

# VMware vCloud Air

## 技術的な質問

### VMware vCloud® Air™ の概要

Q：VMware vCloud Director® を所有していませんが、このサービスを利用できますか

A：もちろんご利用いただけます。ハイブリッドクラウドの最大のメリットは、互換性と拡張性を備えたクラウドインフラストラクチャを利用してVMware vSphere® のリソースを拡張できることです。必要な場合は、プライベートデータセンターと分けて、個別に本サービスを利用することもできます。

Q：サービスの変更およびメンテナンスのスケジュールについて教えてください

A：VMware vCloud Air は vSphere vMotion® を利用するため、計画的なメンテナンスはほとんど発生せず、発生してもサービス上のワークロードが影響を受けることはほとんどありません。メンテナンスが必要になった場合は、遅くとも 24 時間前にはお客様にお知らせします。

Q：ユーザーがデータセンターまで実際に出向く必要はありますか

A：いいえ。当社のデータセンターは、専任のエキスパートによって管理されており、厳重なセキュリティ管理を行っています。お客様がデータセンターの敷地内に立ち入ることは禁止されています。すべてのお客様の資産を守るためにこのような方法がとられています。

### コンピューティング サービス

Q：このサービスで提供されるリソースはどのようなものですか

A：**専有型クラウド**には、30 GHz のコンピューティング（仮想 CPU）キャパシティ、120 GB の仮想メモリ、および 6 TB のストレージが標準で含まれます。さらに、3 個のパブリック IP アドレス、1 Gbps までバースト可能（従量課金）の 50 Mbps のネットワークリンクが提供されます。

**仮想プライベートクラウド**には、5 GHz のコンピューティング（仮想 CPU）キャパシティ、20 GB の仮想メモリ、および 2 TB のストレージが標準で含まれます。さらに、2 個のパブリック IP アドレス、50 Mbps までバースト可能（従量課金）の 10 Mbps のネットワークリンクが提供されます。

Q：リソースはほかのユーザーと共有することになりますか

A：**専有型クラウド**の場合、物理的に分離した仮想 CPU と仮想メモリのプールが提供されます。専有型クラウドのコンピューティングノードは、当社のデータセンター内で「エアギャップ」で隔離された環境に置かれています。ネットワークとストレージは、最新のハイエンドマルチテナントインフラストラクチャで論理的に分離され、適切な量のリソースを確保しています。また、ほかのユーザーと共有されない、お客様のサービス固有の分離されたクラウド管理スタックが用意されます。

**仮想プライベートクラウド**の場合、仮想 CPU と仮想メモリのプール、およびネットワークとストレージは、専有型クラウドと同じ設計アーキテクチャですが、論理的に分離されています。vSphere のリソースの分離機能によって、マルチテナント環境で物理リソースを運用しながら、各テナントに一定のリソースを確保することが可能です。また、インフラストラクチャ内で負荷が均等に分散されるため、クラウドを利用するすべてのユーザーに堅牢性と拡張性に優れた可用性を提供できます。

Q：このサービスに使用されているハードウェアについて教えてください

A：VMware vCloud Air には、セキュリティ、堅牢性、および拡張性に優れ、vSphere データセンターとの互換性を備えた x86 ベースのインフラストラクチャが使用されます。vCloud Air の各サービスは、最高水準のハードウェアを使用するクラウドを想定した設計になっています。常に最先端のクラウドテクノロジーを取り入れるため、利用するハードウェアベンダーを変更する可能性があります。これらのベンダーは開示されません。

Q：どのようなタイプのワークロードがこのクラウドに適していますか

A：vCloud Air は本番環境での運用が可能で、要件の厳しいミッションクリティカルなワークロードを実行でき、その管理性と俊敏性により、あらゆる種類のワークロードに対応します。

Q：使用状況の確認に、どのようなレポートやダッシュボードが提供されますか

A：vCloud Air のダッシュボードには、仮想データセンター全体におけるクラウドリソースの割り当てがまとめて表示されます。各仮想データセンター内のクラウドキャパシティの使用状況を表示するだけでなく、CPU とメモリの使用状況や、ディスクの読み取りおよび書き込みを、仮想マシンレベルでポータルから直接監視できます。ゲスト内のエージェントを使用するサードパーティパートナー製のツールを用いてキャパシティと使用状況を監視することも可能です。

Q：すでに所有している管理ソフトウェアやその他のツールを環境の監視に使用できますか

A：はい。お客様が管理スタックを直接監視することはできませんが、VMware vCloud® Automation Center™、vCenter™ Server、vCenter Orchestrator™ などの vCloud API を利用するテクノロジーは使用できます。vCenter Operations Management Pack for vCloud Air は、単一の vCenter Operations Manager™ コンソールで、社内のリソースと vCloud Air のリソースの両方の運用状況を確認できます。また、ローカルのデータセンターにレポートを送るため、Hyperic HQ などのエージェントベースのツールを導入することも可能です。

Q：どのようなユーザー インターフェイスや API が提供されますか

A：統合サービス ダッシュボードにアクセスして、vCloud Air の運用や操作を行うことができます。また、vCloud Director のテナント用ユーザー インターフェイスも使用可能です。さらに、vCloud Automation Center など、vCloud 対応のアプリケーションやプラットフォームとの連携を可能にする vCloud API にアクセスして、vCloud Air の拡張機能をご利用いただけます。

Q：VMware は、vCloud Air 環境の可用性と冗長性をどのように確保していますか

A：vCloud Air のインフラストラクチャは、高可用性を提供するように設計されています。vSphere vMotion、vSphere Distributed Resource Scheduler™ (DRS)、および vSphere HA を使用して、ワークロードのライブ マイグレーションが実行され、予期しない問題が発生した場合には仮想マシンが自動的に再起動されます。また、Edge Gateway もアクティブ / スタンバイのペアで高い可用性が実現されており、障害発生後もネットワークが保護され、確実に使用できるようにします。

Q：クラウド内のアプリケーションに機密性が非常に高いデータが含まれる場合、どのように保護されますか

A：vSphere と vCloud プラットフォームではリソースを高度に分離しているため、未承認のユーザーがクラウド内のアプリケーションにアクセスすることはできません。ユーザー側のセキュリティ保護も重要であるため、お客様ご自身で必要に応じて暗号化やセキュリティ対策を採用、導入していただくことが推奨されます。また、ユーザー レベルのアクセス コントロール、ポータルへの https 接続、IPsec VPN トンネルのほか、膨大な数の物理的セキュリティ対策で物理データセンター自体を強化しています。

## ストレージおよびネットワーク サービス

Q：このサービスではどのようなストレージが提供されますか

A：vCloud Air には、2 種類のブロック デバイス ストレージがあります。

- SSD を使用するストレージ層は、最も要求の厳しいアプリケーションに対応します。
- 標準ストレージ層は、最も費用対効果に優れたソリューション向けです。

ワークロードはこれらのストレージ層の間で移動させることが可能で、1 台の仮想マシンを複数のストレージ層にあるディスクに接続できます。

Q：帯域幅やトラフィックの制限または制約はありますか

A：**専用型クラウド** サービスでは、50 Mbps の帯域幅が確保され、1 Gbps までバースト可能（従量課金）です。

**仮想プライベート クラウド** サービスの場合は、10 Mbps の帯域幅が確保され、50 Mbps までバースト可能（従量課金）です。

また、Direct Connect ポートを通じて帯域幅を追加できます。

Q：VPN トンネルを使用してこのサービスに接続することはできますか

A：はい。このサービスでは、Edge Gateway サービスを利用して任意の IPsec VPN デバイスへの IPsec VPN トンネルを作成できます。セルフサービスでの VPN トンネル作成にはいくつかの方法があります。同じ仮想データセンター内のネットワーク間、異なる複数の仮想データセンター間のネットワーク（専用型クラウドのみ）、およびローカル データセンター内のネットワーク間を、ソフトウェアまたはハードウェア VPN ソリューションを使用して接続できます。

IPsec VPN の確立はセルフサービスでご利用いただく機能ですが、必要な場合は vCloud Air の運用チームがサポートいたします。

Q：他の環境またはデータセンターから、データやワークロードを移行する方法を教えてください

A：ワークロードは次のような方法で移行できます。

- vCloud Connector® を使用して、社内の vSphere 環境または vCloud 環境から vCloud Air 環境にワークロードを移行できます。
- また、vCloud Air 環境に非常に大規模なデータ セットを移行する場合は、外付けのストレージ デバイスを使用して、オフラインでデータを移行できます。これは、使用分に応じて料金を支払う、VMware の有償サービスとして提供されます。
- vCloud Director には、OVF 形式の仮想マシン イメージやその他のメディアをインポートまたはエクスポートする機能もあります。

Q：VMware vCloud Air Direct Connect について教えてください

A：Direct Connect は、標準の IPsec VPN 接続のほかに利用できる、プライベートな高スループットの vCloud Air 専用接続オプションです。VMware は、主要な通信事業者の協業により、リモート サイトまたは同じ共用サイト内にあるお客様のデータセンターから、vCloud Air の専有型クラウド インスタンスまたは仮想プライベート クラウド インスタンスへの高スループットで安全なリンクを確立しています。

詳細については、[Direct Connect データ シート](#)を参照してください。

Q：標準の vCloud Air 接続と Direct Connect の違いについて教えてください

A：標準の vCloud Air 接続はインターネット経由でルーティングされるのに対し、vCloud Air Direct Connect では専用の安全なプライベート リンクが提供されます。主な違いは次のとおりです。

	標準接続	Direct Connect
速度	専有型クラウド： 最大 1 Gbps 仮想プライベート クラウド：最大 1 Gbps	専有型クラウド： 最大 10 Gbps 仮想プライベート クラウド：最大 1 Gbps
接続タイプ	インターネット経由の ルーティング	専用リンク
接続の保護	IPsec VPN 経由	デフォルトで プライベート
シングル ポイント またはマルチ ポイント	IPsec はポイント ツー ポイント	ポイント ツー ポイント またはマルチ ポイント (パートナー通信事業者 によって異なる)
価格設定	基本サービスに含まれる 専有型クラウド： 50 Mbps 仮想プライベート クラウド：10 Mbps	月単位のポート接続料金 追加の回線料金は通信 事業者によって異なる

## 可用性サービス：Data Protection

Q：vCloud Air Data Protection について教えてください

A：Data Protection は、専有型クラウド インスタンスおよび仮想プライベート クラウド インスタンス向けのバックアップおよびリカバリ ソリューションで、オプションとして提供されます。Data Protection は、エージェントを使用しない、セルフサービス型のポリシー ベースのバックアップおよびリカバリ サービスです。イメージ レベルのバックアップによって、仮想マシン内のオペレーティング システム、ファイル システム、およびアプリケーション データのすべてをスナップショットとしてキャプチャしてから、バックアップ メディアに格納します。

Q：どのようなバックアップ ポリシーを利用できますか

A：ポリシーは、単一の仮想マシン (vApp 形式) に対して、または仮想データセンター全体に対して定義できます。保護対象のアイテムごとに、最長 365 日間までのデータ保持ポリシーを複数設定でき、バックアップ開始時間も選択できます。vApp のバックアップは、vCloud Air の UI から手動で開始できます。

Q：どのようなリカバリ オプションを利用できますか

A：利用可能な任意のリカバリ ポイントから、バックアップをリカバリできます。バックアップからのリカバリでは、保護対象の仮想マシンを置き換える (インプレース リストア) ことも、別の仮想マシンとして展開する (アウトオブプレース リストア) こともできます。

Q：バックアップは、契約しているクラウド インスタンスのストレージ容量を消費しますか

A：いいえ。Data Protection では、バックアップ専用のストレージを使用します。お客様のクラウド インスタンスのストレージがバックアップによって消費されることはありません。

Q：バックアップに消費されるストレージ容量は毎回同じですか

A：Data Protection では、合成フル バックアップと変更ブロックのトラッキングを利用して、vApp レベルまたは仮想データセンターレベルで仮想マシンをバックアップします。初回のバックアップはフル バックアップですが、それ以降のバックアップでは、日々の変更箇所のみをキャプチャするため、ストレージの占有量を節約できます。

Q：vApp または仮想マシンのリストアにはどの程度時間がかかりますか

A：リカバリの所要時間は、仮想マシンのサイズおよびストレージ層によって異なります。たとえば、40 GB の仮想マシンを SSD を使用するストレージにリストアする場合は、200 GB の仮想マシンを標準ストレージにリストアする場合よりも迅速に処理されます。

## 可用性サービス：Disaster Recovery

Q：vCloud Air Disaster Recovery について教えてください

A：vCloud Air Disaster Recovery は、最小限の投資でアプリケーションを保護しながら、ビジネスの耐障害性強化を実現するディザスタ リカバリ サービスです。このサービスでは、災害が発生した場合でも確実にリカバリできるフェイルオーバー環境が提供されます。また、現実的なコストでリソースを節約しながら、一貫した運用を維持できます。詳細については、[Disaster Recovery に関する FAQ](#) を参照してください。

**Q：vCloud Air Disaster Recovery の最小要件を教えてください**

A：プライマリ データセンターでの要件は次のとおりです。

- vSphere 5.1 以降、Essentials Plus または上位のエディション (Standard、Enterprise、Enterprise Plus を含む)
  - vCenter Server 5.1 以降
  - vSphere Replication アプライアンス 5.6
  - 外部へのインターネット接続
- また、仮想インフラストラクチャの管理権限と、vCloud Air Disaster Recovery の有効なサブスクリプション契約も必要です。

**Q：主に使用しているバックアップ方法を教えてください**

A：vCloud Air Disaster Recovery は VMware vSphere Replication™ テクノロジーを利用して、バックアップを行います。vSphere Replication は、ハイパーバイザー ベースのレプリケーション ソリューションで、個別の仮想マシン ディスク (VMDK) レベルで機能するため、あらゆるタイプのストレージからのレプリケーションが可能になります。プライマリ サイトに置かれた仮想マシン ディスク内で変更されたブロックは、仮想マシンの構成や管理に変更を加えずに、負荷の少ない方法で vCloud Air に送られます。

**Q：SQL などのアプリケーションの静止はサポートされますか**

A：はい。vSphere Replication は、Microsoft Volume Shadow Services (VSS) での静止をサポートします。アプリケーションが VSS 対応である場合は、レプリケーションの構成で VSS の静止を選択できます。

**Q：初期レプリケーションをオフラインでできますか**

A：はい。vCloud Connector または OVF のエクスポートによる初期レプリケーションのオフライン化がサポートされます。オフライン データ転送を使用して初回のレプリケーションをシードし、お客様に物理 NAS デバイスを送付します。このサービスには追加料金がかかります。VMware が送付した物理 NAS デバイスに保護対象の仮想マシンのシード コピーを格納して VMware にお送りいただくと、VMware がお客様の環境にコピーします (送料は料金に含まれます)。

**Q：レプリケーションは安全ですか。データはインターネット経由で送信されますか**

A：はい。レプリケーション トラフィックの送受信はインターネット経由で行われます。このトラフィックを保護するため、vSphere Replication アプライアンスには、vCloud Air へのポイント ツー ポイント暗号化を行うための暗号化モジュールが含まれています。個別に VPN トンネルを用意する必要はありません。

**Q：ディザスタ リカバリ環境内で利用できるネットワーク オプションについて教えてください**

A：vCloud Air のディザスタ リカバリ環境には、標準の仮想プライベート クラウドと同じネットワーク機能が備わっています。各環境には1つの Edge Gateway が配置されていますが、これを利用して、分離されたネットワークまたはルーティングされたネットワークを最大 9 個作成できます。NAT ルール、ファイアウォール ルール、DHCP または固定 IP の割り当てを Edge Gateway に構成することもできます。また、Edge Gateway を使用して VPN やロード バランシングを設定することも可能です。レプリケーションの構成時に、どのネットワークに接続するか選択いただけます。

**Q：ディザスタ リカバリは、最大でどの程度拡張できますか**

A：現在は、ディザスタ リカバリ環境ごとに最大 500 台の仮想マシンを利用できます。これは、vCenter Server とディザスタ リカバリ環境とが 1 対 1 でマッピングされており、現在、vCenter Server 1 台ごとに vSphere Replication アプライアンス 1 台、vSphere Replication アプライアンス 1 台ごとに仮想マシン 500 台に制限されているためです。そのため、vCloud Air へのレプリケーション用に指定されている vCenter Server 環境を、別のデータセンターへのレプリケーション用に同時にマッピングすることはできません。

**Q：フェイルオーバーの自動化オプションについて教えてください**

A：ディザスタ リカバリはセルフサービス機能であるため、運用手順書を使用した手動操作によるソリューションは提供していません。フェイルオーバーの自動化オプションには、vCenter Orchestrator、vCloud Automation Center、Puppet などのツールと vCloud API を併用する方法があります。また、現時点では、フェイルバックの操作は手動で行う必要があります。

**Q：フェイルオーバー テストの開始方法について教えてください**

A：まずグローバル サポート サービス (GSS) に連絡して、フェイルオーバー テストを有効にしてください。テストは 7 日間実行できます。テストが完了したら、テストのクリーンアップ プロセスを開始して、vCloud Air 内の仮想マシンをスタンバイ状態に戻します。

**Q：災害を「宣言」する方法を教えてください**

A：マシンをフェイルオーバーする際に、災害を「宣言」し、誰かに通知する必要はありません。vCenter Server、vCloud Air のユーザー インターフェイス、または API コールを通じて、フェイルオーバー プロセスを開始するだけです。VMware は、お客様がサブスクリプション登録したリソースが利用可能になることを確認してから、お客様のマシンをオンラインにします。その後、お客様の運用手順書に則ったプロセスを開始して、アプリケーションをオンラインにすることができます。

