VMware vCloud Air

Enterprise IT ハイブリッド データセンター

テクニカル マーケティング ドキュメント
2014 年 10 月

vmware®

目次

目的および概要

VMware vCloud® Air ™ は、多種多様な使用環境を考慮して開発されています。このホワイト ペーパーは、エンタープライズ IT やアウトソーシング型データセンターの具体例をケース スタディの形式で紹介することを目的としています。この使用事例は、これ以降にお読みになるソリューション概要の基礎になるものです。基盤となる構成要素を理解することで、他のソリューション概要に記載されている概念を十分に理解する準備が整います。

このケース スタディでは主に、パブリック クラウド リソースをエンタープライズ IT に利用することの必要性について説明しています。企業の IT 部門は、パブリック クラウド リソースを利用すると、事業部門の要求にさらに迅速に対応できるようになるほか、今日の企業が必要とする管理レベルを維持することが可能になります。

また、このケース スタディでは、最新エンタープライズ IT の運用に関連するアウトソーシング型データセンターの基盤についても説明します。

1.1 背景

企業の IT 部門のお客様は、社内のキャパシティが限界に達する岐路に近づきつつあります。また、必須のインフラストラクチャを IT 部門が提供できるペースが、ビジネスのスピードに追いついていないことも少なくありません。IT チームにはこれまで、ビジネス ニーズを満たすために、増え続けるインフラストラクチャを個別に設計、調達、導入、構成、管理することが求められてきました。このプロセスは時間がかかる上に、肝心のビジネスのペース自体を低下させてしまう場合もあります。既存の VMware vSphere® インフラストラクチャにキャパシティを追加するという一見シンプルなタスクであっても、多くの場合、長期にわたる社内審査と承認のプロセスを経なければなりません。

vCloud Air では、IT 部門は VMware vCloud Suite® から構成されるクラウド上のコンピューティング、メモリ、およびストレージの各リソースを社内データセンターに追加するかのように、すばやく簡単にアクセスできます。VMware のテクノロジーをベースとしたサービスとしてのインフラストラクチャ（IaaS）をいつでも利用できるため、IT 部門はアプリケーション レイヤーのコンポーネントに変更を加えることなく、vCloud Air への新しいワークロードの展開や既存のワークロードの移行を短時間で実行できます。ただし、効果的なアウトソーシング型データセンターやハイブリッド クラウドを構築するには、新規ワークロードの展開や既存ワークロードの移行のプロセスを開始する前に、次に挙げる主な考慮事項に対処する必要があります。

- クラウド ネットワークの確立と構成
- vCloud Air への社内 vSphere の接続
- 基本的なインフラストラクチャの展開
- テンプレートとメディアの移行

これら 4 つの基本的な問題に適切に対処して初めて、アウトソーシング型データセンターでワークロードを受け入れる準備が整います。このドキュメントでは、ユーザーがこれらの考慮事項について理解を深め、サービスとしての IT という新たな時代に自らのペースでクラウドを活用する準備を整えられるようにすることを狙いとしています。

1.2 対象読者

このドキュメントは、vSphere の設計者および管理者を対象としています。本書では、説明している概念を構成する方法について詳細な手順は記載していませんが、本書をお読みになれば、vSphere の設計者と管理者はいずれも、アウトソーシング型データセンターのさまざまな要素の働きについて理解を深められるようになり、これらの概念を自社の環境に適用することが可能になります。次のトピックについては、利用者ごとに要件が大きく異なる場合があるため、このケース スタディでは詳しく扱いません。

- コンプライアンス
- ライセンス
- サードパーティ製ツール

アウトソーシング型データセンターの設計

アウトソーシング型データセンターの設計方法は比較的シンプルです。ほとんどの場合、IT 部門が管理している他のデータセンターと同じように理解し、取り扱うことができます。従来型の物理コンピューティング環境と異なるのは設計で、すべてがソフトウェアで定義されているため、エンド ユーザーや管理者に公開されている範囲が違います。vCloud Air へのアクセスが提供され、実際のインフラストラクチャの構築、管理、および更新の必要がありません。ユーザーは、必要な基本サービスを設計して構成すれば、ワークロードの展開をすぐに開始できます。これにより、IT 部門は、基盤となるインフラストラクチャ自体の管理ではなく、ビジネス ニーズへの対応に注力することができます。なお本書では、現在提供されている下記のサブスクリプションまたは従量課金型を利用するユーザーを念頭においております。

- VMware vCloud Air Virtual Private Cloud（共有型クラウド サービス）
- VMware vCloud Air Dedicated Cloud（専有型クラウド サービス）
- VMware vCloud Air Virtual Private Cloud OnDemand（従量課金サービス）

2.1 vCloud ネットワークの展開

いずれのコンピューティング サービス オプションでも、すべてのお客様に VMware vCloud Networking and Security Edge ™ ゲートウェイへのアクセスが提供されます。vCloud Air Dedicated Cloud の場合は、追加の Edge Gateway の展開を選択できます。展開された各ゲートウェイでは、vCloud Air ネットワークの定義に使用できるインターフェイスが 9 個提供されます。これらのネットワークにはいずれも、次の属性があり、ネットワークごとに一意に設定する必要があります。提示する使用事例によっては構成する必要のない属性もありますが、いずれも各サービスの一部として提供されます。

- **NAT およびファイアウォール**：どちらもデフォルトで有効になっています。ファイアウォール ルールは定義されておらず、デフォルトのルールではすべてのトラフィックが拒否されています。
- **Edge Gateway の IP アドレス**：これは、ネットワークがルーティングされる Edge Gateway インターフェイスに割り当てられるアドレスです。
- **ドメイン ネーム システム（DNS）サーバ構成**：Edge Gateway は DNS を提供できますが、代替サーバも指定できます。
- **固定 IP プールの範囲**：これは、仮想マシンを展開する際に使用される NAT IP アドレスのプールです。
- **DHCP**
- **ロード バランシング**
- **IPsec 仮想プライベート ネットワーク（VPN）**

注：Edge Gateway は 10 個のインターフェイスをサポートしますが、パブリック IP が割り当てられている場合に「外部」アクセス用として使用されるインターフェイスは 1 つです。どちらのサービスでも、利用者にはサブスクリプション サービスの一部としてパブリック IP アドレスが付与され、追加の IP アドレスもサービス インターフェイスを通じていつでも追加できます。

図 1 は、各種ネットワークと IP アドレスの例を示す論理図です。

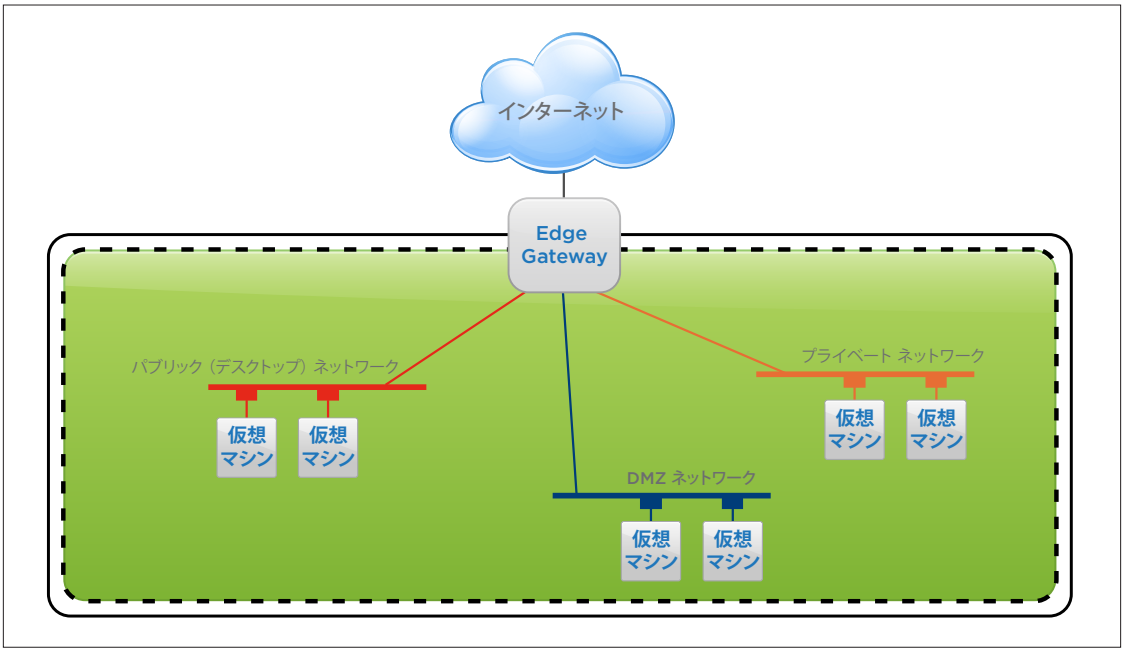

図 1：各種ネットワークと IP アドレス

2.1.1 ファイアウォール ルールと NAT ルールの構成

基本のネットワーク セグメントを決定したら、いくつかのファイアウォール ルールを作成する必要があります。すでに説明したように、デフォルトで構成されているルールはありません。前述のとおり、どちらのサービスでも利用者が使用できる多数のパブリック IP アドレスが付与されます。そのデフォルトの数は、サービスの種類によって異なりますが、いつでも増やすことができます。以下は、参考用として図示したネットワークを使用する場合に作成が必要になる可能性のあるルールの例です。

ルール	送信元	送信先
すべての送信を許可	内部：任意	外部：任意
プライベートからデスクトップへの送信を許可	192.168.50.0/24：任意	192.168.51.0/24：任意
デスクトップからプライベートへの送信を許可	192.168.51.0/24：任意	192.168.50.0/24：任意

注: Edge Gateway セグメントのすべての仮想マシンが、Edge Gateway をデフォルト ゲートウェイとして使用します。前述のルールを構成すると、すべてのセグメントが直接インターネットにアクセスでき、「プライベート」セグメントが「デスクトップ」ネットワークと通信できます。「DMZ」はどちらのアクセスでも拒否されます。

コンピュータがインターネットに直接アクセスできるようにするには、1 つ以上の送信元 NAT（SNAT）ルールも定義する必要があります。

タイプ	元の IP	元のポート	変換後の IP	変換後のポート
SNAT	192.168.50.0/24	任意	74.204.180.41	任意
SNAT	192.168.51.0/24	任意	74.204.180.41	任意
SNAT	192.168.52.0/24	任意	74.204.180.41	任意

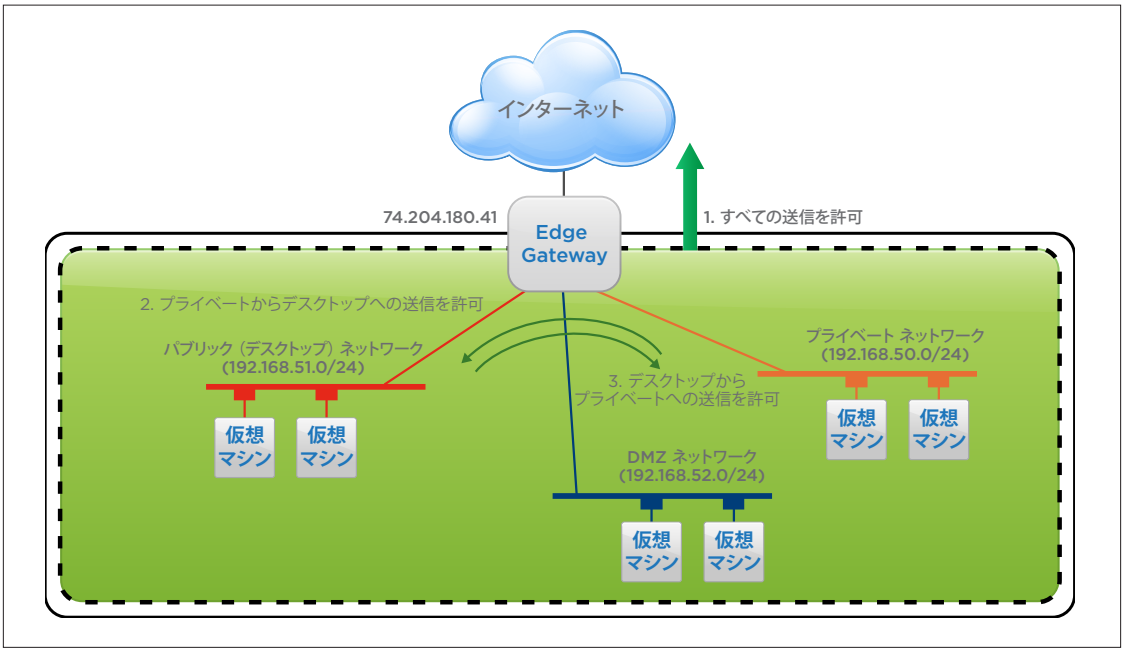

図 2：送信元 NAT ルールの定義

2.2 社内データセンターへのネットワークの接続

ここで説明している新しい vCloud Air ネットワークはインターネットにアクセスできます。デスクトップとプライベートの 2 つのネットワークは、先ほど定義したファイアウォール ルールにより、Edge Gateway を介して相互に通信することもできます。これでも実用になりますが、この時点ではまだ社内データセンターへの接続がありません。これらのネットワークの橋渡しとして、以下のオプションを使用すると、vCloud Air を社内データセンターに接続できます。

- IPsec VPN
- Direct Connect

このケース スタディでは、IPsec VPN を中心に説明します。vCloud Air Edge Gateway は、IPsec に準拠した任意の数の社内デバイスと連携できます。図 3 は、vCloud Air で構成された IPsec VPN の例です（IPsec VPN の構成の詳細については、こちらを参照してください）。

図 3： vCloud Air で構成された IPsec VPN

構成が完了すると、IPsec トンネルが確立されます。ただし、トラフィックが通過できるようにファイアウォール ルールを定義する必要があります。前述のとおり、デフォルトではルールは定義されていません。この使用事例では、vCloud Air のプライベート ネットワークから社内ネットワークへのトラフィックと、その逆のトラフィックを許可する必要があります。そのため、Edge Gateway のルールは次のようになります。

ルール	送信元	送信先
プライベートから社内への送信を許可	192.168.50.0/24：任意	192.168.110.0/24：任意
社内からプライベートへの送信を許可	192.168.110.0/24：任意	192.168.50.0/24：任意

これで、トラフィックがネットワーク間を正常に流れるようになります。このように構成することで、2 つのネットワーク間の、IPsec VPN トンネルを介した、ポート制限のない最も基本的な接続が実現します。

注：ブラウザまたは Web トラフィックを社内のプロキシ経由でルーティングする必要がある場合は、これを実行できるよう、「ローカル」の Web ブラウザを構成できます。vCloud Air Edge Gateway でネクスト ホップがスタティック ルートを経由するよう定義し、ファイアウォールと SNAT の当該ルールを削除することで、直接インターネット ルーティングに強制的に社内のゲートウェイを経由させることもできます。Edge Gateway が備える高度なネットワーク機能は柔軟性に優れているため、多種多様な要件に基づいて、希望するソリューションを作成できます。場合によっては、各種オプションと機能を使用した検証が必要になることもあります。

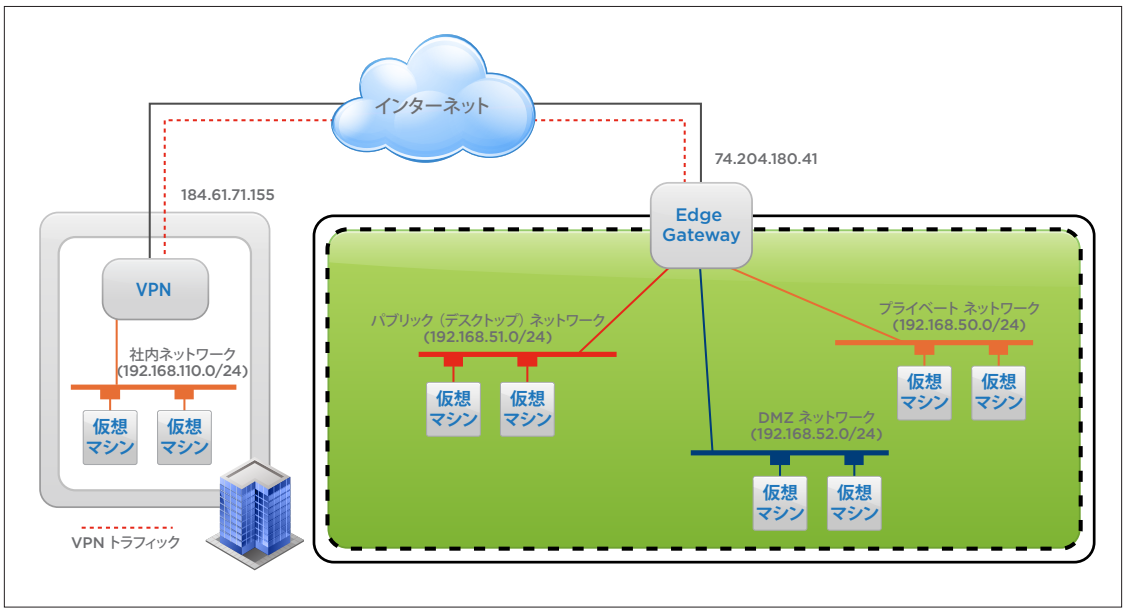

図 4：IPsec VPN トンネルを介したハイブリッド ネットワーク接続

2.3 ディレクトリ サービスと DNS サービスの導入

ここまでで、社内データセンターに接続された機能的な仮想データセンターを vCloud Air 内に構築できました。ファイアウォール ルールと VPN 接続を作成して構成しましたが、Microsoft Active Directory などのディレクトリ サービスと、DNS など、一部の基本インフラストラクチャ サービスが不足している可能性があります。このケース スタディでは、展開されたワークロードがまったくの新規で Microsoft Windows をベースとしているため、この環境は新しい Active Directory の「サイト」として扱う必要があると想定しています。グローバル カタログから Windows テンプレートを選択して、ドメイン コントローラに必要な仕様を満たすように構成したり、カスタム テンプレートをアップロードして展開することができます。

少なくとも、次の作業を完了するか考慮に入れる必要があります。

- 冗長仮想ドメイン コントローラを展開する。
  - 既存の企業ドメイン、セカンダリ ドメイン、または第 3 ドメインに参加する。
- 新しい Active Directory「サイト」を構成する。
  - vCloud ネットワークを Active Directory「サイトとサービス」に追加し、新しい「サイト」に割り当てる。
- Edge Gateway の代わりに新しいドメイン コントローラを DNS に使用するよう、vCloud ネットワークの設定を編集する。

vCloud ネットワークを構成したときに、DNS は Edge Gateway を使用するように設定されています。Active Directory と DNS をクラウド上に展開したら、この設定を、ローカル サーバを表すように変更することをお勧めします。このように変更することで、展開時に新しい仮想マシンの設定を 1 つずつ再構成しなくても、更新された設定が、クラウドに展開された新しい仮想マシンに反映されます。

いずれかのネットワーク セグメントの Edge Gateway 上に DHCP を構成した場合は、各 vCloud ネットワークで実施したこのオプションの変更が、その Edge Gateway で処理されるすべての DHCP リクエストに適用されます。

2.4 テンプレートと仮想マシンの移行

この時点で、社内 vSphere 環境から vCloud Air プライベート カタログに移行できるテンプレートを特定できます。VMware vCloud Connector® を活用すれば、手動による移行プロセスが容易になりますが、カタログ同期機能を使用して、このカタログや他の VMware インフラストラクチャ ベースのクラウド、および社内データセンターの間のテンプレートの同期と移行を自動化することでメリットが得られる可能性もあります。

また、vCloud Connector を使用して、ゲスト オペレーティング システムへの変更を最小限に抑えながら、既存の仮想マシンを vCloud Air に簡単に移行することもできます。仮想マシンの既存の IP アドレスや MAC アドレスを維持する必要がある場合は、データセンターの拡張機能を使用して実現できます。ただし、ほとんどの場合は、IP アドレスや MAC アドレスを変更してもアプリケーションに問題は生じません。

vCloud Connector サーバとノードの個々の機能とセットアップの方法の詳細については、VMware vCloud Connector のドキュメントを参照してください。vCloud Air には、事前構成済みのノードが用意されており、環境にノードを手動で展開して構成する必要がありません。各クラウドのノードと安全に通信するには、vCloud Connector サーバを社内に導入し、インターネットへのアクセスを設定する必要があります。

注：本書では触れていませんが、各組織は Windows Server ライセンスの可搬性について理解し、その条件を遵守する必要があります。Windows ライセンスの移動に関する条件により、現時点では、組織が自社ライセンスを移動できるのは、vCloud Air Dedicated Cloud 内のみです。

まとめ

物理データセンターで一般的に必要とされる基本的なネットワーク サービスおよびインフラストラクチャ サービスを提供することが、アウトソーシング型データセンター構築の基盤になります。このようなソフトウェア定義のインフラストラクチャおよびサービスの構成と、従来型モデルとの顕著な違いは、これまでの方法では数日から数か月かかった作業を、VMware vCloud Air では数時間で完了できる点です。また、アプリケーションからインフラストラクチャ レイヤーが分離されているため、ビジネスと IT においてこれまでにないレベルの俊敏性を達成できます。これらのタスクが完了した後は、リソースのプールを迅速かつ信頼性の高い方法で活用して、新規ワークロードの展開や既存ワークロードの移行を簡単に実行できます。

執筆者について

Chris Colotti は、vCloud Air チームの主任テクニカル マーケティング アーキテクトです。Chris は 10 年以上にわたり、IT ハードウェアおよびソフトウェア ソリューションの分野に携わってきました。また、ダニエル ウェブスター大学で情報システムの学士号を取得しています。VMware に入社する前は、ニューハンプシャー南部の Fortune 1000 に数えられる企業でシステム アーキテクトと管理者を務め、新しいアプリケーションの展開をサポートする VMware ソリューションを設計していました。VMware では、コンサルティング アーキテクトの役職に就き、パートナーとお客様が VMware のソリューションを実践できるようにサポートし、データセンターの移行から長期にわたる常駐のアーキテクチャ サポートまで、さまざまなお客様プロジェクトのコンサルティングにあたってきました。Chris は現在、VMware vCloud Air への移行を望んでいる vSphere のお客様を対象に、最新の vCloud Air ソリューションおよびアーキテクチャの推進に取り組んでいます。また、Chris は、VMware Certified Design Expert（VCDX #37）でもあります。

ヴイエムウェア株式会社 〒105-0013 東京都港区浜松町1-30-5 浜松町スクエア 13F www.vmware.com/jp
Copyright © 2014 VMware, Inc. All rights reserved. 本製品は、米国および国際的著作権法および知的財産法によって保護されています。VMware 製品は、http://www.vmware.com/go/patents のリストに表示されている 1 件または複数の特許対象です。VMware は、米国およびその他の地域における VMware, Inc. の登録商標または商標です。他のすべての名称ならびに製品についての商標は、それぞれの所有者の商標または登録商標です。
アイテム No.： VMW-TWP-vCLOUD-AIR-SB-A4-102 2014/10