AWS Summits 2014

Active Directory on AWS

アマゾン データ サービス ジャパン株式会社
吉松 龍輝

2014 年 7 月 17 日

Session #TA-04

amazon web services

自己紹介

- 名前
  - 吉松 龍輝（よしまつ りゅうき）
- 所属
  - アマゾン データ サービス ジャパン株式会社
  - エンタープライズ ソリューション部
  - ソリューション アーキテクト
- 経歴
  - 某ソフトウェア ベンダーにて、Windows のエンジニアを 12 年ほど。高度障害解析エンジニア、中規模小規模・大手企業へのソリューション提案、パートナー企業の案件支援などを担当。
- 好きな AWS のサービス
  - Windows インスタンス

アジェンダ

- ドメイン・サイトの構造
- ドメイン コントローラー（DC）の配置
- 名前解決に関する考慮事項
- ドメインのバックアップ・リストア
- AWS と Active Directory の ID 連携

- ※ Active Directory に関する運用知識をお持ちの方を対象にした内容です

ドメイン・サイトの構造

ドメイン構造

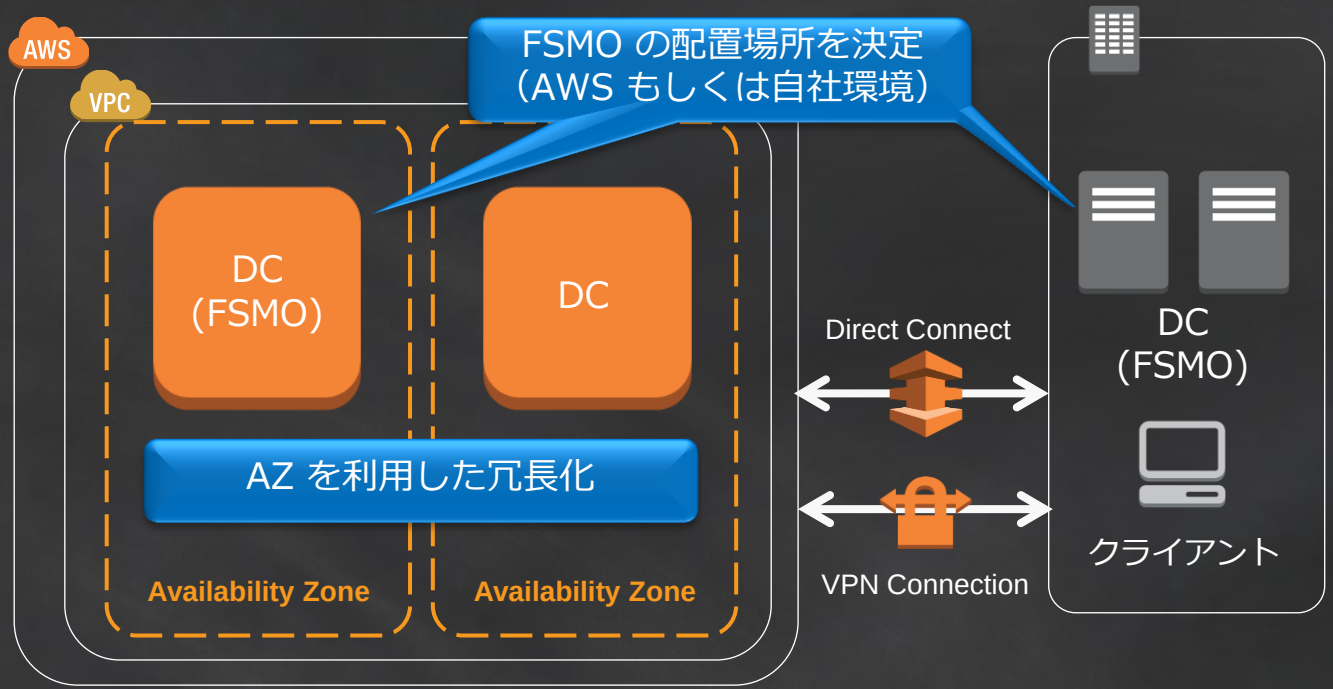
- 子ドメイン、信頼関係の採用に関する留意点
  - 特別な理由がない限り、AWS 上に配置する DC は、現在稼働中の Active Directory ドメインの DC として構築する
  - 「クラウドに DC を配置するから」という理由でドメインを分割しない
- ドメインを分割する際の判断基準
  - セキュリティの境界
  - 企業・組織体の境界
  - 地域の境界
  - etc

サイトの設計

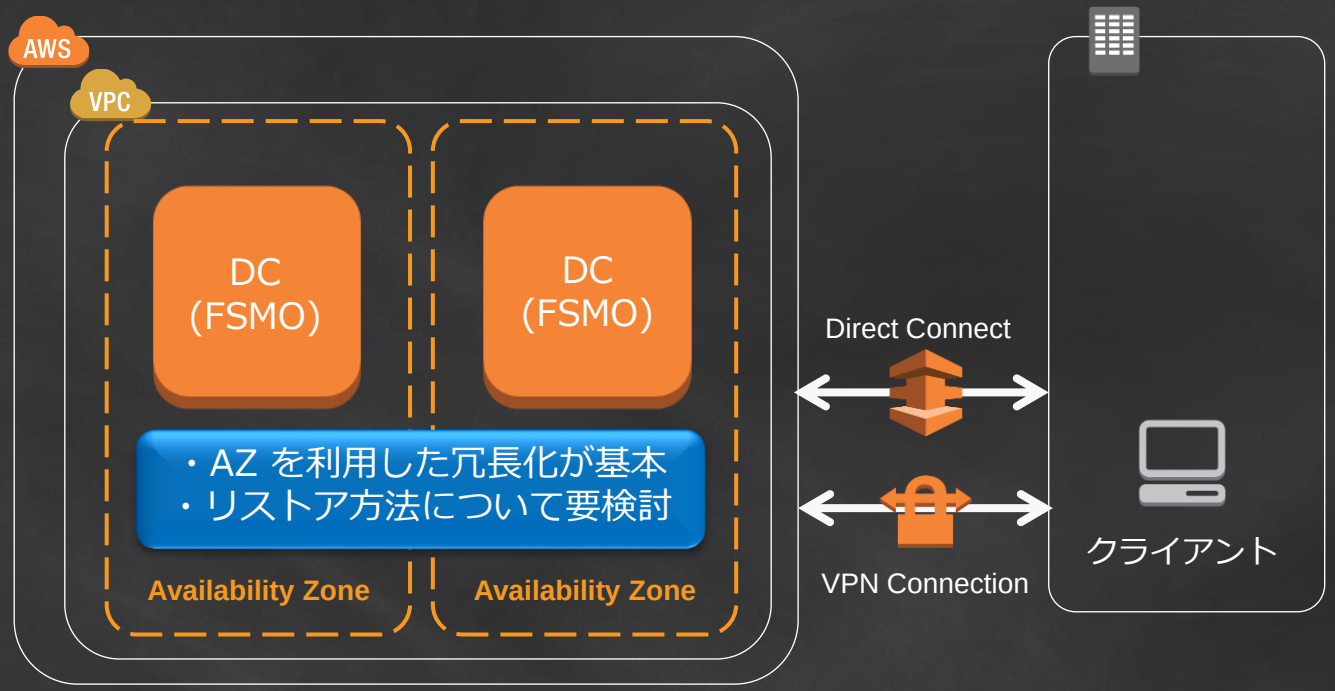
- 考慮事項については、従来の設計方法と同様
  - レイテンシーと複製にかかるコストを考慮
    - Amazon VPC との接続に、VPN を利用している場合には要注意
  - 複製（接続オブジェクト）のトポロジー
- AWS 用のサイトを作成して DC を配置した場合
  - 複製トポロジーが意図した通りに作成されているか、要確認
    - 適切な複製パートナーが接続されているか？
    - サイト間複製の間隔は既定で 180 分
      - 参考情報：サイト間レプリケーションの頻度を構成する http://technet.microsoft.com/ja-jp/library/cc730954.aspx
  - グローバル カタログ（GC）の配置を検討
    - 特に Exchange Server のような GC へのアクセス頻度が高いサーバーを AWS 上に配置する場合は必ず GC を設定

ドメイン コントローラー（DC）配置

AWS と自社環境とのハイブリッド運用



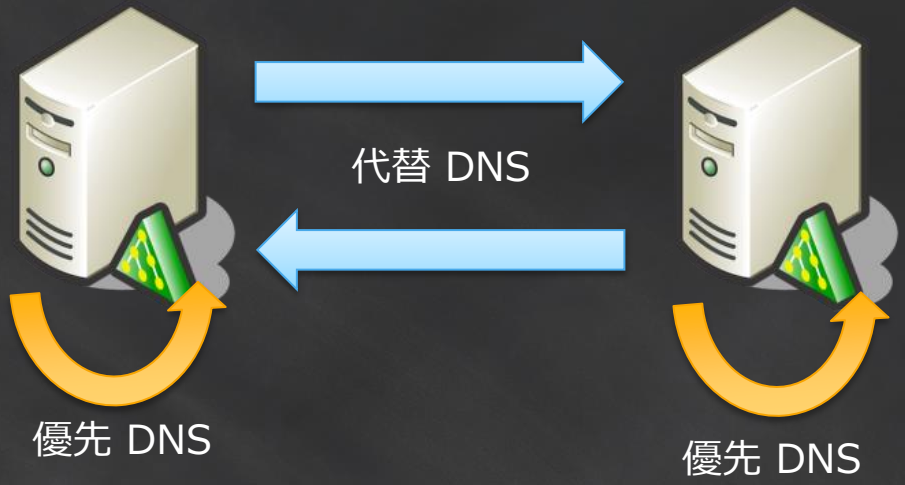
AWS 上に全ての DC を配置



名前解決に関する考慮事項

DNS の相互参照

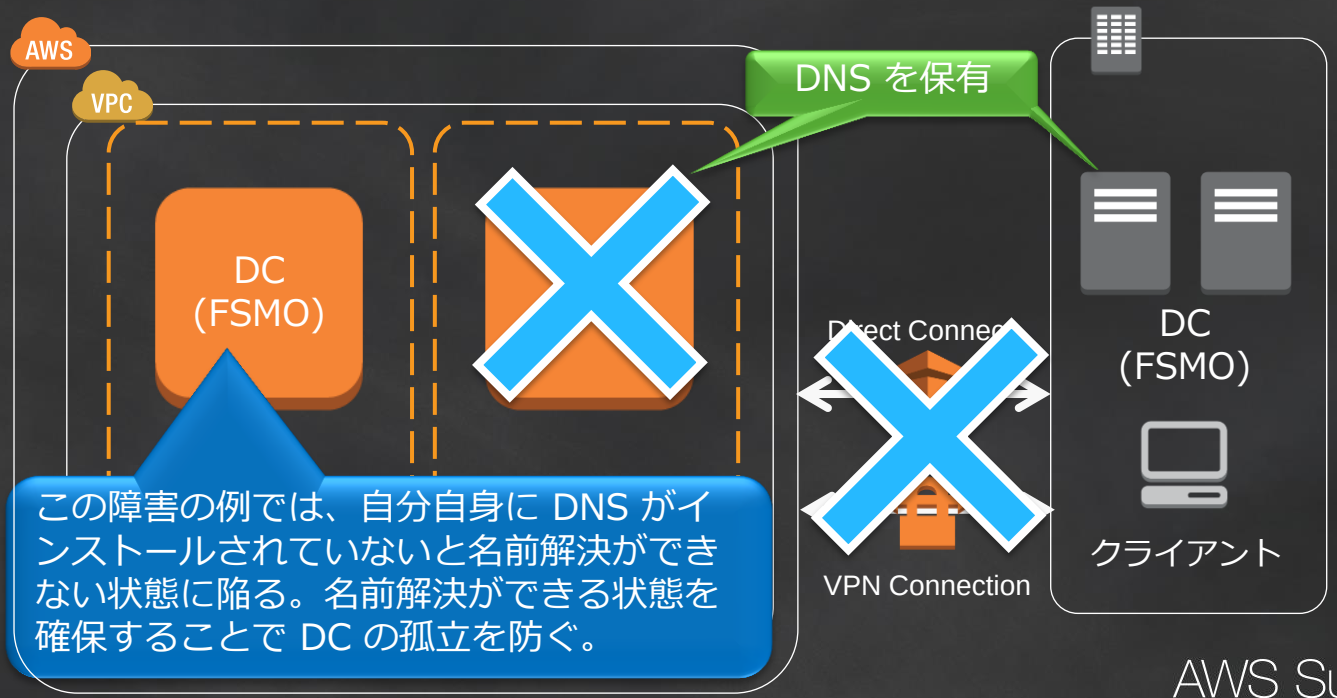
- 参照先 DNS の推奨設定
  - 優先 DNS に自分自身が保有する DNS を参照
  - 代替 DNS に他 DC が保有する DNS を参照



参考情報：Windows 2000 および Windows Server 2003 の DNS に関してよく寄せられる質問
http://support.microsoft.com/kb/291382/ja

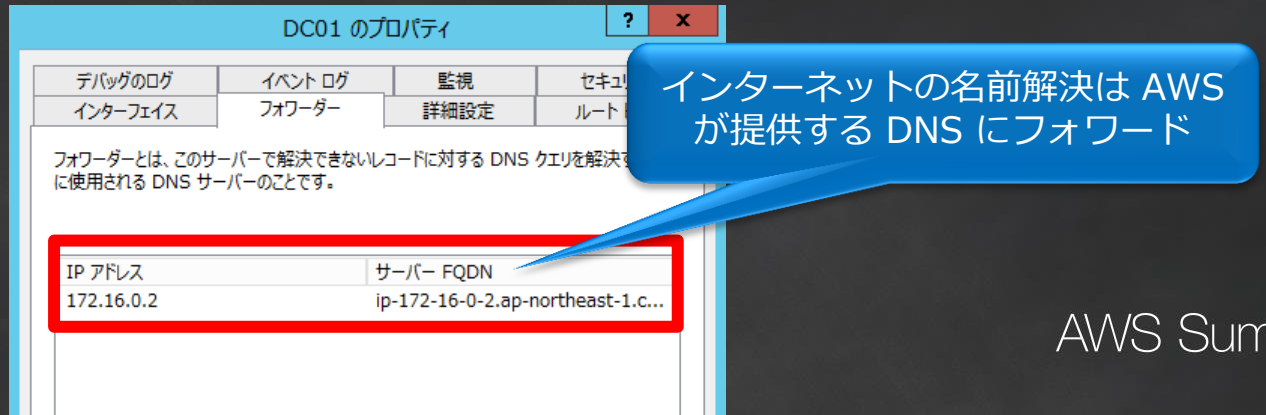
DNS の配置

- 障害発生時にも名前解決ができる状態を確保する



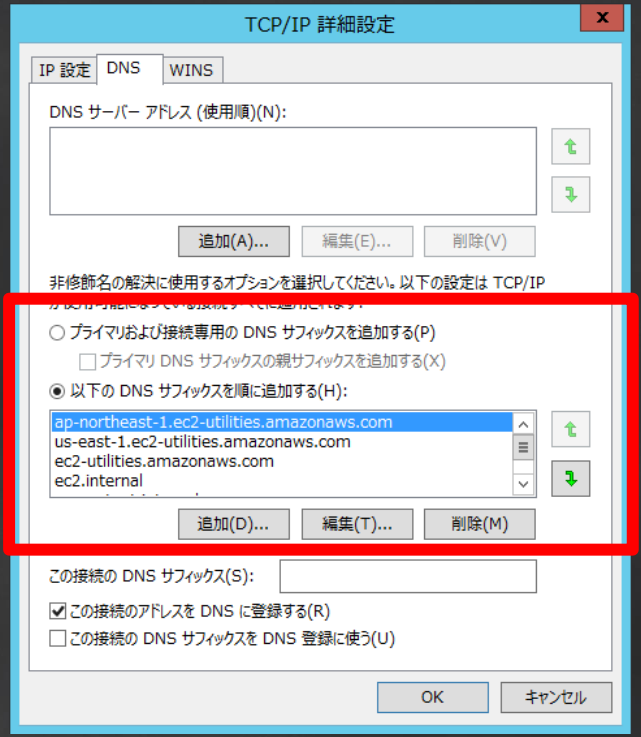
参照先 DNS の指定

- NIC の TCP/IP の設定
  - 参照先 DNS には、DC 上の DNS を指定する
  - AWS が提供する DNS は、（代替 DNS としても）参照しない
    - DC の参照ができなくなり、ログオン障害が発生する恐れ
    - DC 間の複製障害が発生する恐れ
- DC 上の DNS のフォワーダーに AWS が提供する DNS を設定する



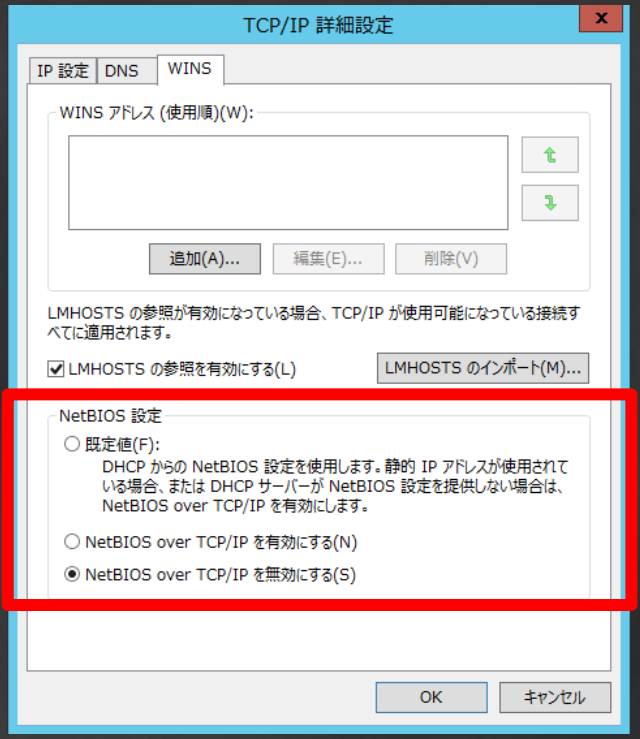
TCP/IP の詳細設定（DNS）

- 既定で DNS サフィックスに AWS 関連のものが追加されている
- 追加されているサフィックスの例
  - ap-northeast-1.ec2-utilities.amazonaws.com
  - us-east-1.ec2-utilities.amazonaws.com
  - ec2-utilities.amazonaws.com
  - ec2.internal
  - ap-northeast-1.compute.internal

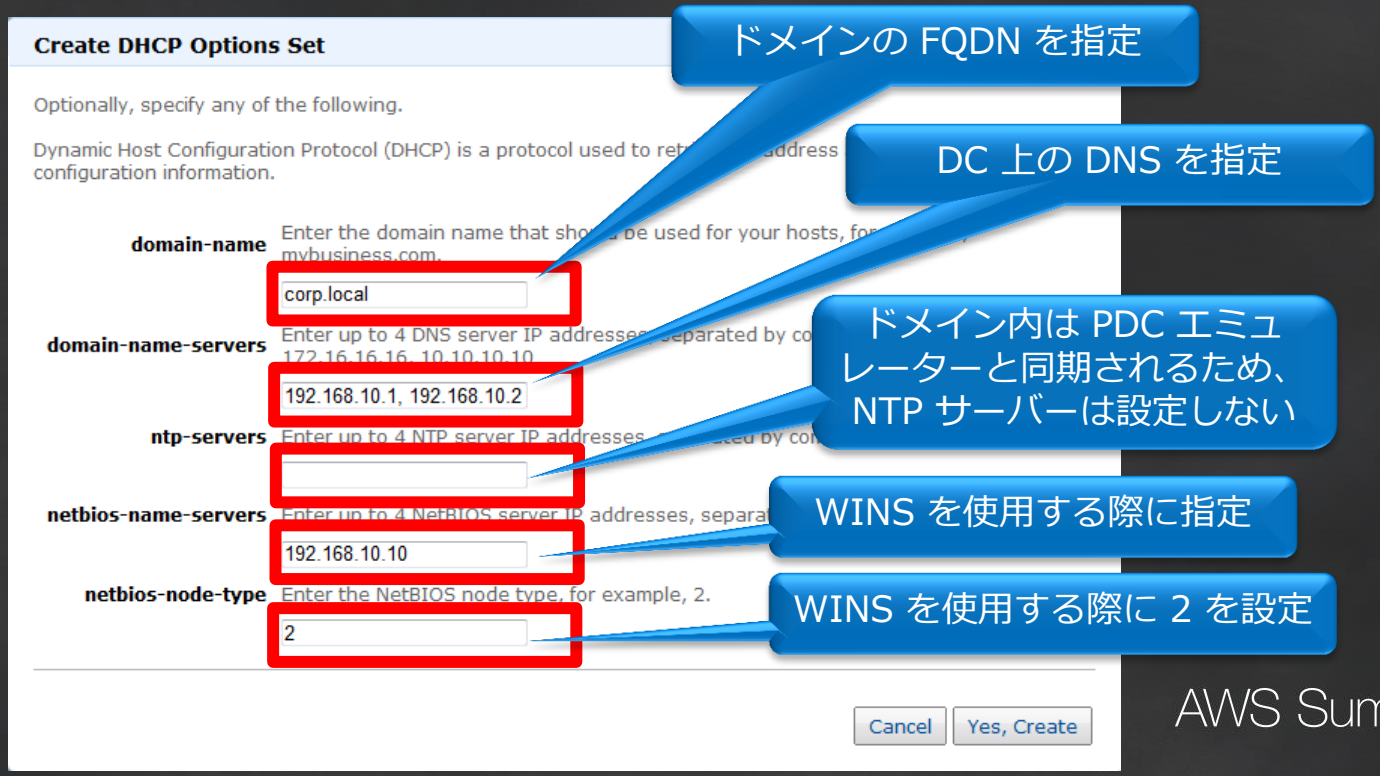


TCP/IP の詳細設定（WINS）

- 既定では [NetBIOS over TCP/IP を無効にする] に設定されている
- NetBIOS 名の名前解決が必要な場合には、WINS の構築を行う
  - Amazon VPC はブロードキャストをサポートしていないため、ブロードキャストを用いた NetBIOS 名の名前解決は利用できない

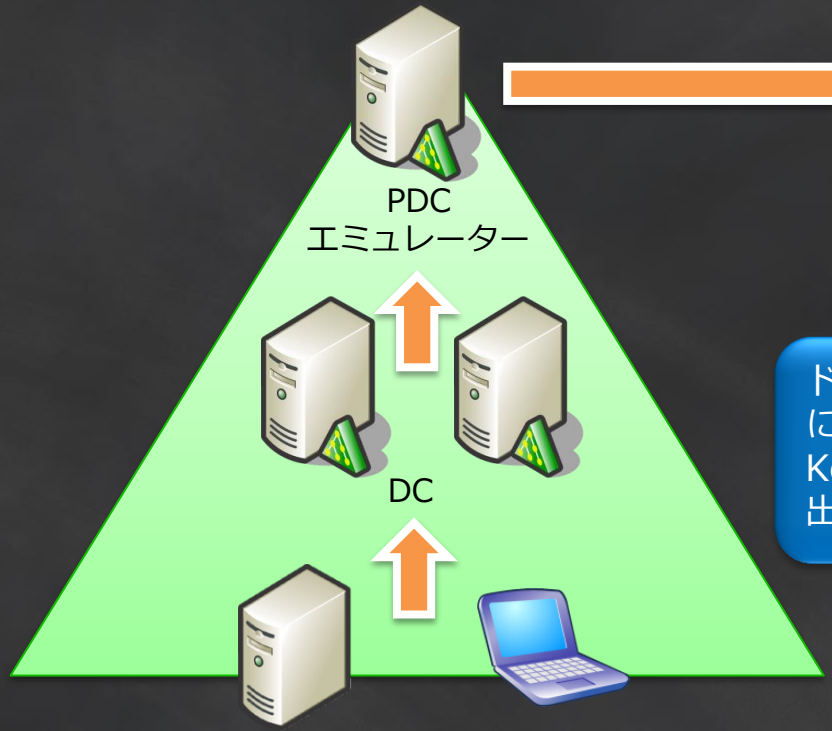


DHCP Options Set の利用



補足：ドメインの時刻同期

- PDC エミュレーターの時刻がドメイン内に展開される



ドメイン内で時刻同期が適切に行われていない場合、Kerberos 認証の動作に問題が出る恐れがある

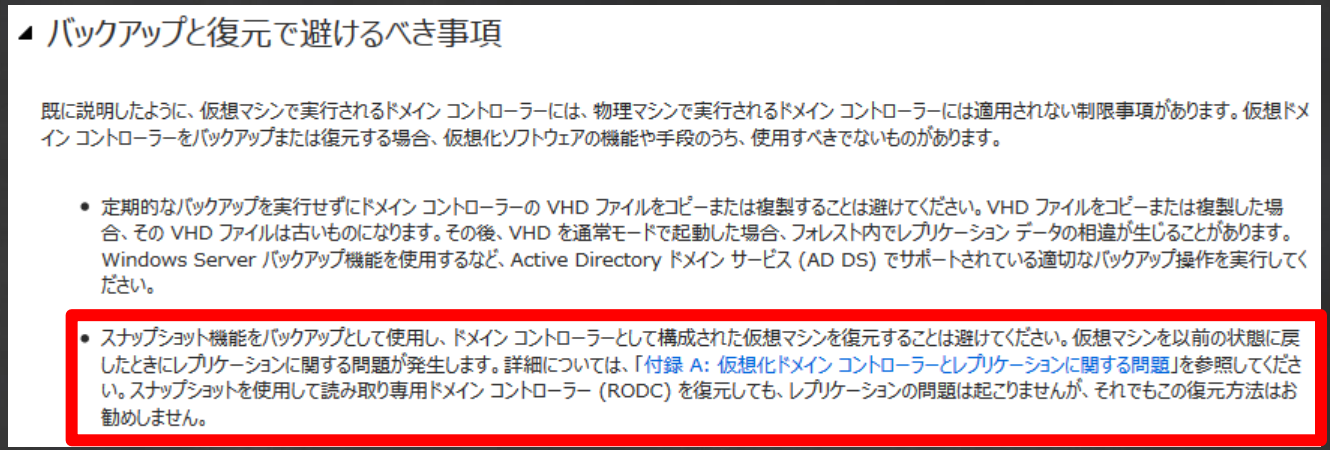
ドメインのバックアップ・リストア

バックアップ

- 従来のバックアップの手法を使用
  - VSS (Volume Shadow Copy Service) に対応したバックアップ ツールを使用する
    - Windows Server バックアップ
    - Wbadmin.exe
    - その他の VSS 対応バックアップ製品
  - Tombstone Lifetime の有効期限に注意
- EC2 スナップショットの利用
  - バックアップ ツールによって取得されたバックアップ データが保管されているボリュームのスナップショットを S3 に取得し、データを保全
  - DC のシステム全体のスナップショットについては、次ページの留意点について十分考慮する必要がある

リストア時の注意

- DC のシステム全体のスナップショットをリストアに使用しない
  - USN ロールバックを誘発
  - ロールバックが発生した DC はドメイン環境から隔離され、複製パートナーとして見なされなくなる



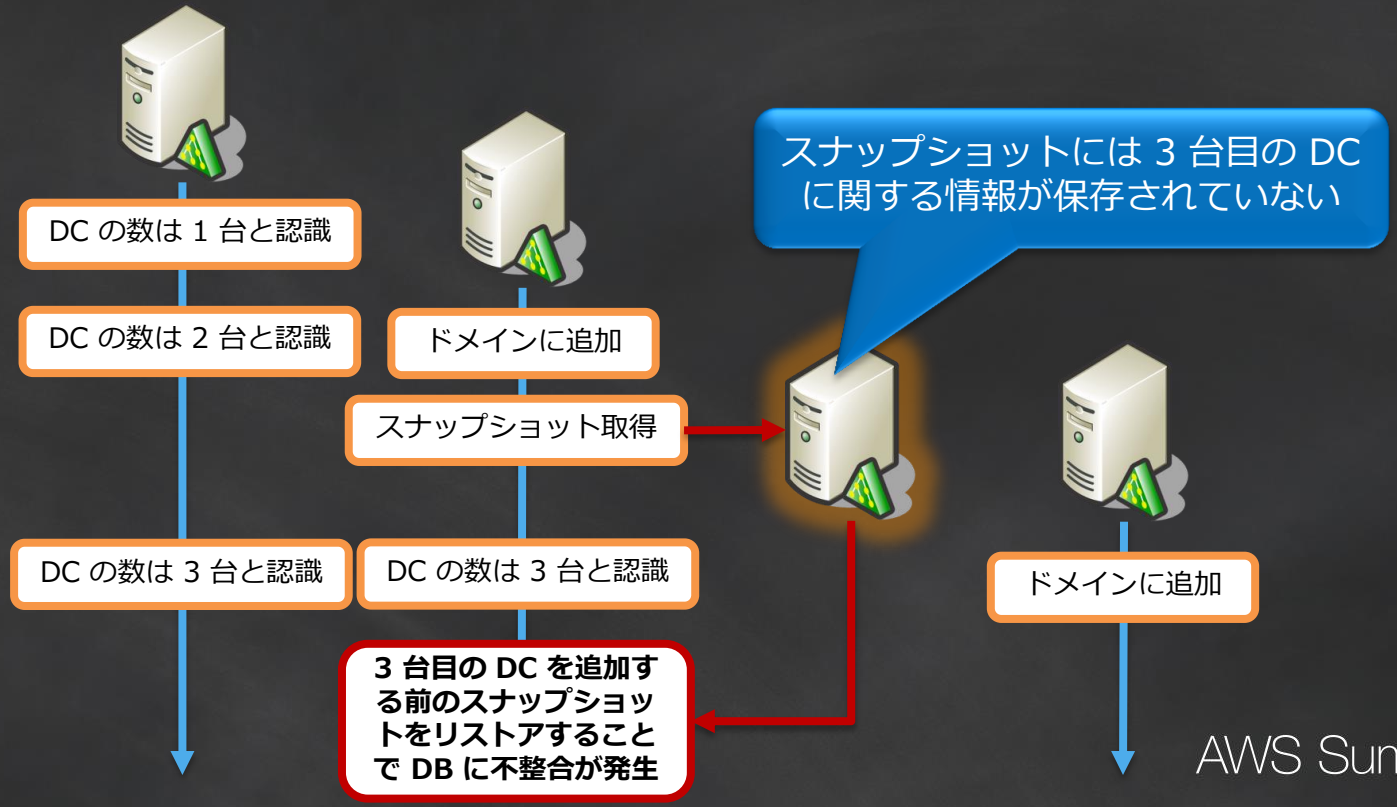
▲ バックアップと復元で避けるべき事項

既に説明したように、仮想マシンで実行されるドメイン コントローラーには、物理マシンで実行されるドメイン コントローラーには適用されない制限事項があります。仮想ドメイン コントローラーをバックアップまたは復元する場合、仮想化ソフトウェアの機能や手段のうち、使用すべきでないものがあります。

- 定期的なバックアップを実行せずにドメイン コントローラーの VHD ファイルをコピーまたは複製することは避けてください。VHD ファイルをコピーまたは複製した場合、その VHD ファイルは古いものになります。その後、VHD を通常モードで起動した場合、フォレスト内でレプリケーション データの相違が生じることがあります。Windows Server バックアップ機能を使用するなど、Active Directory ドメイン サービス (AD DS) でサポートされている適切なバックアップ操作を実行してください。
- スナップショット機能をバックアップとして使用し、ドメイン コントローラーとして構成された仮想マシンを復元することは避けてください。仮想マシンを以前の状態に戻したときにレプリケーションに関する問題が発生します。詳細については、「付録 A: 仮想化ドメイン コントローラーとレプリケーションに関する問題」を参照してください。スナップショットを使用して読み取り専用ドメイン コントローラー (RODC) を復元しても、レプリケーションの問題は起こりませんが、それでもこの復元方法はお勧めしません。

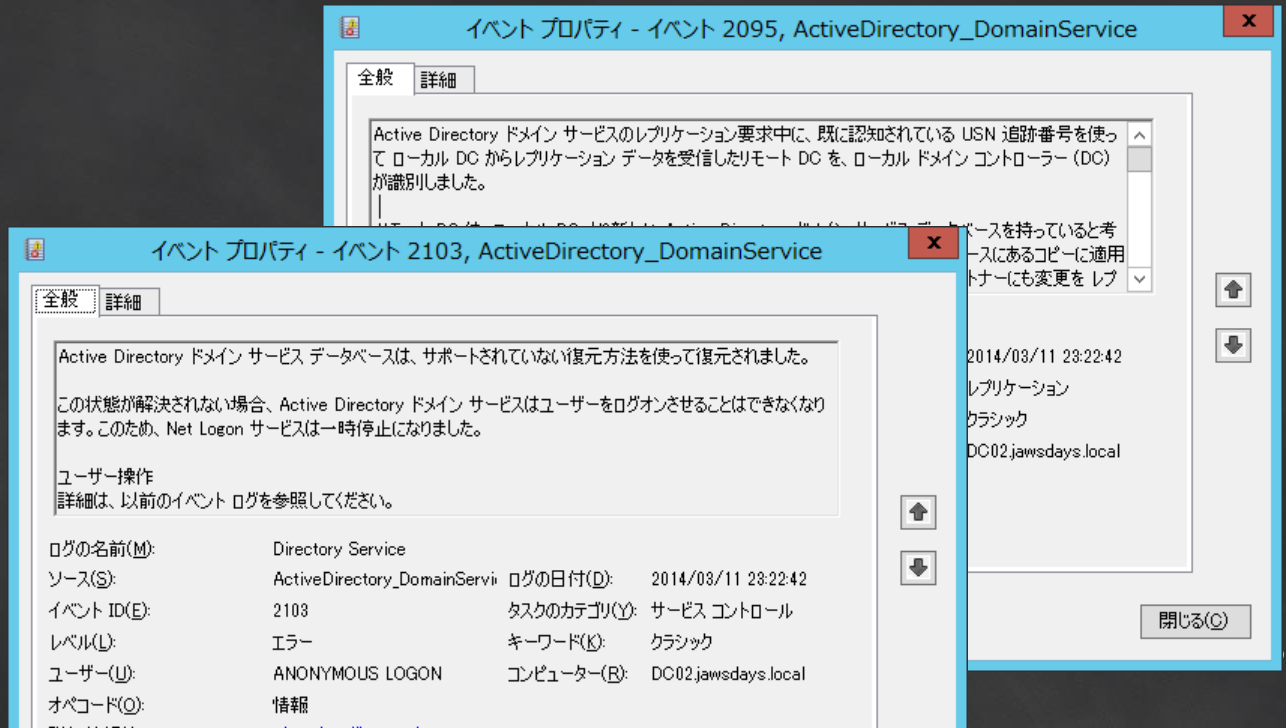
仮想化ドメイン コントローラーのバックアップと復元に関する考慮事項
http://technet.microsoft.com/ja-jp/library/dd363545%28v=ws.10%29.aspx

USN ロールバック発生のメカニズム



USN ロールバック発生時のイベント ログ

- イベント ID 2103 / 2095 / 1113 / 1115

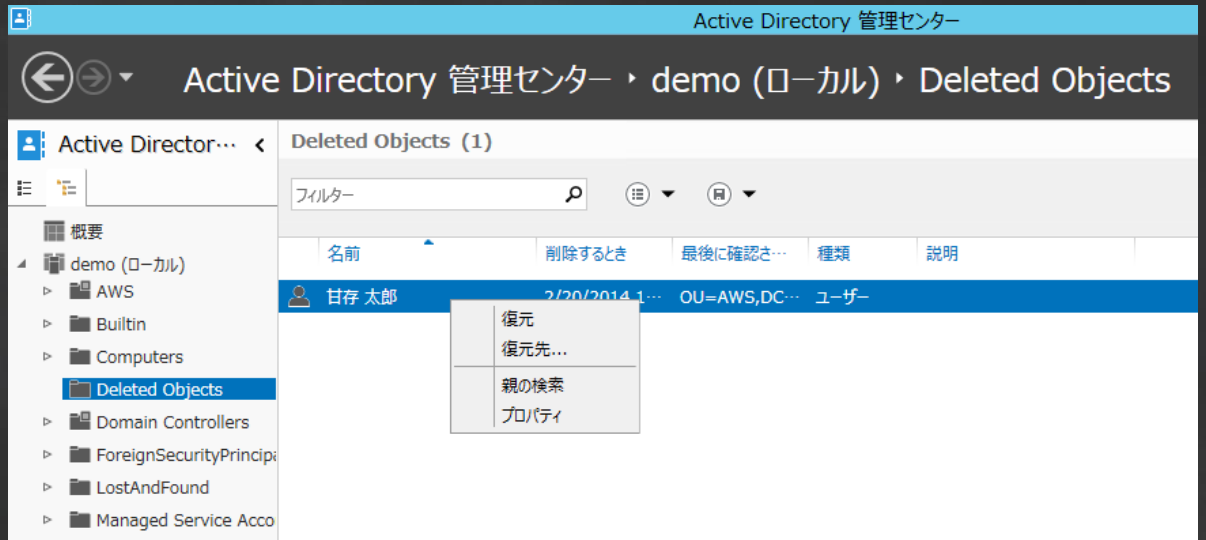


ディレクトリ サービス復元モード（DSRM）の利用

- 下記のリストアを行うための起動モード
  - Authoritative Restore（権限のあるリストア）
  - Non-Authoritative Restore（権限のないリストア）
  - 参考情報：AD DS をバックアップおよび回復するための手順 http://technet.microsoft.com/ja-jp/library/cc753359%28v=ws.10%29.aspx
- Windows Server のブート中に F8 を入力し、起動メニューから DSRM を選択してサーバーを起動する
  - ハイブリッド運用の場合、自社環境の DC から DSRM を利用
  - AWS 上の DC の場合、DSRM でブート不可（以下の手法が使用できない）
    - 参考情報：Restart the Domain Controller in Directory Services Restore Mode Remotely http://technet.microsoft.com/ja-jp/library/cc794729(v=ws.10).aspx

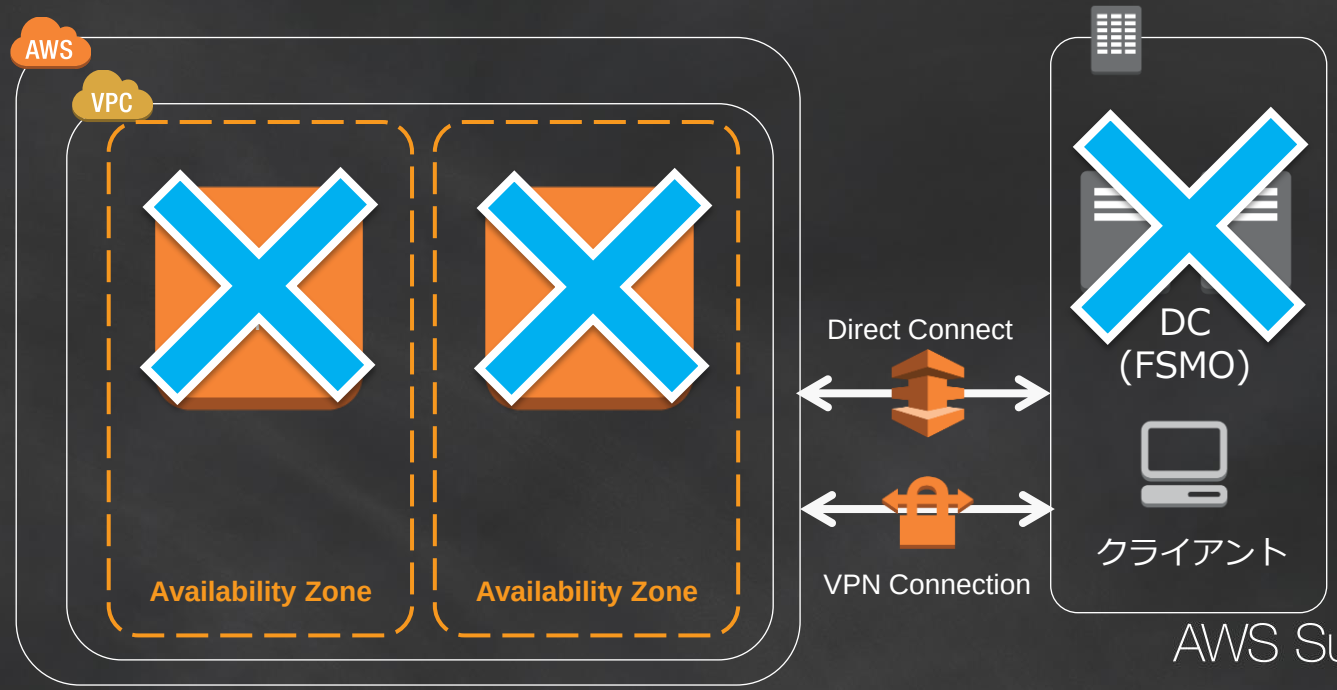
Active Directory ごみ箱の活用

- 誤って削除したオブジェクトをリストア可能
  - DSRM から Authoritative Restore を実行する必要がない
- Windows Server 2012/2012 R2 の場合は GUI から実行
- Windows Server 2008 R2 の場合は PowerShell から実行



致命的な障害が発生した場合の考慮事項

- 例：全ての DC が破損



フル リストアの手順の例

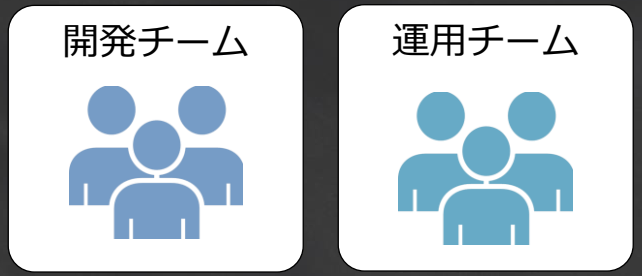
- AWS と自社環境とのハイブリッド運用の場合
  - 自社環境側の DC を DSRM でブートし、Authoritative Restore を実行
  - AWS 側の DC に、自社環境側のリストア情報を複製
- AWS 上に全ての DC を配置している場合
  1. AWS 上の DC で取得したバックアップ データを用意
  2. バックアップ データを用いて、自社環境で DSRM を利用して仮 DC を構築
  3. ntdsutil metadata cleanup で存在しない DC を削除
  4. AWS 上に DC を新規で構築し、仮 DC からデータを複製
  5. 複製完了後、FSMO を仮 DC から AWS 上の DC に移動（ntdsutil transfer）
  6. 仮 DC を降格し、AWS 上の DC を稼動

参考情報：Ntdsutil.exe を使用してドメイン コントローラーに FSMO の役割を強制または転送する
http://support.microsoft.com/kb/255504

AWS と Active Directory の ID 連携

AWS Identity and Access Management (IAM)

- AWS の操作をよりセキュアに行うための認証・認可の仕組み
- AWS の利用者の認証と、アクセス ポリシーを管理
  - AWS操作のためのグループ・ユーザー・ロールの作成が可能
  - グループ、ユーザーごとに、実行出来る操作を規定できる
  - ユーザーごとに認証情報の設定が可能



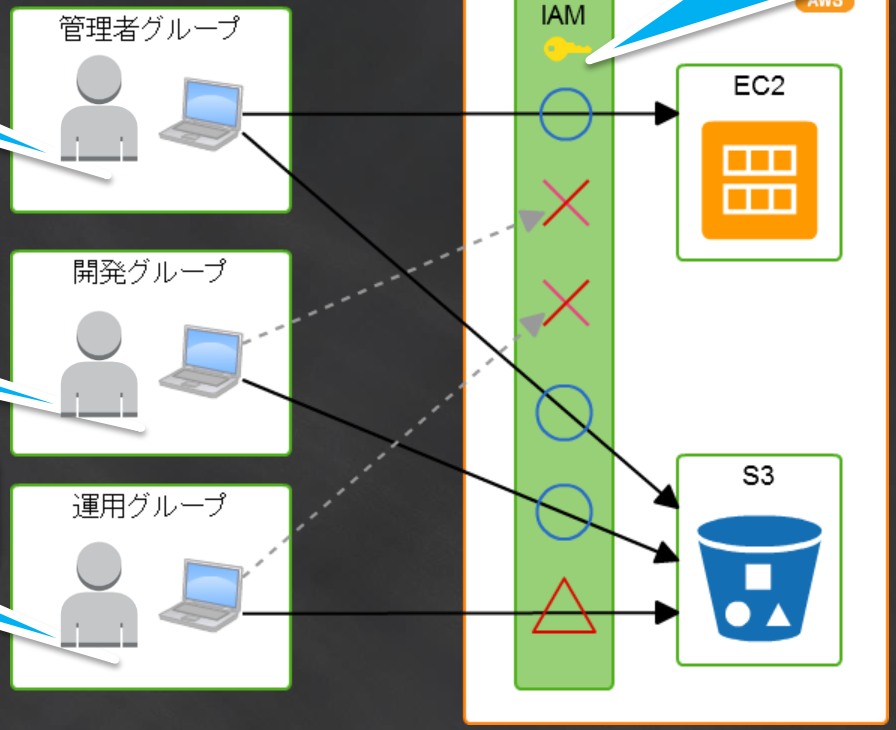
IAM の動作イメージ

APIやマネジメントコンソールからのアクセスに対して、権限をチェック

全機能の操作権限を保有

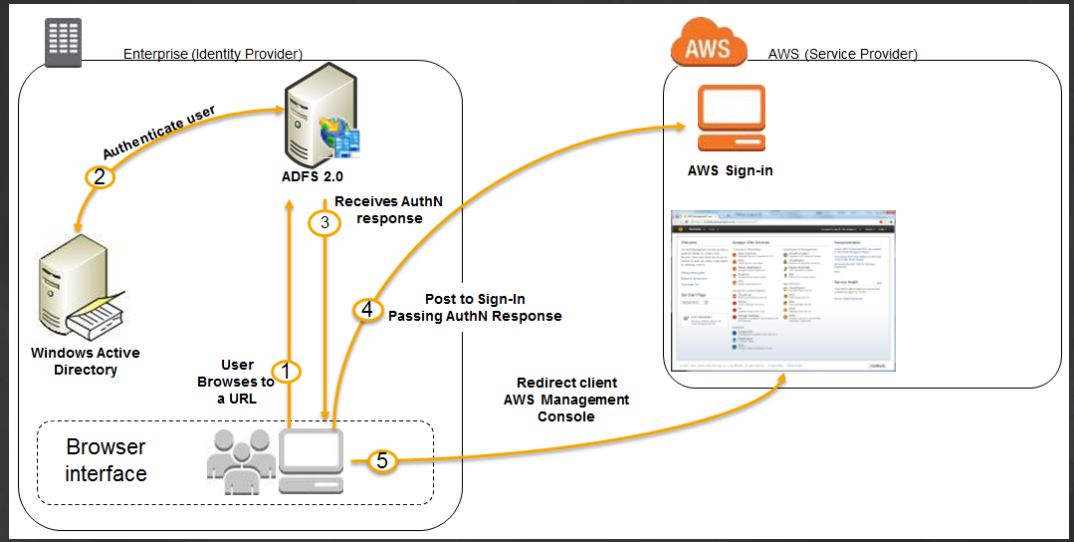
S3 の操作権限のみを保有

S3 の参照権限のみを保有



AWS と Active Directory の認証連携

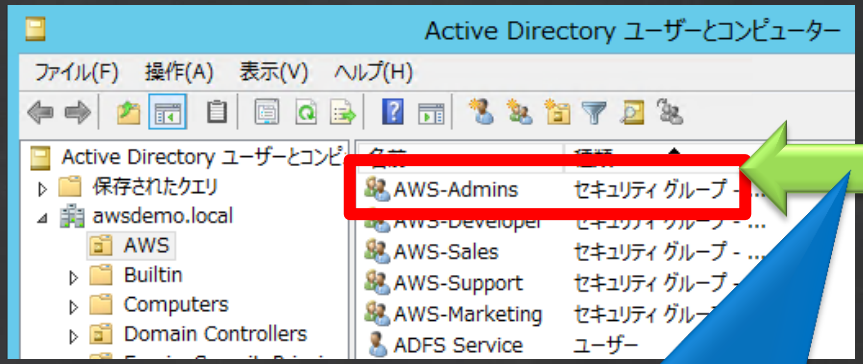
- AWS IAM の SAML 2.0 サポート
- Active Directory と SAML 2.0 による ID 連携が可能
  - Active Directory Federation Services を利用
- Active Directory のユーザーとグループを認証と認可に使用

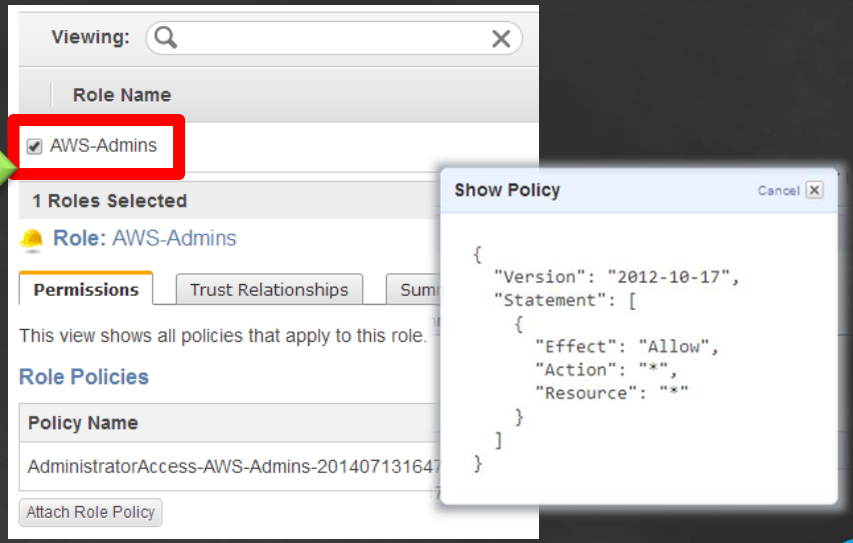


参考情報：Enabling Federation to AWS using Windows Active Directory, ADFS, and SAML 2.0
http://blogs.aws.amazon.com/security/post/Tx71TWXXJ3UI14/Enabling-Federation-to-AWS-using-Windows-Active-Directory-ADFS-and-SAML-2-0

グループのマッピング

- AWS の操作権限の単位をセキュリティ グループとして作成
- IAM ロールを作成し、AWS の操作権限を IAM ポリシーで定義

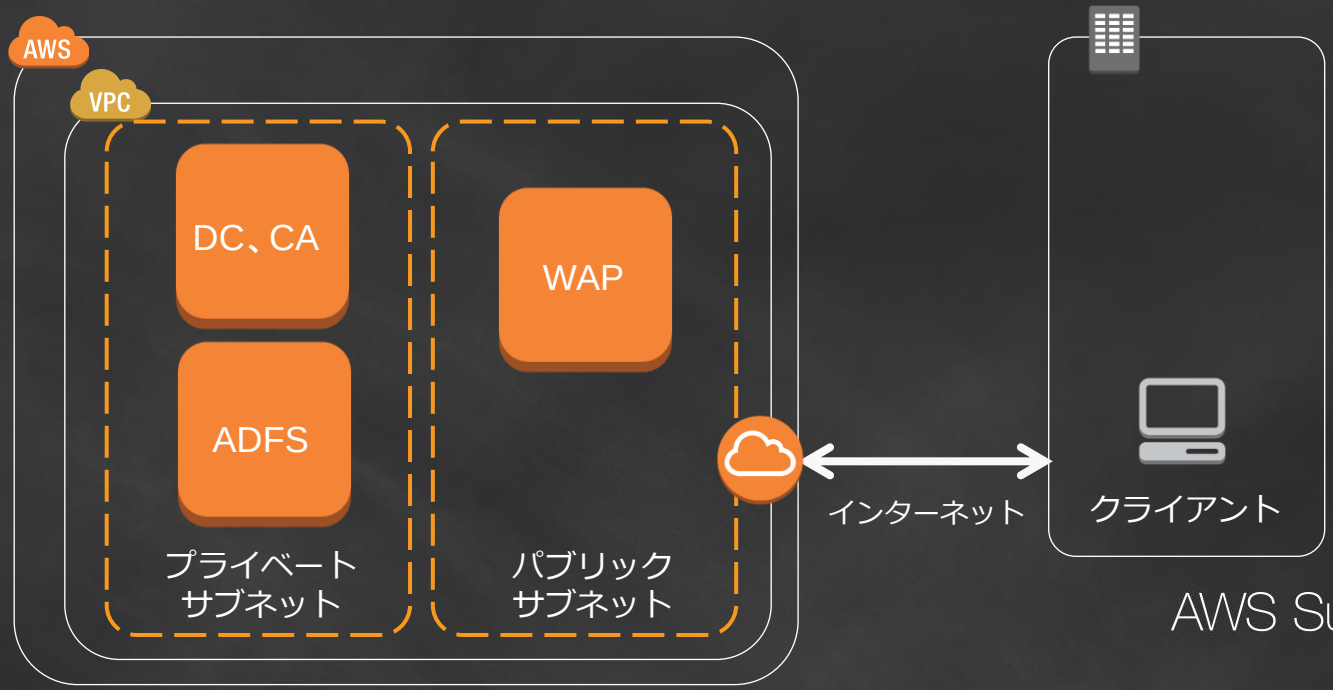




Active Directory Federation Services により、セキュリティ グループと IAM ロールをマッピング

デモ： IAM と AD の ID 連携

- IAM と AD を連携し、AD のセキュリティ グループに応じた AWS の操作権限をユーザーに付与
  - EC2 の操作権限
  - 所属組織に応じた S3 バケットの読み取り・書き込み権限



まとめ

- AWS 上に Active Directory を構築する際には、以下のテーマについて設計指針を検討する
  - ドメイン構造
  - サイト設計（DC 間の複製）
  - 名前解決
  - バックアップ・リストア
    - ドメインが破損するパターンをいくつか想定し、自社環境にとって最適なリストア方法を事前に検証する
- Active Directory と IAM との連携により、組織に対してAWS の操作権限を適切に付与する
  - 物理的なデータセンターの資産に対する権限付与と同等の ID 管理を行う

2014.09.09 SAVE THE DATE

http://csd.awseventsjapan.com/

Cloud Storage & DB Day　検索

amazon web services

AWS Summits 2014

AWS Summits
2014

amazon web services

AWS Summits
2014