Cisco SD-WAN セルフサービスポータル

Cisco SD-WAN セルフサービスポータル の概要

Cisco SD-WAN セルフサービスポータル（SSP）は Amazon Web Services（AWS）GovCloud でホストされる Web アプリケーションで、次の操作を実行できます。

- Cisco SD-WAN オーバーレイネットワークを作成および管理します。
- オーバーレイネットワークの正常性をモニタリングします。

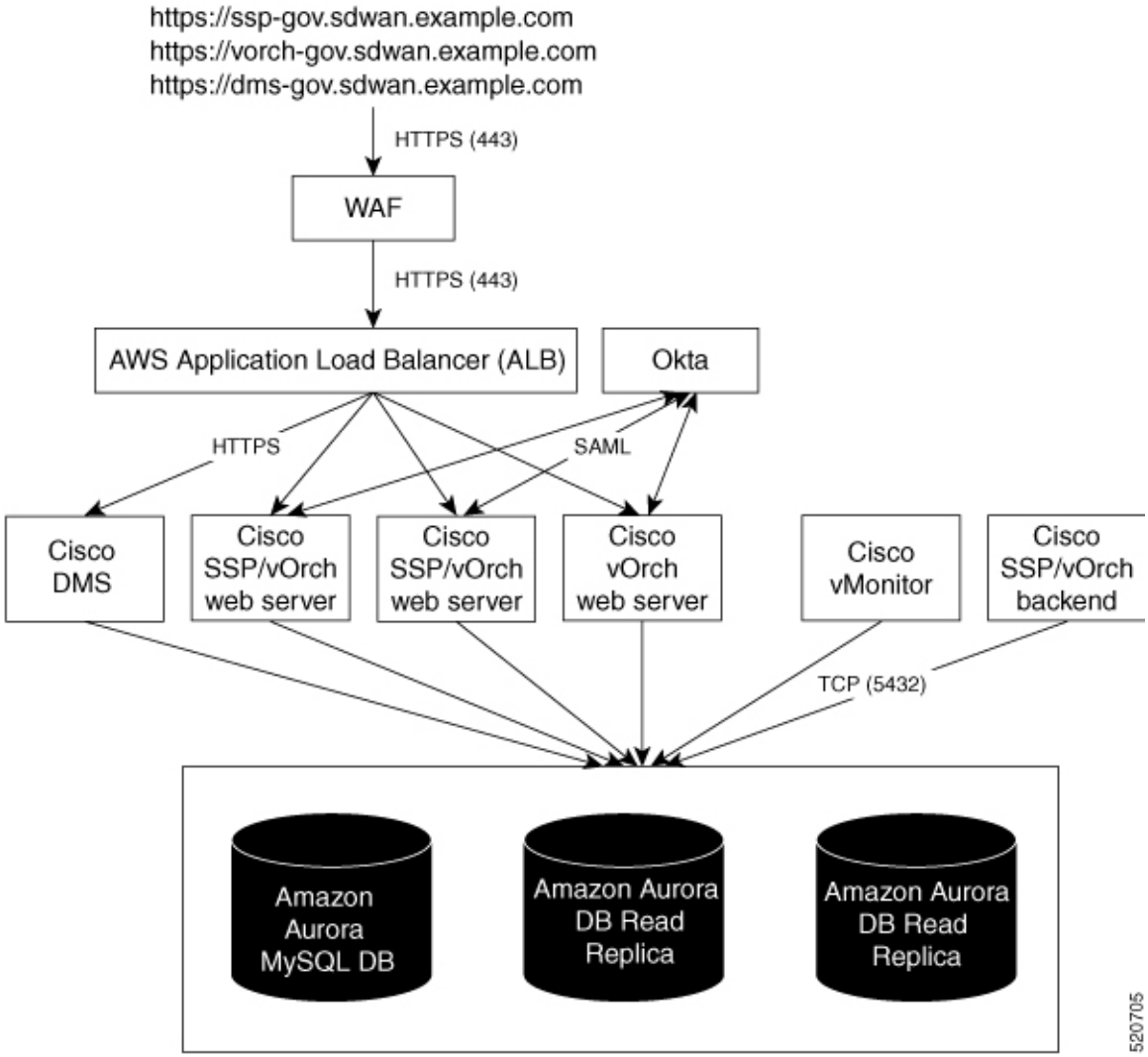
Cisco SD-WAN SSP は、DoS（Denial of Service）攻撃や DDoS 攻撃を防ぐために、ファイアウォールとアプリケーションロードバランサによって保護されます。Okta またはその他の IdP を使用して Cisco SD-WAN SSP に接続し、すべてのログインについて MFA を提供することができます。IdP を使用すると、シングルサインオン（SSO）を使用して任意のユーザーを任意のデバイスの任意のアプリケーションに接続できるセキュアな ID 管理サービスを確実に使用できます。Cisco SD-WAN SSP は、ソフトウェアの拡張性を実現するために、モジュール化されて個別の Web サーバー、バックエンドサーバー、およびデータベースクラスタに組み込まれます。

Cisco vMonitor は、クラウドインフラストラクチャをモニタリングし、お客様のオーバーレイインフラストラクチャに関する正常性通知を共通データベースに更新します。Cisco vOrchestrator Web サーバーは、高度な機能や、使用している既存のインフラストラクチャ層のカスタマイズ（ある場合）にもアクセスできます。Cisco SD-WAN SSP は、Cisco vMonitor および Cisco vOrchestrator を使用して、アクション を調整し、オーバーレイをモニタリングします。

（注） Cisco vOrchestrator および Cisco vMonitor には、Cisco FedOps のみがアクセスできます。

高可用性を維持するためおよびディザスタリカバリ用の複数のリードレプリカが備わっている共通のグローバルデータベースは、3つのアプリケーションすべてで使用され、アプリケーションは Transport Layer Security（TLS）または Secure Socket Layer（SSL）接続を使用してデータベースに接続します。

図 *1 : Cisco SD-WAN SSP* の概要



官公庁向け Cisco SD-WAN のユーザーには、 次の 2 つのタイプがあります。

- お客様（サービスプロバイダー、パートナー、その他のエンドユーザーなど）。
- Cisco Federal Operations（FedOps）：官公庁向け Cisco SD-WAN を維持およびモニタリングするシスコのチーム。

（注） Cisco FedOps はお客様の Amazon VPC にアクセスできません。

初めての Cisco SD-WAN セルフサービスポータル の使用

Cisco SD-WAN SSP に初めてログインすると、ガイド付きワークフローが表示されます。このワークフローは、任意の操作として、一部の機能を設定し、最初の Cisco SD-WAN オーバーレイネットワークを作成するために役立ちます。

以下のセクションでは、このワークフローについて詳しく説明します。

Cisco SD-WAN セルフサービスポータル へのログイン

Cisco SD-WAN SSP にログインするときは、シスコのログイン情報を使用する必要があります。

1. Cisco SD-WAN SSP URL に移動します。
2. ログインページで、[Login via external Cisco IDP] をクリックします。
3. シスコのログイン情報を入力します。
4. プロンプトが表示されたら、MFA ログイン情報をセットアップまたは入力します。

   オンボーディングウィザードが表示されます。

（任意）Cisco SD-WAN SSP の IdP の設定

Cisco SD-WAN SSP に初めてログインするときに、任意で、組織の IdP を使用するように Cisco SD-WAN SSP を設定できます（Okta ID 管理など）。IdP とロールを設定すると（「（任意）IdP ユーザーの Cisco SD-WAN セルフサービスポータル ロールの設定」を参照）、Cisco.com アカウントのログイン情報の代わりに独自の IdP を使用してログインできます。

（注） Cisco SD-WAN SSP で IdP を設定する前に、組織の IdP に次の変数を作成する必要があります。Cisco SD-WAN SSP では、ログインするユーザーごとにこれらの変数が必要です。

- firstName
- lastName
- 電子メール
- SSP_User_Role

1. IdP の次の情報を指定します（この情報は IdP で確認できます）。
   - Domain Name
   - IdP の発行元 URL
   - IdP SSO URL

- IdP 署名証明書（.pem 形式）

2. （連邦政府の環境にのみ適用）、[I acknowledge that this is a Federal IDP] チェックボックスにチェックを入れます。
3. [Submit Request] をクリックします。
4. IdP サイトで、IdP の作成を確認します。
5. [Go to Role Management] をクリックします。

（任意）IdP ユーザーの Cisco SD-WAN セルフサービスポータル ロールの設定

1. 権限の名前を入力します。
2. バーチャルアカウントごとに、次のリストからロールを割り当てます。
   - [Monitor]：Cisco SD-WAN SSP のすべてのオーバーレイオプションを表示およびモニタできます。
   - [Overlay Management]：オーバーレイネットワークを作成、変更、およびモニタできます。
   - [Administration]：モニタおよびオーバーレイ ネットワーク ロールによって定義されたすべてのタスクを実行し、新しい IdP をオンボードできます。
3. [**ロールの追加（Add Role**）] をクリックします。
4. Cisco SD-WAN SSP からログアウトする。
5. IdP とログイン情報を使用して Cisco SD-WAN SSP に再度ログインします。

Cisco SD-WAN クラウドホスト型オーバーレイネットワークの作成

1. [Go to Overlay Creation] をクリックします。
2. [Overlay] をクリックし、オーバーレイネットワークを関連付ける仮想アカウントの名前を選択します。
3. [Cisco Hosted] または [Non-Cisco Hosted] を選択します。

   [Non-Cisco Hosted] を選択した場合は、データストレージの場所を設定します。
4. [Next] をクリックします。
5. [Amazon Web Services] を選択します。
6. 選択したホスティングモデリングに応じて、次を設定できます。

- [Cisco Hosted]
  1. クラウドホスト型コントローラのプライマリとセカンダリの場所を選択します。

     地理的な冗長性を実現するために、プライマリとセカンダリの異なる場所を選択することを推奨します。
  2. モニタリングデータを保存する場所を選択します。
  3. Cisco SD-WAN バージョンを選択します。
- [Non-Cisco Hosted]
  1. モニタリングデータを保存する場所を選択します。

7. [Next] をクリックします。
8. Cisco SD-WAN オーバーレイネットワークの所有者または管理者の電子メールアドレスを入力します。
9. [Overlay Status] で、[Production] を選択します。
10. **[サマリー（Summary）]** をクリックします。
11. （任意）サブネット、DNS名、またはスナップショット設定をカスタマイズするには、[Advanced Options] で [Edit] をクリックします。
    - Subnets
      - プライマリおよびセカンダリサブネットに対して、VPC サブネットを指定します。最大 3 つのサブネットを指定できます。
      - TACACS ベースのユーザー認証および許可用に Cloud vEdge をプロビジョニングする場合は、チェックボックスをオンにします。
    - DNS 名
      - Cisco vBond オーケストレーション のカスタム DNS 名を入力します。
      - Cisco vManage のカスタム DNS 名を入力します。
    - スナップショット設定
      - 次のいずれかからスナップショットを取得する頻度を選択します。
        - **1 日に 1 回**
        - **2 日に 1 回**
        - **3 日に 1 回**
        - **4 日に 1 回**

最大 10 個のスナップショットを選択できます。

（注） デフォルトでは、ネットワークオーバーレイ設定は 1 日に 1 回バックアップされ、10 個のスナップショットが保存されます。

12. 入力した詳細を確認します。
13. [Submit Request] をクリックします。
14. 一意のコントローラパスワードが表示されます。このパスワードは、作成後にオーバーレイネットワークにアクセスするために使用できます。

（注） 環境を保護するために、ログイン後すぐにパスワードを変更することをお勧めします。

IP アドレスに対するオーバーレイネットワークへのアクセスの許可

シスコがホストするオーバーレイネットワークでは、オーバーレイネットワークにアクセス可能な、信頼できる IP アドレス（プレフィックスを含む）を指定できます。ユーザーアクセスを要求するには、アクセスが必要なルールタイプ、プロトコル、ポート範囲、および送信元IP（IP アドレスとプレフィックス）を指定します。

（注） Cisco IOS XE SD-WAN デバイス の IP アドレスを追加する必要はありません。Cisco IOS XE SD-WAN デバイス を稼働させるときに、IP アドレスとプレフィックスが自動プロセスによって追加されます。

1. Cisco SD-WAN SSP ダッシュボードから、オーバーレイネットワークに移動します。
2. ドロップダウンリストから、[Cisco Hosted Overlays] をクリックします。

   オーバーレイネットワークのリストが表示されます。
3. オーバーレイネットワークの名前をクリックします。
4. [Inbound Rules] をクリックします。
5. IP アドレスまたはプレフィックスの次のパラメータを指定します。
   - **ルールタイプ**：[All]、[SSH]、[HTTPS]、[Custom TCP rule]、または [Custom UDP rule] を選択します。
   - **ポート範囲**：カスタム TCP および UDP ルールの場合、ポート範囲を指定します。

- **送信元**：IP アドレスまたは IP アドレスプレフィックスを指定します。

6. [Add] をクリックします。
7. （任意）許可する IP アドレスまたは IP アドレスプレフィックスを追加します。
8. [保存（Save）] をクリックします。

Cisco SD-WAN セルフサービスポータル の設定

Cisco SD-WAN SSP を初めて設定した後に、追加のオーバーレイネットワーク、ユーザーとロール、および子 IdP をセットアップすることもできます。同じ IdP に対して複数の子 IdP を設定できます。子 IdP にサブ子 IdP を設定することもできます。

追加のオーバーレイネットワークの作成

Cisco SD-WAN クラウドホスト型オーバーレイネットワークを作成するには、次の手順に従います。

1. [Go to Overlay Creation] をクリックします。
2. [Overlay] をクリックし、オーバーレイネットワークを関連付ける仮想アカウントの名前を選択します。
3. [Cisco Hosted] または [Non-Cisco Hosted] を選択します。

   [Non-Cisco Hosted] を選択した場合は、データストレージの場所を設定します。
4. [Next] をクリックします。
5. [Amazon Web Services] を選択します。
6. 選択したホスティングモデリングに応じて、次を設定できます。
   - [Cisco Hosted]
     1. クラウドホスト型コントローラのプライマリとセカンダリの場所を選択します。

        地理的な冗長性を実現するために、プライマリとセカンダリの異なる場所を選択することを推奨します。
     2. モニタリングデータを保存する場所を選択します。
     3. Cisco SD-WAN バージョンを選択します。
   - [Non-Cisco Hosted]
     1. モニタリングデータを保存する場所を選択します。
7. [Next] をクリックします。

8. Cisco SD-WAN オーバーレイネットワークの所有者または管理者の電子メールアドレスを入力します。
9. [Overlay Status] で、[Production] を選択します。
10. **[サマリー（Summary）]** をクリックします。
11. （任意）サブネット、DNS名、またはスナップショット設定をカスタマイズするには、[Advanced Options] で [Edit] をクリックします。
    - Subnets
      - プライマリおよびセカンダリサブネットに対して、VPCサブネットを指定します。最大 3 つのサブネットを指定できます。
      - TACACS ベースのユーザー認証および許可用に Cloud vEdge をプロビジョニングする場合は、チェックボックスをオンにします。
    - DNS 名
      - Cisco vBond オーケストレーション のカスタム DNS 名を入力します。
      - Cisco vManage のカスタム DNS 名を入力します。
    - スナップショット設定
      - 次のいずれかからスナップショットを取得する頻度を選択します。
        - **1 日に 1 回**
        - **2 日に 1 回**
        - **3 日に 1 回**
        - **4 日に 1 回**

    最大 10 個のスナップショットを選択できます。

（注） デフォルトでは、ネットワークオーバーレイ設定は 1 日に 1 回バックアップされ、10 個のスナップショットが保存されます。

12. 入力した詳細を確認します。
13. [Submit Request] をクリックします。
14. 一意のコントローラパスワードが表示されます。このパスワードは、作成後にオーバーレイネットワークにアクセスするために使用できます。

（注） 環境を保護するために、ログイン後すぐにパスワードを変更することをお勧めします。

子 IdP のセットアップ

（注） Cisco SD-WAN SSP で IdP をセットアップする場合、発行者、ログイン URL、および PEM キーを組織の IdP から使用できません。この情報は、ACS URL とオーディエンスを組織の IdP に設定した後に使用できます。組織の IdP を設定する場合は、ACS URL とオーディエンスのプレースホルダ値を追加することをお勧めします。後で、Cisco SD-WAN SSP で IdP を設定し、Cisco SD-WAN SSP で編集可能な ACS URL およびオーディエンスの URI の正しい値で組織の IdP を更新できます。

1. IdP のドメイン名を入力します。

   そのドメイン名がユーザーのルーティングに使用できる一意の電子メールドメインであることを確認してください。
2. IdP の発行者 URI を入力します。
3. IdP SSO URL を入力します。
4. IdP 署名証明書をアップロードします。

追加ロールの作成

追加のロールを作成するには、スマートアカウント管理者が次の手順を実行する必要があります。

1. Cisco SD-WAN セルフサービスポータル の左側にあるメニューアイコンをクリックします。
2. [Manage Roles] をクリックします。
3. 権限の名前を入力します。
4. 次のいずれかのオプションから、仮想アカウントごとに権限を割り当てます。
   - [Monitor]：Cisco SD-WAN SSP のすべてのオーバーレイオプションを表示およびモニタできます。
   - [Overlay Management]：オーバーレイネットワークを作成、変更、およびモニタできます。
   - [Administration]：モニタおよびオーバーレイ ネットワーク ロールによって定義されたすべてのタスクを実行し、新しい IdP をオンボードできます。

5. [ロールの追加（**Add Role**）] をクリックします。

CiscoSD-WANオーバーレイネットワークのモニタリング

オーバーレイネットワーク内の Cisco SD-WAN コントローラおよびデバイスをモニタリングできます。また、AWS インスタンスに関するアラートを表示したり、アクション設計とマイルストーンのレポートを表示することもできます。

オーバーレイネットワークの Cisco SD-WAN コントローラとデバイスのモニタリング

1. Cisco SD-WAN SSP ダッシュボードから、オーバーレイネットワークに移動します。
   - オーバーレイがシスコによってホストされている場合は、[Cisco Hosted Overlays] をクリックします。
   - オーバーレイがシスコ以外によってホストされている場合は、[Non-Cisco Hosted Overlays] をクリックします。

   オーバーレイのリストが表示されます。
2. オーバーレイの名前をクリックします。
3. [Controller View] タブで、[Cisco vManage]、[Cisco vBond Orchestrator] などモニタリングするコントローラをクリックします。
4. このウィンドウで、ネットワーク使用率または CPU 使用率でフィルタリングできます。ウィンドウの下部にはコントローラに関する情報（オンラインかどうか、IP アドレス、リージョンなど）が表示されます。

アラートの表示

[Alerts] ウィンドウには、AWS インスタンスに関連するさまざまなアラートが表示されます。

1. Cisco SD-WAN SSP ダッシュボードで、[Notifications] をクリックします。

   [Alerts] ウィンドウが表示されます。

   このウィンドウには、AWS インスタンスのインフラストラクチャレベルの問題について Cisco SD-WAN SSP から収集されたアラートが表示されます。

アクション計画とマイルストーンの表示

POA&M レポートを表示するには、次の手順に従います。

1. Cisco SD-WAN SSP ダッシュボードで、[Regulatored] をクリックします。

オーバーレイネットワークの脆弱性フィードを提供する [POAM] ウィンドウが表示されます。Qualys、Wazuh などのソースを使用すると、[POAM] ウィンドウにさまざまな問題が一覧表示されます。このレポートを検索、分類、およびダウンロードできます。ダウンロードしたレポートは、Splunk などのセキュリティ情報イベント管理（SIEM）ソフトウェアに提供できます。

2. [POAM] ウィンドウで、次のタスクを実行します。
   - 検索バーを使用して、問題をフィルタリングおよび検索します。POAM ステータス、リスク評価、問題検出のカスタム日付範囲といったさまざまなパラメータでフィルタリングできます。
   - 特定の問題に関する情報を表示するには、[Details] をクリックします。

     アラートに関する追加情報（問題の説明など）を示すダイアログボックスが表示されます。
   - 特定の列でフィルタリングするには、列の下にあるテキストボックスをクリックします。たとえば、[Adjusted Risk] 列の下をクリックし、「**high**」と入力すると、すべての高リスク問題を一覧表示できます。