

取扱注意

大阪大学仮想サーバホスティング 利用ガイド

平成 30 年 3 月

大阪大学

情報推進部情報基盤課

目次

1.	はじめに.....	3
2.	仮想サーバホスティングの概要	3
3.	仮想サーバホスティング利用方法.....	3
3. 1	概要.....	3
3. 2	リソース.....	3
3. 3	ゲスト OS.....	3
3. 4	ネットワーク	4
3. 5	ストレージ.....	4
3. 6	セキュリティ	4
3. 7	ファイアウォール・負荷分散装置	5
3. 8	バックアップ	5
4.	システムの保守運用.....	5
5.	おわりに.....	5

1. はじめに

本利用ガイドでは、大阪大学仮想サーバホスティングサービス（以降 仮想サーバホスティングと記述）が提供する仮想マシン環境等の利用方法を解説しています。

2. 仮想サーバホスティングの概要

仮想サーバホスティングは、学内の基幹システムや各種アプリケーションシステムの構築に必要なハードウェアを仮想化技術によって効率よく利用できるようにしています。基本的な構成としては、サーバ（CPU、メモリ、ローカルストレージ）、ネットワーク、ネットワークアクセスストレージといったハードウェアを VMware vSphere により仮想マシン（VM）として利用可能にしています。ネットワークは、サービスセグメント、管理・バックアップセグメント、ストレージセグメントの3つの VLAN セグメントのいずれかを用いて構成し、ODINS（大阪大学キャンパスネットワーク）を經由して外部のネットワークとの接続が可能です。その他、仮想サーバアプリケーションで共同利用する負荷分散装置の利用が可能です。

3. 仮想サーバホスティング利用方法

3. 1 概要

仮想サーバホスティングでは、VMware vSphere ESXi6.0 update 1 を利用して VM 環境を提供しています。基本的な手順は次の通りです。

- ① ゲストシステムを稼働させるために必要な VM と CPU、メモリ、ストレージ等のそれぞれの VM に必要なリソースを申請してください。その申請に基づいて運用担当が VM を作成します。（様式 1. 大阪大学仮想サーバホスティングサービス申請書）
- ② 作成された VM 上に OS、ミドルウェア、アプリケーション等のソフトウェアをインストールし、ゲストシステムを構築してください。

※OS として CentOS を希望する場合は、その最新版でのインストール作業およびネットワークに関する基本的な初期設定を運用担当が行うことが可能です。

3. 2 リソース

1VM 当たり CPU は 24 コア、メモリは 128GB、ストレージは 500GB の制限を設けます。ただ、それを下回るリソースであっても仮想化システムの運用状況により希望されるリソースを用意できない場合もありますので、まずは運用担当者までご相談ください。

3. 3 ゲスト OS

ゲスト OS として Linux、Windows 等の OS が利用可能です。利用可能な OS の詳細は運用担当にご相談ください。なお、OS のインストールは仮想サーバホスティングシステムの管理系ネットワーク内で行う必要があるため、運用担当と調整の上、サイバーメディアセン

ターでの作業をお願いします。

3. 4 ネットワーク

ネットワークインタフェースとして、サービス用、管理・バックアップ用、ストレージ用の3セグメントがあります。これらはプライベートネットワークで構成しており、ファイアウォール装置（以下、FW）によりサービス用ネットワークをグローバルアドレスにNATすることで、ODINSを経由した外部ネットワークとの接続が可能となります。（付録1参照）なお、FWに関しては「3. 7 ファイアウォール・負荷分散装置」を参照ください。用途に応じて必要なネットワークインタフェースを事前に申し出て、ご相談ください。

3. 5 ストレージ

ストレージは基本的にローカルストレージが申請に応じて割り当てられます。DBMSのライセンスや性能条件等で仮想ストレージが利用できない場合や大容量のストレージが必要な場合は、ゲストシステムから直接マウントできるネットワークアクセスストレージを提供しますので、運用担当に相談してください。

3. 6 セキュリティ

仮想サーバホスティングシステムはVLAN環境に構築されており、共通のFW装置で守られていますが、OS等のセキュリティ設定はゲストシステムで行ってください。基本的なセキュリティ設定は以下のポリシーに従ってください。

- ・ 不要なサービスは起動したままの設定にしないこと。
- ・ ファイル、ディレクトリへの適切なアクセス制御をすること。
- ・ 仮想サーバでのアクセス制御機構（firewalld、.htaccess等）を設定し、不要なIPアドレスからのアクセスとポートへのアクセスを遮断すること。
- ・ 外部公開しているサービス（apache等）に関しては、そのアプリケーションやミドルウェアに特化した攻撃を防ぐよう対策すること。加えて、セキュリティアップデート情報に注意し、初期設定時だけでなく、適宜バージョンアップ及びパッチの適用を実施すること。
- ・ 不要なアカウントの削除や管理者権限をもつアカウントでのアクセス制限等、ゲストシステムで発行するアカウントは適切に管理すること。
- ・ アカウント認証にパスワードを利用する場合は、文字数や文字種別等のルールを強固なものに設定すること。また、必要に応じてアカウントロック機能も設定すること。
- ・ 認証後のアカウントにシステムを利用させるか否かの制御（認可）も適切に行うこと
- ・ 使用しているソフトウェアに関する各種ログは、最低1年以上は保存し、必要となっ

た際に調査可能な環境としておくこと。また、運用担当者からの調査依頼には、ログからの情報を元に報告を行うこと。

- ・重要な情報に関しては、保存時・通信時ともに十分な暗号強度で暗号化を施すこと。
- ・遠隔保守用に ssh アクセスする際は公開鍵認証に限定し、パスワード認証を許可しないように設定したうえで、root アカウントを用いたログインを禁止すること。また、ssh 以外のプロトコルを使用する場合もそれと同等の機能を有する設定とすること。

3. 7 ファイアウォール・負荷分散装置

FW 装置では内向き・外向きとも通信を制限しています。デフォルトで許可されている通信は仮想サーバホスティングのサーバから外部の Web サーバへアクセスする外向きの http(s) 通信のみです。サービス提供に必要な通信許可設定がある場合は、運用担当まで事前に申し出の上、ご相談ください。FW 装置の設定は運用担当が実施します。

負荷分散装置では、複数のアプリケーションサーバ (VM) へのトランザクション振分けポリシー等をゲストシステム毎に設定できますので、必要に応じて運用担当にご相談ください。負荷分散装置の設定は運用担当が実施します。

3. 8 バックアップ

VM 環境については、構築時にシステムイメージを取得しますので、構築完了後のサービス開始前にご連絡ください。また、要望に応じて設定変更時にバックアップを取得しますので、運用担当に相談してください。また、ゲストシステムで必要なデータのバックアップは、利用者で行っていただきます。

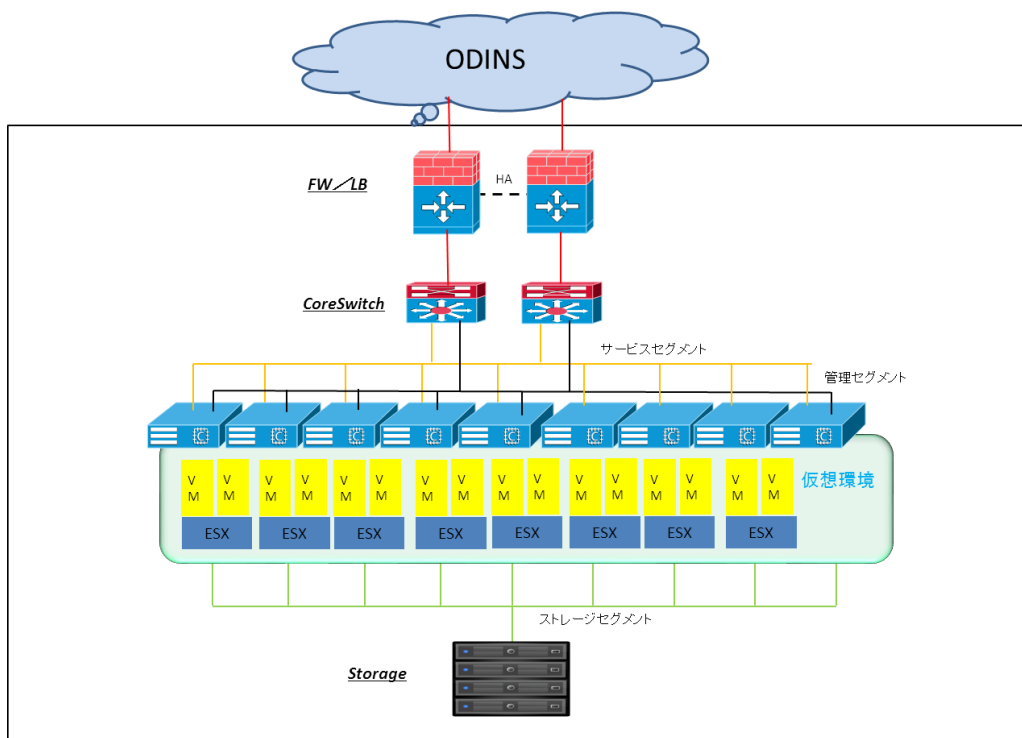
4. システムの保守運用

ハードウェア及び VM の障害監視については、運用担当で実施しています。アプリケーションのプロセス監視等、ゲストシステムで監視が必要なものがありましたら、ゲストシステムで監視ツール等を組み込んでください。また、障害発生時は、運用担当とゲストシステム運用担当が協力して障害原因の切り分けを行いますので、ゲストシステムの保守体制を整備し、連絡窓口を報告してください。

5. おわりに

本利用ガイドは、仮想サーバホスティングの基本的な利用法等について説明しています。障害連絡、不明な点や要望がありましたら、次ページに記載の運用担当にお問い合わせください。

付録 1 大阪大学キャンパスクラウドシステム構成図



Firewall / Load Balancer : F5 BIG-IP ADF-2200S

CoreSwitch : Cisco Nexus 5548UP

Main Host : Cisco UCS C240 M3, Cisco UCS C220 M4

Storage : EMC VNX5200

Hypervisor : VMware ESXi 6.0 update 1b

大阪大学キャンパスクラウド運用担当

情報推進部情報基盤課研究系システム班

メールアドレス : cc-admin@ml.office.osaka-u.ac.jp

内線 : 7951, 7952, 3864