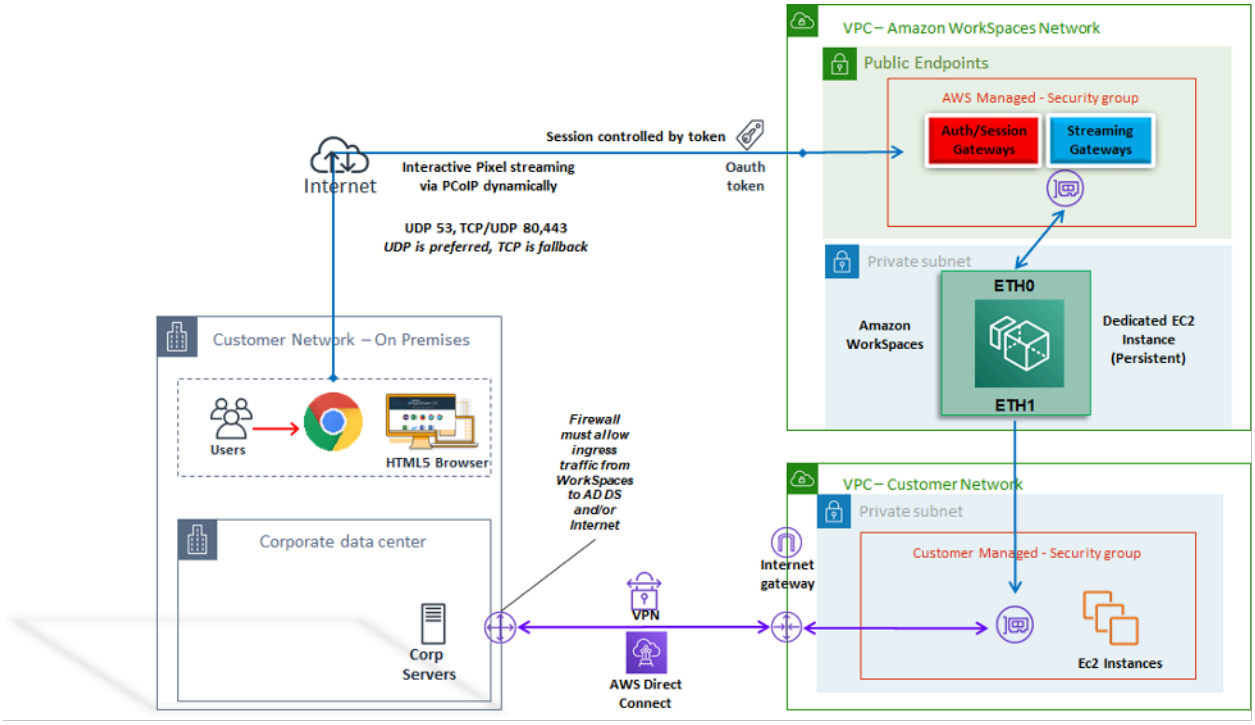

図 20: ウェブアクセスクライアントアーキテクチャ

図に示すように、Web Access クライアントには、ユーザーにセッションをストリーミングするためのさまざまなネットワーク要件があります。Web Access は、PCoIP または WSP プロトコル WorkSpaces を使用して Windows で使用できます。 WorkSpaces ゲートウェイへの認証と登録には、DNS と HTTP/HTTPS が必要です。WSP プロトコル WorkSpaces を使用するには、UDP/TCP 4195 の直接接続を WSP ゲートウェイの IP アドレス範囲に開く必要があります。ストリーミングトラフィックは、完全な Amazon WorkSpaces クライアントとは異なり、固定ポートに割り当てられず、動的に割り当てられます。ストリーミングトラフィックには UDP が適していますが、UDP が制限されている場合、ウェブブラウザは TCP にフォールバックします。TCP/UDP ポート 4172 がブロックされ、組織的な制限によりブロック解除できない環境では、Web Access クライアントはユーザーに代替の接続方法を提供します。

デフォルトでは、Web Access クライアントはディレクトリレベルで無効になっています。ユーザーがウェブブラウザ WorkSpaces から Amazon にアクセスできるようにするには、 AWS Management Console を使用してディレクトリ設定を更新するか、プログラムで WorkspaceAccessProperties API を使用して を Allow DeviceTypeWeb に変更します。さらに、管理者はグループポリシー設定がログイン要件と競合しないようにする必要があります。

Amazon WorkSpaces タグ

```
Tags enable you to associate metadata with AWS resources. Tags can be used with Amazon
 WorkSpaces to registered directories,
  bundles, IP Access Control Groups, or images. Tags assist with cost allocation to
 internal cost centers. Before using tags with Amazon WorkSpaces,
  refer to the Tagging Best Practices whitepaper.

Tag restrictions
```

- リソースあたりのタグの最大数 – 50
- キーの最大長 – 127 文字 (Unicode)
- 値の最大長 – 255 文字 (Unicode)
- タグのキーと値は大文字と小文字が区別されます。使用できる文字は、UTF-8 で表現できる文字、スペース、および数字と、特殊文字 (+、-、=、.、_、:、/、@) です。ただし、先頭または末尾にはスペースを使用しないでください。
- タグの名前または値に aws: または aws:workspaces: プレフィックスは使用しないでください。これらは AWS 用に予約されています。これらのプレフィックスが含まれるタグの名前または値は編集または削除できません。

タグ付けできるリソース

- タグは、作成時に WorkSpaces、インポートされたイメージ、IP アクセスコントロールグループなどのリソースに追加できます。
- 、登録済みディレクトリ WorkSpaces、カスタムバンドル、イメージ、および IP アクセスコントロールグループの既存のリソースにタグを追加できます。

コスト配分タグの使用

Cost Explorer で WorkSpaces リソースタグを表示するには、 AWS Billing and Cost Management 「」および「コスト管理ユーザーガイド」の「ユーザー定義のコスト配分タグのアクティブ化」の手順に従って、リソースに適用したタグをアクティブ化します WorkSpaces。 Cost Explorer

タグはアクティブ化されてから 24 時間後に表示されますが、それらのタグに関連付けられた値が Cost Explorer に表示されるまでに 4 ~ 5 日かかる場合があります。Cost Explorer にコストデータが表示されて提供するには、その間にタグが付いた WorkSpaces リソースに料金が発生する必要があ

ります。Cost Explorer には、タグがアクティブ化された時点からのコストデータのみが表示されます。現時点では、履歴データはありません。

タグの管理

を使用して既存のリソースのタグを更新するには AWS CLI、create-tags コマンドと delete-tags コマンドを使用します。一括更新や多数の WorkSpaces リソースでのタスクの自動化のために、Amazon WorkSpaces は AWS Resource Groups タグエディタのサポートを追加します。 AWS Resource Groups タグエディタを使用すると、他の AWS リソース WorkSpaces とともに から AWS タグを追加、編集、または削除できます。

Amazon WorkSpaces Service Quotas

Service Quotas を使用すると、制限 とも呼ばれる特定のクォータ の値を簡単に検索できます。特定のサービスのすべてのクォータを検索することもできます。

のクォータを表示するには WorkSpaces

1. Service Quotas コンソール に移動します。
2. 左側のナビゲーションペインで、AWS サービス を選択します。
3. リストから Amazon WorkSpaces を選択するか、先行入力検索フィールドに Amazon WorkSpaces を入力します。
4. 説明や Amazon リソースネーム (ARN) など、クォータに関する追加情報を表示するには、クォータ名を選択します。

Amazon WorkSpaces は、、イメージ、バンドル、ディレクトリ WorkSpaces、接続エイリアス、IP コントロールグループなど、特定のリージョンのアカウントで使用できるさまざまなリソースを提供します。Amazon Web Services アカウントを作成すると、作成できるリソースの数にデフォルトのクォータが設定されます (制限とも呼ばれます) 。

Service Quotas コンソールを使用して、デフォルトの Service Quotas を表示したり、調整可能なクォータのクォータの引き上げをリクエストすることができます。

詳細については、「Service Quotas ユーザーガイド」の「Service Quotas の表示」および「クォータの引き上げのリクエスト」を参照してください。 Service Quotas

Amazon WorkSpaces デプロイの自動化

Amazon を使用すると WorkSpaces、Microsoft Windows または Amazon Linux デスクトップを数分以内に起動し、オンプレミスまたは外部ネットワークからデスクトップソフトウェアに安全、確実、迅速に接続してアクセスできます。Amazon のプロビジョニングを自動化 WorkSpaces して、Amazon WorkSpaces を既存のプロビジョニングワークフローに統合できます。

一般的な WorkSpaces 自動化方法

お客様は、Amazon の迅速な WorkSpaces デプロイを可能にするために、多数のツールを使用できます。このツールを使用すると、 の管理を簡素化し WorkSpaces、コストを削減し、迅速に拡張および移行できるアジャイル環境を実現できます。

AWS CLI および API

サービスを安全に大規模に操作するために使用できる Amazon WorkSpaces API オペレーションがあります。すべてのパブリック APIs は AWS CLI SDK および Tools for で使用できますが PowerShell、イメージ作成などのプライベート APIs は でのみ使用できます AWS Management Console。Amazon の運用管理とビジネスセルフサービスを検討するときは WorkSpaces、WorkSpaces APIs を使用するには技術的専門知識とセキュリティ許可が必要であることを考慮してください。

API コールは、 AWS SDK を使用して行うことができます。AWS Tools for Windows PowerShell および AWS Tools for PowerShell Core は PowerShell 、 AWS SDK for .NET によって公開される機能に基づいて構築されたモジュールです。これらのモジュールを使用すると、コマンドラインから AWS リソースに対するオペレーションを PowerShell スクリプト化し、既存のツールやサービスと統合できます。例えば、API コールでは、AD と統合して WorkSpaces ライフサイクルを自動的に管理し、ユーザーの AD グループメンバーシップ WorkSpaces に基づいてプロビジョニングおよび廃止できます。

AWS CloudFormation

AWS CloudFormation では、インフラストラクチャ全体をテキストファイルでモデル化できます。このテンプレートは、インフラストラクチャの唯一の信頼できるソースになります。これにより、組織全体で使用されるインフラストラクチャコンポーネントを標準化し、設定コンプライアンスと迅速なトラブルシューティングが可能になります。

AWS CloudFormation は、安全かつ反復可能な方法でリソースをプロビジョニングし、インフラストラクチャとアプリケーションを構築および再構築できるようにします。 CloudFormation を使

用して環境のコミッショニングと廃止を行うことができます。これは、繰り返し可能な方法で構築および廃止するアカウントが多数ある場合に便利です。Amazon の運用管理とビジネスセルフサービスを検討するときは WorkSpaces、 を使用するには技術的専門知識とセキュリティ許可AWS CloudFormationが必要であることを考慮してください。

セルフサービス WorkSpaces ポータル

お客様は、 WorkSpaces API コマンドやその他の AWS サービスに基づいて構築し、セルフサービスポータルを作成できます WorkSpaces 。これにより、お客様は大規模なデプロイと再利用のプロセスを合理化 WorkSpaces できます。 WorkSpaces ポータルを使用すると、各リクエストに IT 介入を必要としない統合承認ワークフロー WorkSpaces を使用して、ワークフォースが独自のをプロビジョニングできます。これにより、IT 運用コストが削減され、エンドユーザーが をより WorkSpaces 迅速に開始できるようになります。追加の組み込みの承認ワークフローにより、企業のデスクトップの承認プロセスが簡素化されます。専用ポータルは、Windows または Linux のクラウドデスクトップをプロビジョニングするための自動化ツールを提供し、ユーザーが を再構築、再起動、または移行できるようにします。また WorkSpace、パスワードをリセットすることもできます。

このドキュメントの「詳細読み取り」セクションで参照されているセルフサービス WorkSpaces ポータルの作成例がガイドされています。 AWS パートナーは、 を介して事前設定された WorkSpaces 管理ポータルを提供しますAWS Marketplace。

Enterprise IT Service Management との統合

企業が Amazon を大規模な仮想デスクトップソリューション WorkSpaces として採用するにつれて、IT サービスマネジメント (ITSM) システムを実装または統合する必要があります。ITSM 統合により、プロビジョニングと運用のためのセルフサービスを提供できます。Service Catalog を使用すると、一般的にデプロイされる AWS サービスとプロビジョニングされたソフトウェア製品を一元管理できます。このサービスは、組織が一貫したガバナンスとコンプライアンス要件を満たすのに役立つと同時に、ユーザーが必要な承認済み AWS サービスのみをデプロイできるようにします。Service Catalog を使用して、 などの IT サービス管理ツール内 WorkSpaces から Amazon のセルフサービスライフサイクル管理サービスを有効にすることができますServiceNow。

WorkSpaces デプロイ自動化のベストプラクティス

Well Architected の WorkSpaces デプロイ自動化の選択と設計の原則を考慮する必要があります。

- 自動化の設計 — 反復性とスケールを可能にするために、プロセスに最小限の手動介入を提供するように設計されています。

- コスト最適化のための設計 — を自動的に作成して再利用することで WorkSpaces、リソースの提供に必要な管理作業を減らし、アイドル状態または未使用のリソースが不要なコストを生成するのを防ぐことができます。
- 効率を考慮した設計 — の作成と終了に必要なリソースを最小限に抑えます WorkSpaces。可能な限り、効率を向上させるために、ビジネスに Tier 0 セルフサービス機能を提供します。
- 柔軟性を考慮した設計 — 複数のシナリオに対応でき、同じメカニズム (タグ付けされたユースケースとプロファイル識別子を使用してカスタマイズ) で拡張できる一貫したデプロイメカニズムを作成します。
- 生産性を考慮した設計 — リソースを追加または削除するための正しい認可と検証を可能にするように WorkSpaces オペレーションを設計します。
- スケーラビリティを考慮した設計 — Amazon が WorkSpaces 使用する pay-as-you go モデルでは、必要に応じてリソースを作成し、不要になったリソースを削除することでコスト削減を実現できます。
- セキュリティのための設計 — リソースを追加または削除するための正しい認可と検証を可能にするように WorkSpaces オペレーションを設計します。
- サポート可能性を考慮した設計 - 無形のサポートと復旧のメカニズムとプロセスを可能にするように WorkSpaces 運用を設計します。

Amazon WorkSpaces パッチ適用とインプレースアップグレード

Amazon では WorkSpaces、Microsoft System Center Configuration Manager (SCCM)、Puppet Enterprise、Ansible などの既存のサードパーティツールを使用してパッチ適用と更新を管理できます。セキュリティパッチのインプレースデプロイでは、通常、毎月のパッチサイクルが維持され、エスカレーションや迅速なデプロイのための追加のプロセスも維持されます。ただし、オペレーティングシステムのインプレースアップグレードや機能の更新の場合は、多くの場合、特別な考慮事項が必要です。

WorkSpace メンテナンス

Amazon WorkSpaces には、 が Amazon WorkSpaces エージェントの更新と使用可能なオペレーティングシステムの更新 WorkSpace をインストールするデフォルトのメンテナンスウィンドウ WorkSpaces があります。スケジュールされたメンテナンスウィンドウ中は、ユーザー接続には使用できません。

- AlwaysOn WorkSpaces のタイムゾーンのデフォルトのメンテナンスウィンドウは、 WorkSpace 毎週日曜日の午前 00:00～4:00 です。

- タイムゾーンのリダイレクトはデフォルトで有効になっており、デフォルトのウィンドウを上書きしてユーザーのローカルタイムゾーンと一致させることができます。
- グループポリシーを使用して、Windows のタイムゾーンリダイレクトを無効にする WorkSpacesことができます。Linux のタイムゾーンリダイレクトを無効にする WorkSpacesには、PCoIP エージェント設定を使用します。

- AutoStop WorkSpaces 重要な更新をインストールするために、 は毎月 1 回自動的に開始されます。その月の第 3 月曜日以降、および最大 2 週間、メンテナンスウィンドウは、 の AWS リージョンのタイムゾーンで毎日午前 0 時から午後 5 時まで開かれます WorkSpace。は、メンテナンスウィンドウの任意の日にメンテナンス WorkSpace できます。

- の維持に使用されるタイムゾーンを変更することはできませんが AutoStop WorkSpaces、 のメンテナンスウィンドウを無効にする AutoStop WorkSpacesことはできます。

- 手動メンテナンスウィンドウは、 の状態を WorkSpace ADMIN_MAINTAKANCE に設定することで、希望するスケジュールに基づいて設定できます。

- AWS CLI コマンドを使用するとmodify-workspace-state、 WorkSpace 状態を ADMIN_MAINMAINANCE に変更できます。

Amazon Linux WorkSpaces

Amazon Linux WorkSpaces カスタムイメージの更新とパッチを管理するための考慮事項、前提条件、および推奨パターンについては、ホワイトペーパー「Linux イメージ用の Amazon を準備するためのベストプラクティス WorkSpaces 」を参照してください。

Linux パッチ適用の前提条件と考慮事項

- Amazon Linux リポジトリは Amazon Simple Storage Service (Amazon S3) バケットでホストされ、パブリックのインターネットアクセス可能なエンドポイントまたはプライベートエンドポイントを介してアクセスできます。Amazon Linux にインターネットアクセス WorkSpaces がない場合は、更新プログラムにアクセス可能にするためのこのプロセスを参照してください。Amazon

Linux 1 または Amazon Linux 2 を実行している EC2 インスタンスで、yum を更新したり、インターネットにアクセスせずにパッケージをインストールしたりするにはどうすればよいですか？

- Linux のデフォルトのメンテナンスウィンドウを設定することはできません WorkSpaces。このウィンドウをカスタマイズする必要がある場合は、手動メンテナンスプロセスを使用できます。

Amazon Windows のパッチ適用

デフォルトでは、Windows WorkSpaces は、VPC からのインターネットアクセスを必要とする Windows Update から更新を受け取るように設定されています WorkSpaces 。Windows 用に独自の自動更新メカニズムを設定するには、Windows Server Update Services (WSUS) および Configuration Manager のドキュメントを参照してください。

Amazon Windows インプレースアップグレード

- Windows 10 からイメージを作成する場合は WorkSpace、以前のバージョンからアップグレードされた Windows 10 システムではイメージの作成がサポートされないことに注意してください (Windows の機能/バージョンのアップグレード)。ただし、Windows の累積更新プログラムまたはセキュリティ更新プログラムは、 WorkSpaces イメージの作成およびキャプチャプロセスでサポートされています。

- カスタム Windows 10 Bring Your Own License (BYOL) イメージは、BYOL インポートプロセスのソースとして VM でサポートされている最新の Windows バージョンから開始する必要があります。詳細については、BYOL インポートドキュメントを参照してください。

Windows インプレースアップグレードの前提条件

- Active Directory グループポリシーまたは SCCM を使用して Windows 10 のアップグレードを延期または一時停止した場合は、Windows 10 のオペレーティングシステムのアップグレードを有効にします WorkSpaces。
- WorkSpace が の場合 AutoStop WorkSpace、アップグレードウィンドウに合わせて AutoStop 時間を少なくとも 3 時間に変更します。
- インプレースアップグレードプロセスでは、デフォルトユーザー (C:\Users\Default) のコピーを作成してユーザープロファイルを再作成します。デフォルトのユーザープロファイルを使用してカスタマイズを作成しないでください。代わりに、グループポリシーオブジェクト (GPOsを使用して

ユーザープロファイルをカスタマイズすることをお勧めします。GPOs によるカスタマイズは簡単に変更またはロールバックでき、エラーが発生しにくくなります。

- インプレースアップグレードプロセスでは、1 つのユーザープロファイルだけをバックアップおよび再作成できます。ドライブ D に複数のユーザープロファイルがある場合は、必要なプロファイルを除くすべてのプロファイルを削除します。

Windows インプレースアップグレードに関する考慮事項

- インプレースアップグレードプロセスでは、2 つのレジストリスクリプト (enable-inplace-upgrade.ps1 と update-pvdrivers.ps1) を使用して に必要な変更を加え WorkSpaces 、Windows Update プロセスの実行を有効にします。これらの変更には、ドライブ D ではなくドライブ C に一時的なユーザープロファイルを作成することが含まれます。ユーザープロファイルがドライブ D にすでに存在する場合、元のユーザープロファイルのデータはドライブ D に残ります。
- インプレースアップグレードがデプロイされたら、ユーザープロファイルを D ドライブに復元して、 を再構築または移行できることを確認し WorkSpaces、ユーザーシェルフォルダのリダイレクトに関する潜在的な問題を回避する必要があります。これを行うには、BYOL アップグレードリファレンスページ「」で説明されているように、PostUpgradeRestoreProfileOnD レジストリキーを使用します。

Amazon WorkSpaces 言語パック

Windows 10 デスクトップエクスペリエンスを提供する Amazon WorkSpaces バンドルは、英語 (米国)、フランス語 (カナダ)、韓国語、日本語をサポートしています。ただし、スペイン語、イタリア語、ポルトガル語、その他の多くの言語オプションには、追加の言語パックを含めることができます。詳細については、「英語以外のクライアント言語で新しい Windows WorkSpace イメージを作成する方法」を参照してください。

Amazon WorkSpaces プロファイル管理

Amazon は、すべてのプロファイル書き込みを別の Amazon Elastic Block Store (Amazon EBS) ボリュームにリダイレクトすることで、ユーザープロファイルを基本オペレーティングシステム (OS) から WorkSpaces 分離します。Microsoft Windows では、ユーザープロファイルは D:\Users \username に保存されます。Amazon Linux では、ユーザープロファイルは /home に保存されます。EBS ボリュームは 12 時間ごとに自動的にスナップショットされます。スナップショットは AWS Managed S3 バケットに自動的に保存され、Amazon WorkSpace が再構築または復元された場合に使用されます。

ほとんどの組織では、自動スナップショットを 12 時間ごとに作成するのは、ユーザープロファイルのバックアップがない既存のデスクトップデプロイよりも優れています。ただし、デスクトップからへの移行、新しい OS/AWS リージョンへの移行 WorkSpaces、DR のサポートなど、ユーザープロファイルをより細かく制御する必要があります。プロファイル管理には、Amazon で利用できる別の方法があります WorkSpaces。

フォルダのリダイレクト

フォルダのリダイレクトは仮想デスクトップインフラストラクチャ (VDI) アーキテクチャでは一般的な設計上の考慮事項ですが、ベストプラクティスでも、Amazon WorkSpaces 設計では一般的な要件でもありません。これは、Amazon WorkSpaces が永続的な Desktop as a Service (DaaS) ソリューションであり、アプリケーションとユーザーデータはそのまま保持されるためです。

ディザスタリカバリ (DR) 環境のユーザープロファイルデータの即時リカバリポイント目標 (RPO) など、ユーザーシェルフォルダのフォルダリダイレクト (例: D:\Users\username\TAKtop が \\Server\RedirectionShare$\username\TAKtop) が必要になる特定のシナリオがあります。

ベストプラクティス

堅牢なフォルダリダイレクトについては、以下のベストプラクティスがリストされています。

- Amazon が WorkSpaces 起動されたのと同じ AWS リージョンと AZ で Windows ファイルサーバーをホストします。
- AD セキュリティグループのインバウンドルールに Windows File Server セキュリティグループまたはプライベート IP アドレスが含まれていることを確認します。含まれていない場合は、オンプレミスのファイアウォールで同じ TCP および UDP ポートベースのトラフィックが許可されていることを確認します。
- Windows File Server セキュリティグループのインバウンドルールに、すべての Amazon WorkSpaces セキュリティグループの TCP 445 (SMB) が含まれていることを確認します。
- Amazon WorkSpaces ユーザーが Windows ファイル共有へのアクセスを許可する AD セキュリティグループを作成します。
- DFS 名前空間 (DFS-N) と DFS レプリケーション (DFS-R) を使用して、Windows ファイル共有がアジャイルであり、特定の Windows File Server に関連付けられておらず、すべてのユーザーデータが自動的に Windows File Server 間でレプリケートされます。
- Windows Explorer でネットワーク共有を参照するときに、ホストしているユーザーデータの共有を表示しないようにするには、共有名の末尾に「$」を追加します。

- リダイレクトされたフォルダに関する Microsoft のガイダンスに従って、ファイル共有を作成します。オフラインファイルによるフォルダのリダイレクトのデプロイ。セキュリティ許可と GPO 設定に関するガイダンスに厳密に従ってください。
- Amazon WorkSpaces デプロイが自分のライセンス使用 (BYOL) の場合は、Microsoft のガイダンスに従ってオフラインファイルの無効化も指定する必要があります。個々のリダイレクトフォルダのオフラインファイルを無効にする。
- Windows File Server が Windows Server 2016 以降である場合は、ストレージの消費量を減らし、コストを最適化するために、データ重複排除 (一般に「重複排除」と呼ばれます) をインストールして実行します。「データ重複排除のインストールと有効化」と「データ重複排除の実行」を参照してください。
- 既存の組織バックアップソリューションを使用して、Windows File Server ファイル共有をバックアップします。

避けるべきこと

- SMB プロトコルは使用向けに設計されていないため、広域ネットワーク (WAN) 接続でのみアクセスできる Windows File Server は使用しないでください。
- ユーザーが誤ってユーザーシェルフォルダを削除する可能性を減らすために、ホームディレクトリに使用されるのと同じ Windows ファイル共有を使用しないでください。
- ファイルを簡単に復元できるようにボリュームシャドウコピーサービス (VSS) を有効にすることをお勧めしますが、これだけでは Windows File Server ファイル共有をバックアップする必要はありません。

その他の考慮事項

- Amazon FSx for Windows File Server は、Windows ファイル共有用のマネージドサービスを提供し、自動バックアップを含むフォルダリダイレクトの運用オーバーヘッドを簡素化します。
- 既存の組織バックアップソリューションがない場合は、AWS Storage Gateway SMB ファイル共有を使用してファイル共有をバックアップします。

プロファイル設定

グループポリシー

エンタープライズ Microsoft Windows デプロイの一般的なベストプラクティスは、グループポリシーオブジェクト (GPO) とグループポリシー設定 (GPP) の設定を使用してユーザー環境設定を定義することです。ショートカット、ドライブマッピング、レジストリキー、プリンターなどの設定は、グループポリシーマネジメントコンソールを使用して定義されます。GPOs を使用してユーザー環境を定義する利点には以下が含まれますが、これらに限定されません。

- 一元化された設定管理
- AD セキュリティグループのメンバーシップまたは OU 配置で定義されるユーザープロファイル
- 設定の削除に対する保護
- 初回のログオン時にプロファイルの作成とパーソナライゼーションを自動化する
- 将来の更新のしやすさ

> **Note**
>
> Microsoft のグループポリシーのパフォーマンスを最適化するためのベストプラクティスに従ってください。

インタラクティブログオングループのポリシーは、Amazon でサポートされていないため、使用しないでください WorkSpaces。 AWS サポートリクエストを通じて Amazon WorkSpaces Client に招待状が表示されます。さらに、Amazon に必要なため、グループポリシーを使用してリムーバブルデバイスをブロックしないでください WorkSpaces。

GPOsは Windows の管理に使用できます WorkSpaces。詳細については、「Windows の管理 WorkSpaces」を参照してください。

Amazon WorkSpaces ボリューム

各 Amazon WorkSpaces インスタンスには、オペレーティングシステムボリュームとユーザーボリュームの 2 つのボリュームが含まれています。

- Amazon Windows WorkSpaces — C:\ ドライブはオペレーティングシステム (OS) に使用され、D:\ ドライブはユーザーボリュームです。ユーザープロファイルは、ユーザーボリューム (AppData、ドキュメント、ピクチャー、ダウンロードなど) にあります。
- Amazon Linux WorkSpaces — Amazon Linux では WorkSpace、システムボリューム (/dev/xvda1) がルートフォルダとしてマウントされます。ユーザーボリュームはユーザーデータとアプリケーション用です。/dev/xvdf1 は /home としてマウントします。

オペレーティングシステムボリュームの場合、このドライブの開始サイズとして 80 GB または 175 GB を選択できます。ユーザーボリュームの場合、開始サイズとして 10 GB、50 GB、または 100 GB を選択できます。両方のボリュームのサイズは必要に応じて最大 2TB まで増やすことができますが、ユーザーボリュームを 100 GB を超えて増やすには、OS ボリュームが 175 GB である必要があります。ボリュームの変更は、ボリュームごとに 6 時間ごとに 1 回のみ実行できます。WorkSpaces ボリュームサイズの変更の詳細については、 管理ガイドの「変更 WorkSpace」セクションを参照してください。

WorkSpaces ボリュームのベストプラクティス

Amazon WorkSpaces デプロイを計画するときは、OS ボリューム上のイメージに追加される OS のインストール、インプレースアップグレード、および追加のコアアプリケーションの最小要件を考慮することをお勧めします。ユーザーボリュームの場合は、ディスク割り当てを小さくし、必要に応じてユーザーボリュームサイズを段階的に増やすことをお勧めします。ディスクボリュームのサイズを最小限に抑えると、 の実行コストを削減できます WorkSpace。

> **Note**
>
> ボリュームサイズを増やすことはできますが、減らすことはできません。

Amazon WorkSpaces ログ記録

Amazon WorkSpaces 環境には、問題のトラブルシューティングや全体的な WorkSpaces パフォーマンスのモニタリングのためにキャプチャできるログソースが多数あります。

Amazon WorkSpaces Client 3.x 各 Amazon WorkSpaces クライアントでは、クライアントログは次のディレクトリにあります。

- Windows — %LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
- macOS — ~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs

- Linux (Ubuntu 18.04 以降) — /opt/workspacesclient/workspacesclient

クライアント側からの WorkSpaces セッションでは、診断またはデバッグの詳細が必要になるインスタンスが多数あります。ワークスペースの実行可能ファイルに「-l3」を追加することで、高度なクライアントログを有効にすることもできます。例:

```
"C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"
workspaces.exe -l3
```

Amazon WorkSpaces サービス

Amazon WorkSpaces サービスは、Amazon CloudWatch メトリクス、 CloudWatch イベント、および と統合されています CloudTrail。この統合により、パフォーマンスデータと API コールを中央 AWS サービスにログインできます。

Amazon WorkSpaces 環境を管理する場合、環境全体のヘルスステータスを判断するために、特定の CloudWatch メトリクスを常にモニタリングすることが重要です。メトリクス

Amazon には他の CloudWatch メトリクスがありますが WorkSpaces（ CloudWatch 「メトリクス WorkSpaces を使用して をモニタリングする」を参照）、次の 3 つのメトリクスがインスタンスの WorkSpace可用性の維持に役立ちます。

- Unhealthy — 異常なステータスを返 WorkSpaces した の数。
- SessionLaunchTime — WorkSpaces セッションの開始にかかる時間。
- InSessionLatency — WorkSpaces クライアントと の間のラウンドトリップ時間 WorkSpace。

WorkSpaces ログ記録オプションの詳細については、「 を使用した Amazon WorkSpaces API コールのログ記録 CloudTrail」を参照してください。追加の CloudWatch イベントは、ユーザーがセッションに接続した日時 WorkSpaces 、および接続中に使用されたエンドポイントをキャプチャするのに役立ちます。これらの詳細はすべて、トラブルシューティングセッション中にユーザーが報告した問題の分離または特定に役立ちます。

> **Note**
>
> 一部の CloudWatch メトリクスは AWS Managed AD でのみ使用できます。

Amazon での Linux 用のコンテナと Windows サブシステム WorkSpaces

コンテナと Amazon WorkSpaces

エンドユーザーコンピューティングは、Amazon でコンテナワークロードを保守したいお客様によってアプローチされることがよくあります WorkSpaces。可能であれば、これは推奨されるソリューションまたは推奨されるソリューションではありません。コンテナの潜在的なコストと運用上の削減額を引き出すことを検討しているお客様は、Amazon Elastic Container Service (Amazon ECS) や Amazon Elastic Kubernetes Service (Amazon EKS) を評価することをお勧めします。

お客様が Amazon を使用してコンテナを有効にすることを義務付ける場合は WorkSpaces、Docker の使用を可能にする技術的なハウツーが公開されています。これを行うには、後続の他のサービスが必要であり、分離されたネイティブコンテナサービスに比べてコストと複雑さが増していることをお客様に通知する必要があります。

Linux 用 Windows サブシステム

Amazon の基盤となるオペレーティングシステムとして Windows Server 2019 がリリースされたことで WorkSpaces、お客様は Windows Subsystem for Linux (WSL)、特に WSL2 の実装を好みました。WSL2 は関数を実行するために仮想マシン (Hyper-V) を呼び出すため、 AWS ハイパーバイザーによって管理 WorkSpacesされる Amazon では実行できません。このため、WSL1 のみが使用可能になることを理解し、WSL1 と WSL2 の違いを理解する必要があります。

Amazon WorkSpaces 移行

Amazon WorkSpaces 移行機能を使用すると、ユーザーボリュームデータを新しいバンドルに取り込むことができます。この機能を使用して、次のことができます。

- を Windows 7 エクスペリエンス WorkSpaces から Windows 10 デスクトップエクスペリエンスに移行します。
- PCoIP WorkSpace から WorkSpaces ストリーミングプロトコル (WSP) に移行します WorkSpace。
- あるパブリックバンドルまたはカスタムバンドル WorkSpaces から別のバンドルに移行します。例えば、GPU 対応 (グラフおよび GraphicsPro) バンドルから GPU 対応以外のバンドルに移行したり、その逆に移行したりできます。

移行プロセス

WorkSpaces 移行では、ターゲット WorkSpaces バンドルを指定できます。移行プロセスでは、WorkSpaceターゲットバンドルイメージの新しいルートボリュームと、最新の元のユーザーボリュームスナップショットのユーザーボリュームを使用して が再作成されます。互換性を高めるため、移行中に新しいユーザープロファイルが生成されます。新しいプロファイルに移動できない古いユーザープロファイルのデータは、.notMigrated フォルダに保存されます。

移行中、ユーザーボリューム (ドライブ D) のデータは保持されますが、ルートボリューム (C:\ ドライブ) のすべてのデータは失われます。つまり、インストールされているアプリケーション、設定、およびレジストリの変更は、いずれも保持されません。古いユーザープロファイルフォルダの名前が .NotMigrated suffix に変更され、新しいユーザープロファイルが作成されます。

移行プロセスには、 あたり最大 1 時間かかります WorkSpace。さらに、移行ワークフローがプロセスを完了できない場合、サービスは移行前に を元の状態に自動的にロールバック WorkSpace し、データ損失リスクを最小限に抑えます。

元の に割り当てられたタグ WorkSpace は、移行中に引き継がれます。の実行モード WorkSpace は保持されます。移行された には、新しい WorkSpace ID、コンピュータ名、および IP アドレス WorkSpace があります。移行手順

WorkSpaces Amazon WorkSpaces コンソール、migrate-workspace コマンド、または Amazon WorkSpaces API AWS CLI を使用して移行できます。すべての移行リクエストがキューに入れられ、移行リクエストの数が多すぎると、サービスは自動的に移行リクエストの合計数を調整します。移行制限

- パブリックまたはカスタムの Windows 7 デスクトップエクスペリエンスバンドルに移行することはできません。
- BYOL Windows 7 バンドルに移行することはできません。
- BYOL は、他の BYOL バンドル WorkSpaces にのみ移行できます。
- パブリックバンドルまたはカスタムバンドルから WorkSpace 作成された を BYOL バンドルに移行することはできません。
- Linux の移行 WorkSpaces は現在サポートされていません。
- 複数の言語をサポートする AWS リージョンでは、言語バンドル WorkSpaces 間で移行できます。
- ソースバンドルとターゲットバンドルは異なっている必要があります（ただし、複数の言語をサポートするリージョンでは、言語が異なる限り、同じ Windows 10 バンドルに移行できます）。同じバンドル WorkSpace を使用して を更新する場合は、代わりに を再構築 WorkSpaceします。
- リージョン WorkSpaces 間で移行することはできません。
- WorkSpaces ADMIN_MAINMAINANCE モードの場合、 は移行できません。

コスト

移行が発生する月には、新しい と元の の両方に対して按分計算された金額が課金されます WorkSpaces。例えば、5 月 10 日に WorkSpace A を WorkSpace B に移行した場合、5 月 1 日から 5 月 10 日までは WorkSpace A に対して課金され、5 月 11 日から 5 月 30 日までは WorkSpace B に対して課金されます。

WorkSpaces 移行のベストプラクティス

を移行する前に WorkSpace、次の操作を行います。

- ドライブ C の重要なデータを別の場所にバックアップします。ドライブ C 上のすべてのデータは、移行中に消去されます。
- 移行 WorkSpace する が 12 時間以上経過していることを確認し、ユーザーボリュームのスナップショットが作成されていることを確認します。Amazon WorkSpaces コンソールの移行 WorkSpacesページで、最後のスナップショットの時刻を参照できます。最後のスナップショット以降に作成されたデータは、移行中に失われます。
- データの損失を避けるため、ユーザーが からログアウトし WorkSpaces、移行プロセスが完了するまでログインし直さないようにしてください。
- 移行 WorkSpaces する のステータスが AVAILABLE、STOPPED、または ERROR であることを確認します。

- 移行する に WorkSpaces十分な IP アドレスがあることを確認します。移行中、 に新しい IP アドレスが割り当てられます WorkSpaces。
- スクリプトを使用して を移行する場合は WorkSpaces、 WorkSpaces 一度に 25 以下のバッチで移行します。

Well-Architected フレームワーク

AWS Well-Architected は、クラウドアーキテクトがアプリケーションとワークロード向けに、安全で高性能、かつ回復力のある効率的なインフラストラクチャを構築するのに役立ちます。クラウドでワークロードを設計および実行するための主要な概念、設計原則、アーキテクチャのベストプラクティスについて説明します。これは、次の 5 つの主要な柱に基づいています。

- オペレーショナルエクセレンス
- セキュリティ
- 信頼性
- パフォーマンス効率
- コスト最適化

Amazon WorkSpaces 環境を設計するときは、これらの主要な柱を評価して成熟度デプロイレベルを決定し、Amazon で使用できる追加機能を見つけることが重要です WorkSpaces。AWS Well-Architect Framework の全体的なガイダンスがありますが、以下では、5 つの柱のそれぞれを考慮するために、 WorkSpaces デプロイの計画段階に含めることができるいくつかの重要な質問について説明します。

全般

- このプロジェクトのビジネスドライバーは何ですか？

オペレーショナルエクセレンス

- ユーザーと異なる管理者グループ間のアクセスコントロールを分離するにはどうすればよいですか？

セキュリティ

1. を WorkSpaces 運用するために考慮すべきセキュリティとコンプライアンスの要件は何ですか？
2. 外部 IP アドレスへのルーティングには制限がありますか？
3. 必要な WorkSpaces ポートは会社のファイアウォールを経由して許可されていますか？
4. このデプロイでは多要素認証が使用されますか、それとも使用されますか？

5. 現在、ユーザー ID と承認リクエストはいくつありますか？

信頼性

1. デスクトップのデータ保持ポリシーとは
2. エンドユーザーデータの目標復旧時点 (RPO) とは
3. エンドユーザーデータの目標復旧時間 (RTO) とは

コスト最適化

1. WorkSpaces バンドルのサイズは、ユーザーケースとアプリケーションに適したものですか？
2. ユーザーは 1 か月あたり WorkSpaces 82 時間以上消費しますか？

上記の質問は考慮すべき項目の完全なリストを構成するものではありませんが、 Well-Architected Amazon WorkSpaces のデプロイを支援する包括的なガイダンスを提供します。

セキュリティ

このセクションでは、Amazon WorkSpaces のサービスを使用する際に暗号化を使用してデータを保護する方法について説明します。転送時と保管時の暗号化、および へのネットワークアクセスを保護するためのセキュリティグループの使用について説明します WorkSpaces。このセクションでは、信頼できるデバイスと IP アクセスコントロールグループ WorkSpaces を使用して、 へのエンドデバイスアクセスを制御する方法についても説明します。

AWS Directory Service での認証 (MFA サポートを含む) に関する追加情報は、このセクションに記載されています。

送信中の暗号化

Amazon WorkSpaces は、暗号化を使用して、通信のさまざまな段階 (転送中) の機密性を保護し、保管中のデータ (暗号化された) も保護します WorkSpaces。Amazon が転送 WorkSpaces 中に使用する暗号化の各段階のプロセスについては、以下のセクションで説明します。

保管時の暗号化の詳細については、このドキュメントの「暗号化 WorkSpaces」セクションを参照してください。

登録と更新

デスクトップクライアントアプリケーションは、HTTPS を使用した更新と登録について Amazon と通信します。

認証ステージ

デスクトップクライアントは、認証ゲートウェイに認証情報を送信することで認証を開始します。デスクトップクライアントと認証ゲートウェイ間の通信には HTTPS が使用されます。この段階の最後に、認証が成功すると、認証ゲートウェイは同じ HTTPS 接続を介して OAuth 2.0 トークンをデスクトップクライアントに返します。

> **Note**
>
> デスクトップクライアントアプリケーションは、ポート 443 (HTTPS) トラフィック、更新、登録、認証用のプロキシサーバーの使用をサポートします。

クライアントから認証情報を受け取ると、認証ゲートウェイは認証リクエストを AWS Directory Service に送信します。認証ゲートウェイから AWS Directory Service への通信は HTTPS 経由で行われるため、ユーザー認証情報はプレーンテキストで送信されません。

認証 — Active Directory Connector (TAK)

AD Connector は Kerberos を使用してオンプレミス AD との認証済み通信を確立するため、LDAP にバインドして後続の LDAP クエリを実行できます。TAK でのクライアント側の LDAPS サポートは、Microsoft AD と AWS アプリケーション間のクエリを暗号化するためにも利用できます。クライアント側 LDAPS 機能を実装する前に、クライアント側 LDAPS の前提条件を確認してください。

AWS Directory Service は、TLS を使用した LDAP もサポートしています。ユーザーの認証情報は、プレーンテキストで送信されることはありません。セキュリティを強化するために、VPN 接続を使用して WorkSpaces VPC をオンプレミスネットワーク (AD が存在する場所) に接続できます。 AWS ハードウェア VPN 接続を使用する場合、お客様は AES-128 または AES-256 対称暗号化キー SAs 、整合性ハッシュ用の SHA-1 または SHA-256 対称暗号化キー、フェーズ 1 用の SHA-14-18、22、23、24、フェーズ 1、25、14-18、22、23、24 を使用して、転送中の暗号化を設定できます (PFS)。 AES-256

ブローカーステージ

OAuth 2.0 トークンを (認証ゲートウェイから、認証が成功した場合) 受信した後、デスクトップクライアントは HTTPS を使用して Amazon WorkSpaces サービス (Broker Connection Manager) にクエリを実行します。デスクトップクライアントは OAuth 2.0 トークンを送信することで自身を認証し、その結果、クライアントは WorkSpaces ストリーミングゲートウェイのエンドポイント情報を受け取ります。

ストリーミングステージ

デスクトップクライアントは、ストリーミングゲートウェイで PCoIP セッションを開くように (OAuth 2.0 トークンを使用) 要求します。このセッションは AES-256 で暗号化されており、通信制御 (4172/TCP) に PCoIP ポートを使用します。

OAuth2.0 トークンを使用して、ストリーミングゲートウェイは HTTPS 経由で Amazon WorkSpaces サービスにユーザー固有の WorkSpaces 情報をリクエストします。

ストリーミングゲートウェイは、クライアントから TGT (クライアントユーザーのパスワードを使用して暗号化されます) を受け取り、Kerberos TGT パススルーを使用して、ゲートウェイは、ユーザーが取得した Kerberos TGT を使用して WorkSpaceで Windows ログインを開始します。

WorkSpace 次に、 は、標準の Kerberos 認証を使用して、設定された AWS Directory Service への認証リクエストを開始します。

WorkSpace が正常にログインすると、PCoIP ストリーミングが開始されます。接続は、ポート UDP 4172 のリターントラフィックを使用して、ポート TCP 4172 でクライアントによって開始されます。さらに、管理インターフェイスを介したストリーミングゲートウェイと WorkSpaces デスクトップ間の初期接続は UDP 55002 経由です。(Amazon の IP アドレスとポートの要件 WorkSpacesに関するドキュメントを参照してください。 最初のアウトバウンド UDP ポートは 55002 です) 。ポート 4172 (TCP および UDP) を使用するストリーミング接続は、AES 128 および 256 ビット暗号を使用して暗号化されますが、デフォルトは 128 ビットです。お客様は、Windows 用の PCoIP 固有の AD グループポリシー設定を使用するか、Amazon Linux 用の pcoip-agent.conf ファイルを使用して WorkSpaces、これを 256 ビットにアクティブに変更できます WorkSpaces。Amazon のグループポリシー管理の詳細については WorkSpaces、「」のドキュメントを参照してください。

ネットワークインターフェイス

各 Amazon WorkSpace には、プライマリネットワークインターフェイス と管理ネットワークインターフェイス と呼ばれる 2 つのネットワークインターフェイスがあります。

プライマリネットワークインターフェイスは、 AWS Directory Service、インターネット、カスタマー企業ネットワークへのアクセスなど、カスタマー VPC 内のリソースへの接続を提供します。このプライマリネットワークインターフェイスにセキュリティグループをアタッチできます。概念的には、セキュリティグループは、deployment: WorkSpaces security group と ENI security groups の範囲に基づいて、この ENI にアタッチされます。

管理ネットワークインターフェイス

管理ネットワークインターフェイスは、セキュリティグループでは制御できません。ただし、 でホストベースのファイアウォールを使用して、ポート WorkSpaces をブロックしたり、アクセスを制御できます。管理ネットワークインターフェイスに制限を適用することはお勧めしません。お客様がホストベースのファイアウォールルールを追加してこのインターフェイスを管理する場合は、Amazon WorkSpaces サービスが のヘルスとアクセシビリティを管理できるように、いくつかのポートを開く必要があります WorkSpace。詳細については、「Amazon Workspaces 管理ガイド」の「ネットワークインターフェイス」を参照してください。

WorkSpaces セキュリティグループ

デフォルトのセキュリティグループは AWS Directory Service ごとに作成され、その特定のディレクトリ WorkSpaces に属するすべての に自動的にアタッチされます。

Amazon は WorkSpaces、他の多くの AWS サービスと同様に、セキュリティグループを利用します。Amazon WorkSpaces は、ディレクトリを WorkSpaces サービスに登録するときに 2 つの AWS セキュリティグループを作成します。ディレクトリコントローラー directoryId _controllers 用の 1 つと、 directory directoryId _workspacesMembers WorkSpaces 内の 用の 1 つです。 directoryId workspacesMembers これらのセキュリティグループを削除しないでください。削除すると、 に障害 WorkSpaces が発生します。デフォルトでは、 WorkSpaces メンバーセキュリティグループの出力は 0.0.0.0/0 に開かれています。デフォルトの WorkSpacesセキュリティグループをディレクトリに追加できます。新しいセキュリティグループを WorkSpaces ディレクトリに関連付けると、起動 WorkSpaces した新しい または再構築 WorkSpaces した既存の に新しいセキュリティグループが追加されます。この新しいデフォルトのセキュリティグループを再構築 WorkSpaces せずに既存のに追加することもできます。複数のセキュリティグループを WorkSpaces ディレクトリに関連付ける場合は、 WorkSpaces各セキュリティグループのルールを 1 つのルールセットに集約します。セキュリティグループルールをできるだけ凝縮することをお勧めします。セキュリティグループの詳細については、「Amazon VPC ユーザーガイド」の「VPC のセキュリティグループ」を参照してください。

WorkSpaces ディレクトリまたは既存の にセキュリティグループを追加する方法の詳細については WorkSpace、WorkSpaces 「管理者ガイド」を参照してください。

一部のお客様は、 WorkSpaces トラフィックが出力できるポートと送信先を制限したいと考えています。からの出力トラフィックを制限するには WorkSpaces、サービス通信に必要な特定のポートを残す必要があります。そうしないと、ユーザーは にログインできません WorkSpaces。

WorkSpaces は、 WorkSpace ログイン中にドメインコントローラーとの通信のために、カスタマー VPC の Elastic Network Interface (ENI) を利用します。ユーザーが に WorkSpaces 正常にログインできるようにするには、ドメインコントローラーまたは _workspacesMembers セキュリティグループにドメインコントローラーを含む CIDR 範囲へのアクセスを次のポートに許可する必要があります。

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 認証
- TCP/UDP 389 – LDAP
- TCP/UDP 445 – SMB

- TCP 3268-3269 – グローバルカタログ
- TCP/UDP 464 - Kerberos パスワードの変更
- TCP 139 - Netlogon
- UDP 137-138 - Netlogon
- UDP 123 – NTP
- RPC の TCP/UDP 49152-65535 一時ポート

他のアプリケーション、インターネット、またはその他の場所にアクセス WorkSpaces する必要がある場合は、_workspacesMembers セキュリティグループ内の CIDR 表記でそれらのポートと宛先を許可する必要があります。これらのポートと送信先を追加しない場合、 WorkSpaces は上記のポート以外には到達しません。最後の考慮事項の 1 つは、デフォルトでは、新しいセキュリティグループにはインバウンドルールがありません。したがって、インバウンドルールをセキュリティグループに追加するまで、別のホストからインスタンスに送信されるインバウンドトラフィックは許可されません。上記の手順は、 からの WorkSpaces出力を制限する場合、またはそれらにアクセスする必要があるリソースまたは CIDR 範囲のみに進入ルールを口ックする場合にのみ必要です。

> **Note**
>
> 新しく関連付けられたセキュリティグループは、変更後に WorkSpaces 作成または再構築された場合にのみアタッチされます。

ENI セキュリティグループ

プライマリネットワークインターフェイスは通常の ENI であるため、さまざまな AWS 管理ツールを使用して管理できます。詳細については、「Elastic Network Interface」を参照してください。WorkSpace IP アドレス (Amazon WorkSpaces コンソールの WorkSpaces ページ内) に移動し、その IP アドレスをフィルターとして使用して、対応する ENI (Amazon EC2 コンソールのネットワークインターフェイスセクション内) を見つけます。

ENI が見つかったら、セキュリティグループによって直接管理できます。セキュリティグループをプライマリネットワークインターフェイスに手動で割り当てる場合は、Amazon のポート要件を考慮してください WorkSpaces。詳細については、「Amazon Workspaces 管理ガイド」の「ネットワークインターフェイス」を参照してください。

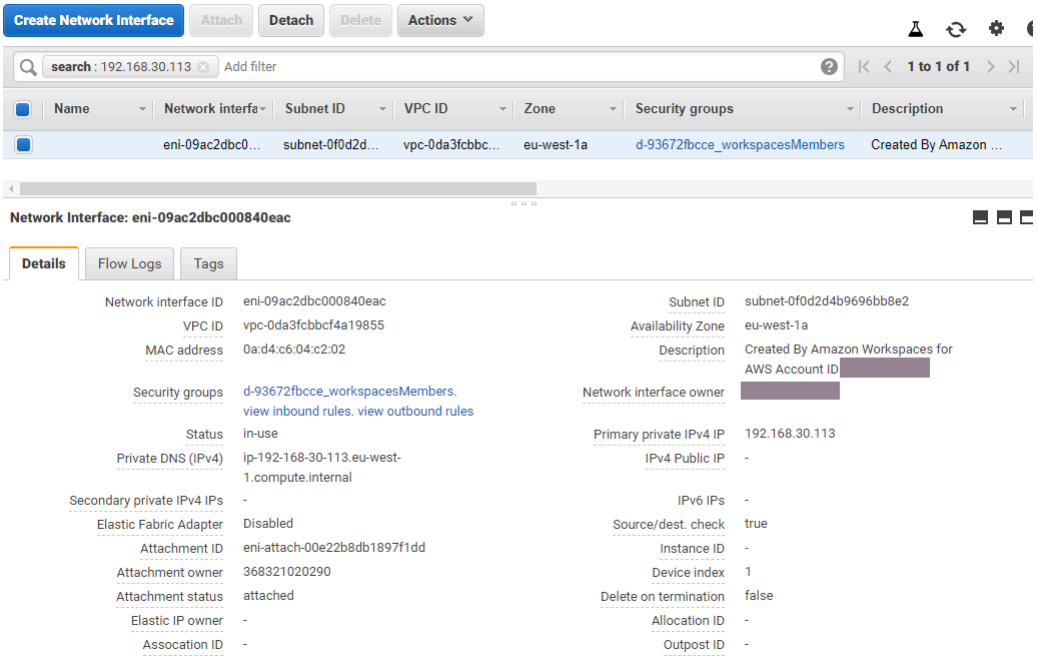

図 21: MFA が有効になっている WorkSpaces クライアント

ネットワークアクセスコントロールリスト (ACL)

ネットワーク ACLs は、さらに別のファイアウォールの管理が複雑になるため、非常に複雑なデプロイでは一般的に使用され、ベストプラクティスとしては通常使用されません。ネットワーク ACLs が VPC 内のサブネットにアタッチされると、OSI モデルのレイヤー 3 (ネットワーク) でその機能に焦点を当てます。Amazon WorkSpaces は Directory Services で設計されているため、2 つのサブネットを定義する必要があります。ネットワーク ACLs は Directory Services とは別に管理され、ネットワーク ACL は が割り当て WorkSpacesたサブネットの 1 つだけに割り当てられる可能性があります。

ステートレスファイアウォールが必要な場合、ネットワーク ACLs はセキュリティのベストプラクティスです。ベストプラクティスとして、デフォルト設定を超えてネットワーク ACLs に加えられた変更は、サブネットごとに検証されていることを確認してください。ネットワーク ACLs が意図したとおりに動作しない場合は、VPC フローログを使用してトラフィックを分析することを検討してください。

AWS Network Firewall

AWS Network Firewall には、ネイティブセキュリティグループとネットワーク ACLs が提供する機能以外にも、コストがかかります。HTTPS ベースのウェブサイトのサーバー名検査 (SNI)、侵入検

知と防止、ドメイン名の許可リストと拒否リストなど、ネットワーク接続に関するセキュリティを強化する権限をお客様に求めると、お客様は で代替ファイアウォールを見つけることが許可されていました AWS Marketplace。これらのファイアウォールのデプロイは複雑であるため、標準の EUC 管理者が慣れている範囲を超える課題が発生していました。 AWS Network Firewall は、レイヤー 3 から 7 の保護を有効にしながら、ネイティブな AWS エクスペリエンスを提供します。NAT ゲートウェイと組み合わせて AWS Network Firewall を使用することは、組織がすべての EUC ネットワーク保護をカバーするために、他の手段 (クラウドまたはファイアウォールを除外した別のチームに転送できるサードパーティーのファイアウォールの既存のオンプレミスライセンス) を所有していない場合のベストプラクティスです。NAT ゲートウェイは AWS Network Firewall でも無料です。

AWS Network Firewall のデプロイは、既存の EUC 設計を中心に設計されています。単一の VPC 設計では、ファイアウォールエンドポイント用のサブネットと個別のインターネット出力ルーティングに関する考慮事項を備えた簡素化されたアーキテクチャを実現できますが、マルチ VPC 設計では、ファイアウォールと Transit Gateways エンドポイントを備えた統合インスペクション VPC の利点を享受できます。

設計シナリオ

シナリオ 1: 基本的なインスタンスのロックダウン

セキュリティ WorkSpaces グループはデフォルトで拒否され、ステートフルであるため、デフォルトのセキュリティグループはインバウンドトラフィックを許可しません。つまり、 WorkSpaces インスタンス自体をさらに保護するために設定する必要がある追加の設定はありません。すべてのトラフィックを許可するアウトバウンドルールと、それがユースケースに適合するかどうかを検討します。例えば、ポート 443 へのすべてのアウトバウンドトラフィックを任意のアドレスに拒否するのが最善です。また、LDAP の場合は 389、LDAPS の場合は 636、SMB の場合は 445 など、ポートのユースケースに適合する特定の IP 範囲を拒否することをお勧めします。ただし、環境の複雑さには複数のルールが必要になる場合があるため、ネットワーク ACLs またはファイアウォールアプライアンスを介してより適切に対応できます。

シナリオ 2: インバウンド例外

一定の要件ではありませんが、ネットワークトラフィックが へのインバウンドで開始されることがあります WorkSpaces。例えば、 WorkSpaces クライアントが接続できないときにインスタンスをトリアージするには、代替のリモート接続が必要です。このような場合は、 WorkSpaceのカスタマー ENI のセキュリティグループへのインバウンド TCP 3389 を一時的に有効にするのが最善です。

もう 1 つのシナリオは、一元化されたインスタンスによって開始されるインベントリまたは自動化関数のコマンドを実行する組織スクリプトです。インバウンドの特定の集中型インスタンスからそのポート上のトラフィックを保護することは永続的に設定できますが、 AWS アカウントの複数のデプロイに適用できるため、ディレクトリ設定にアタッチされた追加のセキュリティグループでこれを行うのがベストプラクティスです。

最後に、ステートフルベースではないネットワークトラフィックがあり、受信例外で工フェメラルポートを指定する必要があります。クエリとスクリプトが失敗する場合は、接続障害の根本原因を判断しながら、少なくとも一時的に一時ポートを許可するのがベストプラクティスです。

シナリオ 3: 単一 VPC 検査

のデプロイを簡素化 WorkSpaces する (スケーリングプランのない単一の VPC など) には、検査用に個別の VPC を必要としないため、他の VPCs への接続は VPC ピアリングを使用して簡素化できます。ただし、ファイアウォールエンドポイントの個別のサブネットは、それらのエンドポイントに設定されたルーティングと、Internet Gateway (IGW) のエグレスルーティングを使用して作成する必要があります。そうしないと、設定する必要はありません。すべてのサブネットが VPC CIDR ブロック全体を利用する場合、既存のデプロイには使用可能な IP スペースがない可能性があります。このような場合、デプロイが初期設計を超えてすでにスケールされているため、シナリオ 4 の方が適している可能性があります。

シナリオ 4: 一元化された検査

多くの場合、 AWS リージョンの複数の EUC デプロイで優先され、 AWS Network Firewall のステートフルルールとステートレスルールの管理を簡素化します。この設計では Transit Gateway アタッチメントと、それらのアタッチメントを介してのみ設定できる検査ルーティングを使用する必要があるため、既存の VPC ピアは Transit Gateway に置き換えられます。この設定にもより高度な制御が行われ、デフォルトの WorkSpaces エクスペリエンスを超えるセキュリティが可能になります。

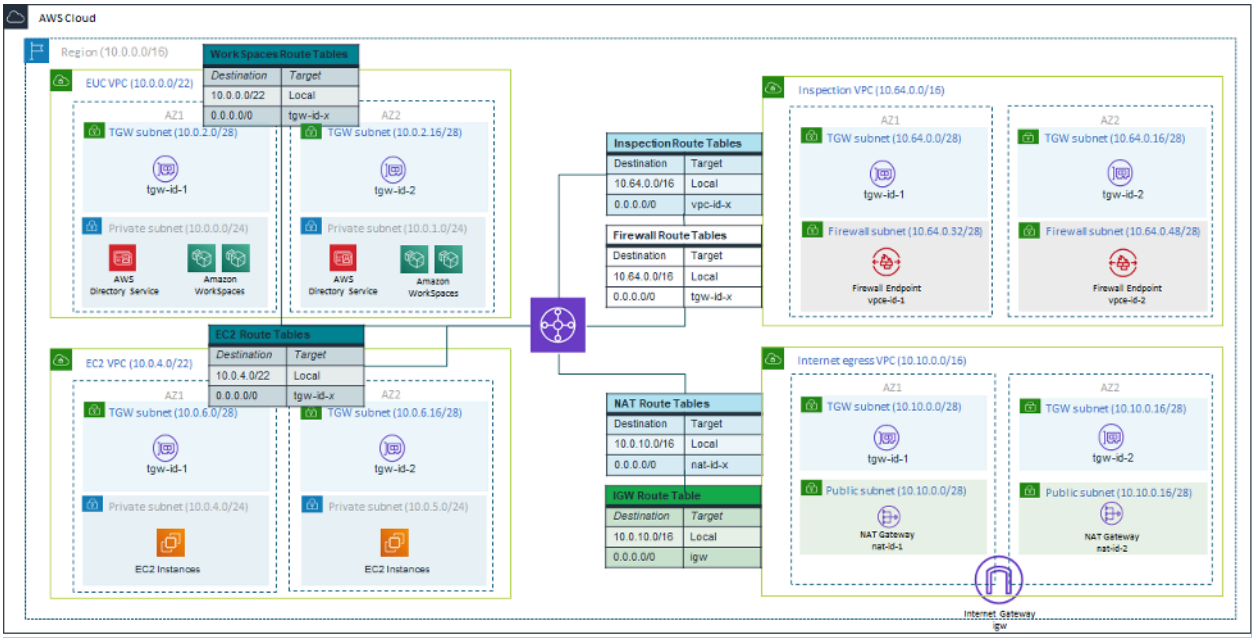

図 22: Transit Gateway アタッチメントを使用したサンプルアーキテクチャ

暗号化済み WorkSpaces

各 Amazon WorkSpace は、ルートボリューム (Windows 用ドライブ、Amazon Linux 用ルート WorkSpaces) WorkSpacesとユーザーボリューム (Windows 用ドライブ WorkSpaces、Amazon Linux 用ホーム) でプロビジョニングされます WorkSpaces。暗号化 WorkSpaces された機能により、一方または両方のボリュームを暗号化できます。

暗号化されるもの

保管時に保存されるデータ、ボリュームへのディスク入出力 (I/O)、および暗号化されたボリュームから作成されたスナップショットはすべて暗号化されます。

暗号化はいつ行われますか？

の暗号化は、. WorkSpaces volumes を起動時にのみ暗号化できる (作成) ときに指定 WorkSpace する必要があります WorkSpace。起動後にボリュームの暗号化ステータスを変更することはできません。次の図は、新しい の起動中に暗号化を選択するための Amazon WorkSpaces コンソールページを示しています WorkSpace。

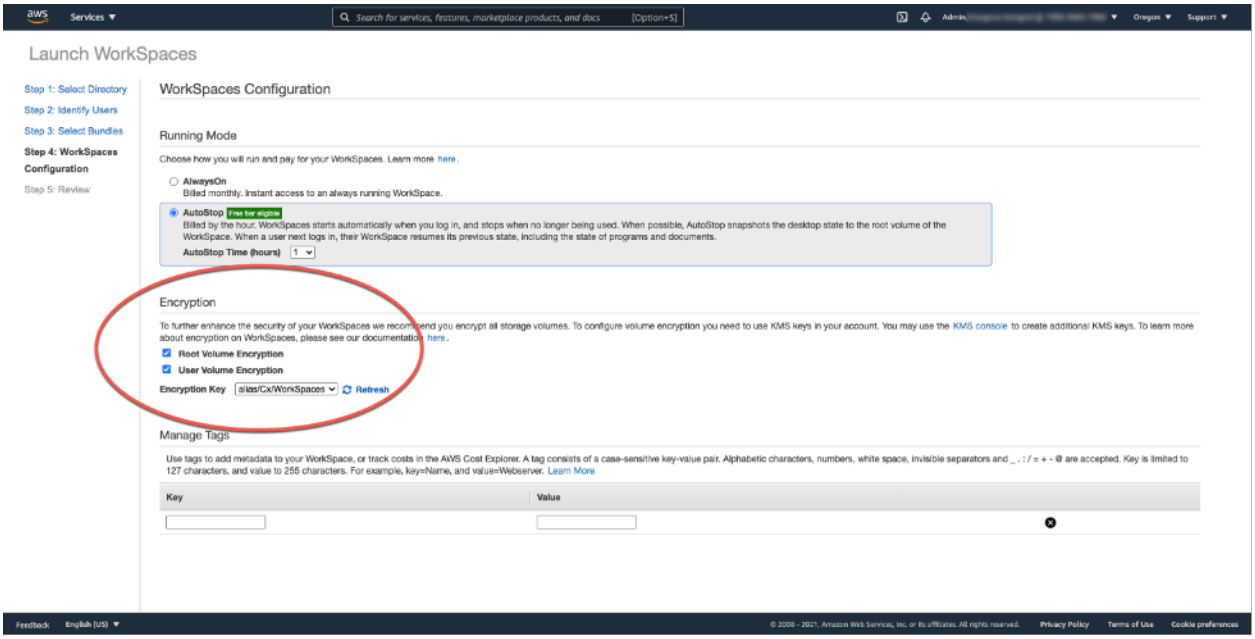

図 23: WorkSpace ルートボリュームの暗号化

新しい はどのように WorkSpace 暗号化されますか？

お客様は、Amazon WorkSpaces コンソールまたは から AWS CLI、またはお客様が新しい を起動するときに Amazon WorkSpaces API を使用して、暗号化 WorkSpaces オプションを選択できます WorkSpace。

ボリュームを暗号化するために、Amazon は AWS Key Management Service () の CMK WorkSpaces を使用しますAWS KMS。デフォルトの AWS KMS CMK は、 WorkSpace がリージョンで初めて起動されたときに作成されます。(CMKsにはリージョンスコープがあります)。

お客様は、暗号化された で使用するカスタマー管理の CMK を作成することもできます WorkSpaces。CMK は、Amazon WorkSpaces サービスが各 WorkSpace ボリュームの暗号化に使用するデータキーを暗号化するために使用されます。(厳密な意味では、ボリュームを暗号化するのは Amazon EBS です)。現在の CMK の制限については、AWS KMS 「リソースクォータ」を参照してください。

> **Note**
>
> 暗号化された からのカスタムイメージの作成 WorkSpace はサポートされていません。また、 WorkSpacesルートボリュームの暗号化を有効にして起動すると、プロビジョニングに最大 1 時間かかる場合があります。

WorkSpaces 暗号化プロセスの詳細については、「Amazon が WorkSpaces を使用する AWS KMS方法」を参照してください。暗号化された のリクエストが正しく処理されていることを確認するために、CMK WorkSpace の使用をモニタリングする方法を検討してください。 AWS KMS キーとデータキーの詳細については、AWS KMS 「」ページを参照してください。

アクセスコントロールオプションと信頼できるデバイス

Amazon WorkSpaces では、どのクライアントデバイスが にアクセスできるかを管理するためのオプションをお客様に提供しています WorkSpaces。お客様は、信頼されたデバイス WorkSpaces へのアクセスのみを制限できます。デジタル証明書を使用して、macOS および Microsoft Windows PCsから へのアクセスを許可 WorkSpaces できます。また、iOS、Android、Chrome OS、Linux、ゼロクライアント、および WorkSpaces Web Access クライアントへのアクセスを許可またはブロックすることもできます。これらの機能により、セキュリティ体制をさらに改善できます。

アクセスコントロールオプションは、ユーザーが Windows、MacOS、iOS、Android、ChromeOS、およびゼロクライアント上のクライアント WorkSpaces から にアクセスするための新しいデプロイで有効になります。Web Access または Linux WorkSpaces クライアントを使用したアクセスは、新しい WorkSpaces デプロイではデフォルトで有効になっていないため、有効にする必要があります。

信頼されたデバイス (マネージドデバイスとも呼ばれます) からの企業データアクセスに制限がある場合は、有効な証明書を持つ信頼されたデバイスへのアクセスを制限 WorkSpaces できます。この機能を有効にすると、Amazon は証明書ベースの認証 WorkSpaces を使用して、デバイスが信頼されているかどうかを判断します。 WorkSpaces クライアントアプリケーションは、デバイスが信頼されていることを確認できない場合、デバイスへのログインまたは再接続をブロックします。

信頼できるデバイスのサポートは、次のクライアントで利用できます。

- Android WorkSpaces および Android 互換の Chrome OS デバイスで実行される Google Play の Amazon Android クライアントアプリ https://www.chromium.org/chromium-os/chrome-os-systems-supporting-android-apps
- WorkSpaces macOS デバイスで実行されている Amazon macOS Client アプリ
- WorkSpaces Windows デバイスで実行されている Amazon Windows クライアントアプリ

にアクセスできるデバイスの制御の詳細については WorkSpaces、「信頼できるデバイス WorkSpaces へのアクセスの制限」を参照してください。

> **Note**
>
> 信頼されたデバイスの証明書は、Amazon WorkSpaces Windows、macOS、および Android クライアントにのみ適用されます。この機能は、Teradici PCoIP ソフトウェアおよびモバイルクライアント、Teradici PCoIP ゼロクライアント、RDP クライアント、リモートデスクトップアプリケーションなど、Amazon WorkSpaces Web Access クライアント、またはサードパーティークライアントには適用されません。

IP アクセスコントロールグループ

IP アドレスベースのコントロールグループを使用すると、お客様は信頼できる IP アドレスのグループを定義および管理し、信頼できるネットワークに接続している WorkSpaces 場合にのみユーザーが にアクセスできるようになります。この機能は、お客様がセキュリティ体制をより詳細に制御するのに役立ちます。

IP アクセスコントロールグループは、 WorkSpaces ディレクトリレベルで追加できます。IP アクセスコントロールグループの使用を開始するには、2 つの方法があります。

- IP アクセスコントロールページ — WorkSpaces マネジメントコンソールから、IP アクセスコントロールページに IP アクセスコントロールグループを作成できます。ルールは、アクセス可能な IP アドレスまたは IP 範囲を入力することで、これらのグループに追加 WorkSpaces できます。これらのグループは、更新の詳細ページでディレクトリに追加できます。
- Workspace APIs — WorkSpaces APIs を使用して、グループの作成、削除、表示、アクセスルールの作成や削除、ディレクトリからのグループの追加や削除を行うことができます。

Amazon WorkSpaces 暗号化プロセスで IP アクセスコントロールグループを使用する方法の詳細については、「 の IP アクセスコントロールグループ WorkSpaces」を参照してください。

Amazon を使用したモニタリングまたはログ記録 CloudWatch

ネットワーク、サーバー、ログのモニタリングは、インフラストラクチャに不可欠な部分です。Amazon をデプロイするお客様は、デプロイ、特に個々の の全体的なヘルスと接続ステータスをモニタリング WorkSpaces する必要があります WorkSpaces。

の Amazon CloudWatch メトリクス WorkSpaces

CloudWatch の メトリクス WorkSpaces は、個々の の全体的なヘルスと接続ステータスに関する追加のインサイトを管理者に提供するように設計されています WorkSpaces。メトリクスは、 ごと WorkSpace、または特定のディレクトリ内の組織 WorkSpaces 内のすべての に対して集計されます。

これらのメトリクスは、すべての CloudWatch メトリクスと同様に、 AWS Management Console (次の図を参照) で表示でき、 CloudWatch APIs経由でアクセスし、 CloudWatch アラームやサードパーティツールでモニタリングできます。

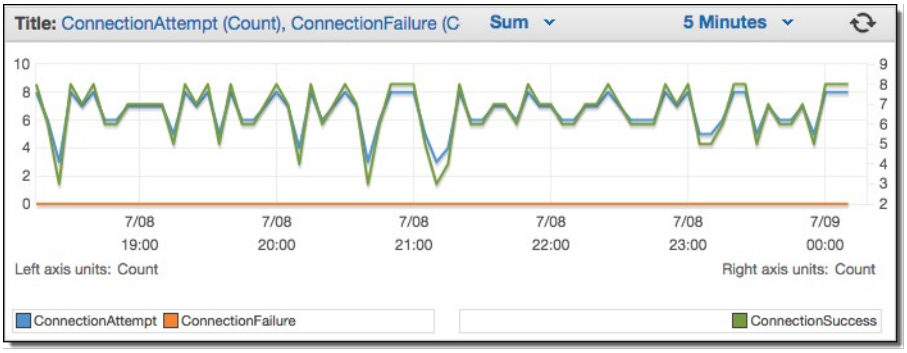

図 24: CloudWatch metrics: ConnectionAttempt / ConnectionFailure

デフォルトでは、以下のメトリクスが有効になっており、追加料金なしで利用できます。

- 利用可能 — WorkSpacesステータスチェックに応答する は、このメトリクスでカウントされます。
- 異常 — 同じステータスチェックに応答しない は、このメトリクスにカウントされます。 WorkSpaces
- ConnectionAttempt — に対して行われた接続試行回数 WorkSpace。
- ConnectionSuccess — 成功した接続試行回数。
- ConnectionFailure — 失敗した接続試行の数。
- SessionLaunchTime — WorkSpaces クライアントによって測定される、セッションの開始にかかる時間。
- InSessionLatency — WorkSpaces クライアントによって測定および報告された WorkSpaces、クライアントと の間のラウンドトリップ時間。
- SessionDisconnect — ユーザーによって開始され、自動的に閉じられたセッションの数。

さらに、次の図に示すように、アラームを作成できます。

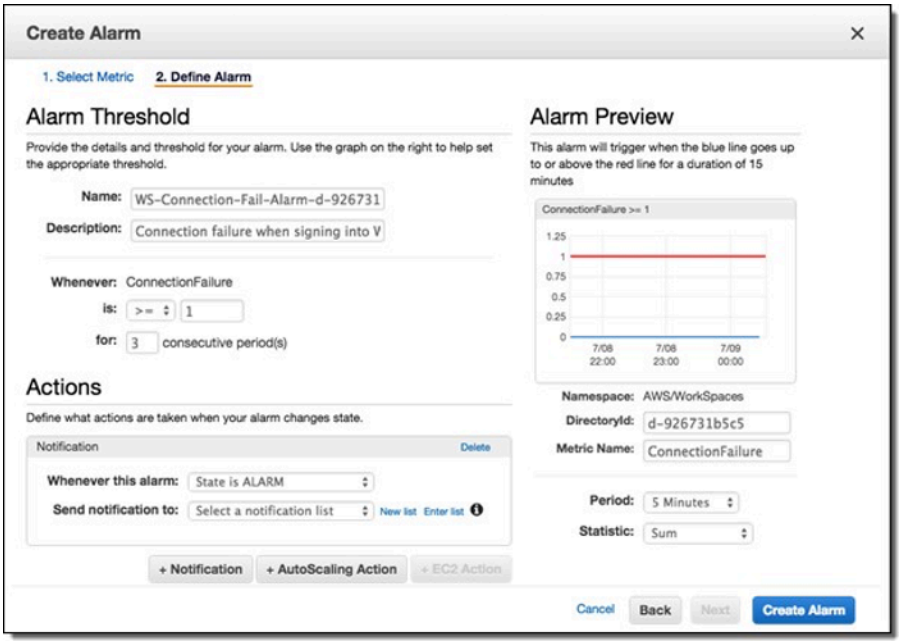

図 25: WorkSpaces 接続エラーの CloudWatch アラームを作成する

の Amazon CloudWatch イベント WorkSpaces

Amazon CloudWatch Events からのイベントを使用して、 への正常なログインを表示、検索、ダウンロード、アーカイブ、分析し、応答できます WorkSpaces。このサービスは、 へのユーザーのログインについて、クライアント WAN IP アドレス、オペレーティングシステム、 WorkSpaces ID、およびディレクトリ ID 情報をモニタリングできます WorkSpaces。例えば、次の目的でイベントを使用できます。

- WorkSpaces ログインイベントを将来の参照用にログとして保存またはアーカイブし、ログを分析してパターンを探し、それらのパターンに基づいてアクションを実行します。
- WAN IP アドレスを使用してユーザーのログイン元を特定し、ポリシーを使用して、WorkSpaces アクセスの CloudWatch イベントタイプで見つかった WorkSpaces アクセス基準を満たす からのファイルまたはデータにのみアクセスすることをユーザーに許可します。
- ポリシー制御を使用して、権限のない IP アドレスからのファイルやアプリケーションへのアクセスをブロックします。

CloudWatch イベントの使用方法の詳細については、「Amazon CloudWatch Events ユーザーガイド」を参照してください。の CloudWatch イベントの詳細については WorkSpaces、「Cloudwatch Events WorkSpaces を使用して をモニタリングする」を参照してください。

YubiKey Amazon の サポート WorkSpaces

追加のセキュリティレイヤーを追加するために、お客様は多要素認証を使用してツールやサイトを保護することを選択することがあります。一部のお客様は、Yubico でこれを行うことを選択しています YubiKey。Amazon は、 によるワンタイムパスコード (OTP) 認証プロトコルと FIDO U2F 認証プロトコルの両方 WorkSpaces をサポートしています YubiKeys。

Amazon WorkSpaces は現在 OTP モードをサポートしており、OTP YubiKey で を利用するために管理者またはエンドユーザーから追加の手順は必要ありません。ユーザーは をコンピュータ YubiKey にアタッチし、キーボードが WorkSpace （ 特に OTP の入力が必要なフィールド) 内でフォーカスしていることを確認し、 のゴールデンコンタクトをタッチできますYubiKey。 YubiKey は、選択したフィールドに OTP を自動的に入力します。

YubiKey と で FIDO U2F モードを使用するには WorkSpaces、追加の手順が必要です。で U2F リダイレクトを利用するには、サポートされている YubiKey モデルのいずれかがユーザーに発行されていることを確認してください WorkSpaces。

- YubiKey 4
- YubiKey 5 NFC
- YubiKey 5 Nano
- YubiKey 5C
- YubiKey 5C Nano
- YubiKey 5 NFC

YubiKey U2F の USB リダイレクトを有効にするには

デフォルトでは、USB リダイレクトは PCoIP WorkSpaces に対して無効になっています。 で U2F モードを利用するには YubiKeys、有効にする必要があります。

1. インストールしたPCoIP (32 ビット) 用の WorkSpaces グループポリシー管理用テンプレート、または PCoIP (64 ビット) 用の WorkSpaces グループポリシー管理用テンプレートが最新であることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、PCoIP セッション変数 に移動します。

3. ユーザーによる設定の上書きを許可する場合には、[Overridable Administrator Defaults] (上書き可能な管理者のデフォルト) を選択します。それ以外の場合は、[Not Overridable Administrator Defaults] (上書き不可の管理者のデフォルト) を選択します。
4. [Enable/disable USB in the PCOIP session] (PCoIP セッションでの USB を有効/無効にする) 設定を開きます。
5. [Enabled] (有効)、[OK] の順に選択します。
6. [Configure PCoIP USB allowed and unallowed device rules] (PCoIP USB の許可および許可されないデバイスのルール設定) を開きます。
7. [有効] を選択し、[USB 認証テーブルを入力 (最大 10 個のルール)] で、USB デバイスの許可リストルールを設定します。
   a. 承認ルール - 110500407。この値は、ベンダー ID (VID) と製品 ID (PID) の組み合わせです。VID/PID の組み合わせの形式は です。ここで1xxxxyyyy、 xxxxは 16 進形式の VID、yyyyは 16 進形式の PID です。この例では、1050 が VID で、0407 が PID です。USB 値の詳細については、 YubiKey YubiKey「USB ID 値」を参照してください。
8. [Enter the USB authorization table (maximum ten rules)] (USB 認証テーブルを入力 (最大 10 個のルール)) で、USB デバイスのブロックリストルールを設定します。
   a. [Unauthorization Rule] (非承認ルール) に、空の文字列を設定します。これは、承認リスト内の USB デバイスだけが許可されることを意味します。

> **Note**
>
> USB 承認ルールと USB 非承認ルールをそれぞれ最大 10 個定義することができます。複数のルールを区切るには、縦棒 (|) 文字を使用します。承認/承認解除ルールの詳細については、「Windows 用 Teradici PCoIP 標準エージェント」を参照してください。

9. [OK] をクリックします。
10. グループポリシー設定の変更は、 の次回のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションの再開後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。
    a. を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し WorkSpace、アクション 、再起動 WorkSpaces を選択します) 。
    b. 管理コマンドプロンプトで、gpupdate/force と入力します。
11. 設定が有効になると、USB デバイスルール設定で制限が設定され WorkSpaces ていない限り、サポートされているすべての USB デバイスを にリダイレクトできます。

YubiKey U2F の USB リダイレクトを有効にする YubiKey と、FTAK U2F モードで を利用できます。

コスト最適化

セルフサービス WorkSpace 管理機能

Amazon では WorkSpaces、セルフサービス WorkSpace 管理機能を有効にすることで、ユーザーは自分のエクスペリエンスをより詳細に制御できます。ユーザーにセルフサービス機能を許可すると、Amazon の IT サポートスタッフのワークロードを減らすことができます WorkSpaces。セルフサービス機能を有効にすると、ユーザーは Windows、macOS 、または Amazon 用の Linux クライアントから直接次のタスクを 1 つ以上実行できます WorkSpaces。

- 認証情報はクライアントにキャッシュされます。これにより、ユーザーは認証情報を再入力 WorkSpace せずに に再接続できます。
- を再起動します WorkSpace。
- のルートボリュームとユーザーボリュームのサイズを増やします WorkSpace。
- のコンピューティングタイプ (バンドル) を変更します WorkSpace。
- の実行モードを切り替えます WorkSpace。
- を再構築します WorkSpace。

の再起動および再構築オプションをユーザーに許可しても、継続的なコストへの影響はありません WorkSpaces。再構築プロセスが実行されるため、 の再構築 WorkSpace によって が WorkSpace最大 1 時間利用できなくなることに注意してください。

ボリュームのサイズを増やし、コンピューティングタイプを変更し、実行モードを切り替えるオプションでは、 の追加コストが発生する可能性があります WorkSpaces。ベストプラクティスは、セルフサービスを有効にしてサポートチームのワークロードを減らすことです。追加コスト項目のセルフサービスは、追加料金の承認を確実に得るワークフロープロセス内で許可する必要があります。これは、 専用のセルフサービスポータルを介して WorkSpaces、または などの既存の Information Technology Service Manage (ITSM) サービスとの統合によって実行できますServiceNow。

詳細については、「ユーザーのセルフサービス WorkSpace 管理機能の有効化」を参照してください。ユーザーセルフサービスの構造化ポータルを有効にする例については、「セルフサービスポータル WorkSpaces を使用して Amazon を自動化する」を参照してください。

Amazon WorkSpaces Cost Optimizer

Amazon WorkSpaces Cost Optimizer ソリューションは、すべての Amazon WorkSpaces 使用状況データを分析します。使用状況に応じて、 WorkSpace を最もコスト効率の高い請求オプション (時間単位または月単位) に自動的に変換します。このソリューションは、 WorkSpace 使用状況のモニタリングとコストの最適化に役立ち、 AWS CloudFormation を使用して 24 時間ごとに使用状況を分析し、個々の を変換するために必要な AWS サービスを自動的にプロビジョニングして設定します WorkSpaces。最新バージョンの 2.4 では、既存の VPC にソリューションをデプロイし、リージョンと終了のオプションを設定できます。また、 WorkSpaces および強化されたレポートメタデータの請求時間計算の精度も向上しました。以前にこのソリューションの以前のバージョン (v2.2.1 以前) をデプロイしたことがある場合は、更新スタックのドキュメントに従って Amazon WorkSpaces Cost Optimizer CloudFormation スタックを更新し、ソリューションのフレームワークの最新バージョンを取得します。

の実行モードによって、その即時の可用性と請求が WorkSpace 決まります。現在の WorkSpaces 実行モードは次のとおりです。

AlwaysOn — の無制限の使用に対して固定月額料金を支払います WorkSpaces。このモードは、 をプライマリデスクトップ WorkSpace として使用し、 WorkSpace 常に実行中の に瞬時にアクセスする必要があるユーザーに最適です。

AutoStop — 時間を WorkSpaces 基準に の支払いを行う場合に使用します。このモードでは、指定した期間非アクティブ状態になり、アプリケーションとデータの状態が保存されると WorkSpaces 停止します。自動停止時間を設定するには、 AutoStop 時間 (時間) を使用します。このモードは、へのパートタイムアクセスのみを必要とするユーザーに最適です WorkSpaces。

ベストプラクティスは、使用状況を監視し、Amazon WorkSpaces Cost Optimizer などのソリューションを使用して、Amazon WorkSpacesの実行モードを最もコスト効率の高いモードに設定することです。このソリューションは、24 時間ごとに AWS Lambda関数を呼び出す Amazon CloudWatch イベントルールをデプロイします。

このソリューションは、しきい値に達した後、いつでも個人を時間単位の請求モデル WorkSpaces から月単位の請求モデルに変換できます。ソリューションが を時間単位の請求 WorkSpace から月単位の請求に変換する場合、ソリューションは翌月の初めまで WorkSpace 時間単位の請求に変換せず、使用量がしきい値を下回った場合に限ります。ただし、請求モデルは、 AWS Management Console または Amazon WorkSpaces API を使用していつでも手動で変更できます。ソリューションの AWS CloudFormation テンプレートには、これらの変換を実行し、リハーサルモードでソリューションを実行してレコメンデーションのレポートを提供できるパラメータが含まれています。

タグによるオプトアウト

ソリューションが請求モデル WorkSpace 間で を変換しないようにするには、タグキー Skip_Convert と任意のタグ値 WorkSpace を使用してリソースタグを に適用します。このソリューションでは、 というタグが付けられますが WorkSpaces、 というタグは変換されません WorkSpaces。タグはいつでも削除して、その の自動変換を再開できます WorkSpace。詳細については、「Amazon WorkSpaces Cost Optimizer」を参照してください。

リージョンのオプトイン

デフォルトでは、このソリューションは、同じ AWS アカウント WorkSpaces で Amazon に登録されているディレクトリをスキャンして、利用可能なすべての AWS リージョン WorkSpaces で をモニタリングします。モニタリングする AWS リージョンのリストの入力パラメータで、モニタリングする AWS リージョンのカンマ区切りリストを指定して、モニタリングするリージョンを制限できます。

既存の VPC へのデプロイ

このソリューションでは、ECS タスクを実行するために VPC が必要です。デフォルトでは、ソリューションは新しい VPC を作成しますが、入力パラメータの一部としてサブネット IDs とセキュリティグループ ID を指定することで、既存の VPC にデプロイできます。現在のサブネットには、ECS タスクがパブリック Amazon ECR リポジトリでホストされている Docker イメージをプルするためのインターネットへのルートがあります。

未使用の の終了 WorkSpaces

このソリューションでは、すべての基準を満たした月の WorkSpaces 最後の日に未使用の を終了できます。TerminateUnusedWorkSpaces 入力パラメータを CloudFormation テンプレートに変更することで、この機能にオプトインできます。ベストプラクティスは、この機能を Dry Run モードで数か月間実行し、月次レポートを確認して、終了の対象として WorkSpaces マークされた を確認することです。

Amazon の Amazon Connect 最適化 WorkSpaces

コンタクトセンターのエージェントのエンドユーザーエクスペリエンスは最優先事項である必要があります。オーディオが低下すると、提供する顧客にとって不適切な通話エクスペリエンスが作成されるからです。リモートデスクトップ内でコンタクトセンターソリューションを実行する場合、音声トラフィックがネットワーク接続よりも優先されない場合、音声パフォーマンスは常に測定可能なスケールに影響します。この影響は、オーディオエンドポイントから仮想セッションにオーディオが流れ、ストリーミングプロトコルで圧縮されてエンドユーザーに配信されるためです。このルーティングを追加すると、ネットワークのボトルネックによってオーディオのパフォーマンスが低下します。

この動作を回避する方法は、音声をセッションから分割することです。つまり、音声ストリームがセッションから外れている間、コンタクトセンターエージェントのリソースはすべてセッション中のままになります。この分割により、エージェントが表示している PII を含む他のすべての通話リソースを安全なセッションに残しながら、音声エンドポイントからエンドユーザーに音声を直接ストリーミングできます。このオーディオ最適化は、顧客の通話エクスペリエンスを可能な限り良いものにするため、ベストプラクティスとして見なされています。

Amazon Connect には、管理者がビジネス要件を満たすように問い合わせコントロールパネル (CCP) をカスタマイズできる Streams API が用意されています。管理者が持つオプションの 1 つは、カスタム CCP が通話の音声を受信できるかどうかを制御することです。これらの設定により、分割 CCP、セッション外用のオーディオのみの CCP、セッション内用のメディアレス CCP を設定できます。管理者がこれらのカスタム CCPs、 の Amazon Connect オーディオ最適化 WorkSpacesを活用できるようになります。CCPs はブラウザ内で配信されるため、この設定により、管理者はオーディオのみの CCP URL を ディレクトリに提供 WorkSpacesできます。設定が完了すると、 WorkSpaces Connect コンタクトセンターのエージェントが に対して正常に認証されると WorkSpaces、 WorkSpaces クライアントは提供されたオーディオのみの CCP URL をエージェントのローカルデフォルトブラウザで自動的に開きます。このアクションにより、メディアレス CCP は安全な WorkSpaces セッション内の他のすべてを処理しながら、音声をエージェントのローカルマシンに直接フローできます。

アーキテクチャ図

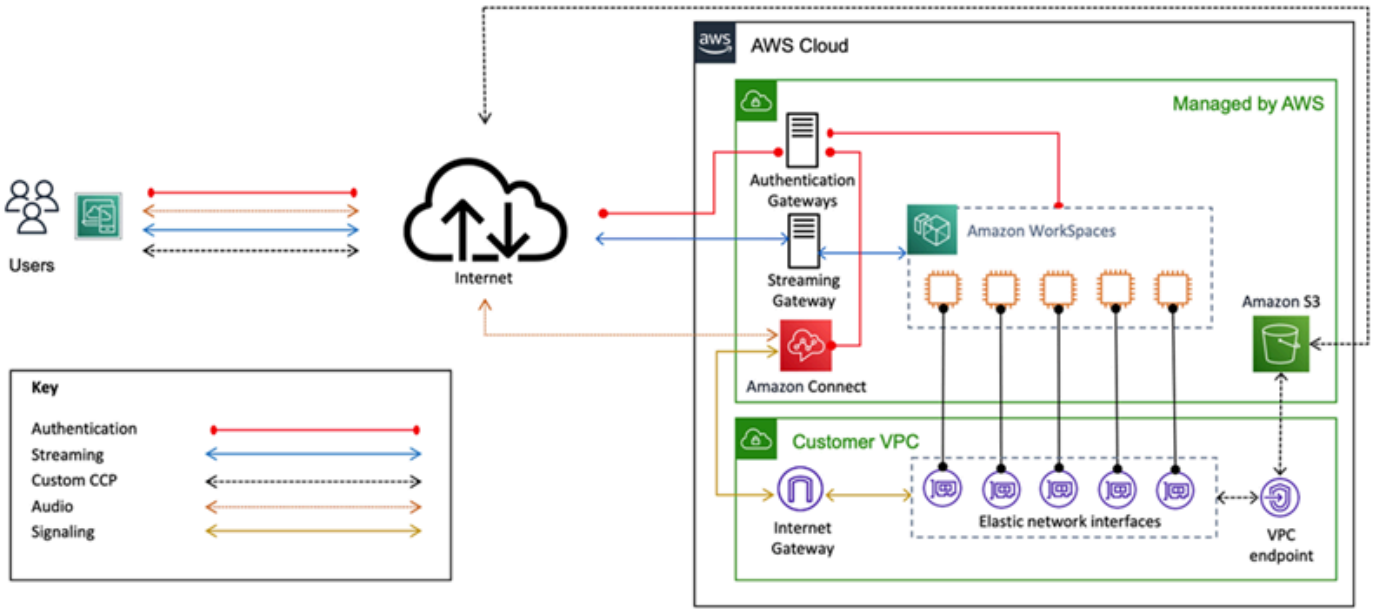

図 26 — Amazon Connect と WorkSpaces アーキテクチャ図

トラブルシューティング

デバイスが WorkSpaces 登録サービスに接続できない、インタラクティブなログオンバナー WorkSpace で に接続できないなどの一般的な管理やクライアントの問題については、Amazon WorkSpaces 管理ガイドの「クライアントと管理者のトラブルシューティング」ページを参照してください。

トピック

- AD Connector が Active Directory に接続できない
- WorkSpace カスタムイメージ作成エラーのトラブルシューティング
- 異常と WorkSpace マークされた Windows のトラブルシューティング
- デバッグ用の WorkSpaces サポートログバンドルの収集
- 最も近い AWS リージョンへのレイテンシーを確認する方法

AD Connector が Active Directory に接続できない

AD Connector をオンプレミスディレクトリに接続するには、オンプレミスネットワークのファイアウォールで、VPC 内の両方のサブネットの CIDRs に対して開かれている特定のポートが必要です。「シナリオ 1: AD Connector を使用してオンプレミスの Active Directory Service への認証をプロキシする」を参照してください。これらの条件が満たされているかどうかをテストするには、次のステップを実行します。

接続をテストするには：

1. VPC で Windows インスタンスを起動し、RDP 経由でインスタンスに接続します。残りのステップは VPC インスタンスで実行されます。
2. DirectoryServicePortTest テストアプリケーションをダウンロードして解凍します。必要に応じて、テストアプリケーションを変更するためのソースコードと Microsoft Visual Studio プロジェクトファイルが含まれています。
3. Windows コマンドプロンプトから、次のオプションを使用して DirectoryServicePortTest テストアプリケーションを実行します。

```
DirectoryServicePortTest.exe -d <domain_name>
```

```
-ip <server_IP_address> -tcp "53,88,135,139,389,445,464,636,49152" -udp
 "53,88,123,137,138,389,445,464" <domain_name>
```

<domain_name> — フォレストとドメインの機能レベルのテストに使用される完全修飾ドメイン名。ドメイン名が除外されている場合、機能レベルはテストされません。

< server_IP_address> — オンプレミスドメイン内のドメインコントローラーの IP アドレス。ポートはこの IP アドレスに対してテストされます。IP アドレスが除外されている場合、ポートはテストされません。

このテストでは、VPC からドメインに必要なポートが開いているかどうかを判断します。テストアプリケーションは、最小フォレストレベルとドメイン機能レベルも検証します。

WorkSpace カスタムイメージ作成エラーのトラブルシューティング

Windows または Amazon Linux WorkSpace が起動およびカスタマイズされている場合、その からカスタムイメージを作成できます WorkSpace。カスタムイメージには、オペレーティングシステム、アプリケーションソフトウェア、および の設定が含まれます WorkSpace。

Windows カスタムイメージを作成するための要件、または Amazon Linux カスタムイメージを作成するための要件を確認してください。イメージの作成では、イメージの作成を開始する前に、すべての前提条件が満たされている必要があります。

Windows がイメージ作成 WorkSpace の要件を満たしていることを確認するには、Image Checker を実行することをお勧めします。Image Checker は、イメージの作成 WorkSpace 時に で一連のテストを実行し、検出された問題を解決する方法に関するガイダンスを提供します。詳細については、「Image Checker のインストールと設定」を参照してください。

がすべてのテストに WorkSpace 合格すると、「検証に成功しました」というメッセージが表示されます。カスタムバンドルを作成できるようになりました。それ以外の場合は、テストの失敗や警告の原因となる問題を解決し、 がすべてのテストに WorkSpace 合格するまで Image Checker の実行プロセスを繰り返します。イメージを作成する前に、すべての障害と警告を解決する必要があります。

詳細については、Image Checker で検出された問題を解決するためのヒントを参照してください。

異常と WorkSpace マークされた Windows のトラブルシューティング

Amazon WorkSpaces サービスは、ステータスリクエストを送信 WorkSpace して、 の状態を定期的にチェックします。からレスポンスが WorkSpace タイムリーに受信されない場合、 WorkSpace は異常とマークされます。この問題に対する一般的な原因は次のとおりです。

- 上のアプリケーション WorkSpace が Amazon WorkSpaces サービスと 間のネットワーク接続をブロックしています WorkSpace。
- の CPU 使用率が高い WorkSpace。
- のコンピュータ名が変更され WorkSpace ました。
- Amazon サービスに応答するエージェントまたは WorkSpaces サービスが実行中の状態ではありません。

以下のトラブルシューティングステップでは、 WorkSpace を正常な状態に戻すことができます。

- まず、Amazon WorkSpaces コンソール から を再起動 WorkSpaceします。を再起動しても問題 WorkSpace が解決しない場合は、RDP を使用するか、SSH WorkSpace を使用して Amazon Linux に接続します。
- 別のプロトコルで にアクセス WorkSpace できない場合は、Amazon WorkSpaces コンソールから を再構築 WorkSpaceします。
- WorkSpaces 接続を確立できない場合は、以下を確認します。

CPU 使用率を確認する

Open Task Manager を使用して、 WorkSpace の CPU 使用率が高いかどうかを判断します。その場合は、次のいずれかのトラブルシューティング手順を試して問題を解決してください。

1. 大量の CPU を消費しているサービスを停止します。
2. を現在使用されているよりも大きいコンピューティングタイプ WorkSpace に変更します。
3. を再起動します WorkSpace。

> **Note**
>
> 高い CPU 使用率を診断したり、上記のステップで高い CPU 使用率の問題が解決しない場合は、「CPU がスロットリングされていないときに EC2 Windows インスタンスで高い CPU 使用率を診断するにはどうすればよいですか？」を参照してください。

のコンピュータ名を確認する WorkSpace

Workspace のコンピュータ名が変更された場合は、元の名前に戻します。

1. Amazon WorkSpaces コンソールを開き、異常を展開 WorkSpace して詳細を表示します。
2. コンピュータ名をコピーします。
3. RDP WorkSpace を使用して に接続します。
4. コマンドプロンプトを開き、ホスト名を入力して現在のコンピュータ名を表示します。
   a. 名前がステップ 2 のコンピュータ名と一致する場合は、次のトラブルシューティングのセクションに進んでください。
   b. 名前が一致しない場合は、sysdm.cpl を入力してシステムプロパティを開き、このセクションの残りのステップに従います。
5. 変更 を選択し、ステップ 2 のコンピュータ名を貼り付けます。
6. プロンプトが表示されたら、ドメインユーザーの認証情報を入力します。
7. SkyLightWorkspaceConfigService が実行中状態であることを確認する
   a. FromServices から WorkSpace、サービスSkyLightWorkspaceConfigServiceが実行中であることを確認します。そうでない場合は、サービスを開始します。

ファイアウォールルールの検証

Windows ファイアウォールと実行中のサードパーティーファイアウォールに、次のポートを許可するルールがあることを確認します。

- ポート 4172 のインバウンド TCP: ストリーミング接続を確立します。
- ポート 4172 のインバウンド UDP: ユーザー入力をストリーミングします。
- ポート 8200 のインバウンド TCP: を管理および設定します WorkSpace。
- ポート 55002 のアウトバウンド UDP: PCoIP ストリーミング。

ファイアウォールがステートレスフィルタリングを使用している場合は、一時ポート 49152-65535 を開いてリターン通信を許可します。

ファイアウォールがステートフルフィルタリングを使用している場合、エフェメラルポート 55002 は既に開いています。

デバッグ用の WorkSpaces サポートログバンドルの収集

WorkSpaces 問題をトラブルシューティングする場合は、影響を受けた WorkSpace と WorkSpaces クライアントがインストールされているホストからログバンドルを収集する必要があります。ログには 2 つの基本的なカテゴリがあります。

- サーバー側のログ： WorkSpace はこのシナリオではサーバーであるため、これらは WorkSpace それ自体に格納されているログです。
- クライアント側のログ: エンドユーザーが への接続に使用しているデバイスのログ WorkSpace。

- Windows クライアントと macOS クライアントのみがローカルにログを書き込みます。
- ゼロクライアントと iOS クライアントはログを記録しません。
- Android ログはローカルストレージで暗号化され、 WorkSpaces クライアントエンジニアリングチームに自動的にアップロードされます。Android デバイスのログを確認できるのは、そのチームのみです。

WSP サーバー側のログ

すべての WSP コンポーネントは、ログファイルを 2 つのフォルダのいずれかに書き込みます。

- プライマリロケーション： `C:\ProgramData\Amazon\WSP\`および `C:\ProgramData\NICE\dcv\log\`
- アーカイブの場所： `C:\ProgramData\Amazon\WSP\TRANSMITTED\`

Windows でのログファイルの詳細度の変更

ログの詳細レベルグループポリシー設定 を設定することで、WSP Windows のログファイルの詳細レベルを WorkSpaces 大規模に設定できます。

個々の のログファイルの詳細度を変更するには WorkSpaces、Windows レジストリエディタを使用して `h_log_verbosity_options` キーを設定します。

1. 管理者として Windows レジストリエディタを開きます。
2. \HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon に移動します。
3. WSP キーが存在しない場合は、右クリックして新規 > キーを選択し、 と名前を付けますWSP。
4. \HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon\WSP に移動します。
5. h_log_verbosity_options 値が存在しない場合は、右クリックして新規 > DWORD を選択し、 と名前を付けますh_log_verbosity_options。
6. 新しい h_log_verbosity_options DWORD をクリックし、必要な詳細レベルに応じて、値を次のいずれかの数値に変更します。
   - 0 — エラー
   - 1 — 警告
   - 2 — 情報
   - 3 — デバッグ
7. [OK] を選択して Windows レジストリエディタを閉じます。
8. を再起動します WorkSpace。

PCoIP サーバー側のログ

すべての PCoIP コンポーネントは、ログファイルを 2 つのフォルダのいずれかに書き込みます。

- プライマリロケーション： C:\ProgramData\Teradici\PCoIPAgent\logs
- アーカイブの場所： C:\ProgramData\Teradici\logs

複雑な問題 AWS Support で作業する場合、PCoIP Server エージェントを詳細なログ記録モードにする必要がある場合があります。これを有効にするには：

1. 次のレジストリキーを開きます。 HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Teradici\PCoIP\pcoip_admin_defaults
2. pcoip_admin_defaults キーで、次の 32 ビット DWORD を作成します。 pcoip.event_filter_mode
3. の値を3「」(12 月または 16 進数) pcoip.event_filter_modeに設定します。

参考までに、これらはこの DWORD で定義できるログしきい値です。

- 0 — (CRITICAL)

- 1 — (エラー)
- 2 — (INFO)
- 3 — (デバッグ)

pcoip_admin_default DWORD が存在しない場合、ログレベルは2デフォルトで になります。詳細なログが不要になったら、 の値を DWORD 2に復元することをお勧めします。これは、はるかに大きく、ディスク容量を不必要に消費するためです。

WebAccess サーバー側のログ

PCoIP および WSP (バージョン 1.0 以降) の場合 WorkSpaces、 WorkSpaces Web Access クライアントは STXHD サービスを使用します。 WorkSpaces Web Access のログは に保存されますC:\ProgramData\Amazon\Stxhd\Logs。

WSP (バージョン 2.0 以降) の場合 WorkSpaces、 WorkSpaces Web Access のログは に保存されますC:\ProgramData\Amazon\WSP\。

クライアント側のログ

これらのログはユーザーが接続する WorkSpaces クライアントから取得されるため、ログはエンドユーザーのコンピュータ上にあります。Windows と Mac のログファイルの場所は次のとおりです。

- Windows: "%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\Logs"
- macOS ~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs :
- Linux: ~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs

ユーザーが遭遇する可能性のある問題をトラブルシューティングするには、任意の Amazon WorkSpaces クライアントで使用できる高度なログ記録を有効にします。高度なログ記録は、無効化されるまで、後続のすべてのクライアントセッションで有効になります。

1. に接続する前に WorkSpace、エンドユーザーは WorkSpaces クライアントの高度なログ記録を有効にする必要があります。
2. エンドユーザーは、通常どおり接続し、 を使用して WorkSpace、問題を再現する必要があります。
3. 高度なログ記録では、診断情報とデバッグレベルの詳細 (詳細なパフォーマンスデータなど) を含むログファイルが生成されます。

この設定は、明示的にオフになるまで保持されます。ユーザーが冗長ログ記録に関する問題を正常に再現したら、大きなログファイルが生成されるため、この設定は無効にする必要があります。

Windows 用のサーバー側のログバンドルの自動収集

このGet-WorkSpaceLogs.ps1スクリプトは、 のサーバー側のログバンドルをすばやく収集するのに役立ちます AWS Support。スクリプトは、サポートケースでリクエスト AWS Support することで、 からリクエストできます。

1. WorkSpace クライアントまたはリモートデスクトッププロトコル (RDP) を使用して に接続します。
2. 管理コマンドプロンプトを起動します (管理者として実行) 。
3. 次のコマンドを使用して、コマンドプロンプトからスクリプトを起動します。

```
powershell.exe -NoLogo -ExecutionPolicy RemoteSigned -NoProfile -File "C:\Program
 Files\Amazon\WorkSpacesConfig\Scripts\Get-WorkSpaceLogs.ps1"
```

4. このスクリプトは、ユーザーのデスクトップにログバンドルを作成します。

   このスクリプトは、次のフォルダを含む zip ファイルを作成します。

   - C — Skylight、EC2Config ProgramData、Teradici、イベントビューワー、および Windows ログ (Panther など) に関連するプログラムファイル、プログラムファイル (x86)、および Windows からのファイルが含まれます。
   - CliXML — インタラクティブフィルタリングImport-CliXMLに を使用して Powershell にインポートできる XML ファイルが含まれています。「Import-Clixml」を参照してください。
   - Config — 実行される各チェックの詳細ログ
   - ScriptLogs - スクリプトの実行に関するログを記録します (調査には関係ありませんが、スクリプトの動作をデバッグするのに役立ちます) 。
   - tmp — 一時フォルダ (空である必要があります) 。
   - トレース — ログ収集中にパケットキャプチャが実行されます。

最も近い AWS リージョンへのレイテンシーを確認する方法

Connection Health Check ウェブサイト WorkSpaces では、Amazon を使用するすべての必要なサービスにアクセスできるかどうかをすばやく確認できます。また、Amazon が WorkSpaces 利用可能な各 AWS リージョンのパフォーマンスチェックを行い、どれが最速かをユーザーに知らせます。

結論

エンドユーザーコンピューティングには戦略的変化があります。組織は、よりアジャイルで、データをより適切に保護し、ワーカーの生産性を高めることを目指しているためです。クラウドコンピューティングですでに実現されている利点の多くは、エンドユーザーコンピューティングにも当てはまります。Windows または Linux のデスクトップを Amazon で AWS クラウドに移行することで WorkSpaces、組織はワーカーの追加時に迅速にスケーリングし、デバイスからのデータをオフにしてセキュリティ体制を改善し、選択したデバイスを使用して、どこからでもアクセスできるポータブルデスクトップをワーカーに提供できます。

Amazon WorkSpaces は既存の IT システムおよびプロセスに統合されるように設計されており、このホワイトペーパーでは、これを行うためのベストプラクティスについて説明しています。このホワイトペーパーのガイドラインに従うことで、 AWS グローバルインフラストラクチャ上でビジネスに合わせて安全にスケールできる、費用対効果の高いクラウドデスクトップデプロイを実現できます。

寄稿者

本ドキュメントの寄稿者は次のとおりです。

- AndrewTAK、Amazon Web Services、EUC ソリューションアーキテクト
- アマゾン ウェブ サービス、シニア EUC スペシャリストコンサルタント、DonTAK
- アマゾン ウェブ サービス、シニア EUC スペシャリストソリューションアーキテクト
- Naviero Magee、Amazon Web Services、プリンシパルソリューションアーキテクト
- RoTAK Fountain、Amazon Web Services、EUC 専門コンサルタント
- Stephen Stetler、Amazon Web Services、シニア EUC ソリューションアーキテクト

詳細情報

詳細については、次を参照してください。

- Amazon WorkSpaces 管理ガイド
- Amazon WorkSpaces デベロッパーガイド
- Amazon WorkSpaces クライアント
- AWS OpsWorks for Puppet Enterprise WorkSpaces を使用した Amazon Linux 2 Amazon の管理
- Amazon Linux のカスタマイズ WorkSpace
- クライアント側の LDAPS を使用して AWS Directory Service の LDAP セキュリティを強化する方法
- Amazon CloudWatch Events を Amazon WorkSpaces と AWS Lambda と併用してフリートの可視性を高める
- Amazon が WorkSpaces を使用する方法 AWS KMS
- AWS CLI コマンドリファレンス – WorkSpaces
- Amazon WorkSpaces メトリクスのモニタリング
- MATE デスクトップ環境
- AWS Directory Service 管理に関する問題のトラブルシューティング
- Amazon WorkSpaces 管理に関する問題のトラブルシューティング
- Amazon WorkSpaces クライアントの問題のトラブルシューティング
- セルフサービスポータル WorkSpaces で Amazon を自動化する

ドキュメントの改訂

このホワイトペーパーの更新に関する通知を受け取るには、RSS フィードにサブスクライブしてください。

変更	説明	日付
マイナーな更新	AD Directory Services、災害対策/ビジネス継続性、クロスリージョンリダイレクトのコンテンツを更新しました。 WorkSpaces と Amazon Connect Audio Optimization を追加しました。フォーマットの軽微な更新。	2022 年 5 月 26 日
マイナーな更新	包括的でない言語を修正します。	2022 年 4 月 6 日
ホワイトペーパーの更新	更新されたコンテンツ	2022 年 3 月 24 日
ホワイトペーパーの更新	AWS Network Firewall、MAD レプリケートディレクトリ、YubiKey サポート、コンテナ、WSLv1、スマートカードサポート、 WorkSpaces Service Quota、および信頼できるデバイスのコンテンツを更新しました。	2021 年 12 月 20 日
ホワイトペーパーの更新	WorkSpaces ストリーミングプロトコル、スマートカード認証、図、クライアントのデプロイ、エンドデバイスの選択、ウェブアクセスに関するコンテンツを更新	2021 年 4 月 28 日

ホワイトペーパーの更新	更新されたコンテンツ	2020 年 12 月 1 日
ホワイトペーパーの更新	初回発行以降にコンテンツを更新し、新しい図を追加しました。	2020 年 5 月 1 日
初版発行	最初に公開されました。	2016 年 7 月 1 日

注意

お客様は、本書に記載されている情報を独自に評価する責任を負うものとします。本書は、(a) 情報提供のみを目的としており、(b) 現在の AWS 製品提供およびプラクティスであり、これらは予告なしに変更されることがあり、(c) AWS および関連会社、サプライヤー、またはライセンス付与者からのコミットメントまたは保証は作成されません。 AWS 製品またはサービスは、明示または黙示を問わず、いかなる種類の保証、表現、または条件もなしに「現状のまま」提供されます。お客様 AWS に対する の責任と責任は契約によって管理され AWS 、本書は AWS とお客様との間の契約の一部でも変更もされません。

AWS 用語集

最新の AWS 用語については、「 AWS の用語集 リファレンスAWS 」の用語集を参照してください。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。