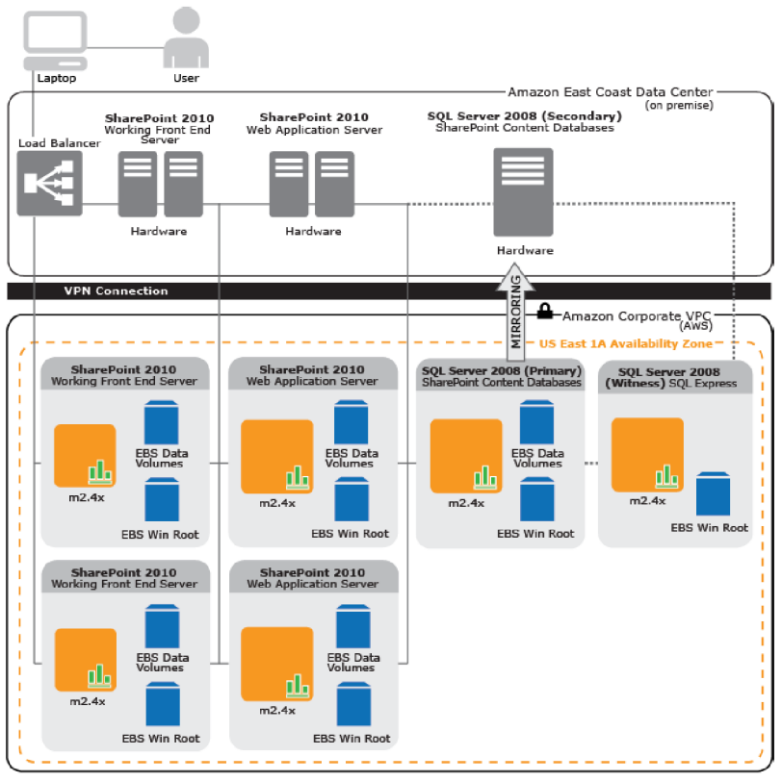
Microsoft SharePoint Server on AWS
リファレンスアーキテクチャー

2012/5/24

アマゾンデータサービスジャパン株式会社

AmazonにおけるSharePointの利用事例

AWS利用によるメリット



インフラの調達時間
　→４～６週間から数分に短縮

サーバのイメージコピー作成
　→手動で半日から、自動化を実現

年間のインフラコスト
　→オンプレミスと比較して22%削減

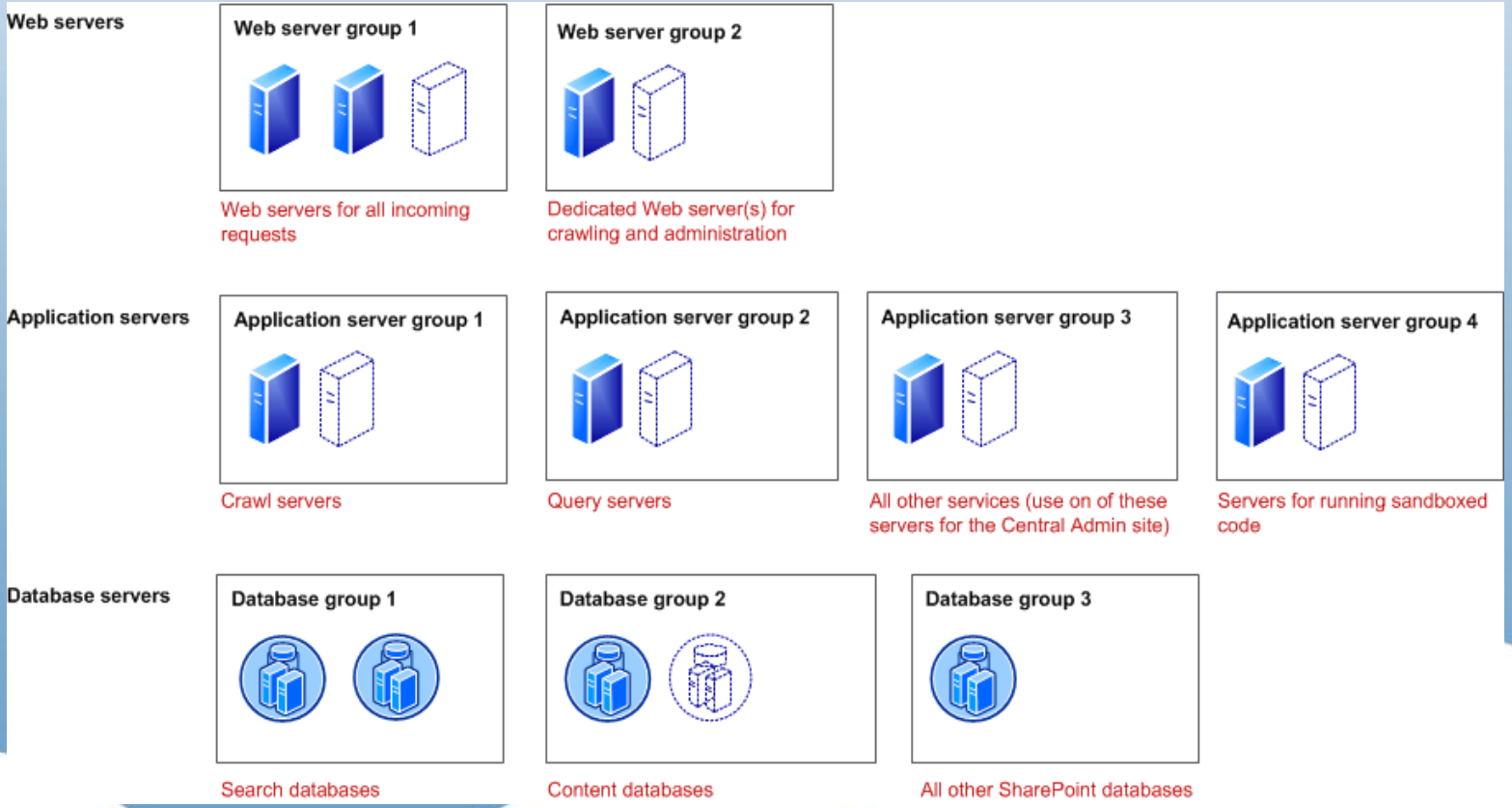
物理サーバの運用や導入時の工数
　→ゼロ

ライセンス
　→ライセンスのクラウド環境への
　　持ち込み（BYOL)に対応

http://d36cz9buwru1tt.cloudfront.net/AWS_Amazon_SharePoint_Deployment.pdf

amazon web services™

SharePoint Serverファーム リファレンスアーキテクチャー



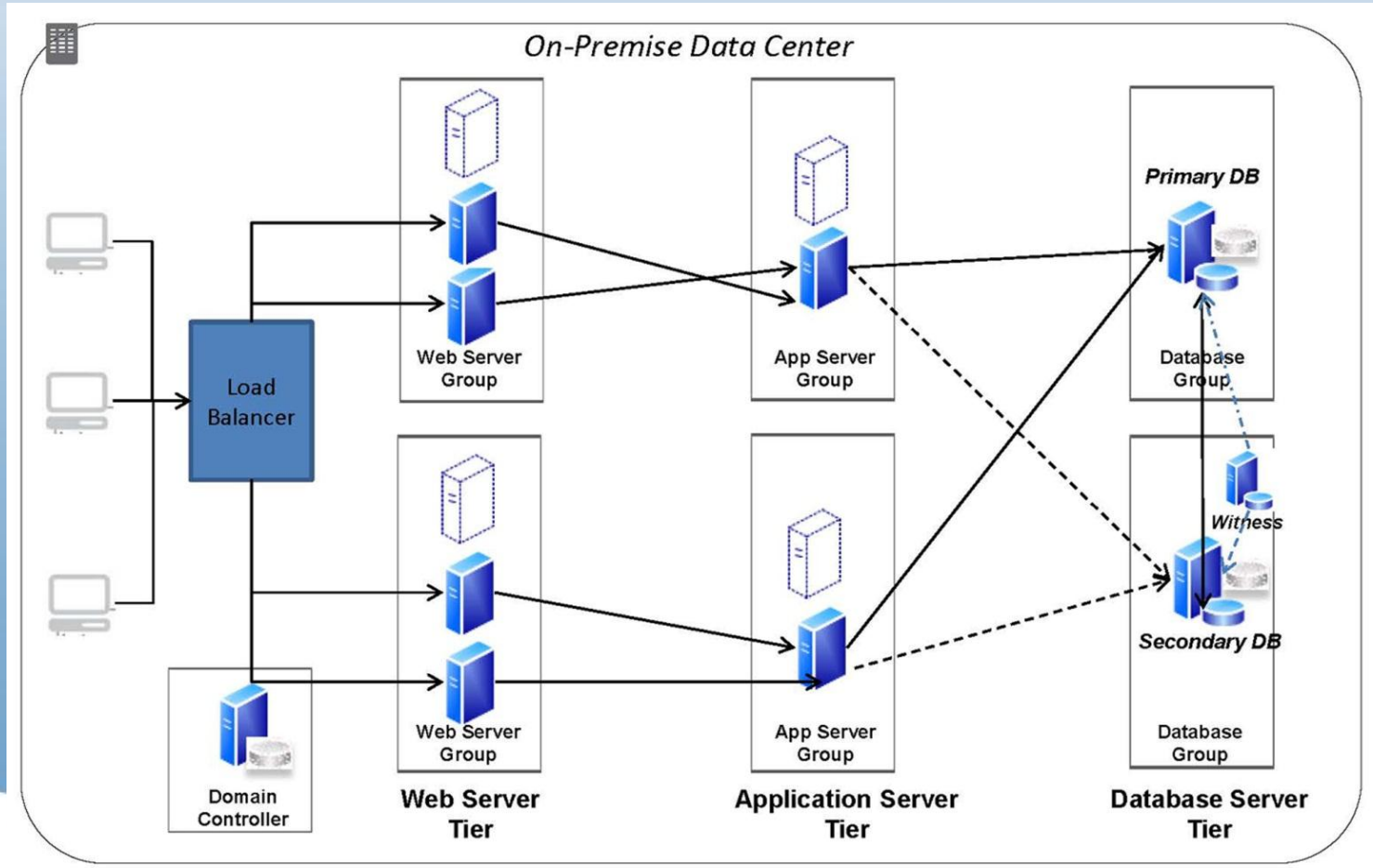
amazon web services™

その他必要なコンポーネント

- Active Directory ドメインサービス
  - SharePoint ServerはID認証の仕組みとしてAD DSを必要とする。AD DS（1台もしくはそれ以上のドイメインコントローラー）がSharePoint Serverファームと同じネットワークにあり、SharePoint Serverファームからアクセス可能になっている必要がある
- 脅威管理と侵入検知
  - このコンポーネントはエクスターナルまたは一般公開のSharePoint Serverのシナリオにおける追加要素として導入される。Windowsベースの環境ではこのコンポーネントは Microsoft Forefront® Threat Management Gateway 2010 などの製品により提供される

amazon web services™

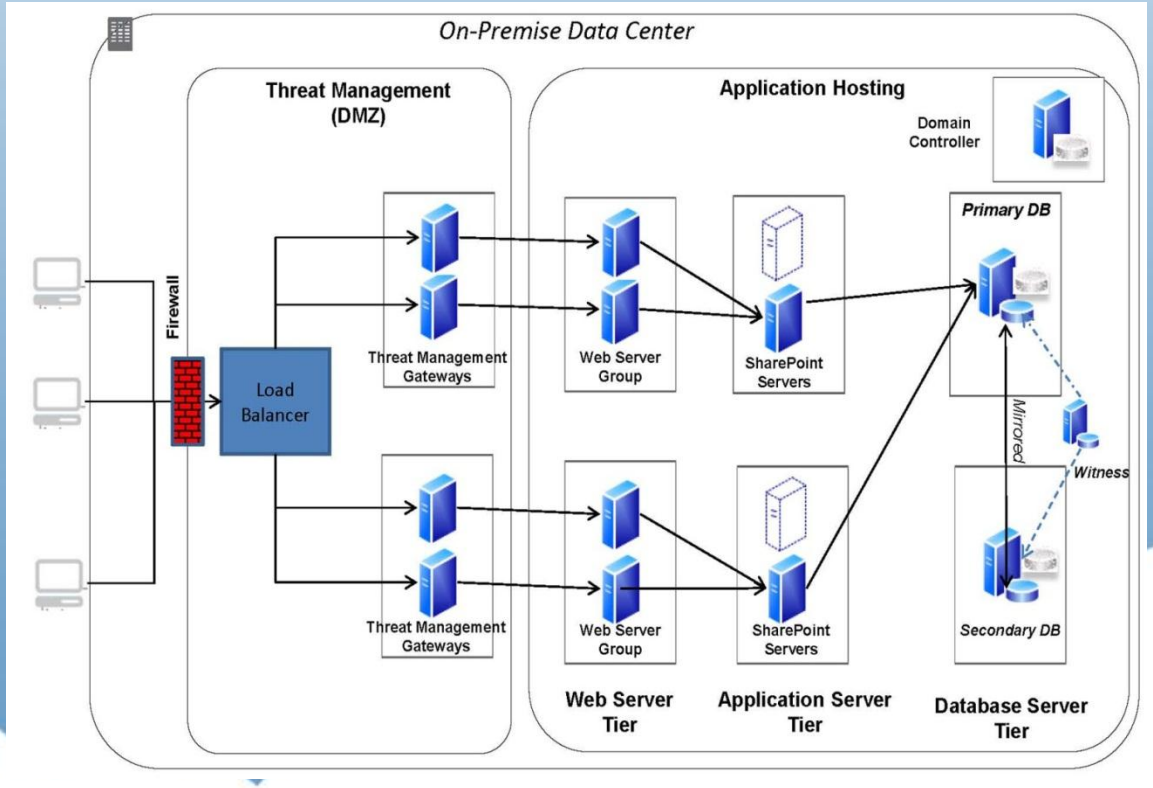
イントラネットにおけるSharePoint Server ファーム構成例



amazon web services™

インターネットWebサイトまたはサービスベースのSharePoint Server

- DMZにファイヤーウォールと脅威管理の機能を提供
- Active Directoryドメインコントローラーをファーム内に配置



amazon web services™

AWSにおけるSharePoint Server 実装のアーキテクチャーシナリオ

- ネットワークのセットアップと構成
- サーバーのセットアップと構成
- セキュリティ
- デプロイメントと管理

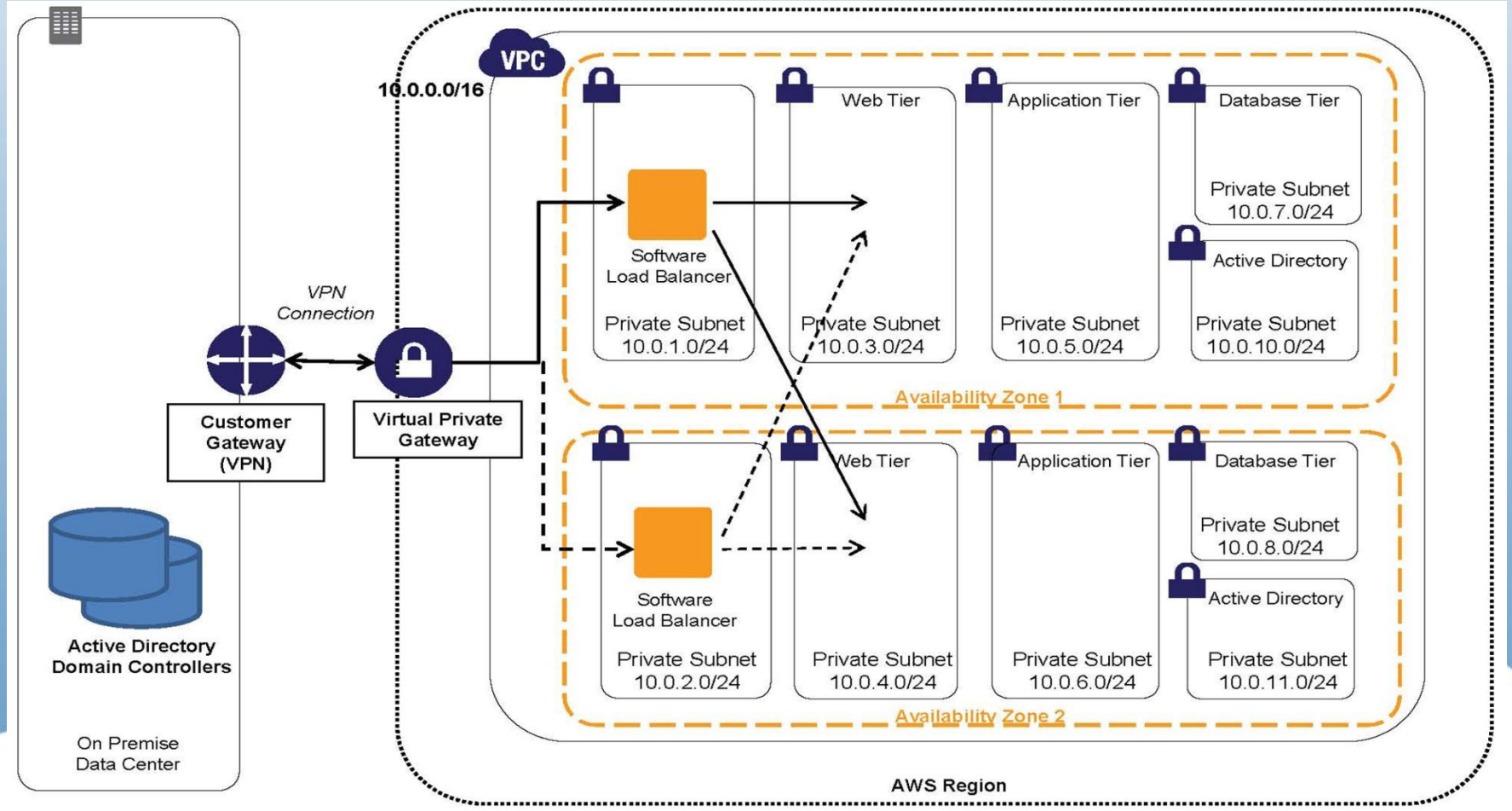
amazon web services™

ネットワークの設定

- Amazon Virtual Private Cloud
  - SharePoint Serverファームを展開するための独立したネットワーク
  - VPNのみのイントラネットシナリオではパブリックサブネット不要
- ロードバランサー
  - Elastic Load Balancing （ELB）
  - サードパーティソフトウェア
    - Riverbed Stingray Traffic Manager
    - HAProxy

amazon web services™

イントラネットシナリオでのネットワーク構成

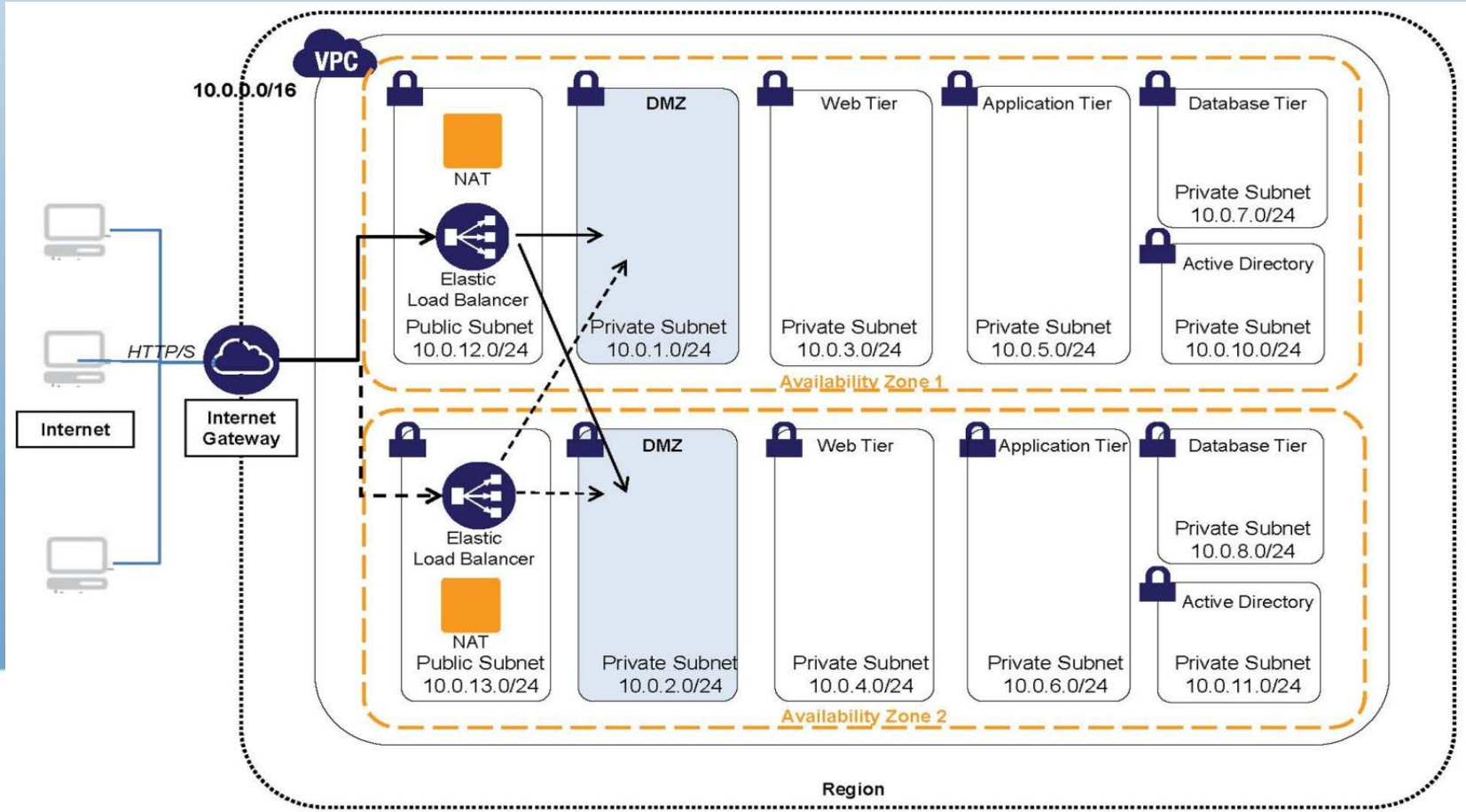


amazon web services

イントラネットシナリオでのVPC構成

- 特定のAWSリージョンに作成されたひとつのVPC に複数のアベイラビリティゾーンにまたがってコンポーネントを構成
- それぞれのアベイラビリティゾーンのプライベートサブネットにロードバランサーを配置
  - それぞれのアベイラビリィゾーンにソフトウェアロードバランサー
- それぞれのアベイラビリティゾーンのプライベートサブネットにWeb、アプリケーション、データベースサーバーおよびAD DSドメインコントローラー
- Virtual Private GatewayおよびCustomer Gateway

インターネットに接続されたパブリックWebサイトのシナリオでのネットワーク構成



パブリックWebサイトのシナリオでのVPC構成

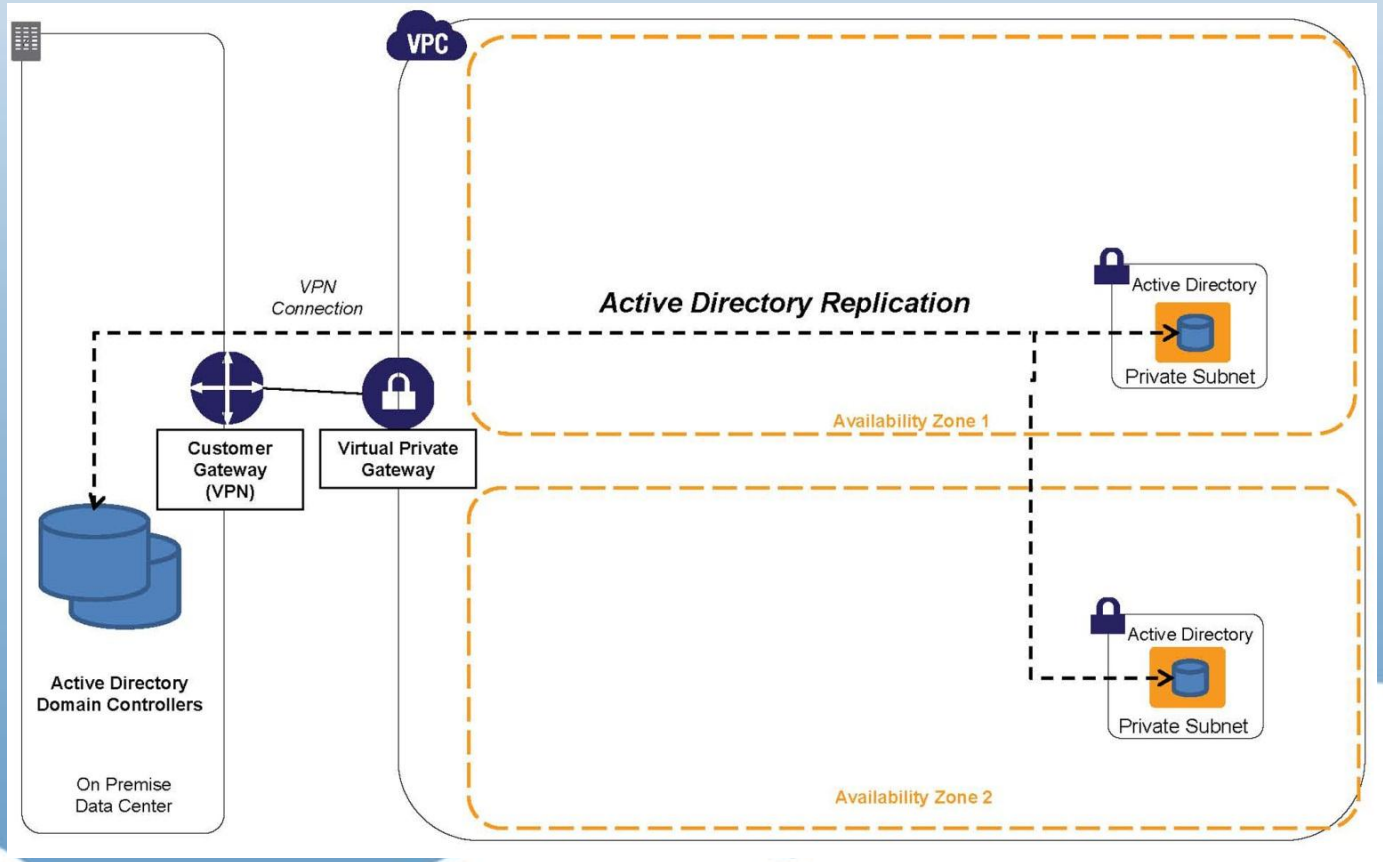
- パブリックWebサイトのシナリオでは、企業内データセンターに接続する必要はないためVPN接続は不要
  - VPN接続の必要がないため、Virtual Private Gatewayが不要
- Elastic Load Balancer（ELB）が利用可能
  - ユーザーがインターネット経由でアクセスできるようにロードバランサーはパブリックサブネットに配置する必要がある
- Web、アプリケーションおよびデータベースサーバーはプライベートサブネットに配置し、ロードバランサー経由でのみアクセス
- ファイヤーウォールおよび脅威管理のための追加コンポーネント
- それぞれのアベイラビリティゾーンにNATインスタンスを追加

AD DSのセットアップとDNS構成

- 以下の二種類のシナリオが選択可能
  - SharePoint ServerインスタンスはVPN-VPC接続を通じて企業内のデータセンターに接続し、オンプレミスのドメインコントローラーで認証可能
  - ドメインコントローラーをAWSに配置し、VPN-VPC接続によりオンプレミスのドメインコントローラーとレプリケーションが可能。それによりAWS内のドメインコントローラーで認証可能になり企業内のユーザーIDが使用できる
- Active Directory Replication Over Firewalls
  - http://social.technet.microsoft.com/wiki/contents/articles/584.active-directory-replication-over-firewalls.aspx

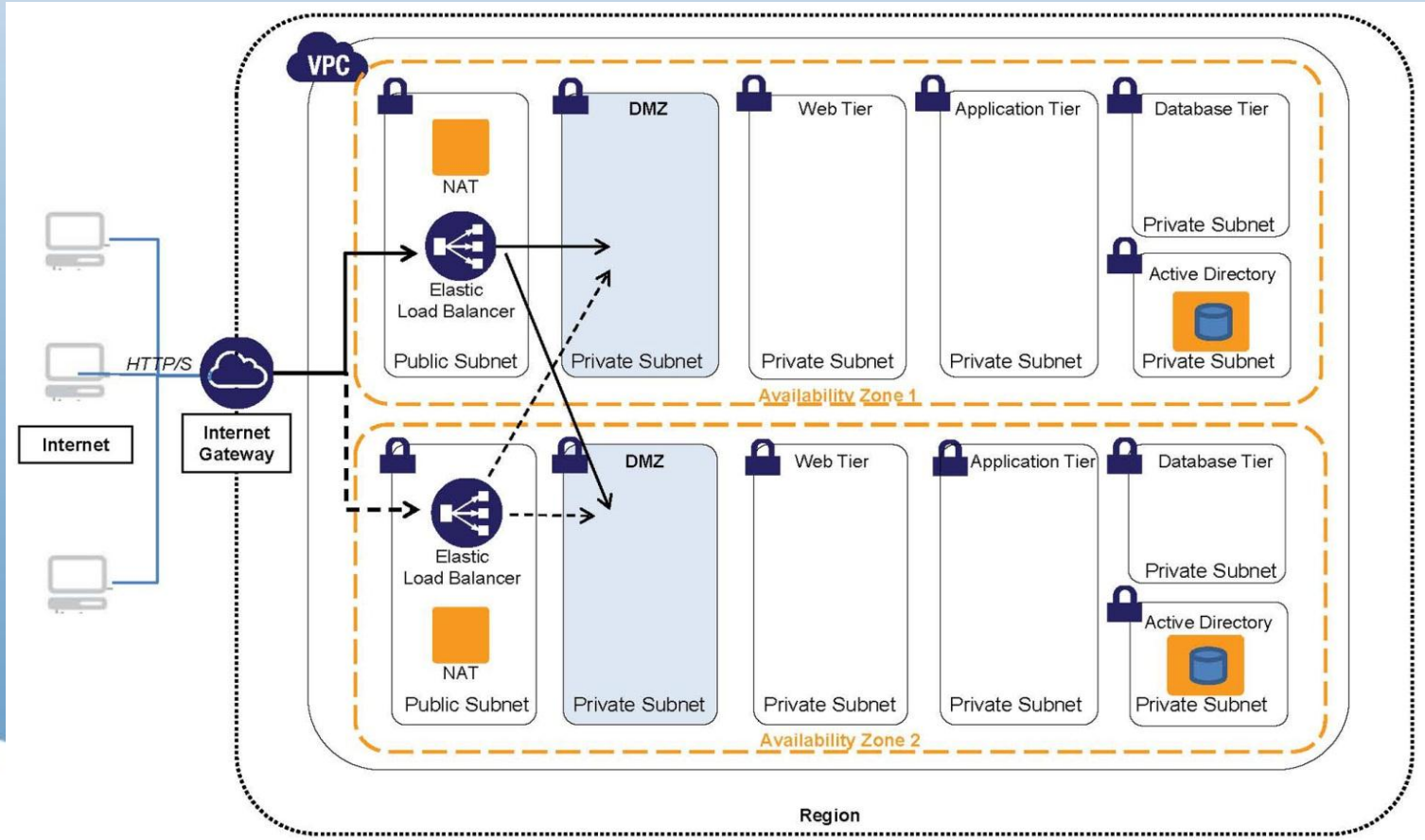
amazon web services™

イントラネットシナリオでのAD DSのレプリケーション



amazon web services™

冗長性と高可用性を実現するアベイラビリティゾーンでのドメインコントローラーの配置



amazon web services™

SharePoint Serverロールによる EC2 AMIとインスタンスタイプの選定

Table 1: SharePoint Serverロールとティアによる最小システム要件

Tier/role	Scenario	Processor	RAM	Hard disk
Web/Application Tier	All	64-bit, 4 core	8 GB	80 GB
Database server	Small deployment	64-bit, 4 core	8 GB	80 GB
Database server	Medium deployment	64-bit, 8 core	16 GB	80 GB
Domain controller	All	64-bit, 4 core	8 GB	80 GB

Table 2: 最小システム要件からのAMIとWindowsインスタンスタイプのマッピング

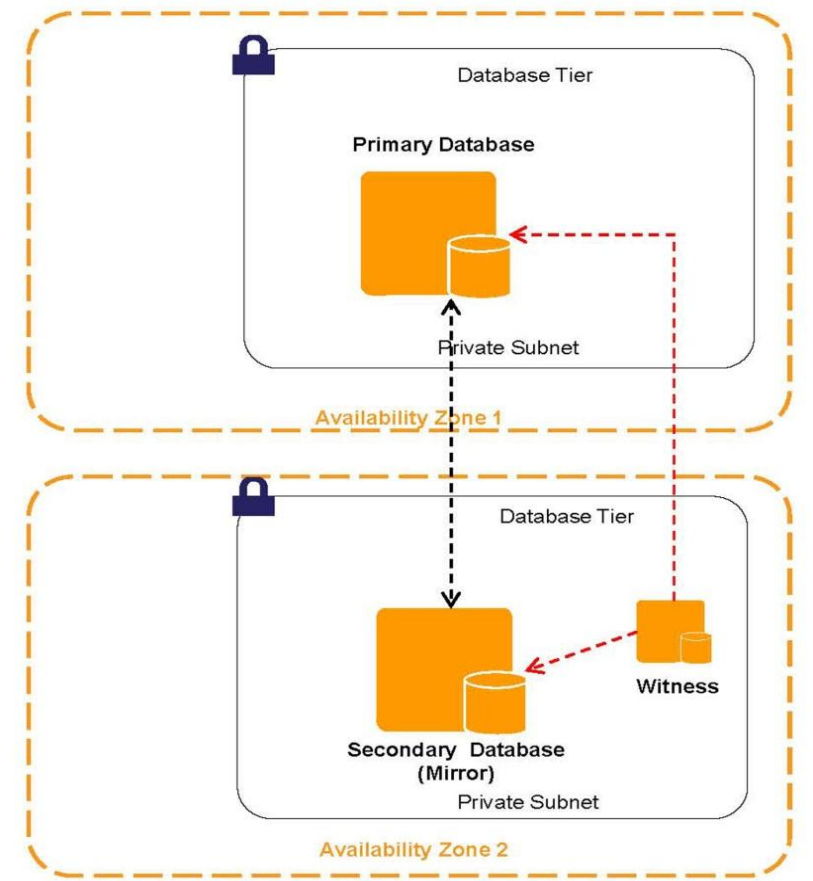
Tier	Applicable Amazon EC2 instance type and range	AMI to use
Web front end	Extra Large (m1.xl)	Windows Server 2008 R2 + IIS
Application server	Extra Large: High Memory Quad Extra Large (m2.xl–m2.4xl)	Windows Server 2008 R2
Database server	High Memory Quadruple Extra Large (m2.4xl)	Optimized SQL Server 2008 R2 AMIs from Microsoft
Domain controller	Extra Large (m1.xl)	Windows Server (in the role of a domain controller)

amazon web services™

SQL Serverの構成

- SQL ServerのためのEBSディスク構成
  - 複数のEBSボリュームにSQL Serverのデータコンポーネントを適切に配置することでパフォーマンスを最適化
  - ソフトウェアRAIDによるストライピングでEBSのIOPSをさらに向上させることが可能
- SQL Serverの高可用性
  - 複数アベイラビリティゾーンでのSQL Serverミラーリングにより SQL Serverの高可用性を実現することが可能

複数アベイラビリティゾーンでのSQL Serverミラーリング

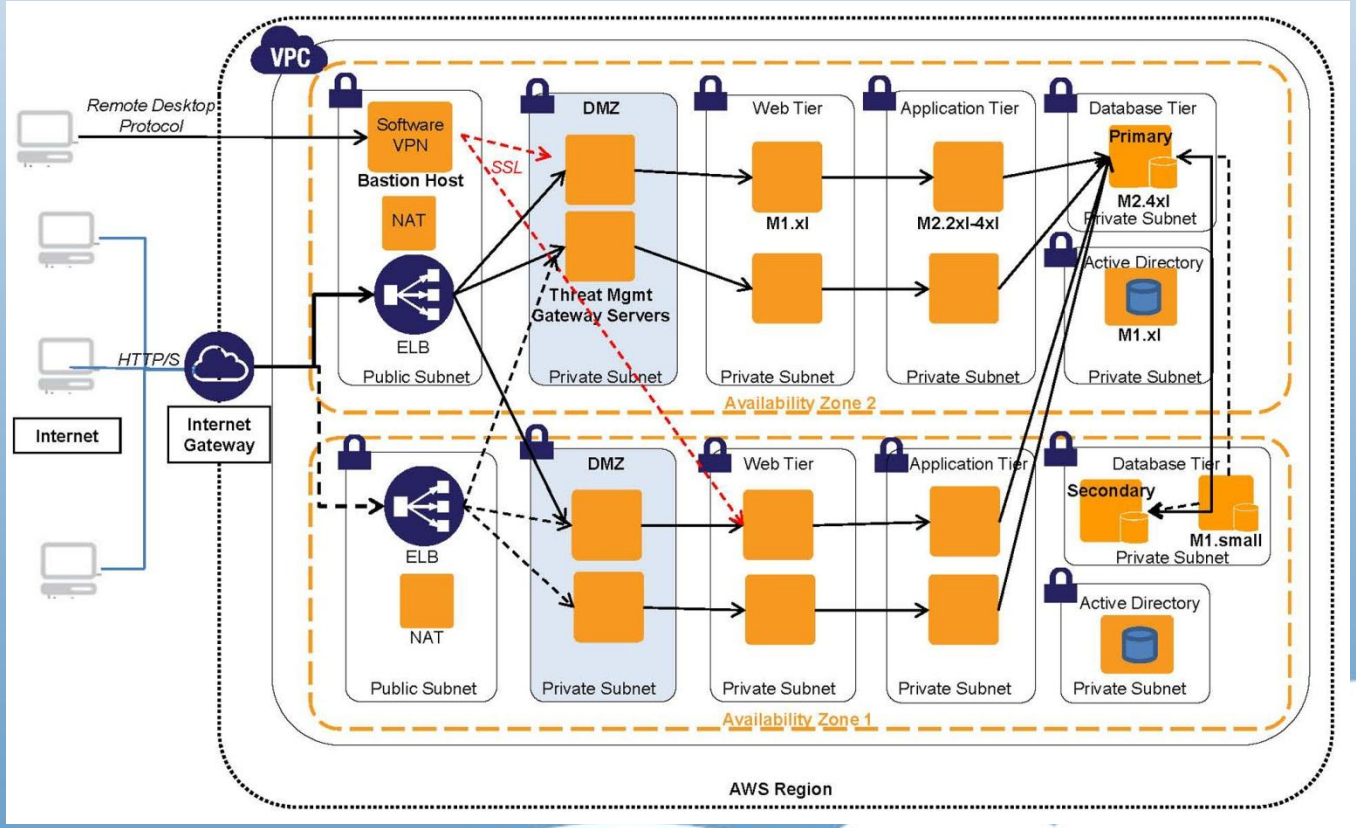


amazon web services™

セキュリティ

- セキュリティグループ
  - インスタンスレベルでのセキュリティにより、レイヤーごとにセキュリティを設定
    - Elastic Load Balancing
    - Web
    - データベース
- ネットワークACL
  - サブネットレベルでのセキュリティ
- Windowsインスタンスのセキュリティ
- 管理者アクセス
  - Bastion host（要塞ホスト）からのアクセス

RDPを使用したbastion host（要塞ホスト）からのアクセス



amazon web services™

データプライバシー

- EBSボリュームの暗号化機能は標準でサポートされないものの、以下の暗号化のテクノロジーを利用することが可能
  - 暗号化ファイルシステム（EFS）
  - BitLockerドライブ暗号化
  - SQL Server Transparent Data Encryption （TDE）
  - サードパーティのEBSボリューム暗号化
- 暗号化キーのセキュアな管理と認証が必要

デプロイメント

- AWSはデプロイメントのための以下のツールを提供
  - AWS Management Console
  - AWS API Tools
  - サンプルコードとライブラリー
  - AWS CloudFormation
- カスタムAMIを作成することによってデプロイメントの自動化が容易

amazon web services™

監視と管理

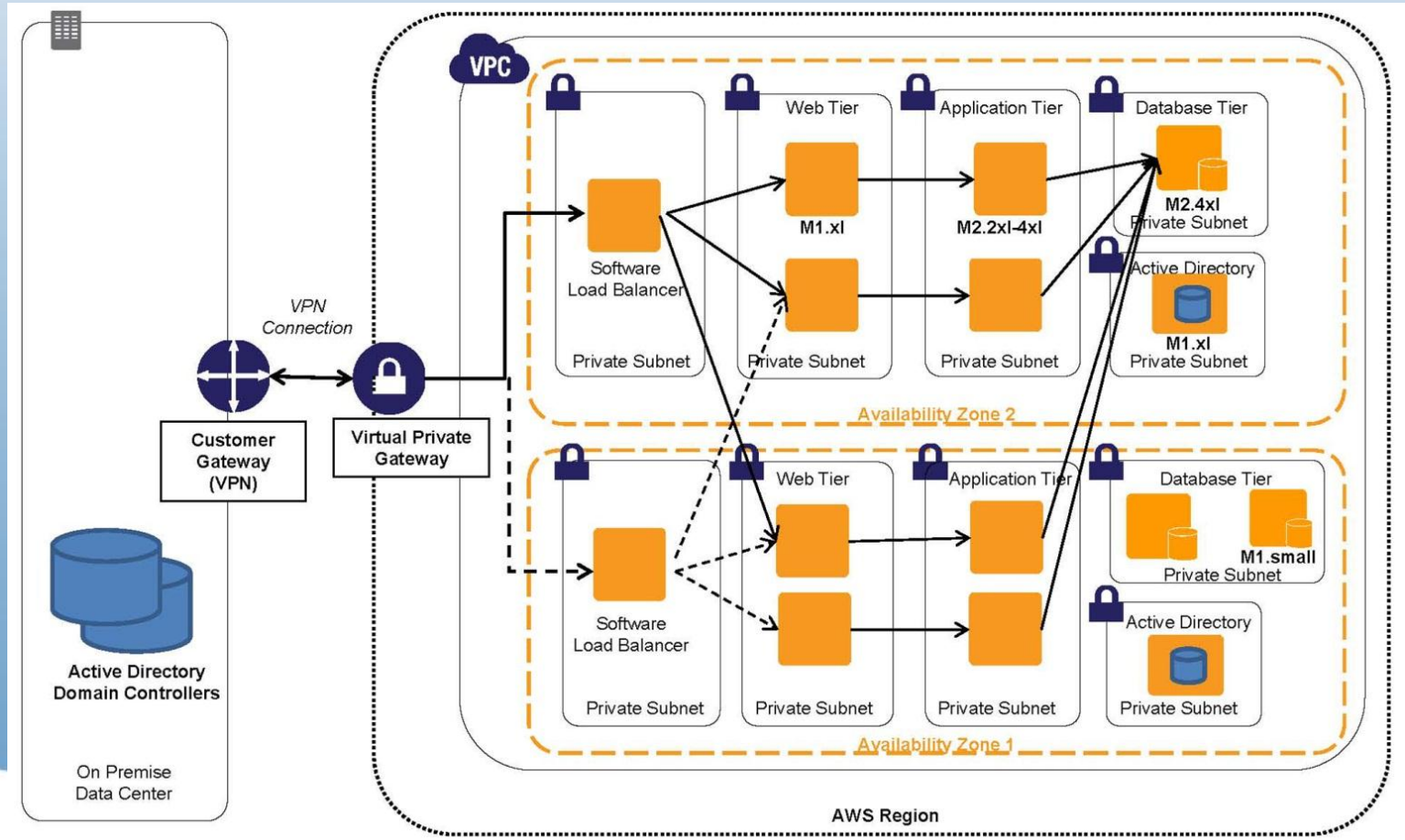
- Amazon CloudWatch
  - CPU使用率、ディスクI/Oなど
  - カスタムメトリックスの作成が可能
- Microsoft System Center Operations Manager
  - Windows Server、SharePoint Server、およびSQL Serverの監視と管理が可能

amazon web services™

バックアップリカバリー

- 以下の要件をもとにしたバックアップ計画
  - RTO（目標復旧時間）
  - RPO（目標復旧地点）
- 二つのアプローチから選択可能
  - SharePoint ServerとSQL Serverのバックアップツールを利用
  - EBSスナップショットなどの仕組みを利用

AWSにおけるイントラネットSharePoint Serverファーム



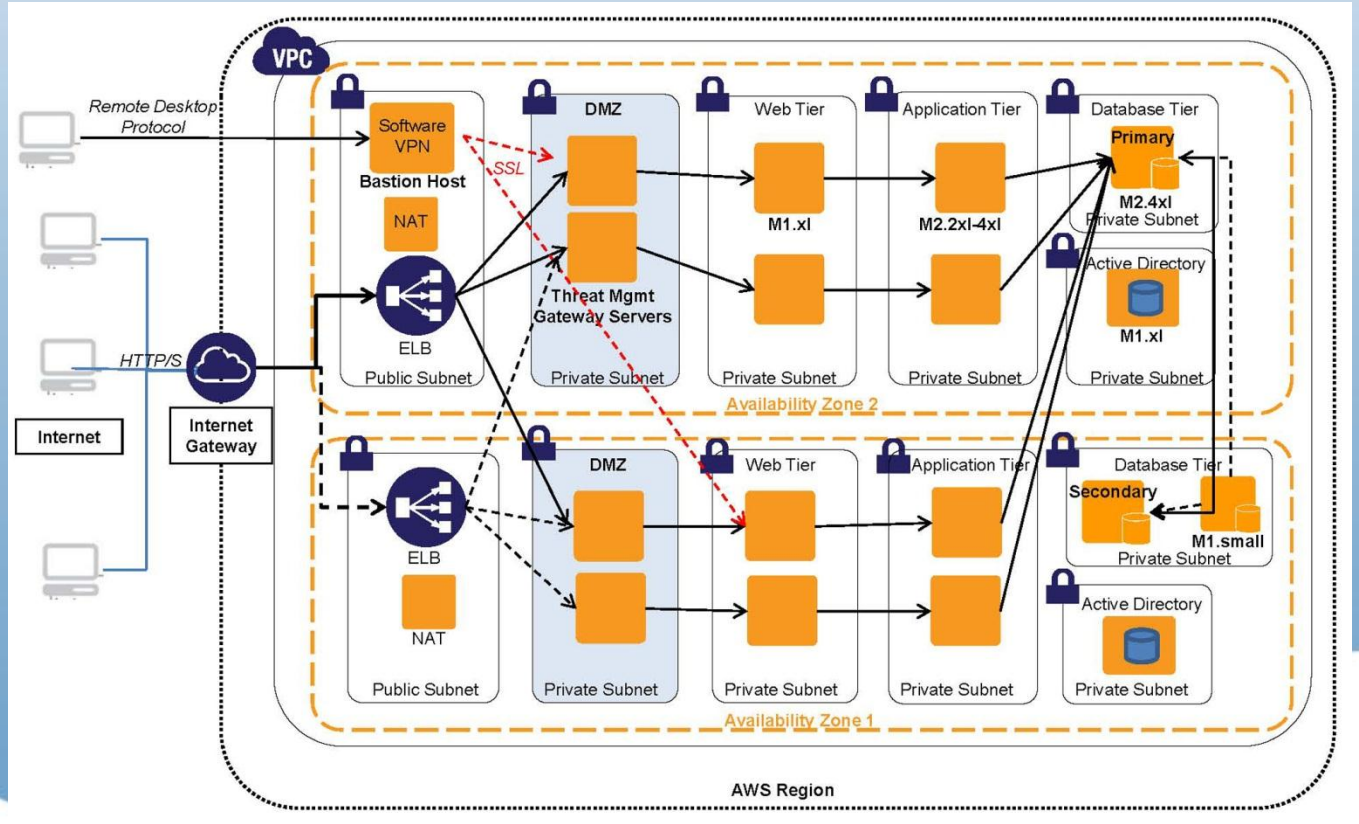
amazon web services

イントラネットのSharePoint Serverファーム

- Amazon VPCと企業内データセンターとのVPN接続
- 企業内ネットワークへVPN接続するプライベートサブネットのみ
- ２つのアベイラビリティゾーンによりアベイラビリティゾーン障害の稀な可能性にも対応
- Webフロントエントサーバーをまたいだソフトウェアロードバランサーの配置
- アベイラビリティゾーンをまたいだSQL Serverのミラーリング 構成
- データベース (EBS ボリューム) スナップショットによるバックアップ

amazon web services™

AWSにおけるインターネット公開Webサイトでの SharePointサーバー



amazon web services™

インターネット公開Webサイトの SharePoint Server

- Amazon VPCによるパブリックおよびプライベートサブネット
- パブリックサブネット上のThreat management gateway（TMG）サーバー
- TMGサーバーをまたいだElastic Load Balancer（ELB）
- パブリックサブネット上の要塞ホストでソフトウェアVPNをホストし内部のインスタンスへの管理者アクセス
- TMGサーバーの背後、プライベートサブネット内のアベイラビリティゾーン内に複数のWebフロントエントサーバー
- AWS内のAD DSドメインコントローラーによるユーザー登録および認証

amazon web services™

まとめ

- イントラネットおよび公開Webサイトのそれぞれのシナリオで、SharePoint ServerをAmazon Web Servicesによるクラウド上で稼働させることが可能
- AWSが提供するネットワーク、サーバー、セキュリティ、展開の機能によりSharePoint Serverがセキュアかつ容易な管理を実現

amazon web services™

参考情報

- Microsoft on AWS
  - http://www.awsmicrosite.com
- Amazon EC2 Windows Guide
  - http://docs.amazonwebservices.com/AWSEC2/latest/WindowsGuide/Welcome.html?r=7870
- AWS Windows and .NET Developer Center
  - http://aws.amazon.com/net
- Microsoft License Mobility
  - http://aws.amazon.com/windows/mslicensemobility

amazon web services™