ソリューションの概要

Zscaler Private Access (ZPA) で サプライ チェーンとサード パーティーの SAP アクセスを保護

サプライ チェーンを運用し、OT や IIoT 資産を所有するグローバル企業では、請負業者やパートナーなどのサードパーティー ユーザーが社内の SAP ビジネス管理アプリケーションに俊敏に接続できる環境が求められます。生産稼働時間を最大化し、機器やプロセスの障害による中断を回避するには、以下の機能を備えた最新のユーザー アクセス アプローチを検討する必要があります。

1. BYOD や請負業者、工場労働者などのサプライ チェーン ユーザー向けに、信頼できないデバイスや管理対象外のデバイスからも Web ブラウザー経由で SAP 製品にアクセスできる、エージェントレスのセキュア リモート アクセスを提供する
2. サプライ チェーンに内部アプリケーションへのアクセスを許可する際、ユーザーを他のアプリケーションや企業ネットワークに接続させるのではなく、ユーザーと SAP アプリケーション間に直接接続を確立することで、SAP アプリケーションの攻撃対象領域が公開されるリスクを軽減する
3. 一貫したアクセス ポリシーを確実に適用しながら、ユーザーの可視性を維持し、過剰なアクセス権限を制限する

しかし、サードパーティーにまでアクセスを拡大するリスクは大きく、サプライ チェーンは常にランサムウェアなどの高度な攻撃の格好の標的となっています。どんなに軽微なインシデントであっても運用が中断すると、その影響は世界経済にまで波及する可能性があります。これまではリスクを軽減するために、多くの組織が VPN を利用して SAP ERP アプリケーションにアクセスしてきましたが、VPN ではリモート アクセス クライアントを導入できなかったり、追加の IT インフラが必要となったりするなどの問題が頻繁に発生します。さらに、パートナーは、このようなクライアントをインストールするために必要なデバイス レベルの権限が付与されていなかったり、インストールを望まなかったりする場合もあります。

Zscaler Private Access (ZPA) とは

サプライ チェーンの運用にSAP へのアクセスが必要な場合、エージェントレスのブラウザー アクセスを利用すれば、Web ブラウザー経由でのユーザー認証とアプリケーション アクセスがZscaler Private Access (ZPA) を通じて可能になります。サイト間 VPN に接続したり、デバイスに Zscaler Client Connector をインストールしたりする必要はありません。これは、IT 組織が外部クライアントを許可していない、または個人所有デバイスの持ち込み (BYOD) がクライアントに対応していない請負業者やパートナーなどのサードパーティー ユーザーに最適なアクセス手段です。

先進的な製造業者である **Schmitz Cargobull** をはじめ、多くの企業がVPN はもはや有効なソリューションではないと考えています。VPN では社内の SAP アプリケーションへのアクセスが頻繁に失敗し、機密性が高く、事業継続に不可欠なサプライ チェーン機能が中断されるためです。ZPA を活用してSAP ERP への安全なアクセスを確保した同社のインフラ責任者である Michael Schöller 氏は、「**従業員やサードパーティーはネットワーク全体を公開することなく、SAP システムに安全かつ確実にアクセスできます**」と話します。ゼロトラスト ポリシーがあらゆるデバイス、拠点、アプリケーションにデフォルトで施行されると、パートナーはネットワークに接続されず、アプリケーションもインターネットに公開されません。許可されている場合にのみアクセスを付与することで、ユーザーの生産性が向上し、組織はラテラル ムーブメントから保護されます。ZPA 管理者は、このサービスを利用することで、ユーザー アクティビティーをリアルタイムで可視化し、ブラウザー アクセス経由でアプリケーションにアクセスするユーザーを特定しながら、これまで認識していなかったアプリを検出できます。

Zscaler for SAP のメリット

- **ユーザーやデバイスから SAP への安全なエージェントレス アクセス：**サードパーティー ユーザーやサプライ チェーン ツールが企業ネットワークに接続されないようにすることで、リスクとラテラル ムーブメントを削減します。
- **アプリ、ワークロード、IoT へのゼロトラストの拡張：**単一のグローバル ポリシー エンジンを活用して、SAP のプライベート アプリ、ワークロード、OT/IIoT デバイスへの高速で安全な直接接続を実現します。
- **優れた SAP ユーザー エクスペリエンスの提供：**ZDX の継続的な監視と可視性で、ハイブリッド ワーカーの生産性を向上させ、ユーザー エクスペリエンスの問題を事前予防的に解決します。
- **データ侵害リスクの軽減：**承認されていないユーザーには SAP アプリケーションが見えないようにし、最小特権アクセスを施行することで、SAP S/4HANA のアプリケーション攻撃対象領域を最小化します。
- **運用の複雑さとコストの削減：**クラウド型のゼロトラスト ネットワーク アクセス (ZTNA) により、ハードウェアやソフトウェアの管理が不要になるため、インフラのコストやリソースが削減されます。

ZPA のエージェントレス アクセスの仕組み

ZPA/SAP のサプライ チェーン設計

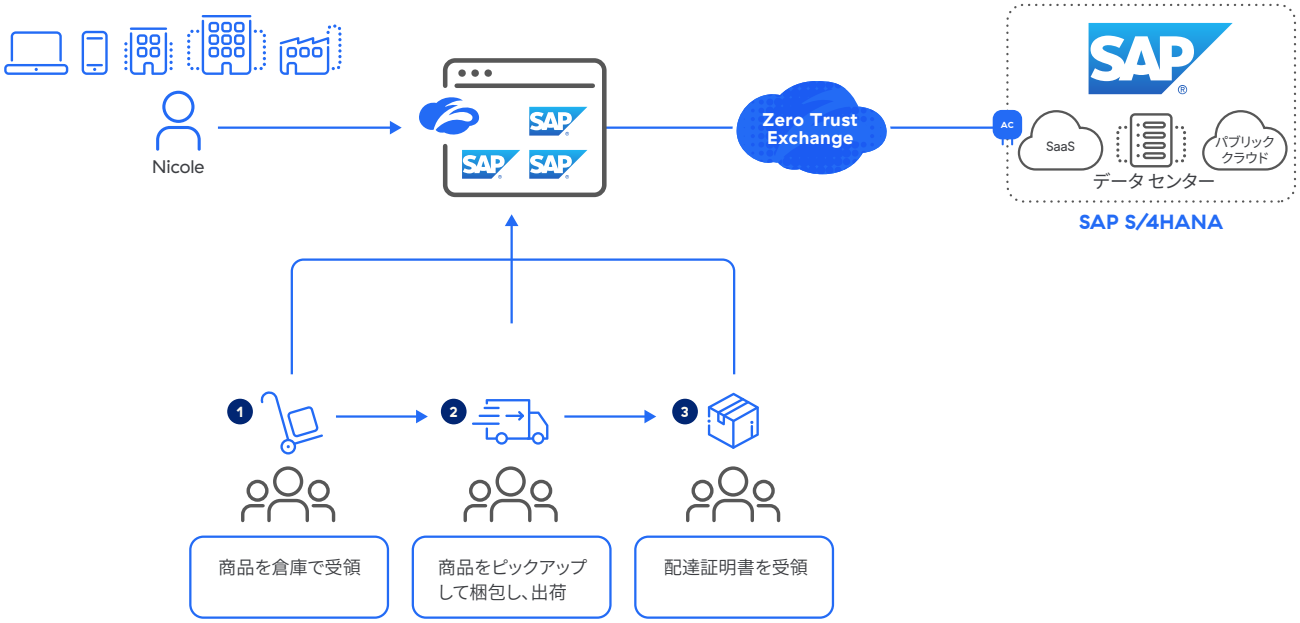


図 1: ZPA Browser Access を使用して SAP アプリケーションにアクセスするサプライ チェーンの従業員とサードパーティー ユーザー

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。
- ブラウザー アクセス ユーザー ポータルは、エージェントをインストールしていないユーザーとデバイスも、従業員やパートナー向けに承認されたアプリケーションにアクセスできるようにします。
- 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。
- **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。

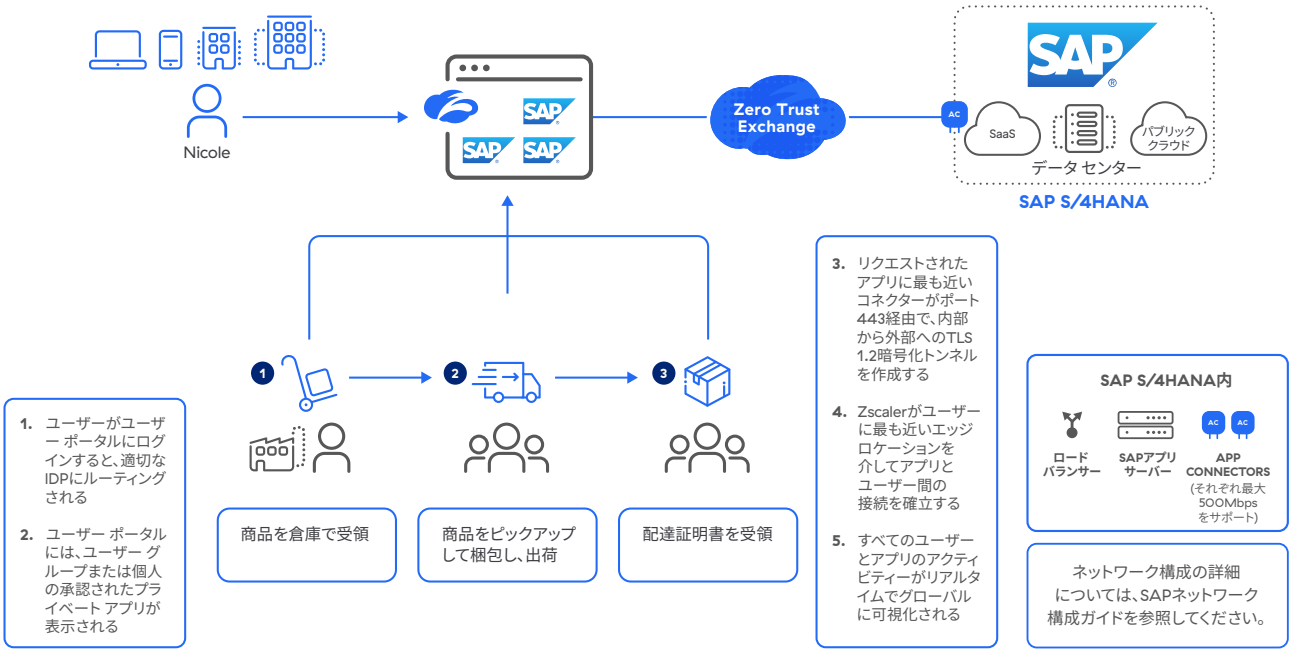
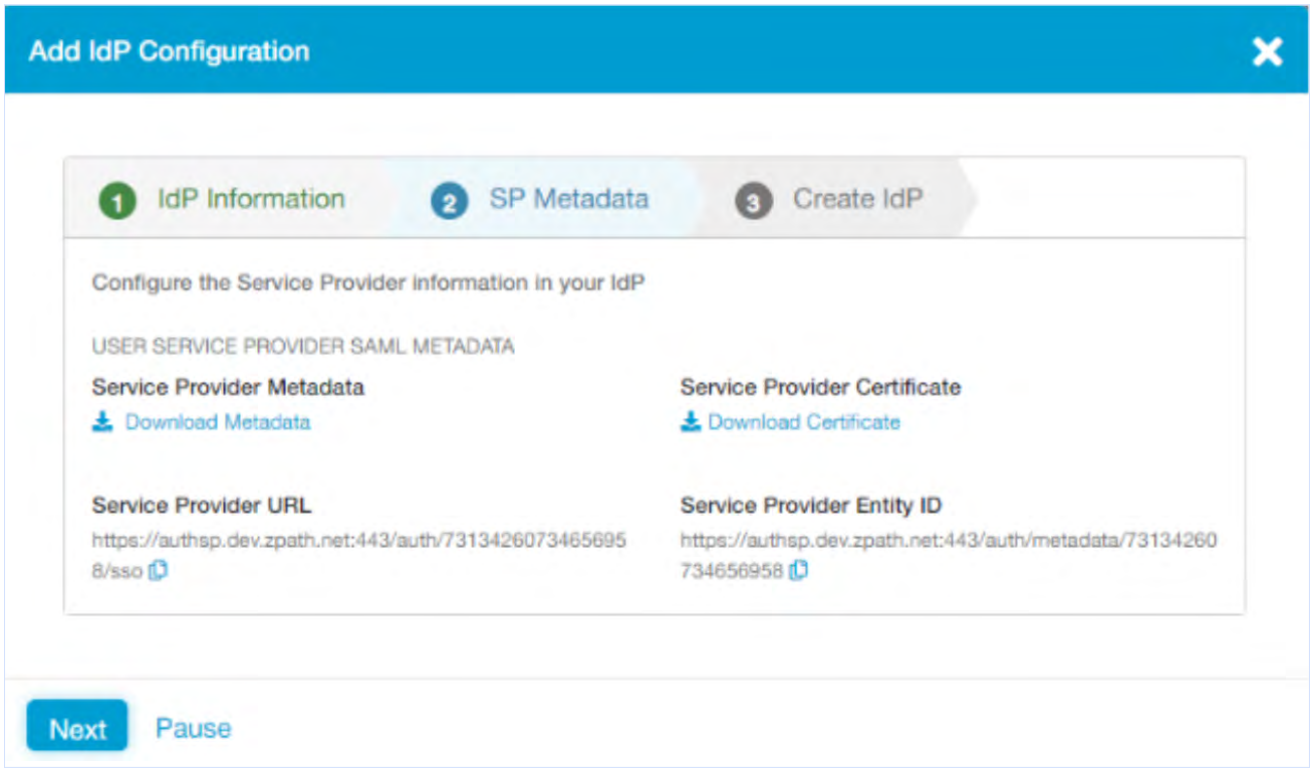


図 2: ZPA Browser Access を使用して SAP アプリケーションにアクセスするサプライ チェーンの従業員とサードパーティー ユーザー (追加の詳細)

図 1 と 2 は、ハイブリッドの SAP 環境で ZPA がどのように機能するかを示したものです。Nicole は ACME の従業員で、サプライ チェーンを移動する製品の追跡を担当しています。Paul は、顧客に出荷する前の ACME 製品を保管しておく倉庫の担当者で、荷物を受け取ると、ZPA Browser Access ポータルから ACME と Nicole に通知します。Paul がタブレットで ACME のユーザー ポータルにアクセスすると、アイデンティティー プロバイダー (IDP) にリダイレクトされて認証が完了します。Paul がアクセスできるアプリケーションがユーザー ポータルに表示され、必要な SAP アプリケーションを選択すると、リクエストされた SAP アプリケーションに最も近い App Connector が Z-Tunnel (Zscaler クラウドへの暗号化された TLS 接続) を作成し、Zscaler クラウドがユーザー ポータルから SAP アプリケーションへの接続を確立します。このプロセスを経て、Paul にアクセスが付与され、製品の場所に関する最新情報を ACME と Nicole に提供できるようになります。ここでポイントとなるのが、Paul は ACME 固有のデバイスを必要とせず、また、デバイスはエージェントレスであるため、管理対象外や信頼できないデバイスも使用できるという点です。必要なのは Web ブラウザーのみで、ZPA Browser Access 機能を通じて SAP アプリケーションに安全に接続できます。

SAP 向けの ZPA エージェントレス アクセスの概要

ステップ 1. シングル サインオン (SSO) 認証と IDP の構成



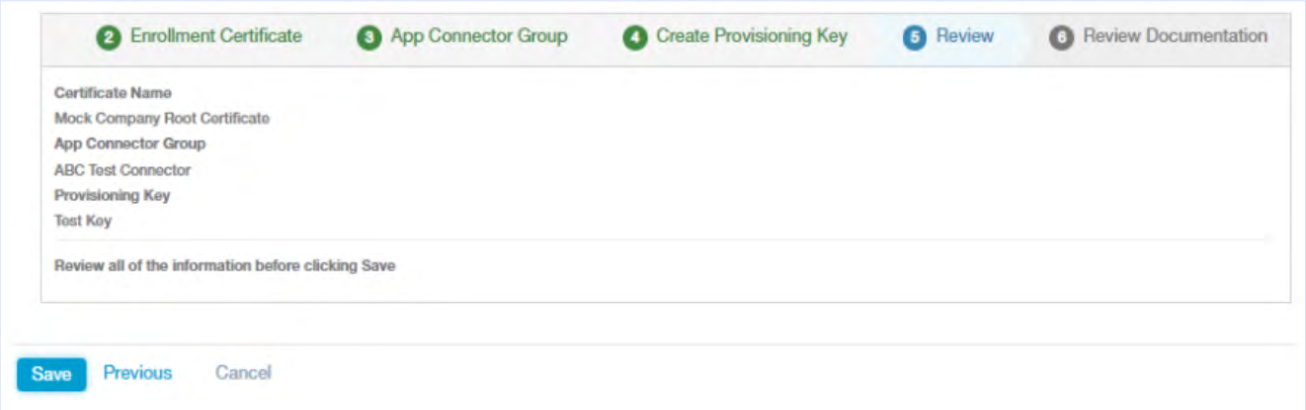
ZPA は、組織の既存のアイデンティティー プロバイダー (IdP) のユーザー アイデンティティーを利用します。複数の IdP ソリューションをサポートするように構成することも可能です。ZPA は SAML 経由のシングル サインオン (SSO) をサポートしているため、リモート ユーザーは ZPA に個別にログインすることなく組織のアプリケーションにアクセスできます。

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 の展開



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、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。

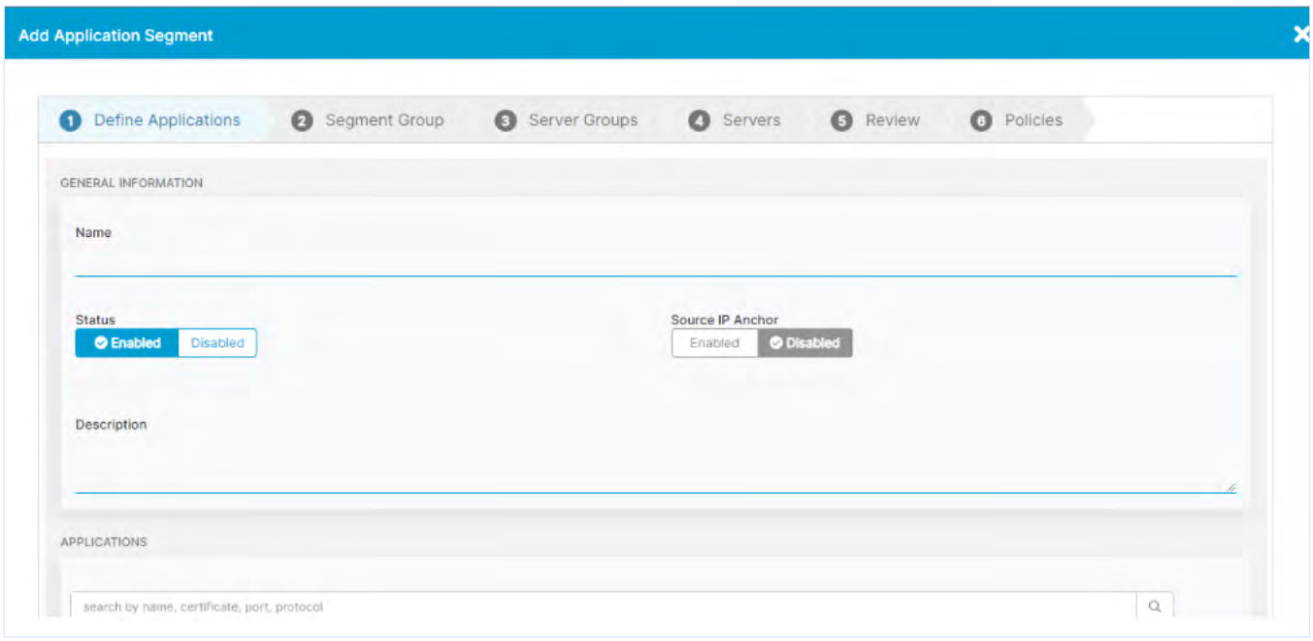
標準的な App Connector 構成では、次の 2 つの主要な手順が実行されます。

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。

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. ブラウザー アクセス用の Application Segments の構成



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。

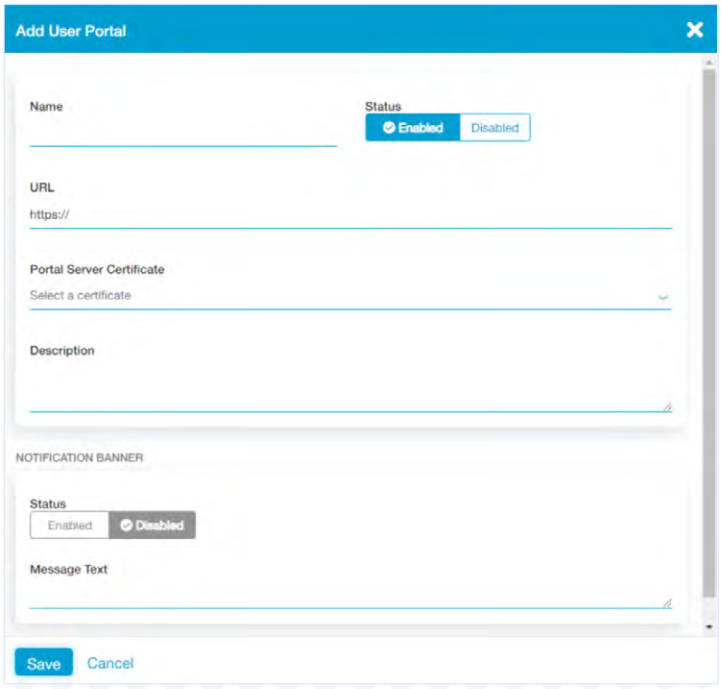
- すべての SAP アプリケーションに対して 1 つの Application Segment を作成します。これにより、ZPA サービスは、これらのアプリケーションに対するユーザー リクエストの負荷を分散できます。ただし、セグメンテーションが必要な場合は、SAP アプリケーション用に複数の Application Segment を作成します。
- FQDN を使用して SAP アプリケーションの Application Segment を作成します。SAP クライアントは、ホストの FQDN を解決できない場合、IP アドレスへの接続を試みます。このサービスは IP アドレスをサポートしていますが、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。
   - [Browser Access (ブラウザー アクセス)] を選択して、ブラウザー アクセス用の Application Segment を有効にします。
2. ZPA 管理ポータルの [Browser Access (ブラウザー アクセス)] ページに移動し、ブラウザー アクセス用に構成した Application Segment を展開したら、正規名 (CNAME) をコピーします。
3. コピーした CNAME 情報をパブリック DNS に追加し、ユーザー ポータルの FQDN がレコードに解決されることを確認します。
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 4. ブラウザー アクセス ポータルの構成



1. ZPA 管理ポータルからブラウザー アクセス ポータルを構成します。新しいポータルを追加する際は、ポータルの名前、URL、ポータル サーバー証明書、説明の入力と、ユーザーにバナーを表示するオプションの選択が求められます。

2. ZPA 管理ポータルの [User Portals (ユーザー ポータル)] ページで行を展開し、表内のポータルの詳細を表示させたら、正規名 (CNAME) の横にあるコピーのアイコンをクリックします。この CNAME レコードは、パブリック DNS に必要になります。

3. コピーした CNAME 情報をパブリック DNS に追加し、ユーザー ポータルの FQDN がレコードに解決されることを確認します。

4. 次に、ブラウザー アクセス ユーザー ポータルに表示されるブラウザー アクセス対応アプリケーションのリンクである、ポータル リンクを追加します。

5. ZPA 管理ポータルの [Portal Links (ポータル リンク)] ページに移動します。ここから、ポータルに表示する各アプリケーションの名前、プロトコル (HTTP/HTTP)、説明、アイコン / 画像を構成できます。

リソース

ZPA: ブラウザー アクセス
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)

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