1. Active Directory 統合設定ガイドの概要

Active Directory 統合の概要

Active Directory（AD）統合とは、適用可能な各 DNS 要求に対して、AD ユーザ、グループ、コンピュータ名の情報を提供することで、Umbrella 仮想アプライアンスを補完するものです。

このガイドでは、Umbrella のダッシュボードからプロビジョニング/メンテナンス可能な Active Directory のコンポーネントをインストールおよび設定する方法を説明します。Active Directory 環境と統合し、シスコのグローバル ネットワークに DNS クエリを転送することで、ユーザ、コンピュータ、グループへの設定の適用や、それらに関するレポートを行うことができます。

Active Directory 統合は 2 つのコンポーネントで構成されており、その 2 つのコンポーネントはそれぞれ、ネットワーク上の個別の AD サイトに設置する必要があります。

注

このドキュメントの文脈における Active Directory の「サイト」とは、ドメイン コントローラ、DNS サーバ、インターネットへの接続をそれぞれ個別に備えている場所を意味しています。

統合を構成する 2 つのコンポーネントのうちの 1 つは、次のようなものとなります。

1. 仮想アプライアンス（VA）

    - 仮想サーバ環境で実行される。
    - ローカル DNS クエリを、既存の DNS サーバへ転送する。
    - 外部 DNS クエリにメタデータ（機密情報ではない）を加えてシスコのグローバル ネットワークに転送する。

重要

VA にローカル DNS クエリと外部 DNS クエリを適切にルーティングさせるため、Umbrella で管理されるすべてのクライアントで、DNS アドレスを VA のアドレスにする必要があります。

2. **コネクタ**

- Active Directory 環境で実行される。
- ユーザおよびコンピュータのログイン情報（機密情報ではない）を、仮想アプライアンスに安全な通信で送信する。
- ユーザおよびコンピュータのグループ情報（機密情報ではない）を、シスコのグローバル ネットワークに安全な通信で送信する。

注：

セキュリティ ポリシー上、必要な場合は、コネクタをドメイン コントローラではない別のサーバにインストールすることができます。詳細については、「付録 C：AD サーバ以外にコネクタをインストールする準備」を参照してください。また、ネットワーク アーキテクチャによっては、すべてのドメイン コントローラにコネクタをインストールする必要もありません。必要なドメイン コントローラへのネットワーク接続がコネクタをインストールしたサーバにある限り、環境全体に対してコネクタが 1 つ、もしくは 2 つであっても問題はありません。

想定されるネットワーク トポロジとトラフィック フローの概要については、「付録 A：通信フローおよびトラブルシューティング」を参照してください。

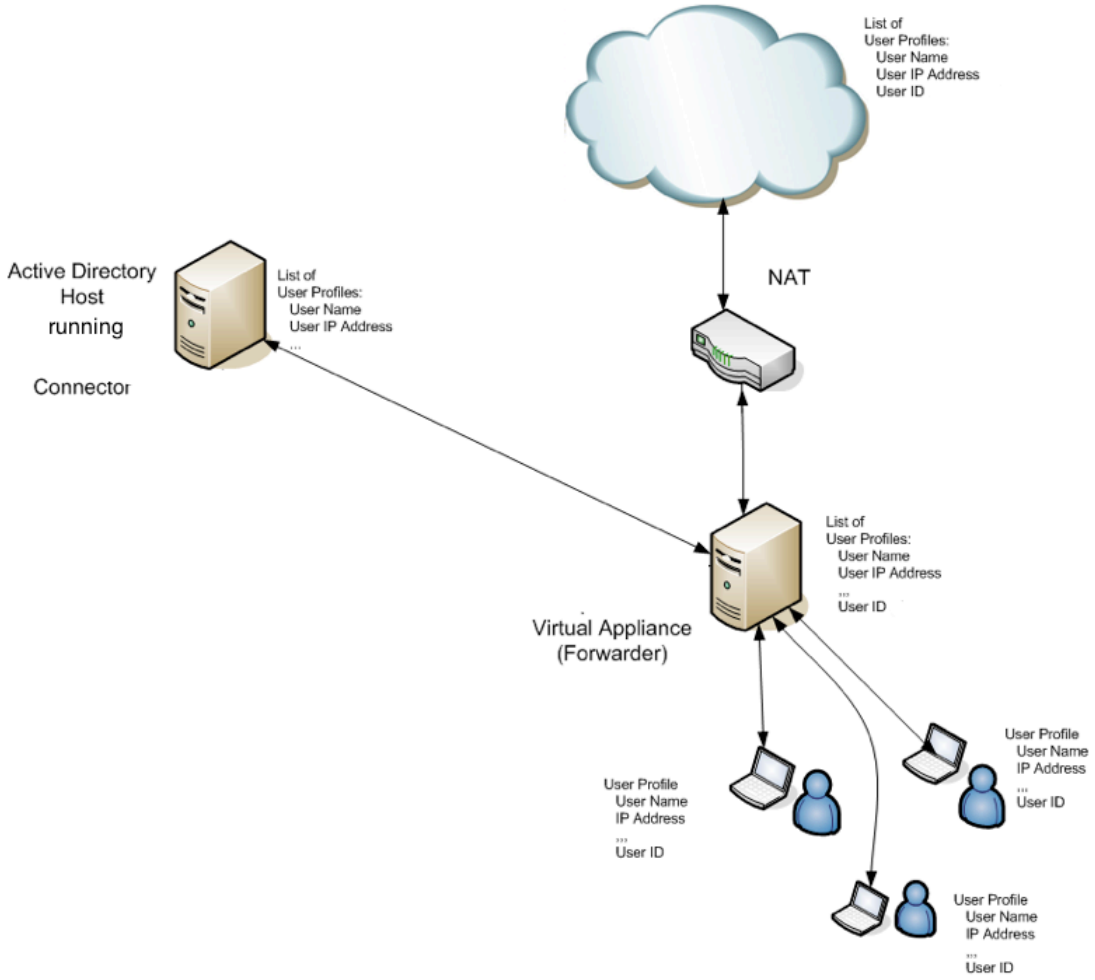
この付録は、計画や導入の進捗状況に応じて参照してください。

ネットワーク図

それぞれの Active Directory サイト内のクライアント マシンは、各サイトの VA を DNS リゾルバとして使用するように設定する必要があります。そうすることで、VA が内部リソースと外部リソースの両方の適切な IP アドレスに DNS クエリをルーティングできるようになります。

また、仮想アプライアンスは AD 環境と通信を行い、ユーザ情報の一覧とクライアントの一致を確認するクエリを送信します。

統合の各コンポーネントの概要を、次の図に示します。



次は、「前提条件」に進みます。

2. 前提条件

前提条件

Umbrella の Active Directory（AD）統合をサポートする上で、次の仮想サーバと AD 環境を設定する必要があります。

仮想サーバ環境

まず、仮想サーバ環境の要件を満たしていることを確認します。現在、サポートされているのは、VMware ESX または ESXi サーバ、Microsoft Server 2008 R2、2012、2012 R2 用の Microsoft Hyper-V です。

VMWare のシステム要件

- 仮想アプライアンス（VA）を作成するための ***VMware ESXi 4.1 Update 2***（またはそれ以降）。
- ESXi サーバのホストに正しい日付と時刻が設定されており、VA の動作が予測可能であること。
- ESXi サーバのホストに、1 つの CPU コア、512 MB の RAM が搭載されており、ハードディスク ドライブに、VA のインスタンスごとに 6.5 GB のプロビジョニングが可能なだけの空きがあること。4 つ以上の CPU コアで動作させる場合は、RAM が少なくとも 1536 MB（1.5GB）プロビジョニングされる必要があります。
- VA の障害や更新の場合に備えて、高い可用性を維持するには、1 つのサイトに最低でも 2 つの仮想アプライアンスを配置することが推奨される。ここでいう「サイト」とは、ローカルの連続サブネット（VA とそのネットワーク間で NAT なし）を意味しています。
- さらに規模を拡張する場合の要件の詳細については、『付録 B：VA のサイズ変更ガイド』を参照してください。

Microsoft Hyper-V のシステム要件

- Hyper-V のロールをもつ Windows Server 2008 R2 サーバまたは Hyper-V Server 2008。
- Hyper-V のロールがインストール/設定された Windows Server 2012（Standard/Datacenter）、Windows Server 2012 SP1（Standard/Datacenter）もしくは Windows Server 2012 R2（Standard/Datacenter）
- Windows サーバに正しい日付と時刻が設定されており、VA の動作が予測可能であること。
- Windows サーバ自体を実行するための最小ハードウェア要件*に加え*、次の内容が推奨されます。
    - 仮想アプライアンス 1 台ごとに、RAM を 512 MB 追加すること。4 つ以上の CPU コアで動作させる場合は、RAM が少なくとも 1536 MB（1.5GB）プロビジョニングされる必要があります。
    - 仮想アプライアンス 1 台ごとに、7 GB のディスク領域が割り当てられていること。
    - 仮想アプライアンス 1 台ごとに、CPU コアが 1 つ追加されていること（注：Hyper-V 用にプロビジョニングされたサーバのスペックが高い場合は、必要でない場合もあります）。
- VA の障害や更新の場合に備えて、高い可用性を維持するには、1 つのサイトに最低でも 2 つの仮想アプライアンスを配置することが推奨される。ここでいう「サイト」とは、ローカルの連続サブネット（VA とそのネットワーク間で NAT なし）を意味しています。
- さらに規模を拡張する場合の要件の詳細については、『付録 B：VA のサイズ変更ガイド』を参照してください。

Active Directory 環境

- Windows Server 2008、2008 R2、2012、2012 R2、2016。最新のサービス パックを適用し、ハードディスク ドライブ容量に 100 MB の空きがあること。
- .NET Framework 3.5、4.0、4.5。
- アンチ ウイルス アプリケーションがローカルで実行されている場合は、*OpenDNSAuditClient.exe*、および *OpenDNSAuditService.exe* のプロセスがホワイトリストされている必要があります。

注：Windows Server 2003 は正式にサポートされているオペレーティング システムではありません。本ドキュメントでは、2003 の場合での AD 統合のインストール方法について示しているため、参考資料とお考えください。Windows Server 2003 でも、実稼働環境で動作する可能性がありますが、推奨はされません。

重要：

読み取り専用ドメイン コントローラ（RODC）でスクリプトを実行したり、またはコネクタをインストールしたりしないでください。読み取り専用ドメイン コントローラ（RODC）をドメインに置き、アイデンティティのレポートに使用することは可能ですが、Active Directory 統合に使用することはできず、サポートされていません。

- サポートされるのは、単一ドメイン環境のみです（子ドメインや信頼については、現在サポートされていません）。
- マルチドメイン環境の場合には、複数のダッシュボード エクスペリエンスが必要です。ドメイン構成やサポート対象に関する質問がある場合は、umbrella-support@cisco.com までお問い合わせください。マルチドメインのサポートについて確認したい場合は、サポート チームまで電子メールにてご連絡ください。

Multi-Org Console の詳細については、こちらのドキュメントを参照してください。

Umbrella の Active Directory コンポーネントを、複数の WAN（MPLS タイプ ネットワーク）に接続する AD サイトに配置する場合は、現在のサイトでのインストールの完了と動作を確認してから、次に進んでください。

- 新しいユーザ アカウントに関して、次の内容を確認してください。
    - ログイン名（sAMAccountName）に、OpenDNS_Connector が設定されていること。
    - [パスワードの有効期限なし（Password never expires）] のボックスにチェックが入っていること。
    - 入力されたパスワードに、バックスラッシュ、引用符（一重、二重）、左右のアングル ブラケット（「<」、「>」）、コロンの記号が含まれていないこと。
    - OpenDNS_Connector ユーザが次のグループのメンバーになっていること。なっていない場合は、該当のグループに追加してください。
        - Event Log Readers
        - Distributed COM users
        - Enterprise Read-only Domain Controllers

Windows Server 2003、Windows Server 2003 R2 の環境では、これらのグループは存在していません。付録 D に移動し、手動で手順を完了させてください。

ネットワーク環境

想定されるネットワーク トポロジとトラフィック フローの概要については、「付録 A: 通信フローおよびトラブルシューティング」を参照してください。

次のポートを、Active Directory サーバに対してオープンに設定してください。

- 仮想アプライアンス（ローカル側）、また外部の api.opendns.com への 443 TCP
- アップデートは、disthost.opendns.com:443 から送信されます。

仮想アプライアンスに、次のポートとプロトコルを設定します。**これらの要件は、VMWare と Hyper-V の両方に適用されます。**

- DC から次の認証局へ（SSL 接続に必須）。
- **443 TCP、UDP（67.215.92.0/24、67.215.71.201、ocsp.digicert.com、crl4.digicert.com）**
- **80 TCP（67.215.92.0/24、67.215.71.201、ocsp.digicert.com、crl4.digicert.com）**

注: Digicert のドメインは、CDN に基づいて複数の IP アドレスに解決されており、変更される場合があります。現時点では、これらのドメインは次の IP に解決されています: 72.21.91.29、117.18.237.29、93.184.220.29、205.234.175.175

コネクタがインストールされているコンピュータの場合（DC もしくはワーク ステーション）

- **80 TCP、UDP（crl.comodoca.com、ocsp.comodoca.com、crl.usertrust.com、ocsp.usertrust.com）**

VA からの**ラベル付きサブネットおよび IP** への通信に対して、次の**アウトバウンドポート**をオープンに設定してください。

- 53 TCP、UDP（208.67.220.220、208.67.222.222、208.67.222.220、208.67.220.222）。これらのポートは DNSCrypt の確立に使用されることに注意ください（下の注記を参照してください）。
- 443 TCP、UDP（67.215.92.0/24、67.215.71.201、ocsp.digicert.com、crl.digicert.com）
- 80 TCP（67.215.92.0/24）
- 2222 TCP（67.215.92.0/24）
- 123 UDP（91.189.94.4 および 91.189.89.199（Canonical の Ubuntu NTP サーバ用））**
- VA と内部 DNS サーバ間の 53 UDP。VA は、内部 DNS 要求の内部 DNS サーバへの転送も行います。

DNSCrypt と仮想アプライアンス

仮想アプライアンスでは、自身とシスコのパブリック DNS リゾルバ（Umbrella）との間の DNSCrypt をサポートしています。つまり、VA から転送される EDNS パケットに含まれる情報が、すべて DNSCrypt により暗号化され、傍受されないことを意味しています。最適な防御を提供するため、この機能はデフォルトで有効になっています。

トラフィックが暗号化されていない場合、それは解決されるべき問題と見なされます。VA とシスコの DNS サービスの間に暗号化を確立できない場合は、ダッシュボードに警告が表示されます。暗号化は、53 番ポート（UDP/TCP）から 208.67.220.220、208.67.222.222 に送信されるプローブによって確立されます。ディープ パケット インスペクションを行うファイアウォールや IPS/IDS があり、DNS トラフィックだけを確認することが予想される場合は、プローブに失敗する可能性があります。つまり、暗号化されたパケットが、そのポートで予想されるトラフィックに一致しない可能性があります。ファイアウォールの設定を確認して上記に当てはまり、そのトラフィックの許可に問題がない場合は、サポートのケースを開いてください。

注：

Digicert のドメインは、CDN に基づいて複数の IP アドレスに解決されており、変更される場合があります。現時点では、これらのドメインは次の IP に解決されています：72.21.91.29、117.18.237.29、93.184.220.29、205.234.175.175

- ネットワーク アドレス変換（NAT）を行うデバイスや、内部 IP アドレスの難読化を任意の方法で行うデバイスを、各サイトのホストと仮想アプライアンスの間に配置しないでください。
- 問題を避けるために、ネットワークに透過プロキシがないことを確認してください。

---

1. Active Directory 統合設定ガイドの概要 <**2. 前提条件**> 3. VA による DNS 転送の設定

3. VA による DNS 転送の設定

仮想アプライアンスを Active Directory と同時に使用する目的は、内部送信元 IP アドレスを AD ユーザおよびコンピュータにマッピングして、そのネットワークからシスコのグローバル ネットワークへ外部 DNS クエリを転送することです。

重要:

仮想アプライアンスにローカル DNS クエリと外部 DNS クエリを適切にルーティングさせるため、Umbrella で管理されるすべてのクライアントで、DNS アドレスを VA のアドレスにする必要があります。

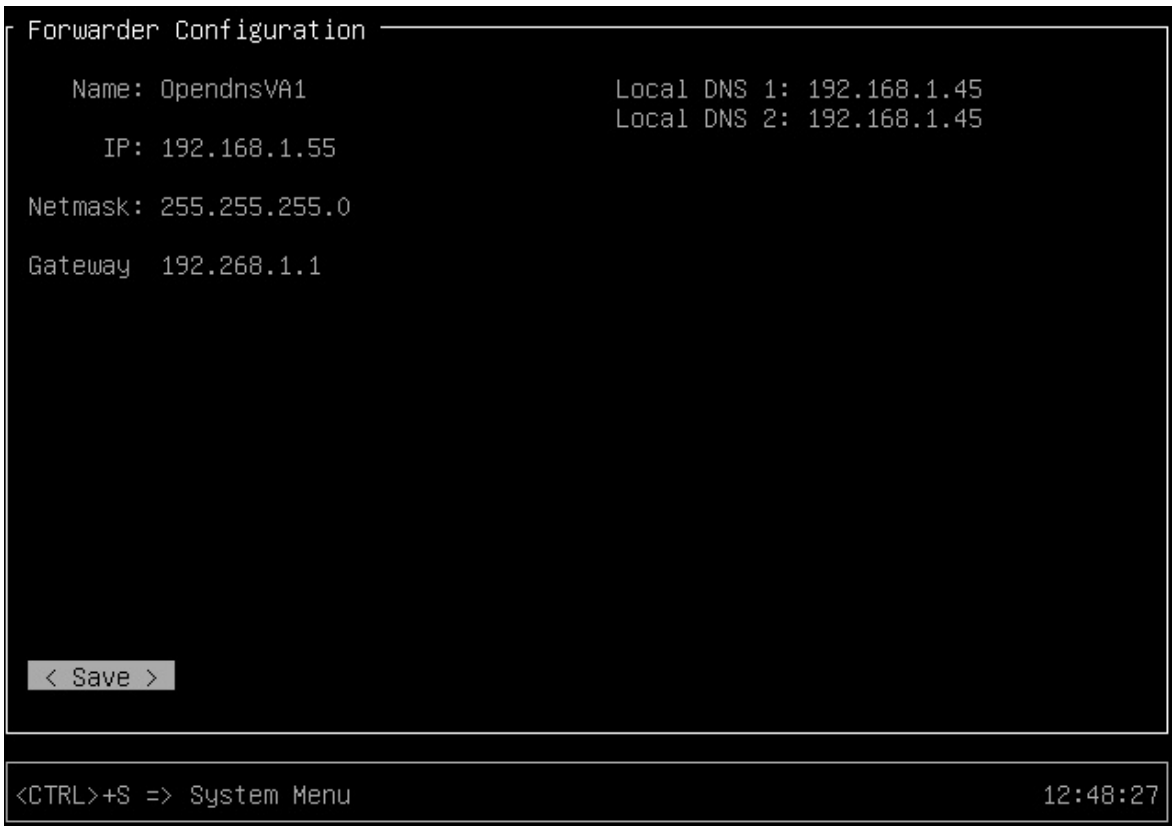
仮想アプライアンス（VA）の作成

VMware ESX または Microsoft Hyper-V のいずれかで仮想アプライアンスを作成するには、シスコの手順ガイドに従ってください。最初の仮想アプライアンスの設定プロセスについて一通り説明しています。シスコの手順ガイド『Virtual Appliance (VA) deployment guide（仮想アプライアンス（VA）導入ガイド）』にアクセスするには、こちらをクリックしてください。次に、簡潔な概要を示します。

仮想アプライアンスの設定

1. 短いブートアップ プロセスの後、VMware または Hyper-V のコンソールに、DNS フォワーダを設定するプロンプトが表示され、タブ キーでフィールドを切り替えることができます。


Forwarder Configuration
Name: _
IP:
Netmask:
Gateway
Local DNS 1:
Local DNS 2:
< Save >
<CTRL>+S => System Menu
12:46:54


Forwarder Configuration
Name: OpendnsVA1
IP: 192.168.1.55
Netmask: 255.255.255.0
Gateway 192.268.1.1
Local DNS 1: 192.168.1.45
Local DNS 2: 192.168.1.45
< Save >
<CTRL>+S => System Menu
12:48:27

注:

[ローカル DNS 1(Local DNS 1)] および [ローカル DNS 2(Local DNS 2)] には、使用しているローカル DNS サーバを入力します。通常は、Active Directory ドメインサービスと DNS サーバ ロールの両方がインストールされた Windows サーバの IP アドレスが入ります。

2. タブ キーで [保存(Save)] を選択し、Return キーを押します。

注:

VA と Umbrella のサービスが通信していることを示す同期メッセージが確認できるはずです。

仮想アプライアンスとダッシュボードの同期の確認

Umbrella のダッシュボードに戻ると、Active Directory の設定ページで、作成したばかりの VA がグレーの丸いアイコンで*非アクティブ*の状態になっていることが示されています。

冗長仮想アプライアンスの作成

上記の手順を繰り返し、セカンダリの仮想アプライアンスを作成します。これは VA のソフトウェアをアップグレードする際に、運用を継続させる上で必要です。

注:

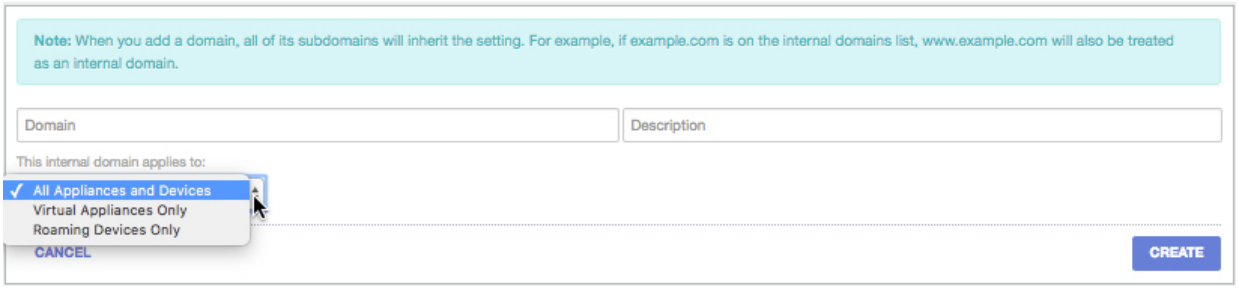
セカンダリの VA により、なんらかの重大な問題が発生した時にも、100 % の稼働時間を確保できます。また、自動アップグレードの際に必要なリブートを順次行うことが可能となります。設定に応じて、それぞれの VA を別々の VMware や Hyper-V ホストに導入することができます。セカンダリの仮想アプライアンスを配置する際には、必ず手順に従ってください。すでに導入済みの仮想アプライアンスを複製して新規に仮想アプライアンスを作成することは避けてください。

ローカル DNS クエリのルーティング

内部ネットワーク内のローカル ホストに確実に正しい DNS 応答が返されるようにするには、既存の DNS サーバにクエリがルーティングされるよう VA を設定する必要があります。

これを行うには、[設定（Settings）] > [内部ドメイン（Internal Domains）] の順に移動します。

詳細については、こちらのドキュメントを参照してください。内部 DNS ゾーン（168.192.in-addr.arpa）が、デフォルトで含まれています。.local も同様です。



VA 用の A レコードおよび PTR レコードの追加

1. ローカルの DNS サーバで、[スタート（Start）] をクリックし、dnsmgmt.msc を実行します
2. ローカル ドメインの前方参照ゾーンに移動します（corp.domain.com など）。
3. ローカル ゾーンを選択します *（corp.domain.com など）*。
4. 右側で右クリックして、[新しいホスト（New Host）] を選択します。
5. VA のホスト名、IP を入力し、[関連するポインタ（PTR）レコードを作成（Create associated pointer (PTR) record）] のチェックボックスが選択されていることを確認します。
6. [ホストの追加（Add Host）] をクリックします。

レコードが正常に作成されたかどうかを確認するには、nslookup でテストを行います。

1. **nslookup**（*VA の IP アドレス*）を入力します。次に例を示します。
    - nslookup 192.168.1.2
      Server:192.168.1.1
      Address:192.168.1.1#53
      Non-authoritative answer:
      1.168.192.in-addr.arpaname = va01.corp.domain.com.

2. nslookup（*VA のホスト名*）を入力します。次に例を示します。
    - nslookup **va01.corp.domain.com**
      Server: 192.168.1.1
      Address: 192.168.1.1#53
      Non-authoritative answer:
      Name: va01.corp.domain.com
      Address: 67.215.92.152

---

2. 前提条件 < **3. VA による DNS 転送の設定**> 4. Active Directory 環境の準備

4. Active Directory 環境の準備

注

まだ仮想アプライアンスを導入していない場合は、前の手順に戻ってください。仮想アプライアンスを使用しないで AD 統合を行うことはできません。

開始するには、Windows の設定スクリプトを各サイトの ***すべての***ドメイン コントローラ（DC）で起動させます（ドメイン上の DC が対象。読み取り専用ドメインや他のドメインの DC は除きます）。これにより、DC とコネクタの通信が準備できます。スクリプトによる変更内容の詳細については、こちらのドキュメントを参照してください。

読み取り専用ドメイン コントローラ

このスクリプトは、環境内の読み取り専用ドメイン コントローラ（RODC）では起動させないでください。*RODC はサポートされていません。*

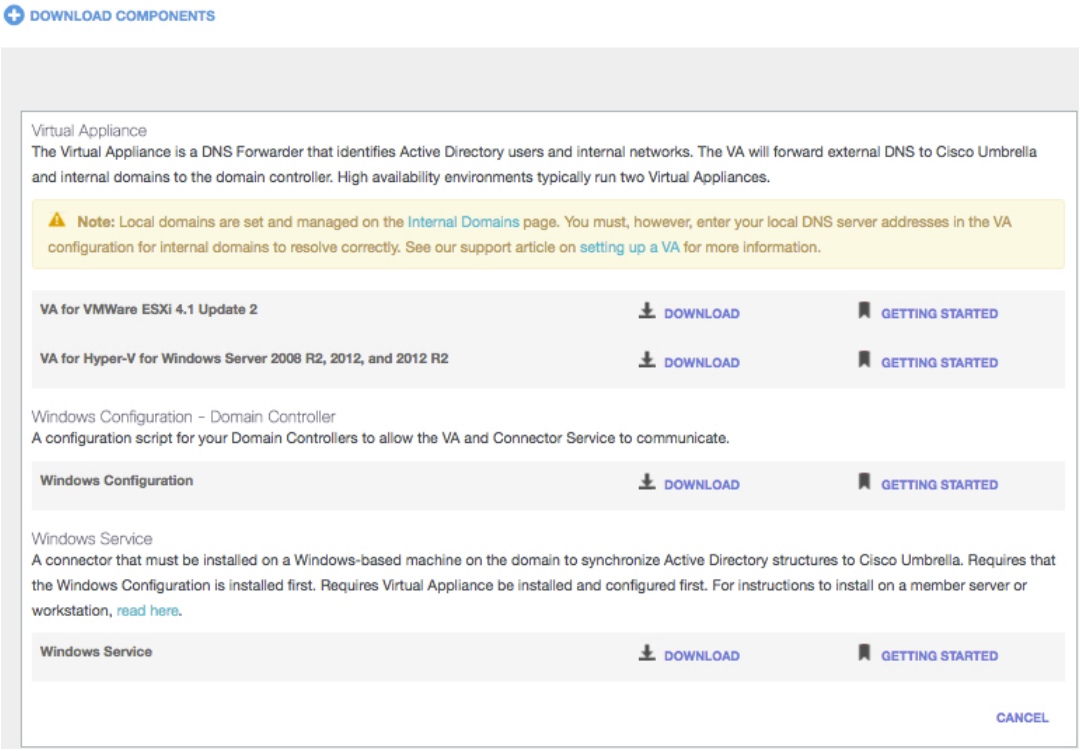
Windows Server 2003 R2 を実行している環境の場合、手順 2 を完了させるには、手動での手順がいくつか必要です。手順については、『Active Directory Integration – Appendix B（Active Directory 統合：付録 B）』を参照してください。

注：Windows Server 2003 は正式にサポートされているオペレーティング システムではありません。本ドキュメントでは、2003 の場合での AD 統合のインストール方法について示しているため、参考資料とお考えください。Windows Server 2003 でも、実稼働環境で動作する可能性がありますが、推奨はされません。

ドメイン コントローラでの設定スクリプトの実行

1. [設定（Settings）] > [サイトおよび Active Directory（Sites and Active Directory）] の順に移動します。

2. [コンポーネントのダウンロード（Download Components）] をクリックして、セクションを展開します。そして、[Windows 設定（Windows Configuration）] スクリプトをダウンロードします。



3. ファイルをダウンロードして、マシンで実行する予定の場所に保存します。

注

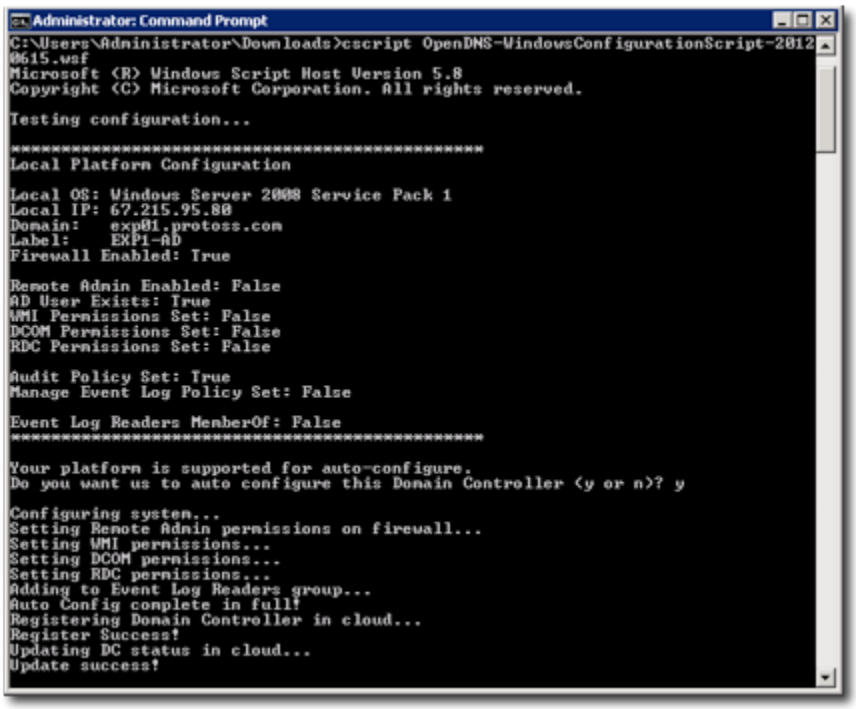
設定スクリプトは、Visual Basic Script で書かれており、人が読むこともできます。付録 B に記載の手順などを自動化したものであり、内容については、同付録を参照してください。詳細については、umbrella-support@cisco.com までお問い合わせください。

4. Admin として、管理者特権でのコマンド プロンプトを開きます。

設定開始前の重要事項

前提条件の項目で説明したように、スクリプトを実行する前に、OpenDNS_Connector のユーザを作成する必要があります。また、システムの動作に影響する複数のグループ ポリシーがあり、その場合は手動設定が必要になる場合があります。スクリプトはこれらの設定に関するステータスを表示します。必要に応じて、変更手順が提供されます。

5. コマンド プロンプトから、***cscript <ファイル名>*** を入力します。*<ファイル名>* には、手順 2 でダウンロードした設定スクリプトの名前が入ります。スクリプトに現在の設定が表示されたあと、画面を操作して、ドメイン コントローラが動作するように自動設定を進めます。自動設定の手順が成功すると、スクリプトにより、ドメイン コントローラが Umbrella のダッシュボードに登録されます。



注

「ドメイン コントローラが Umbrella の API（67.215.92.210）に 443 番ポートでアクセスできるか確認してください（Please verify that the Domain Controller can access the Umbrella API(67.215.92.210) at port 443!）」というエラー メッセージが表示され、443 番ポートが api.opendns.com、crl4.digicert.com、ocsp.digicert.com に対してオープンになっていることを確認できた場合は、DC で、DigiCert の CA が失効している可能性もあります。確認するには、https://api.opendns.com/v2/OnPrem.Asset にブラウザでアクセスしてください。証明書のエラーが表示される場合は、DigiCert から最新の DigiCert CA をダウンロードおよびインストールして、設定スクリプトを再実行してください。

ダッシュボードへの AD サーバのレポートの確認

ダッシュボードに戻ると、[Active Directory 設定（Active Directory Configuration）] ページで、直前にスクリプトを実行した AD サーバのホスト名が [非アクティブ（Inactive）] の状態で表示されます。

設定スクリプトの実行は一度のみです。これはアプリケーションやサービスではありません。ドメイン コントローラの IP アドレスやホスト名を変更する場合は、Umbrella のダッシュボードにある円形の X アイコンをクリックしてドメイン コントローラから前のインスタンスを削除します。そして、上述の手順 1 から 5 を繰り返して、ドメイン コントローラを再登録します。

すべてのドメイン コントローラでの繰り返し

単一ドメインの環境でドメイン コントローラを追加し、それぞれがコネクタと適切に通信するようにするには、上記の手順を繰り返してください。サービスを期待通りに動作させ、高可用性と全体での信頼性を保つには、単一ドメイン環境内のドメイン コントローラごとに、設定スクリプトを実行することが ***重要*** です。

---

3. VA による DNS 転送の設定 < **4. Active Directory 環境の準備**> 5. Active Directory の Umbrella への接続

5. Active Directory の Umbrella への接続

コネクタの目的は、複数のドメイン コントローラをモニタすることです。セキュリティ イベントのログを通じて、ユーザおよびコンピュータのログインをリッスンします。その後、仮想アプライアンス（VA）での IP とユーザのマッピング、IP とコンピュータのマッピングができるようになります。また、ユーザとグループ、コンピュータとグループ、グループとグループのメンバーシップが Umbrella Security Cloud と同期されます。これにより、グループ ベースの設定の作成と適用、ユーザ、コンピュータ、グループ ベースのレポートの閲覧が可能になります。

コネクタにより、Active Directory のユーザ、グループ、コンピュータのインポートが可能となり、それらのマッピングが実現します。組織単位（OU）などの他の Active Directory（AD）のオブジェクトはインポートされません。

注:

必要となるコネクタは、Umbrella のサイトごとに 1 つですが、必要に応じて冗長性を持たせるために、2 番目のコネクタをオプションとして追加できます。コネクタをすべての DC へインストールすることは推奨されません。

コネクタ サービスは、ドメイン コントローラにインストールする必要はありません。また、コネクタ サービスはドメインのメンバーである Windows Server にインストールすることができます。ただし付録 C に記載されている要件を満たす必要があります。

コネクタのインストール

1. Umbrella ダッシュボードから、[設定（Settings）] > [サイトおよび Active Directory（Sites and Active Directory）] に移動します。

2. [+] アイコン（[追加（Add）] アイコン）をクリックして、セクションを展開し、[Windows サービス（Windows Service）] のアーカイブをダウンロードします。

zip ファイルは、そのファイルを実行する予定のマシン内のフォルダにダウンロードするか、別のマシンからローカルにコピーする必要があります。圧縮ファイルから直接 setup.msi を実行したり、ネットワーク ドライブからコネクタをインストールしたりすると、問題が発生します。

3. Admin として zip ファイルの内容を展開し、フォルダにダウンロードします。
4. 展開したフォルダに移動します。
5. **setup.msi** を実行します。
6. 作成済みの **OpenDNS_Connector** ユーザに設定したパスワードを入力します (*前提条件*を参照してください)。
7. セットアップ ウィザードのプロンプトに従います。
8. 完了したら、[閉じる(Close)] をクリックします。
9. ダッシュボードに戻ります。

コネクタとダッシュボードの同期の確認

注:

コネクタがダッシュボードに表示されず、443 番ポートが api.opendns.com、crl4.digicert.com、ocsp.digicert.com に対してオープンになっていることを確認できた場合は、DC の DigiCert CA が失効している可能性があります。確認するには、https://api.opendns.com/v2/OnPrem.Asset にブラウザでアクセスしてください。証明書のエラーが表示される場合は、DigiCert から最新の DigiCert CA をダウンロードおよびインストールして、コネクタ サービスを再実行してください。それでも表示されない場合は、サポートに連絡してください。

1. ダッシュボードに戻ると、[設定(Settings)] > [Active Directory 設定(Active Directory Configuration)] のページで、コネクタをインストールしたドメイン コントローラもしくは他の Windows マシンのホスト名が確認できます。

2. Umbrella Security Cloud によって、自動的に VA が設定され、設定済みのサイトごとに、VA とドメイン コントローラがコネクタを通じて接続されます。すべての VA、AD サーバ、コネクタのステータスが [非アクティブ（Inactive）] から [アクティブ（Active）] に変わります。そのようにならない場合は、サポートに連絡してください。

3. [設定（Configuration）] > [ポリシー（Policies）] を選択します。
    - ドメイン コ（またはその他の Windows マシン）で、ユーザおよびコンピュータ グループのメンバーシップとそれ以降の変更が、コネクタ経由で Umbrella と自動的に同期されます。[新しいポリシーの追加（add a new policy）] をクリックして、グループが表示されることを確認することで、正常な同期を検証できます。
    - 他のグループの入れ子構造になっているグループを含め、ポリシー ウィザードのアイデンティティ選択内に、あらゆる AD グループが表示されるはずです。
    - グループが表示されない場合は、Active Directory の設定ページで、すべてのコンポーネントのステータスが [アクティブ（Active）]（緑色）になっているかを確認します。確認できない場合は、umbrella-support@cisco.com までお問い合わせください。

注：

多数の AD ユーザ、コンピュータ、グループ オブジェクトが初めて同期する場合には、10 分以上かかる場合があります。この間、最初の同期が完了するまでは、コネクタのステータス アイコンが赤色に表示されることがあります。同期が完了すれば、[アクティブ（Active）]（緑色）に表示されます。

すべての Active Directory コンポーネントの動作確認

1. 続行する前に、次のコマンドを入力して、VA を通じて opendns.com にクエリを送信し、DNS トラフィックを解決できるか確認します。

テキスト

```
C:¥>nslookup
> server {VA の IP アドレスを入力}
> opendns.com
```

2. さらに、次のコマンドを入力して、VA を通じて debug.opendns.com に *TXT レコード*のクエリを送信し、DNS トラフィックを確認します。

テキスト

```
> set type=TXT
> debug.opendns.com
> exit
```

VA を経由している場合は、クエリにより文字列情報が返されます。そのクエリからドメインが存在しないという結果が返される場合は、設定に問題が残っているため、サポートに連絡する必要があります。

---

4. Active Directory 環境の準備 < **5. Active Directory の Umbrella への接続**>
6. ポリシーの設定

6. ポリシーの設定

すべての Active Directory コンポーネントが正常に統合されたことが確認できたら、セキュリティとアクセプタブル ユース ポリシーを定義し、AD グループに適用します。

1. [ポリシー（Policies）] > [ポリシー リスト（Policy List）] の順に移動し、[+] アイコン（[追加（Add）] アイコン）をクリックして、新しいポリシーを追加するか、既存のポリシー名をクリックします。

2. すべての AD ユーザ、コンピュータに単一のポリシーを適用する場合は、[AD グループ（AD Groups）] ボックスをチェックします。もしくは、アイデンティティ選択で特定のグループの隣にあるボックスを 1 つないし複数チェックします。選択したグループを削除するには、アイデンティティ選択でボックスのチェックをはずすか、名前の右側の赤い X アイコンをクリックします。次に [次へ（Next）] をクリックします。

注:

グループをクリックすると、メンバーの他に、入れ子構造になっているグループ、ユーザアカウント、コンピュータ アカウントも表示されます。グループを選択すると、そのすべてのメンバーにポリシーが適用されます。入れ子構造になっているグループだけを選択することはできますが、個々のユーザやコンピュータ アカウントだけを選択することはできません。ベスト プラクティスとしては、グループのメンバーシップを Active Directory を通じて一元的に管理する方法が挙げられます。すべての変更が、Umbrella で数分のうちに同期されます。

3. このポリシーの希望するパスを選択します。DNS 層にセキュリティ設定を適用して、コンテンツ設定を制限し、1 つまたは複数のアイデンティティに宛先リストを適用することが推奨されます。

4. 関連する設定が組織のニーズに一致するように適用されることを確認した上で、ウィザードを終了します。

5. ポリシー ウィザードの最後のステップでは、ポリシーに適切な説明を入力し、設定を確認した上で、[保存（Save）] クリックします。

注:

作成したポリシーは、VA を経由して Umbrella に送信されるすべての新しい接続に、60 秒から 90 秒で適用されます。

6. ドラッグ ハンドル アイコンをクリックしてホールドし、既存のポリシーの位置を上下に入れ替えることができます。サンドイッチ アイコンを表示させてポリシーをドラッグするには、マウスオーバーする必要があります。

> **ポリシーは、上から下の順に確認され、最初に一致するものが適用される仕組みになっています。アイデンティティに最初に割り当てられたポリシーが適用され、同じアイデンティティに割り当てられているそれ以降のポリシーはすべて無視されます。デフォルトのポリシーは編集可能ですが、無効化はできず(常に一番下になります)、すべてのアイデンティティでそれまで一致しなかった対象に対応します。詳細については、『Policy Guide(ポリシーガイド)』を参照してください。**

---

5. Active Directory の Umbrella への接続 < **6. ポリシーの設定**> 7. DNS トラフィックのルーティング

7. DNS トラフィックのルーティング

設定の適用を開始するには、ネットワーク上の各クライアントからのすべての DNS トラフィックが、仮想アプライアンスを経由するようにルーティングする必要があります。

1. まず、数台のデバイスで仮想アプライアンスを使用するように DNS 設定を手動で設定して、テストします。複数のオペレーティング システムやハードウェア タイプ（モバイル デバイスなど）で試し、すべてのデバイスとの互換性を確認します。

   重要: ***ポリシーの適用をテストする際には、数分から数日分の DNS 応答がすでにキャッシュされている可能性があります。ブラウザで DNS キャッシュを消去し、OS がキャッシュされた応答が期限切れになるまで待機しないようにする必要があります。***

2. 可能な場合、次の手順として組織内の特定の DHCP サーバ プールまたはスコープの DNS 設定を変更することが推奨されます。

3. 検証用のコンピュータ グループへのポリシーの適用に問題がないことを確認できたら、その後順次、DNS に仮想アプライアンスを使用した環境、組織全体の環境に進むことができます。環境に反映させる最適なタイミングは、通常、ユーザがログアウトしてから 1 日程度後になります。クライアントの DHCP スコープをリモートまたは自動で容易に更新する方法はない点に留意してください。

4. インストールの完了後にユーザがログインすると、DNS トラフィックを転送する VA のいずれかに、すべての DNS クエリの送信を開始されるはずです。

注:

ほとんどのスタブ DNS リゾルバ、特にエンドポイント デバイスのスタブ DNS リゾルバには、DNS サーバのプライマリとセカンダリの関係はありません。スタブ DNS リゾルバの動作で、どのような時に、どの DNS サーバを使用するかということについては、多くのオペレーティング システムで文書化されていません。

付録 A: 通信フローおよびトラブルシューティング

Umbrella と Active Directory の統合における通信フローについて

統合の範囲は、Active Directory（AD）設定の複数の領域にまたがっており、各運用コンポーネント間の通信フローを理解することが重要です。こうした知識は、トラブルシューティングにも役立ちますし、導入前の設定が適切になされているか確認する上でも有用です。

コネクタのスクリプトを DC で実行する場合:

Windows Connector のスクリプトは、ドメイン コントローラ（DC）から Umbrella Cloud への一度限りの接続を確立します。その際のポートは、TCP/443 で、HTTPS を使用します。これは、DC をダッシュボードに登録するためのもので、登録によりコネクタにそのことが通知されます。特定のパラメータを使用して、https://api.opendns.com へのコールが実行されます。

スクリプトにより、DC が正常に登録されると、[サイトおよび Active Directory（Sites & Active Directory）] ページ（[設定（Settings）] > [サイトおよび Active Directory（Sites and Active Directory）] ）に一覧が表示されるはずです。

なお、Windows の「ルート証明書の更新」に関連する問題が以前から確認されています。問題に該当するかどうかを確認するには、Internet Explorer を開き、https://api.opendns.com/v2/OnPrem.Asset にアクセスするのが簡単な方法です。

アクセスすると、**「1005 Missing API key（1005 API キーがありません）」**のようなメッセージが表示されるはずです。

そのページで証明書のエラーや警告が表示される場合は、Microsoft の最新の「ルート証明書の更新」がインストールされているか確認してください。

AD のコネクタと Umbrella Cloud サービスまたは仮想アプライアンスが通信する際の方法:

コネクタ > クラウド

コネクタは、*変更がある場合に*、すべての AD データを、**TCP の 443 番**ポートで HTTPS 接続を使用して、2 分おきにアップロードします。アップロードされる情報は、グループ、ユーザ、コンピュータのみで、パスワードは送信されません。すべてのユーザ情報はローカルでハッシュされており、送信されるデータは一意になります。データは Umbrella Cloud サービスに 2 分おきに送信されますが、ダッシュボードに変更が反映されるには 30 分程度を要する場合があります。

コネクタ > 仮想アプライアンス

コネクタは、**TCP の 443 番**ポートを使用して、AD のイベントを仮想アプライアンス（VA）に常に送信しています。この通信は一方向の通信で、アプライアンスがコネクタに通信を返すことはありません。コネクタのログは、**TCP の 8080 番**ポートで VA に送信されます。

コネクタ > ドメイン コントローラ

コネクタは、同一サイトに存在するすべてのドメイン コントローラと通信を行います。その際には **TCP の 389 番**ポートを使用し、LDAP の同期に **TCP/UDP の 3268 番**ポートを使用します。また、コネクタはドメイン コントローラとの通信に、RPC や WMI も使用します。一般的に、RPC や WMI の標準ポートは、**TCP の 135 番**ポートです。

AD バージョンによっては、WMI の場合、ランダムに割り当てられたエフェメラル ポートも使用されます。Windows 2003 以前では、**TCP 1024 番**から **TCP 65535 番**の間、Windows 2008 以降では、**TCP 49152 番**から **TCP 65535 番**の間になります。

通信に関してなんらかの問題がみられる場合は、レイヤ 7 のアプリケーション プロキシでデータがブロック/ドロップされていないか確認することを、まず推奨しています。一般的な事例としては、DNS、HTTP、HTTPS などのプロトコルで動作するシスコ デバイスの検査機能が影響している場合が挙げられます。
http://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/inspect.html

仮想アプライアンス（VA）からクラウド、他のインターネット接続、内部 DNS サーバへの通信

VA は、Umbrella の API と頻繁に通信を行います。その際、TCP の 443 番ポートで api.opendns.com と通信します。また、443 番ポートで、disthost.opendns.com からアップデートを受信します。VA は、TCP の 443 番ポートでコネクタからデータを受信しますが、コネクタへ通信を返す必要はありません。

さらに、サポート トンネルを確立するために、TCP の 443 番、80 番、2222 番ポートでの通信を必要とします。VA は、内部 DNS 要求の内部 DNS サーバへの転送も行います。VA と内部 DNS サーバ間で、UDP の 53 番ポートがオープンになっていることを確認してください。

次の表に、要求の送信元と宛先、および各リクエストの機能について示します。

ポート	送信元/送信先	機能
53/UDP 53/TCP	208.67.222.222、 208.67.220.220 （アウトバウンド） ローカル クライアント （インバウンド） 内部 DNS （アウトバウンド）	• DNS クエリの送信および受信。 • 可能な場合、Umbrella へのアウトバウンドの DNS クエリは、DNSCrypt で暗号化されます。そのため、パケット インスペクション ルールがトリガーされる場合があります。
443/TCP	api.opendns.com disthost.opendns.com （アウトバウンド）	• Umbrella API および Umbrella ダッシュボードへの最初の登録。 • 自動アップデート • Umbrella ダッシュボードでのヘルス ステータスのレポート。
123/TCP	ntp.ubuntu.com	• NTP。ブート時にのみ使用。
80/TCP	*ocsp.digicert.com*、 crl4.digicert.com （アウトバウンド）	*HTTPS ハンドシェイクにおける SSL の失効確認の際に必要。

2222/TCP または 80/TCP または 443/TCP	67.215.92.28 （アウトバウンド）	• Umbrella の SSH ハブへの接続。VA に関係する問題が発生した場合に、サポートがログインしてトラブルシューティングを実行できるようにします。*SSH トンネルに関する詳細については、本ドキュメントの最後の項目を参照してください。*

注：Digicert のドメインは、CDN に基づいて複数の IP アドレスに解決されており、変更される場合があります。現時点では、これらのドメインは次の IP に解決されています：72.21.91.29、117.18.237.29、93.184.220.29、205.234.175.175

AD コンポーネントを使用している（内部 IP アドレスの粒度のために VA を使用しているのではない）場合は、さらに加えて、次のインバウンド ネットワーク トラフィックが AD コネクタ サービスから発生します。

ポート	送信元/送信先	
443/TCP 8080/TCP（インバウンド）	AD コネクタ	• ログイン イベントや IP アドレッシングに関する情報を送信。トラフィックは 443/TCP で行われますが、HTTPS 接続ではありません。多くの IDS や IPS システムは、このようなトラフィックに疑わしいものとしてフラグを付けます。IDS や IPS を実行しており、ローカル ネットワークをリッスンさせている場合は、適用ログをチェックして、このトラフィックがブロックされていないことを確認してください。

AD コネクタ サービス

ポート	送信元/送信先	機能
389/TCP 3268/TCP 135/TCP 1024-65535/TCP（Server 2003）	AD サーバ（ドメイン コントローラ） （アウトバウンド）	• ドメイン コントローラ間での WMI/RPC/DCOM 通信 • LDAP の同期

49152-65535/TCP （Server 2008/2012）		
443/TCP （非 SSL） 8080/TCP	仮想アプライアンス （アウトバウンド）	• ログイン イベントや IP アドレッシングに関する情報を送信。このトラフィックは 443/TCP で行われますが、SSL 接続ではないことに注意する必要があります。多くの IDS や IPS システムは、このようなトラフィックに疑わしいものとしてフラグを付けます。IDS や IPS を実行しており、ローカル ネットワークをリッスンさせている場合は、適用ログをチェックして、このトラフィックにフラグが付与されていないことを確認してください。
443/TCP	api.opendns.com disthost.opendns.com （アウトバウンド）	• Umbrella API および Umbrella ダッシュボードとの最初の統合。 • 自動アップデート • Umbrella ダッシュボードでのヘルス ステータスのレポート。
80/TCP 80/UDP	crl.comodoca.com ocsp.comodoca.com crl.usertrust.com ocsp.usertrust.com	• Online Certificate Status Protocol（OCSP）と、SSL の失効に関する証明書失効リスト（CRL）の維持に必要。
80/TCP	*ocsp.digicert.com*、 crl4.digicert.com （アウトバウンド）	• HTTPS ハンドシェイクにおける SSL の失効リストの確認の際に必要。

注：Digicert のドメインは、CDN に基づいて複数の IP アドレスに解決されており、変更される場合があります。現時点では、これらのドメインは次の IP に解決されています：72.21.91.29、117.18.237.29、93.184.220.29、205.234.175.175

AD サーバ(ドメイン コントローラ)

ポート	送信元/送信先	機能
389/TCP 3268/TCP 135/TCP 1024- 65535/TCP（Server 2003） 49152-65535/TCP（Server 2008/2012）	AD コネクタ（アウトバウンド）	• ドメイン コントローラ間での WMI/RPC/DCOM 通信 • LDAP の同期
443/TCP	api.opendns.com（アウトバウンド）	• Umbrella API の最初の登録。
80/TCP	*ocsp.digicert.com*、crl4.digicert.com（アウトバウンド）	*HTTPS ハンドシェイクにおける SSL の失効リストの確認の際に必要。

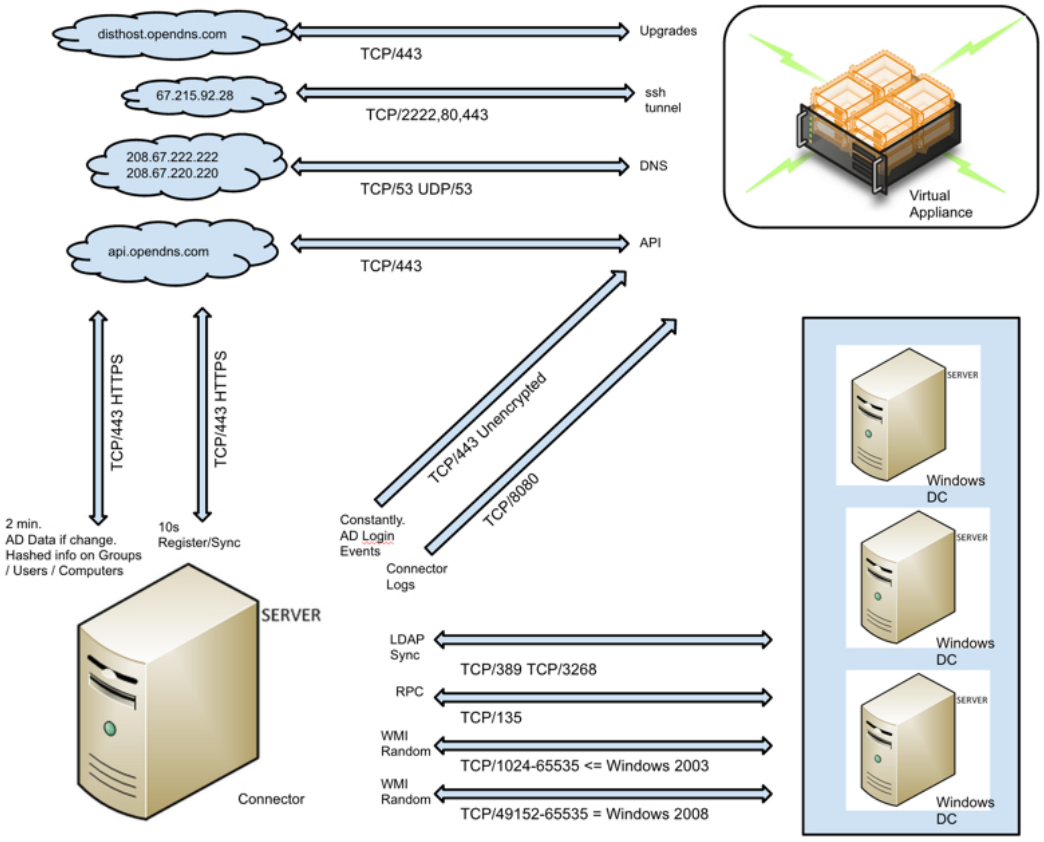
注:Digicert のドメインは、CDN に基づいて複数の IP アドレスに解決されており、変更される場合があります。現時点では、これらのドメインは次の IP に解決されています:72.21.91.29、117.18.237.29、93.184.220.29、205.234.175.175

Umbrella の Windows Connector のスクリプトの内容

Windows Connector のスクリプトは、OpenDNS_Connector ユーザの特定のユーザ権限を設定しています。ユーザが削除されると、スクリプトによる影響も失われます。非常に厳しく制御された AD 環境でスクリプトを実行する場合、管理者に VB スクリプトの実行が許可されない場合があります。その場合は、サポートまでお問い合わせください。

概要図

次の図は、Umbrella と Active Directory の統合におけるコンポーネント間のトラフィック フローについて概要を示したものです。



SSH サポート トンネル:トンネルの許可またはブロックの方法について

トラブルシューティングやサポートの支援を行うために、VA が Umbrella へのサポート トンネルの確立を試行する場合があります。このサポート トンネルは VA から開始され、特定の権限を有したサポート担当者のみがアクセスできる特定の終端サーバに接続する SSH トンネルです。この終端サーバへアクセスは厳しく制限されており、アクセス権を得るには、サーバに有効なキーが存在する必要があります。また、このサーバはサポート チームのネットワーク スペースの範囲内からでないとアクセスできません。

この SSH トンネルはオプションであり、VA が正常に機能するために必要なものではありません。67.215.92.28 に対する TCP 2222 番ポート、TCP 80 番ポート、TCP と UDP の 443 番ポートをブロックすることで、サポート トンネルの使用を防ぐことができます。

なお、トンネルの確立をブロックすることで、サポート担当者が仮想アプライアンスに関連する問題のトラブルシューティングやリモートでの解決を行う際に制約が生じる点に留意してください。問題の診断にあたり、サポート担当者がポートのオープンを求める場合があります。SSH サポート トンネルのハブの IP アドレスについては、シスコの裁量により変更される場合があります。その場合、事前にお客様に通知されます。

---

7. DNS トラフィックのルーティング < **付録 A: 通信フローおよびトラブルシューティング** > 付録 B: 複数の Active Directory と Umbrella サイト

付録 B: 複数の Active Directory と Umbrella サイト

Umbrella サイト

Umbrella のサイト機能により、管理者は Umbrella 環境を分割することができます。Umbrella サイトはそれぞれ独立した環境であり、Umbrella サイト内のコンポーネントは同一サイト内のコンポーネントのみと通信します。Umbrella サイトは、大規模な複数サイト ネットワークの一部をグループに分割するためのコンテナです。グループでは、コンテナ内の他のコンポーネントとだけ同期します。たとえば、Umbrella サイトは、北米/アジア/ヨーロッパ、米国北東部/カリフォルニア/アトランタ オフィス、南部/ロンドン、などのように分割できます（各 Umbrella サイトは、AD サイトを 1 つ、もしくは複数の AD サイトの組み合わせとすることができます）。

このような仕組みは、接続が大幅に遅延するサイトを含む Active Directory 環境や、一部で内部 IP アドレス空間が重複する環境などに対して、特に有効です。

Active Directory サイトと Umbrella サイト

サイトとは、ローカル エリア ネットワーク（LAN）などの高速ネットワークで接続されたコンピュータ群を意味します。通常、同じ物理サイトにあるコンピュータは、すべて同じ建物か同じキャンパス ネットワーク上に存在します。Active Directory と Umbrella の両方で「サイト」という用語を使用していますが、関連はしているものの、その意味は若干異なります。

Active Directory のサイトとサービス

- AD では、サイト オブジェクトとは、ドメイン コントローラ間で複製される実際のディレクトリのデータを意味します。
- AD のサイトは、サイトやサイトに存在するサーバを表しているオブジェクトを管理するために使用されます。

Umbrella サイト

- Umbrella では、サイトとは、互いに通信を行うコンポーネント（VA、コネクタ、DC）の組み合わせを意味しています。
- Umbrella サイトは単なるラベルというよりはコンテナに近いものです。ただし、AD のサイトとは同じではありません。複数の AD サイトが、Umbrella のサイトの一部になることができます。しかし、単一の AD サイトを複数の Umbrella のサイトに分割することはできません。
- サイトには、少なくとも 2 つの VA と、AD 統合ごとにコネクタと DC が 1 つずつ必要になります。

Umbrella のサイトは、それぞれ独立した環境として機能するため、それぞれの Umbrella サイトに最低でも 2 つの**仮想アプライアンス（VA）**が必要です。Active Directory 統合も使用される場合は、各サイトに少なくとも AD コネクタを 1 つ追加する必要があります。また、そのロケーションのユーザは**すべての**ドメイン コントローラに対して認証を行う必要があります。

Umbrella サイトが有効な場面

- ロケーション間の WAN トラフィックを制限する必要があり、Active Directory のサイトを使用してローカル サーバへの認証を制限している場合（http://technet.microsoft.com/en-us/library/cc782048(v=ws.10).aspx）。
- 各ロケーションの NAT デバイス間で通信が行われており、そのため、ロケーション間で通信が発生する場合、エンド マシンの内部 IP アドレスが失われる場合。
- ロケーションで重複する内部 IP 範囲を使用している場合。
- 接続が大幅に遅延するロケーションが存在する場合（異なる大陸の支社間で大幅な遅延が発生するなど）。接続が大幅に遅延する場合、特にコネクタと VA 間で大幅な遅延が発生する場合、ユーザ マッピングの更新に遅延が発生する可能性があります。

注意事項

特定の Umbrella サイトのコンポーネントを分離すると、同じ Umbrella サイトに割り当てられたドメイン コントローラで認証されていたユーザが、特定の VA でしか認識されなくなります。そのため、単一の Active Directory サイトで複数の Umbrella サイトを使用することは、AD サイトが複数の地理的ロケーションから構成されているとしても、推奨されません。そのような状況においては、あるロケーションに位置するユーザが、別のロケーションの DC で認証を行う可能性があり、この場合、Umbrella コンポーネントがユーザのマッピングに失敗する可能性があります。

Umbrella サイトの使用

個々の Umbrella サイトは、それぞれが完全な環境として設定される必要があります。つまり、各 Umbrella サイトで次のようにします。

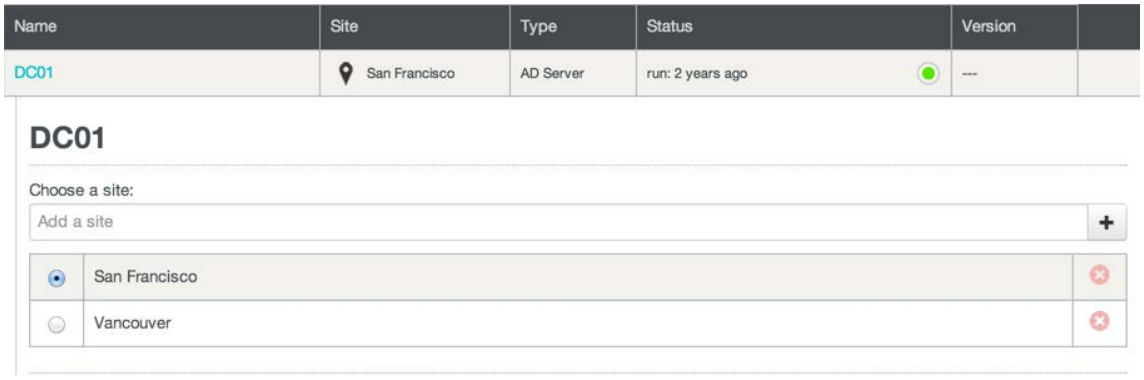
- 本ガイドの前の手順を再び実施します。コンポーネントが同期され、ダッシュボードへのレポートが行われていることを確認する各サブステップの後に、サイトの名前を選択するか、既存サイトを選択するか、新しいサイトを作成して、コンポーネントを**サイト**に割り当てます。
- また、デフォルトもしくは既存のサイトについては、名前を変更することもできます。

重要

少なくとも VA が 2 つ、AD サーバが 1 つ、AD コネクタが 1 つ、各サイトに割り当てられていることを確認します。次のサイトの設定に進む前に、それぞれのサイトの導入の完了と動作を確認するようにしてください。

コンポーネントにサイトを割り当てるには、既存の Insights のアイデンティティをクリックします（ダッシュボードの [設定（Settings）] > [サイトおよび Active Directory（Sites and Active Directory）] の下）。ドロップダウンには、新しいサイトを追加したり、コンポーネントのサイトを変更したりするメニューがあります。

Active Directory のみ：コネクタ サービスをインストールした後に、Insights のコンポーネントのロケーションを変更する場合は、新規の Umbrella サイトと既存の Umbrella サイトの両方で、Windows のサービス管理ツールから各コネクタのコネクタ サービスを停止/起動する必要があります。



付録 C　: AD サーバ以外の別のサーバにコネクタをインストールする準備

プロセス

セキュリティ ポリシーから必要とされる場合は、コネクタを AD サーバ以外のマシンにインストールすることもできます。ただし、コネクタをモニタする AD サーバとして同じドメインに参加させる必要があります。

注: 現在、コネクタは .NET 4.0 または .NET 4.5 のみでインストールすることができます（.NET 3.5 のインストールは不要です）。

1. スタティック IP を使用して、物理マシンまたは仮想マシンをプロビジョニングします。

2. 検証済みでサポート対象となっている、次の 3 つの Windows OS バージョンとその他のコンポーネントをインストールします。

Windows Server 2008 R2 SP1、Windows Server 2012 R2、Windows Server 2016（推奨 OS）

1. [リモート サーバ管理ツール（Remote Server Administration Tools）] > [ロール管理ツール（Role Administration Tools）] > [AD DS および AD LDS ツール（AD DS & AD LDS Tools）] > [AD DS ツール（AD DS Tools）] から、AD ドメイン サービス スナップインとコマンドライン ツール機能をインストールします。

2. .NET バージョン 3.5、4.0、4.5 のいずれかをインストールします。
   OS 固有の手順については、次を参照してください:
   https://support.microsoft.com/en-us/kb/2693643

Windows Server 2008 SP2

1. Active Directory の Lightweight Directory Services のロールをインストールします。

2. .NET バージョン 3.5、4.0、4.5 のいずれかをインストールします。

Windows 7（ホーム ライセンス以外）

1. リモート サポート管理ツールをインストールします。次からダウンロードします：http://go.microsoft.com/fwlink/?LinkID=137379

2. AD DS および AD LDS ツールの有効化：
   a. ウィザードの要求するすべて完了させ、[完了（Finish）] をクリックします。
   b. [スタート（Start）] からコントロール パネルをクリックし、[プログラム（Programs）] をクリックします。
   c. [プログラムと機能（Programs and Features）] のエリアで、[Windows の機能の有効化または無効化（Turn Windows features on or off）] をクリックします。
   ユーザ アカウント制御のプロンプトが表示され、[Windows の機能（Windows Features）] ダイアログ ボックスを開く許可が求められた場合は、[続行（Continue）] をクリックします。

3. [Windows の機能（Windows Features）] ダイアログ ボックスで、[リモート サーバ管理ツール（Remote Server Administration Tools）] を展開し、[AD DS および AD LDS ツール（AD DS and AD LDS Tools）] を選択して、[OK] をクリックします。

4. .NET バージョン 3.5、4.0、4.5 のいずれかをインストールします。

3. 接続されている AD サーバ（ドメイン コントローラ）と同じドメインにマシンを参加させます。

4. 次のコマンドを管理者権限で実行し、WMI ポートをオープンにします:
   netsh advfirewall firewall set rule group="Windows Management Instrumentation (WMI)" new enable=yes

---

付録 B: 複数の Active Directory と Umbrella サイト < **付録 C: AD サーバ以外の別のサーバにコネクタをインストールする準備** > 付録 D: Windows Server 2003 R2 での AD サーバの設定

付録 D: Windows Server 2003 R2 での AD サーバの設定

「監査およびセキュリティ ログの管理」グループ ポリシーの設定

注:

特有の Windows Server 2008 の設定では、OpenDNS_Connector のユーザをすべての AD サーバ(DC)用のこのグループ ポリシーに追加する必要があります。

1. デフォルトでは、Windows Server 2003 にはグループ ポリシー管理コンソール(GPMC)がありませんが、こちらからダウンロードできます: http://www.microsoft.com/en-us/download/details.aspx?id=21895

注:

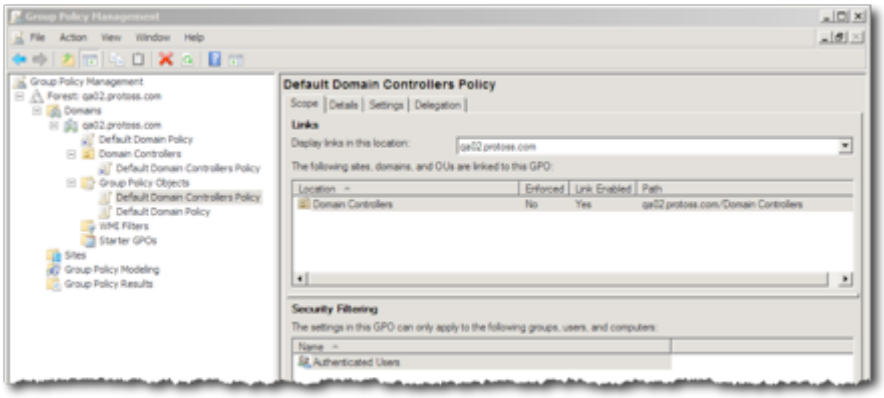
もしくは、2008 R2 サーバには、GPMC がインストールされているはずなので、次の権限を適用して、そのサーバから 2003 R2 サーバに複製することができます。

2. GPMC を起動させ([スタート(Start)] > [管理ツール(Administrative Tools)])、ドメイン コントローラに適用するグループ ポリシーを選択します。

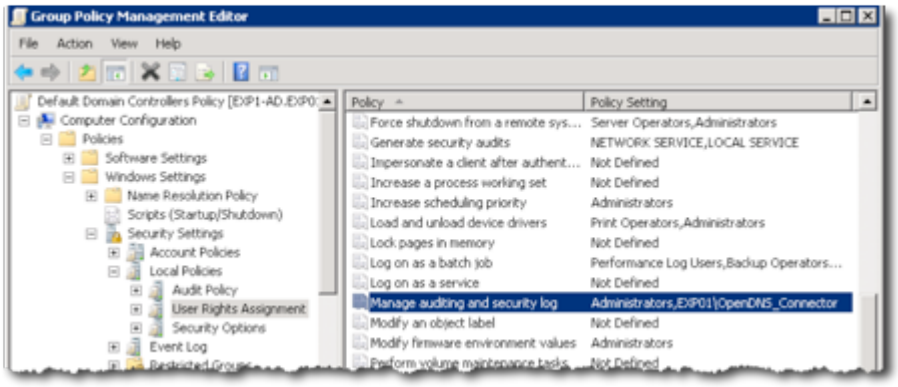
注:

変更すべきポリシーが不明な場合は、コマンド プロンプトを開き、次のコマンドを入力します:「gpresult /scope computer /r] 。「Applied Group Policy Objects」の行を確認します。その行の下に、ドメイン コントローラに適用されているポリシーの一覧が表示されます。すべてのドメイン コントローラに適用されている可能性が高いポリシーに注意してください(たとえば、「Default Domain Controllers Policy」)。

1. ポリシーを右クリックして、[編集(Edit)] を選択すると、グループ ポリシー管理エディタが起動します。



2. 「Computer Configuration¥Policies¥Windows Settings¥Security Settings¥Local Policies¥User Rights Assignment」フォルダを参照し、「Manage audit and security log」を選択して、プロパティを表示させます。



3. [これらのポリシー設定を定義(Define these policy settings)] にチェックを入れ、[ユーザまたはグループの追加(Add user or group)] をクリックし、OpenDNS_Connector のユーザを参照して選択します。

4. ドメイン コントローラで、「gpupdate」コマンドを実行し、ポリシーが適用されていることを確認します。

DCOM 権限の設定

1. コマンドラインから **dcomcnfg** を実行します。
2. [コンソール ルート(Console Root)] > [コンポーネント サービス(Component Services)] > [コンピュータ(Computers)] の順に移動します。
3. [マイ コンピュータ(My Computer)] を右クリックし、[プロパティ(Properties)] を選択します。
4. [マイ コンピュータのプロパティ(My Computer Properties)] から、[COM セキュリティ(COM Security)] タブを選択します。
5. [起動およびアクティベーション権限(Launch and Activation Permissions)] のエリアで、[制限の編集(Edit Limits)] をクリックします。
6. OpenDNS_Connector のユーザを追加し、[リモート起動(Remote Launch)] と [リモート アクティベーション(Remote Activation)] の権限を許可します。
7. [OK] をクリックして確認し、[マイ コンピュータのプロパティ(My Computer Properties)] を閉じます。

WMI 権限の設定

1. **wmimgmt.msc**(Windows インフラストラクチャ管理制御コンソール)を実行します。
2. [WMI 制御(WMI Control)] を右クリックします。[プロパティ(Properties)] > [セキュリティ(Security)] タブをクリックします。
3. [ルート(Root)] > [CIMV2] の名前空間を選択し、[セキュリティ(Security)] をクリックします。

4. OpenDNS_Connector のユーザを追加し、次の権限を [許可(Allow)] します: [アカウントの有効化(Enable Account)]、[リモートでの有効化(Remote Enable)]、[セキュリティの読み込み(Read Security)] 。

5. 各ダイアログ ウィンドウを終了するには [OK] をクリックします。[保存(Save)] をクリックして、変更を適用します。

付録 C: AD サーバ以外の別のサーバにコネクタをインストールする準備 <**付録 D: Windows Server 2003 R2 での AD サーバの設定** >