ソリューションの概要

# SAP の安全なクラウド移行とアプリの近代化を Zscaler Private Access (ZPA) で実現

パフォーマンスを改善し、コストや運用の複雑さを軽減するために、多くの組織が DX を推進しています。特に SAP を利用する組織では、オンプレミスのエンタープライズ リソース プランニング システムである SAP ERP Central Component (SAP ECC) 6.0 のサポート終了が DX を加速させる要因の一つとなっており、これは、2025 年までに新しいデジタル ワークロードの 95% がクラウドネイティブとして導入されるという Gartner の予測とも一致しています。一方で、SAP S/4HANA への移行プロセス中のエンドユーザー エクスペリエンスは後回しにされやすく、その結果、移行プロジェクトが遅れたり、複雑化したり、リスクが増大したりするなどの新たな課題が生じる可能性があります。

従来型のテクノロジーでは、ユーザーをネットワークに接続する際に複雑さが生じ、それがクラウド移行の遅延につながることがあります。このような状況では、クラウドへの投資効果を十分に引き出すことができません。つまり、城と堀のアーキテクチャーやハブ&スポーク アーキテクチャーでは、クラウド環境に必要な拡張性や高速でシームレスなユーザー エクスペリエンスを実現できないのです。

## Zscaler Private Access (ZPA) とは

SAP S/4HANA クラウド移行を加速し、トランスフォーメーション プロセス全体を通じてユーザー エクスペリエンスと生産性を確保するために、Zscaler Private Access (ZPA) を活用して、シームレスで一貫性のあるエクスペリエンス、アプリケーションの近代化、アプリケーションベースのセキュリティを実現できます。Zscaler の 150 以上のポイント オブ プレゼンスは、世界最大のクラウド プロバイダーとピアリングされているため、農業機械メーカーの Kubota などのお客様は業務の迅速な拡張と拡大を成功させています。「次に倉庫を開設する際は、在庫管理用の SAP ERP システムに接続するためのネットワーク構築作業に多額の費用を投じて何週間も待つ必要はありません。どこでも初日から稼働できる体制が整っています」(Kubota)

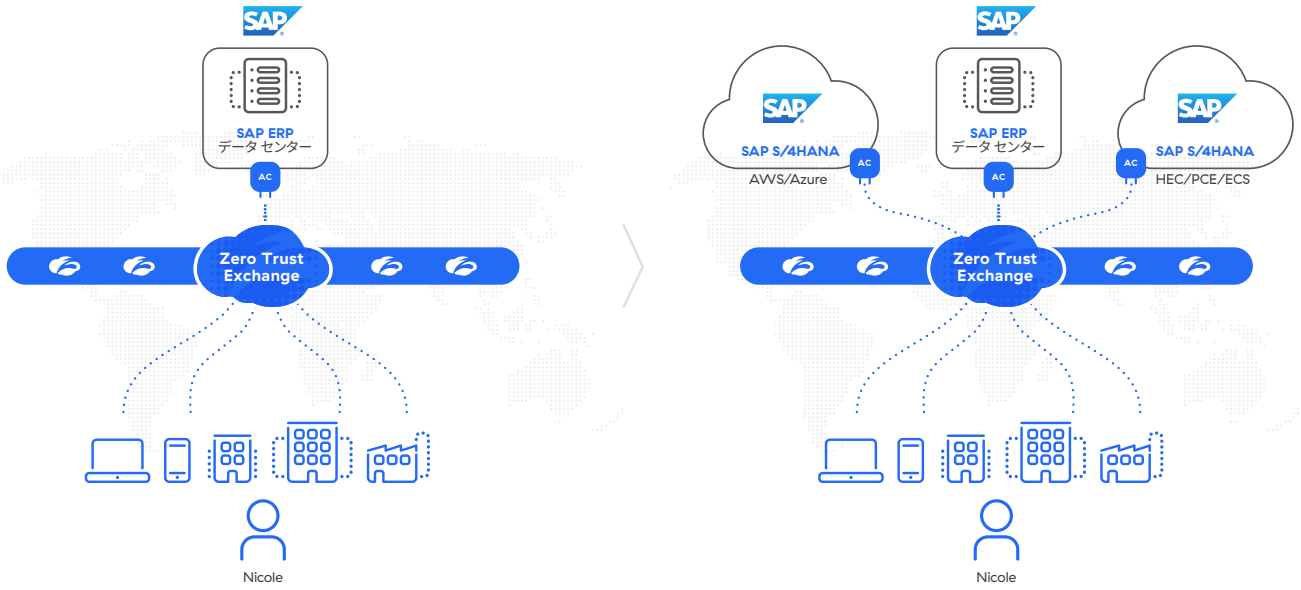
ユーザーとアプリの間の抽象化レイヤーとして機能する ZPA の単一のグローバル ポリシー エンジンは、すべてのデバイス、場所、アプリケーションにゼロトラストの原則を適用します。アプリの実行場所がデータセンターであってもクラウドであっても、ユーザーは、あらゆる場所やデバイスから同じ方法でアプリにアクセスできます。アプリの場所はポリシーを更新するだけで変更できるため ( データ センターからパブリック クラウド、または VPC から VPC など )、ユーザーは優れたユーザー エクスペリエンスを維持したまま、プライベート アプリに安全に直接接続できます。

## Zscaler Private Access (ZPA) のメリット：

- SAP アプリケーションの移行とクラウド化を加速
- SAP スイート アプリケーションへのユーザー アクセスをきめ細かく制御
- 移行前も移行後もワークロードへの安全なアクセスを確保
- SAP アプリケーションをエンドツーエンドで可視化し、ユーザー エクスペリエンスを改善

> “次に倉庫を開設する際は、ネットワーク構築作業に多額の費用を投じて何週間も待つ必要はありません。Zscaler Client Connector を使用して、4G 接続の RF スキャナーを在庫管理用の SAP ERP システムに接続させられるため、どこでも初日からすぐに運用を開始できます。”
>
> **Jonathon Bonnici 氏**
> Kubota Australia
> IT サービス デリバリー
> マネージャー

## Zscaler Private Access の仕組み

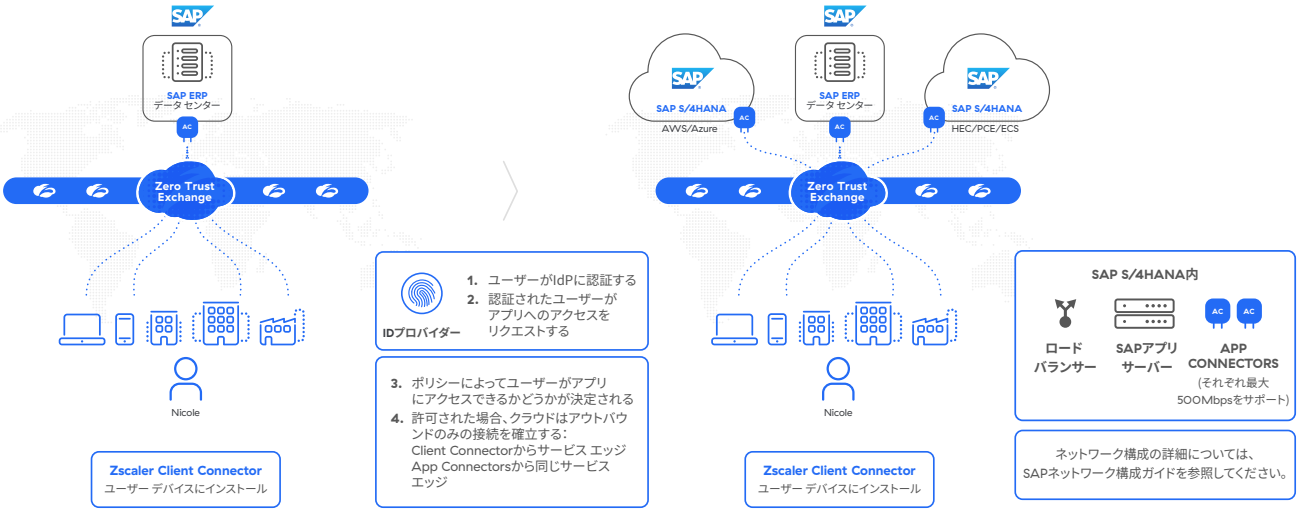



### ZPA/SAP コンポーネント

- App Connectors は、組織のアプリケーション サーバーと ZPA クラウド間に認証された安全な インターフェイスを確立します。
- Zscaler Zero Trust Exchange (ZTE) プラットフォームは、高速で安全な接続を可能にし、インターネットを企業ネットワークとして使用することで従業員がどこからでも作業できる環境を確保します。世界 150 拠点以上のデータ センターで稼働する Zero Trust Exchange は、Microsoft 365 や AWS などのクラウド プロバイダーやアプリケーションと同じ場所に配置されているため、ユーザーに最も近い場所でサービスを提供します。これにより、ユーザーと接続先の経路が最短となり、包括的なセキュリティと優れたユーザー エクスペリエンスを実現できます。
- Zscaler Client Connector はデバイスにインストールされるアプリケーションで、インターネット トラフィックや社内アプリへのアクセスを保護し、これらが組織のポリシーに準拠していることを保証します。
- アプリケーションは、標準のポート セットで定義する完全修飾ドメイン名 (FQDN)、ローカル ドメイン名、または IP アドレスです。アプリケーションは、Application Segment 内で定義する必要があります。
- App Segment は、アクセスの種類やユーザーの権限に基づいて定義されたアプリケーションのグループです。
- ZPA のポリシーは、ユーザーがアプリケーションにアクセスする方法を制御します。ユーザーがアプリケーションにアクセスする前にポリシーを定義する必要があります。ポリシーには多くの種類があります。ポリシーの種類の詳細については、リソース リンクを参照してください。
- Zscaler Tunnel (Z-Tunnel) は、Zscaler Client Connector と Zscaler が管理する ZPA Public Service Edge 間、または App Connector と組織が管理する ZPA Private Service Edge 間のポイントツーポイント接続です。この接続は TLS で暗号化され、相互に認証されています。Z-Tunnel には、直接 IP データは含まれていません。また、Z-Tunnel は、Microtunnel と呼ばれる複数の通信チャネルを内部で伝送できます。

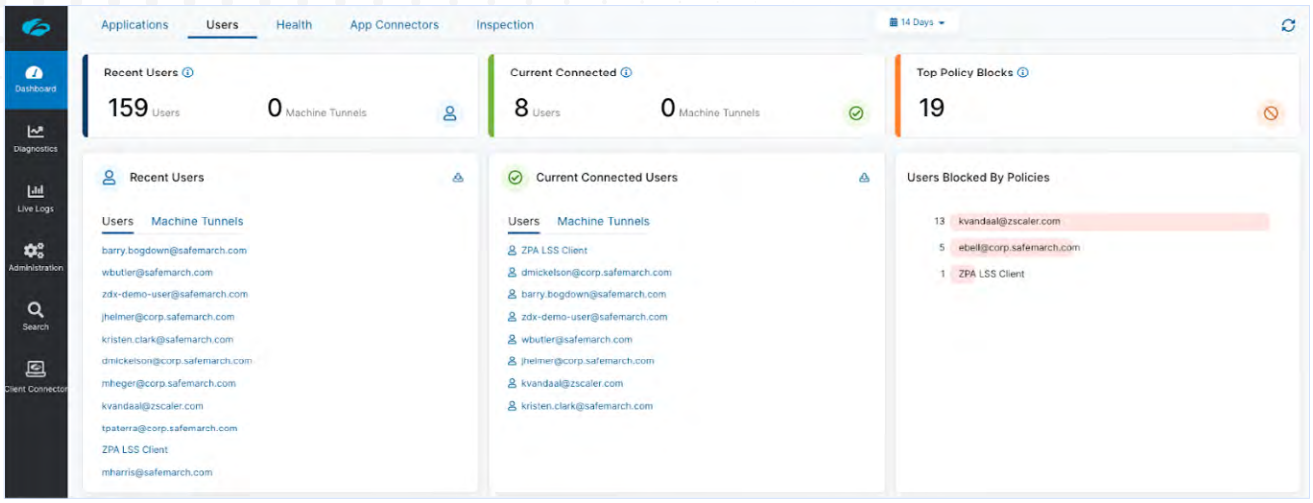
- Microtunnel (M-Tunnel) は、Zscaler Client Connector と内部アプリケーション間で作成されるエンドツーエンドの通信チャネルです。これは、ZPA Public Service Edge または ZPA Private Service Edge と App Connector を介してオンデマンドで作成されます。
- サーバーは ZPA で利用可能なアプリケーションをホストし、組織のデータ センターまたは仮想パブリック クラウドに配置できます。
- サーバー グループはサーバーの集合体です。各 Application Segment は、サーバー グループにマッピングする必要があります。
- SAP アプリ サーバーは、SAP アプリケーションをホストするサーバーです。

### ZPA と SAP の設計



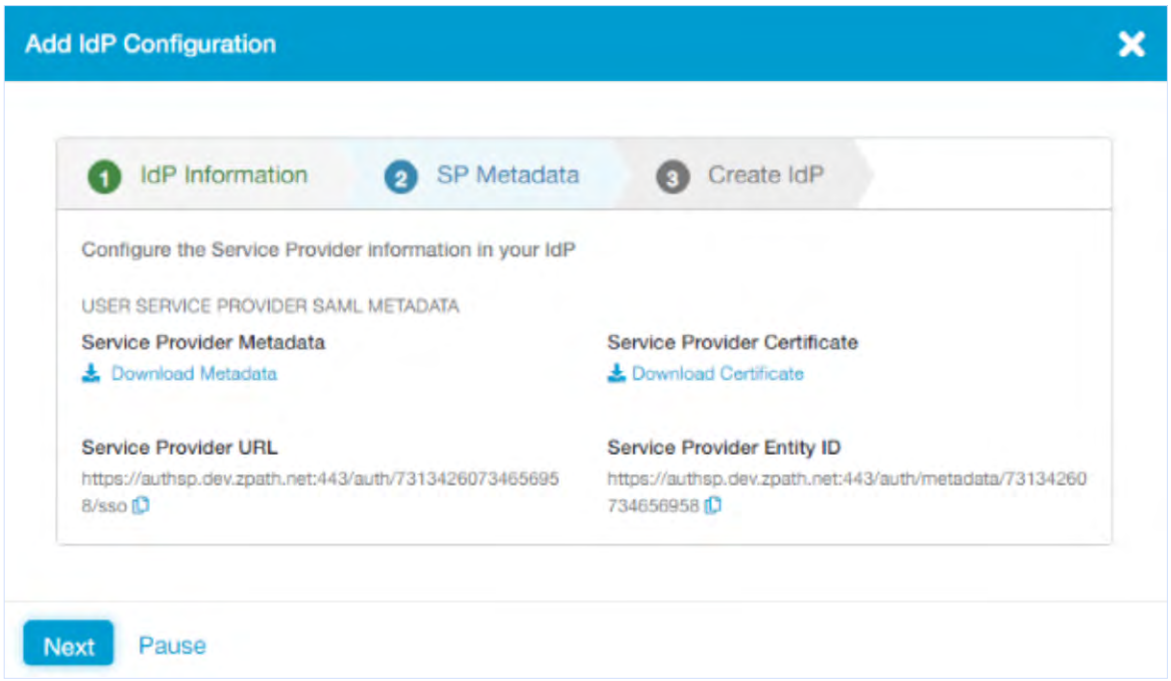

たとえば、ACME は現在、本社のオンプレミス データ センターで SAP ERP システムをホストしています。同社はネットワークとアプリケーションの近代化を進めており、組織のすべての SAP アプリケーションを AWS および Azure 上の S/4HANA に移行する予定です。DX ジャーニーの開始時に Zscaler Zero Trust Exchange (ZTE) の一部である ZPA を導入した同社は、プロセス全体のさまざまな課題を解消して、シンプルかつシームレスなエクスペリエンスを確保しています。

ACME の従業員である Nicole がオンプレミスのデータ センターでホストされている SAP アプリケーションへのアクセスをリクエストすると、ACME のアイデンティティー プロバイダー (IdP) で認証するように求められます。認証後、ZTE は Nicole のアプリケーション リクエストを既存のポリシーに照らして評価します。アイデンティティーとコンテキストに基づいてアプリケーション アクセスが許可されると、ZTE はそのアプリケーションに最も近い App Connector に接続し、アプリケーションから ZTE への暗号化された TLS 接続であるインサイドアウト Z-Tunnel を確立します。同時に、ZTE は Nicole のデバイスの Client Connector から ZTE へのインサイドアウト Z-Tunnel を開始します。その後、ZTE は Z-Tunnel を結合して、その内部で Nicole とアプリケーション間のエンドツーエンドの通信チャネルである M-Tunnel を形成します。ACME が SAP アプリケーションをクラウドに移行する場合でも、これと同じプロセスが適用されます。ACME 側で、オンプレミスのデータ センターからクラウドにアプリケーションを複製し、そのアプリケーションをオンプレミスのデータ センターから削除すれば、Nicole が SAP アプリケーションにアクセスした場合、自動的にクラウド内のアプリケーションにルーティングされるようになります。




## クラウド移行とアプリの近代化の概要

**ステップ 1. シングル サインオン (SSO) 認証と IDP の構成**

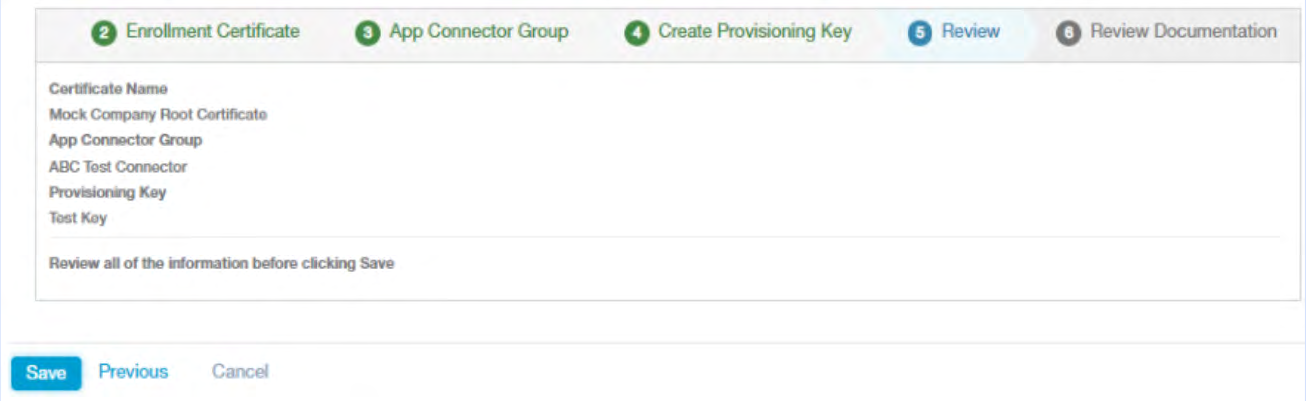



ZPA は、組織の既存のアイデンティティー プロバイダー (IdP) のユーザー アイデンティティーを利用します。複数の IdP ソリューションをサポートするように構成することも可能です。ZPA は SAML 経由のシングル サインオン (SSO) をサポートしているため、リモート ユーザーは ZPA に個別にログインすることなく組織のアプリケーションにアクセスできます。

ユーザーが ZPA 経由でアプリケーションにアクセスするには、最初に SAML2.0 準拠のアイデンティティー プロバイダー (IdP) を使用して Zscaler Client Connector に認証する必要があります。認証プロセスはサービス プロバイダー開始 (SP 開始 ) モデルに従います。ZPA ユーザーの SSO は SP によって開始されますが、ZPA 管理者の SSO は SP または IdP によって開始されます。

1. IdP を設定し、ZPA を SP として指定します。ZPA 管理ポータルを使用して IdP 構成を追加する前に、組織に IdP が導入されている必要があります。
2. ZPA 管理ポータルから IDP 構成を追加します。

**ステップ 2. App Connectors と App Connector グループの構成**




App Connectors は、SAP アプリケーションと ZPA クラウドの間に認証された安全なインターフェイスを確立します。高可用性のためにペアで展開されるのが一般的で、通常は SAP アプリケーション サーバーの隣に展開されます。App Connectors はさらに App Connector グループに分類されます。App Connector は特定の App Connector グループに属し、App Connector グループは、任意のアプリケーションを提供するために少なくとも 1 つのサーバー グループに関連付けられています。App Connectors は、いくつかの形式で展開できます。Zscaler は、企業のデータ センターや VMware などのローカル プライベート クラウド環境、Amazon Web Services (AWS) EC2 などのパブリック クラウド環境に展開するための標準の仮想マシン (VM) イメージを配布します。また、サポートされている Linux ディストリビューションにインストールできるパッケージも提供します。

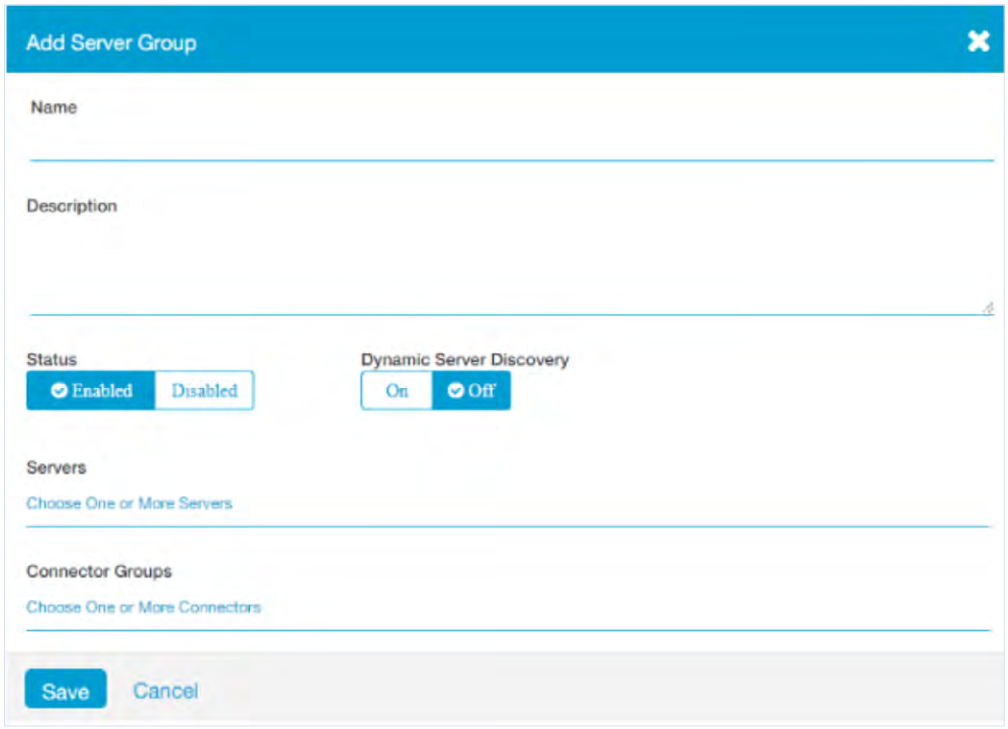
標準的な App Connector 構成では、次の 2 つの主要な手順が実行されます。

1. ZPA 管理ポータルから App Connector を追加します。
2. 選択したサポート対象のプラットフォームに App Connectors を展開します。
3. クラウド移行の場合は、App Connectors をオンプレミスのデータ センターのサーバー グループとクラウドのサーバー グループに関連付ける必要があります。

ただし、SAP HEC/PCE 用に App Connectors を構成する場合は、以下の手順が必要です。

1. SAP のお客様が、SAP のアカウント担当者またはカスタマー デリバリー マネージャーに Zscaler Endpoint Service をリクエストします。
2. SAP がお客様に代わって高可用性 App Connectors を SAP HEC/PCE にインストールします。
3. お客様が App Connector に適用する ZPA ライセンスを SAP に提供します。

**ステップ 3. サーバーとサーバー グループの構成**



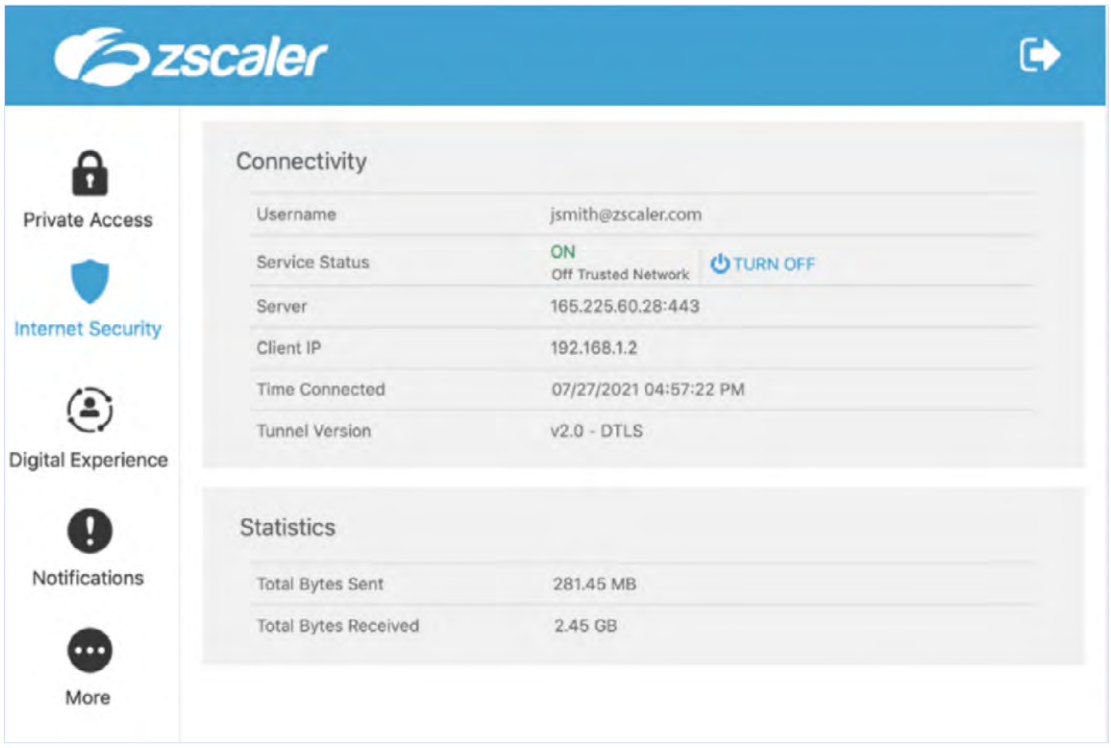

サーバーが企業のデータ センターにあるか、仮想パブリック クラウド (VPC) にあるかによらず、ZPA で使用できるようにするアプリケーションをホストするサーバーを構成する必要があります。

サーバーの構成には、主に次の 2 つの方法があります。

- **サーバーとサーバー グループを明示的に定義する：**1 つ以上のアプリケーションをホストするすべてのサーバーを明示的に定義できます。各サーバーに名前と IP アドレスまたは完全修飾ドメイン名 (FQDN) を指定し、その後、これらのサーバーを手動でサーバー グループに配置します。
- **動的サーバー検出を有効にする：**各サーバーを明示的に定義する代わりに、動的サーバー検出を有効にして、ユーザー リクエストに応じて ZPA がアプリケーションに適したサーバーを検出できるようにします。この方法では、動的サーバー検出が有効化された空のサーバー グループの作成のみが必要になります。

各 Application Segment は、サーバーとサーバー グループに関連付けられます。動的サーバー検出が有効になっている場合、アプリケーションがクラウドに移行されると、ZPA は自動的に変更を登録し、顧客をクラウド内のアプリケーションにルーティングします。動的サーバー検出が有効になっていない場合は、ZPA 管理者はクラウドのアプリケーションに関連付けられているサーバーとサーバー グループを手動で変更する必要があります。

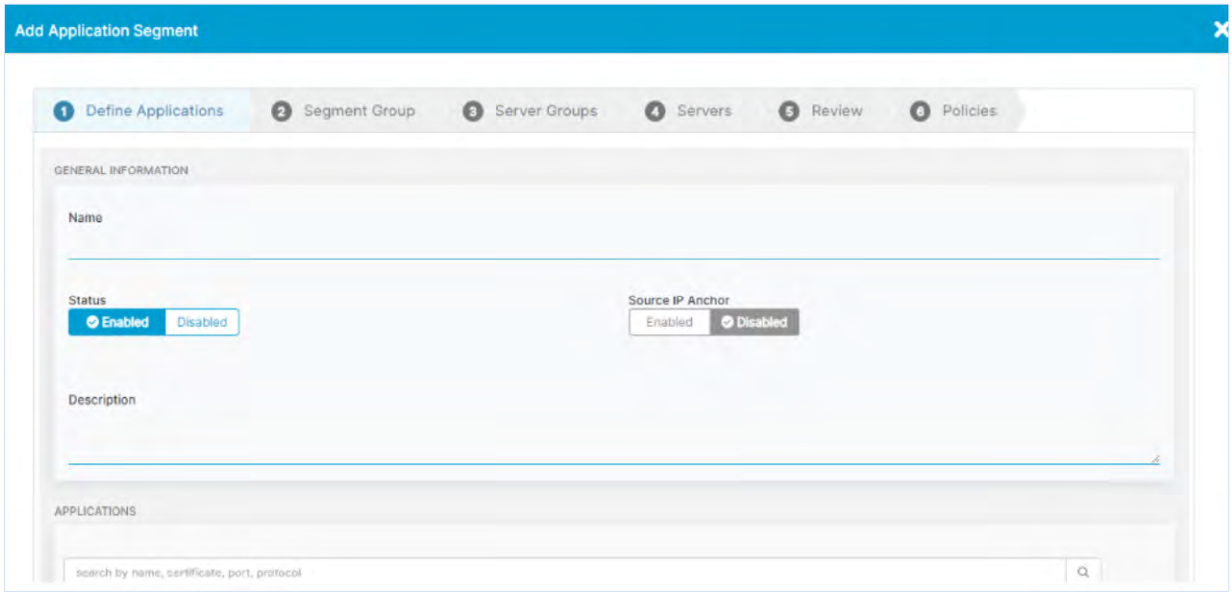
### ステップ 4. Client Connector の構成




Zscaler Client Connector は、組織が管理するノートパソコンやモバイル デバイス、BYOD、ハンドヘルド デバイスなどのユーザーのエンドポイントにインストールされる軽量のアプリで、デバイス、場所、アプリケーションに関係なく、セキュリティ ポリシーとアクセス制御を適用します。Zscaler Client Connector アプリは、トラフィックを最も近い Zscaler クラウドのポイント オブ プレゼンスに転送します。トラフィックはそこで Zero Trust Exchange から SAP アプリケーションにルーティングされます。

1. システム要件と前提条件タスクを完了します。
   - ZPA 管理ポータルで適切なセキュリティとアクセス設定を構成します。
   - SAML ベースの認証を構成し、ユーザーをプロビジョニングします。Zscaler Client Connector ポータルを ZPA サービスの IdP として使用することはできません。
   - Zscaler Client Connector が ZPA のトラフィックを適切に処理していることを確認します。
2. Zscaler Client Connector の管理設定を構成します。利用規定、更新設定、転送ポリシー、サポートとログ記録へのユーザー アクセス、フェイル オープン設定はすべて構成可能です。
3. Client Connector プロファイルを構成します。Zscaler Client Connector ポータルでは、各プロファイルにポリシー ルールを追加することで、アプリ プロファイルを構成できます。ルール間の優先順位と各ルールの適用対象 ( すべてのユーザーまたは異なるユーザー グループ ) を選択できます。ユーザーが Zscaler サービスにアプリを登録すると、アプリは適切なポリシー ルールでアプリ プロファイルをダウンロードするために、優先順位とユーザーのアイデンティティーを考慮します。
4. Client Connector ストアから Zscaler Client Connector をダウンロードします。
5. インストーラー オプションで Client Connector をカスタマイズします。Zscaler Client Connector インストーラー ファイルをインストール オプションで構成すると、ユーザー登録プロセスから手順を削除できます ( 例:ユーザーが Zscaler Client Connector で登録ページやクラウド選択のプロンプトをスキップできるようにする )。
6. Client Connector を展開します。Zscaler Client Connector は、個々のデバイスに手動でインストールできます。また、組織のデバイス管理メカニズムを使用してユーザーのデバイスに Zscaler Client Connector を展開することもできます。

### ステップ 5. Application Segment の追加



Application Segment は、アプリケーション インスタンスの集合体です。アプリケーションは自動検出され、一致条件に基づいて自動的にグループ化されます。Application Segment は、1 つ以上のホストまたはホスト セグメントに固定できます。Application Segment は、他の複数のセグメントを含むポリシー、または他の複数のセグメントにまたがるポリシーに対応するために使用されます。

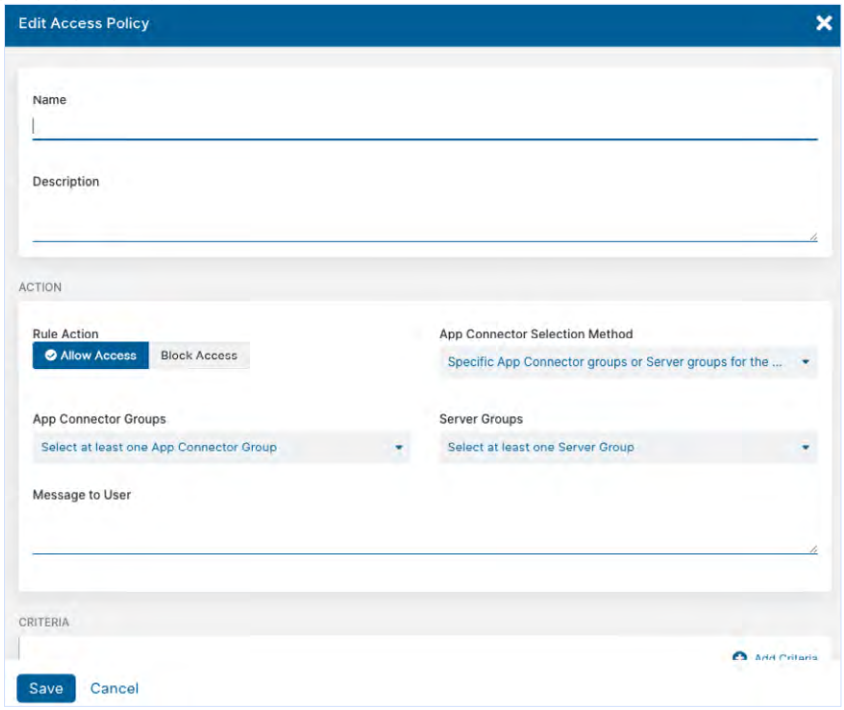
Zscaler では、SAP の App Segment を構成する際に次のベスト プラクティスを推奨しています。

- すべての SAP アプリケーションに対して 1 つの Application Segment を作成します。これにより、ZPA サービスは、これらのアプリケーションに対するユーザー リクエストの負荷を分散できます。ただし、セグメンテーションが必要な場合は、SAP アプリケーション用に複数の Application Segment を作成します。
- FQDN を使用して SAP アプリケーションの Application Segment を作成します。SAP クライアントは、ホストの FQDN を解決できない場合、IP アドレスへの接続を試みます。このサービスは IP アドレスをサポートしていますが、ゼロトラスト モデルでは FQDN を使用して接続する方がより安全です。
- SAP ホスト名が FQDN でない場合は、DNS 検索ドメインが必要です。クライアントに検索サフィックスが設定されていない場合、SAP の接続に必要な完全な FQDN を形成できません。クライアントは、SAP メッセージ サーバーが提供する IP アドレスにフォールバックしますが、これによってゼロトラスト モデルの有効性が弱まったり、ZPA サービス経由でルーティングできなくなったりする可能性があります。
- Wireshark トレースまたは SAP 構成を使用して、すべての SAP サーバーの IP アドレスを識別し、これらの IP アドレスと適切な TCP ポートのみを含む Application Segment を作成します。サブネット範囲全体 (192.168.1.0/24 など ) をアドバタイズしないでください。
- SAP メッセージ サーバーまたはアプリケーション サーバーにアクセス制御リスト (ACL) が構成されている場合、それに App Connector の IP アドレスを追加します。ZPA サービスはクライアントに送信元 NAT を実行するため、すべてのトラフィックは App Connector から送信されているように見えます。Application Segment に関連付けられている App Connector グループの場合、ZPA はこの App Connector グループ内の App Connector 間でユーザー リクエストの負荷を分散させます。そのため、App Connector グループのすべての App Connector の IP アドレスを ACL に追加することが推奨されます。

ZPA で SAP アプリケーションをサポートするには、Application Segment および DNS 検索ドメインを構成する必要があります。

1. ZPA 管理ポータルから Application Segment を追加します。
   - [Add Application ( アプリケーション追加 )] ウィンドウの [Define Applications ( アプリケーションの定義 )] に移動し、SAP アプリケーションに対応する完全修飾ドメイン名 (FQDN) を入力します。IP アドレスも入力できますが、より安全性を確保するために、可能な限り FQDN を使用することをお勧めします。クライアントに検索サフィックスが設定されていない場合、SAP の接続に必要な完全な FQDN を形成できません。クライアントは、SAP メッセージ サーバーが提供する IP アドレスにフォールバックします。
   - Zscaler Client Connector からのアクセスを確保するには、アプリケーションの TCP ポート範囲を必ず入力してください。
2. DNS 検索ドメインを追加します。SAP の場合、ZPA 管理ポータル内で FQDN の DNS 検索ドメインを構成できるため、SAP クライアントは検索サフィックスを追加して、FQDN を構築できるようになります。ただし、短い名前ではなく、FQDN を提供するように SAP を構成することも可能です。これにより、DNS 検索ドメインの構成が不要になります。

### ステップ 6. ( 省略可 ) – ポリシーによるアプリの移行




一般的なクラウド移行では、レガシー アプリケーションからクラウド アプリケーションへのユーザー アクセスの移行を完了するために、追加のポリシー変更は必要ありません。組織によっては、すべてのユーザーを一度にクラウド アプリケーションに移行したくないケースもあります。たとえば、すべてのユーザーを移行する前に、少数のユーザーのグループでクラウド アプリケーションをテストしたい場合は、クラウド移行に対してポリシーベースのアプローチを使用できます。

1. ZPA 管理ポータルで、クラウド内のアプリケーションにアクセスするユーザーのポリシーを作成し、「Specific App Connector groups or Server groups ( 特定の App Connector グループまたはサーバー グループ )」のオプションを選択します。
2. 次に、クラウドでホストされているアプリケーションの App Connector グループを選択します。
3. データ センター内のアプリケーションにアクセスするユーザーに対して、このプロセスを繰り返します。オンプレミスのデータ センター内のアプリケーションの App Connector グループを必ず選択してください。
4. 準備ができたら、クラウドに関連付けられた App Connector グループでポリシーを更新して、残りのユーザーをクラウドに移行します。

## リソース

ZPA のポリシー
ZPA: SAP アプリケーションのサポート
RISE with SAP S/4HANA Cloud, private edition and SAP ERP, PCE（英語）

> “ZPA を使用すると、ユーザーの接続を終了させる場所を柔軟に制御できます。ある AWS リージョンから別のリージョンに SAP システムがフェイル オーバーした場合でも、ポリシーを更新すればシームレスなユーザー アクセスを確保できます。ZPA により、ユーザーはレガシー アプリだけでなく、クラウド上の新しい SAP 環境にもアクセスできるようになります。”
>
> **Growmark**

zscaler™ | Experience your world, secured.™

**Zscaler について**
Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange は、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータ センターに分散された SASE ベースの Zero Trust Exchange は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、**zscaler.com/jp** をご覧いただくか、Twitter で **@zscaler** をフォローしてください。



+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com/jp