Resumo da solução

Acesso remoto seguro e confiável ao SAP com o Zscaler Private Access (ZPA)

Com 98% das 100 marcas mais valiosas confiando na SAP, 85 das quais são clientes do SAP S/4HANA com mais negócios migrando cargas de trabalho todos os dias, é crucial fornecer acesso remoto confiável e seguro a aplicativos SAP essenciais aos negócios. Além disso, à medida que o trabalho híbrido se torna a nova norma e os usuários acessam o SAP de qualquer lugar, em qualquer dispositivo e de qualquer local, o perímetro virtual se expandiu além da rede, chegando até usuários, dispositivos e aplicativos. No entanto, as organizações continuam a depender de tecnologias legadas e centradas em rede, como VPNs e firewalls, para controlar o acesso aos aplicativos.
Essas abordagens tradicionais são ineficazes no mundo da nuvem e dos dispositivos móveis, criando gargalos de desempenho e aumentando os riscos de segurança.

Em vez disso, sua empresa pode aproveitar uma abordagem zero trust que depende da identidade e do comportamento para verificar usuários e máquinas em tempo real e restringe dados e acesso com base no privilégio mínimo. De fato, a Gartner afirma que até 2025, pelo menos 70% das novas implantações de acesso remoto serão realizadas predominantemente por acesso à rede zero trust (ZTNA).

Apresentamos o Zscaler Private Access (ZPA)

O Zscaler Private Access (ZPA) é a plataforma de ZTNA mais implantada do mundo, com mais de 150 pontos de presença alimentados por energia 100% renovável em todo o mundo e pareados com os maiores provedores de nuvem do mundo, fornecendo conectividade direta e segura a aplicativos privados. Os usuários que acessam aplicativos SAP executados no local ou na nuvem pública nunca são inseridos na rede, tornando os aplicativos invisíveis para a internet e usuários não autorizados ou invasores. Os endereços IP nunca são expostos usando conexões de dentro para fora, e os aplicativos são segmentados para que os usuários possam acessar apenas um aplicativo específico, limitando a movimentação lateral.

Quando o acesso remoto se torna fácil, a conectividade e a disponibilidade melhoram. Para clientes como a Growmark, uma cooperativa de suprimentos agrícolas, o ZPA possibilitou a continuidade e a resiliência dos negócios ao permitir que 98% de seus funcionários continuassem a realizar seu trabalho efetivamente em casa. Eric Fisher, diretor de TI da Growmark, observou que com o ZPA para SAP "estamos obtendo uma melhor presença de segurança, melhor visibilidade e mais conformidade".

Benefícios da Zscaler para SAP

- **Ofereça uma experiência de usuário do SAP superior:** aumente a produtividade das suas equipes híbridas e resolva proativamente problemas de experiência do usuário com o monitoramento e a visibilidade contínuos do ZDX.
- **Estenda o zero trust para aplicativos, cargas de trabalho e IoT:** aproveite um único mecanismo de política global para fornecer acesso rápido e direto a aplicativos SAP privados, cargas de trabalho e dispositivos de OT/IIoT.
- **Reduza a complexidade operacional e os custos:** sem hardware ou software para gerenciar, as implantações de acesso à rede zero trust (ZTNA) fornecidas pela nuvem eliminam a sobrecarga de infraestrutura.
- **Mitigue os riscos de violação de dados:** torne os aplicativos SAP invisíveis para usuários não autorizados e aplique o acesso de privilégio mínimo, minimizando a superfície de ataque do aplicativo SAP S/4HANA.

> "Com o ZPA para SAP, temos uma melhor cobertura da segurança, melhor visibilidade e mais conformidade. Podemos permitir que nossos usuários trabalhem de qualquer lugar, uma vitória para todos."
>
> **Eric Fisher**
> Diretor de TI, Growmark

Como funciona o Zscaler Private Access

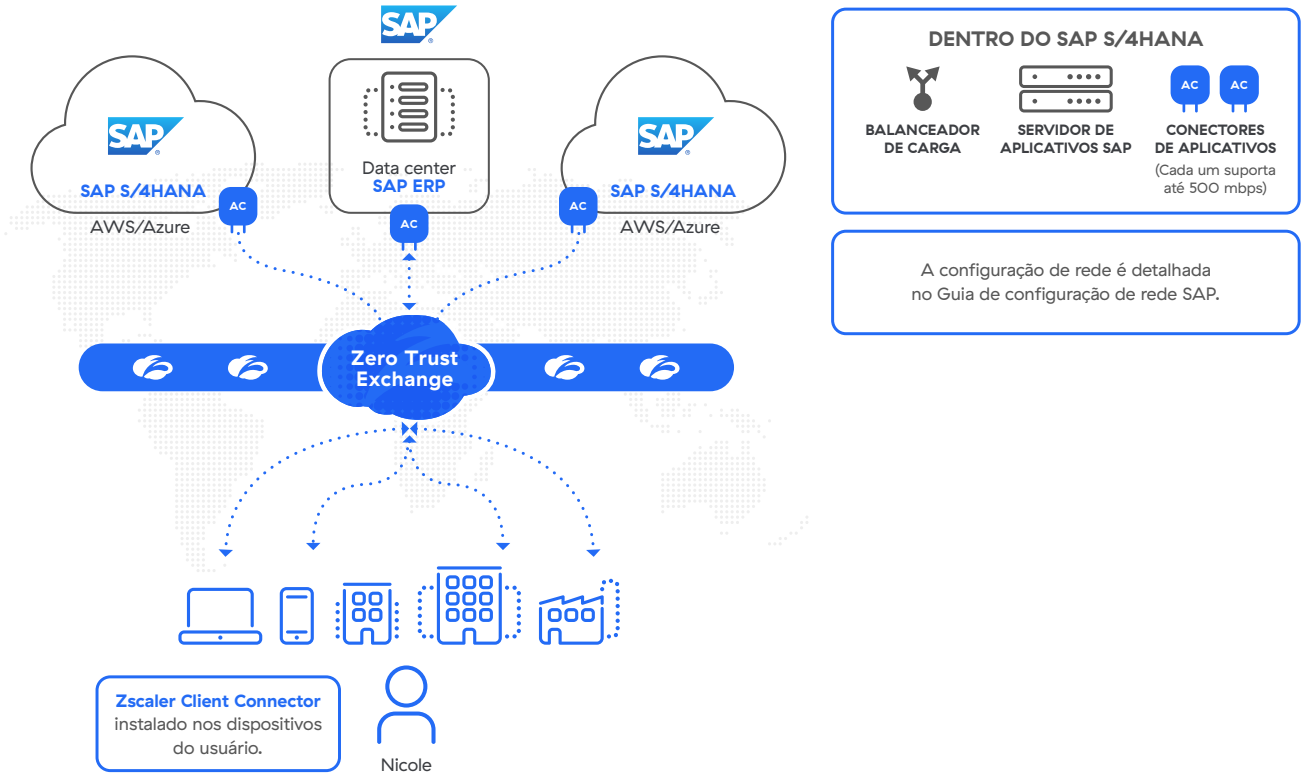


Figura 1: usuário confiável ao acessar com segurança os aplicativos SAP no S/4HANA com ZPA

O ZPA e o SAP podem ser facilmente configurados entendendo esses componentes comuns, etapas de configuração e seguindo as práticas recomendadas do SAP.

Componentes do ZPA/SAP

- **Os App Connectors** fornecem uma interface segura e autenticada entre os servidores de aplicativos das organizações e a nuvem do ZPA.
- **A plataforma Zscaler Zero Trust Exchange (ZTE)** oferece conexões rápidas e seguras e permite que seus funcionários trabalhem de qualquer lugar usando a internet como rede corporativa. A Zero Trust Exchange consiste em 150 data centers em todo o mundo, garantindo que o serviço esteja próximo de seus usuários, co-localizado com os provedores de nuvem e aplicativos que eles estão acessando, como Microsoft 365 e AWS. Ela garante a rota mais curta entre seus usuários e seus destinos, fornecendo segurança abrangente e uma experiência de usuário incrível.
- **O Zscaler Client Connector** é um aplicativo instalado no seu dispositivo para garantir que o tráfego da internet e o acesso aos aplicativos internos da sua organização estejam seguros e em conformidade com as políticas da sua organização.
- **Os aplicativos** são um nome de domínio totalmente qualificado (FQDN), nome de domínio local ou endereço IP que você define em um conjunto padrão de portas. Os aplicativos devem ser definidos dentro de um segmento de aplicativos.
- **O segmento de aplicativos** é um agrupamento de aplicativos definidos, com base no tipo de acesso ou privilégios do usuário.

- **As políticas** no ZPA controlam como os usuários acessam os aplicativos. Antes que um usuário possa acessar um aplicativo, uma política deve ser definida. Há muitos tipos de políticas. Consulte nosso link de recursos para obter mais informações sobre os tipos de políticas.
- **Um Zscaler Tunnel (Z-Tunnel)**é uma conexão ponto a ponto criptografada por TLS e mutuamente autenticada entre o Zscaler Client Connector e um ZPA Public Service Edge gerenciado pela Zscaler, ou entre um App Connector e um ZPA Private Service Edge gerenciado por uma organização. Um Z-Tunnel não contém nenhum dado de IP direto. Além disso, o Z-Tunnel pode transportar dentro dele vários canais de comunicação chamados Microtunnels.
- **Um Microtunnel (M-Tunnel)** é um canal de comunicação de ponta a ponta criado entre o Zscaler Client Connector e um aplicativo interno por meio de um ZPA Public Service Edge ou ZPA Private Service Edge e um App Connector mediante demanda.
- **Servidores de aplicativos SAP** são servidores que hospedam aplicativos SAP.

Proteção do acesso remoto dos usuários ao SAP S/4HANA com o ZPA

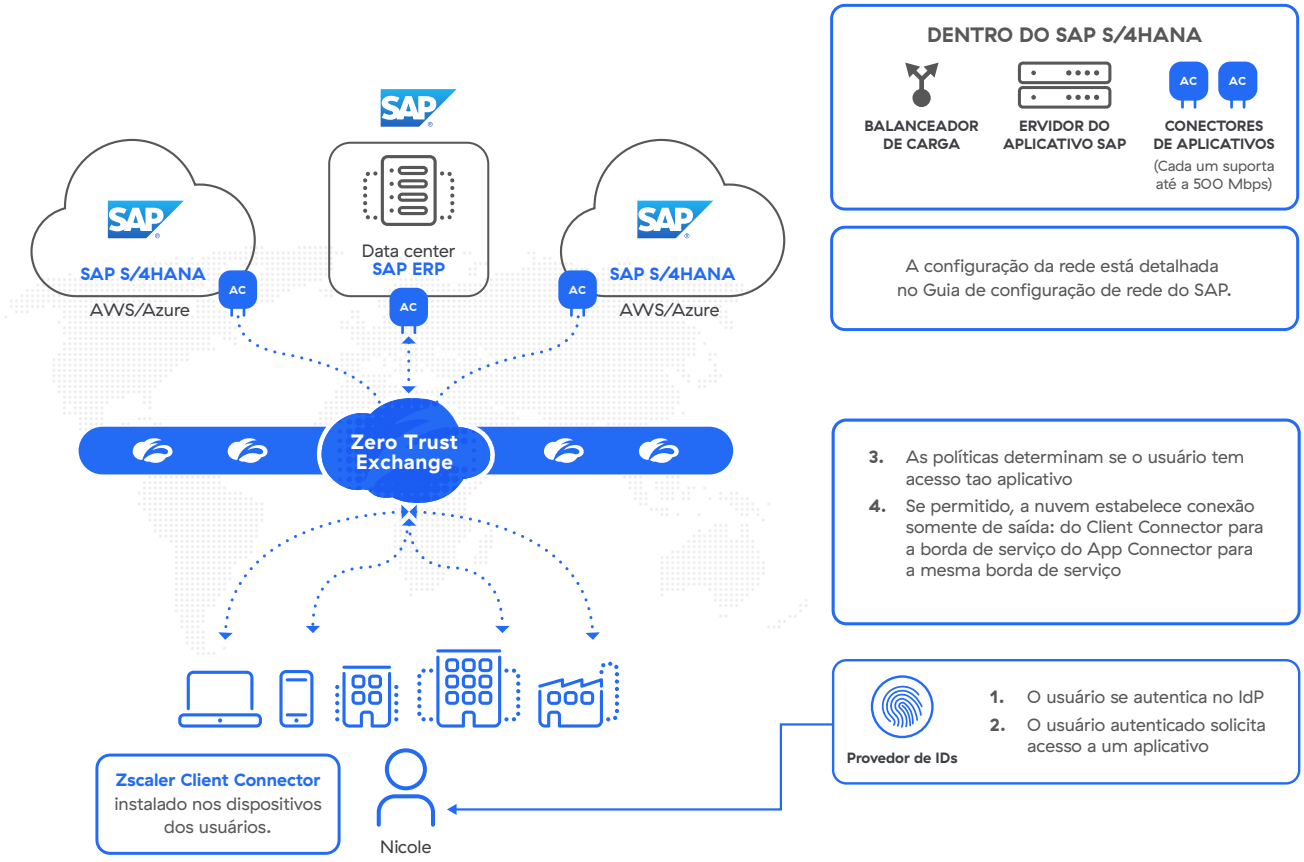
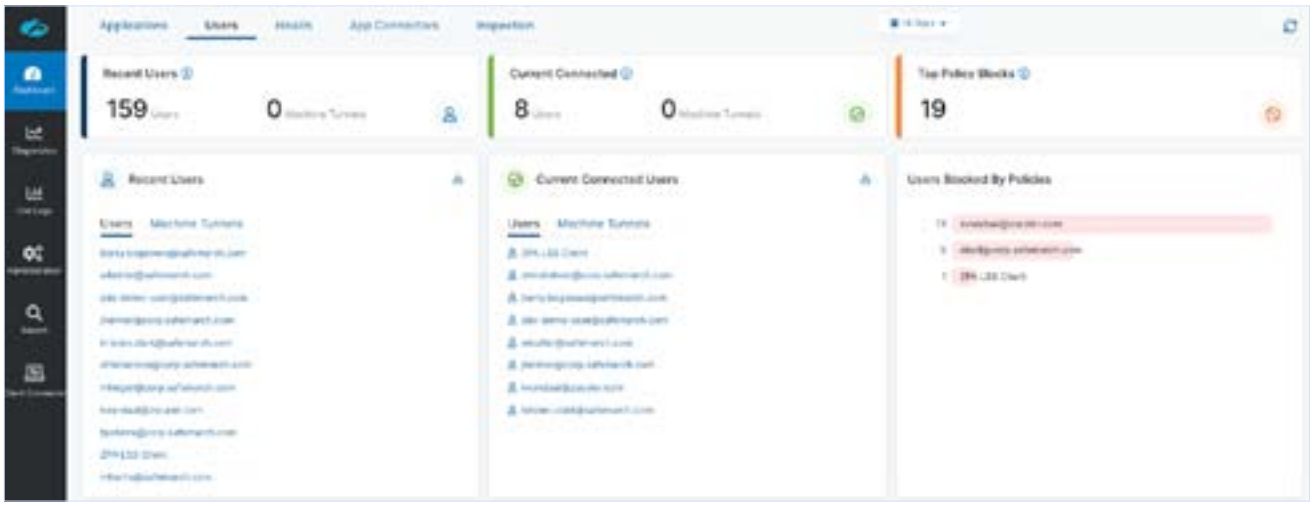


Figura 2: usuário confiável ao acessar com segurança os aplicativos SAP no S/4HANA com ZPA (detalhes adicionais)

As figuras 1 e 2 descrevem uma implantação do ZPA para um ambiente SAP híbrido. Nicole é uma funcionária da ACME que precisa acessar um aplicativo SAP. Nicole pode estar em qualquer lugar: na sede da empresa, em sua casa, em uma fábrica da empresa ou em uma cafeteria na cidade.

Quando Nicole solicita acesso a um aplicativo SAP pela primeira vez, precisa se autenticar com o IDP de sua organização. Após a autenticação, a Zscaler Cloud avalia a solicitação de aplicativo da Nicole em relação à política existente. Se Nicole tiver permissão para acessar o aplicativo, a Zero Trust Exchange entrará em contato com o App Connector mais próximo do aplicativo, que estabelecerá um Z-Tunnel de dentro para fora, uma conexão TLS criptografada, do aplicativo para a Zero Trust Exchange. Ao mesmo tempo, a Zscaler Cloud iniciará um Z-Tunnel de dentro para fora do Client Connector no dispositivo de Nicole de volta para a Zscaler Cloud. A Zscaler Cloud então unirá os Z-Tunnels e formará um M-Tunnel dentro dele, um canal de comunicação de ponta a ponta entre Nicole e o aplicativo. Nicole agora tem acesso seguro ao aplicativo SAP com a melhor experiência de usuário possível, aproveitando a conexão mais rápida de um dos mais de 150 pontos de presença globais da Zscaler.

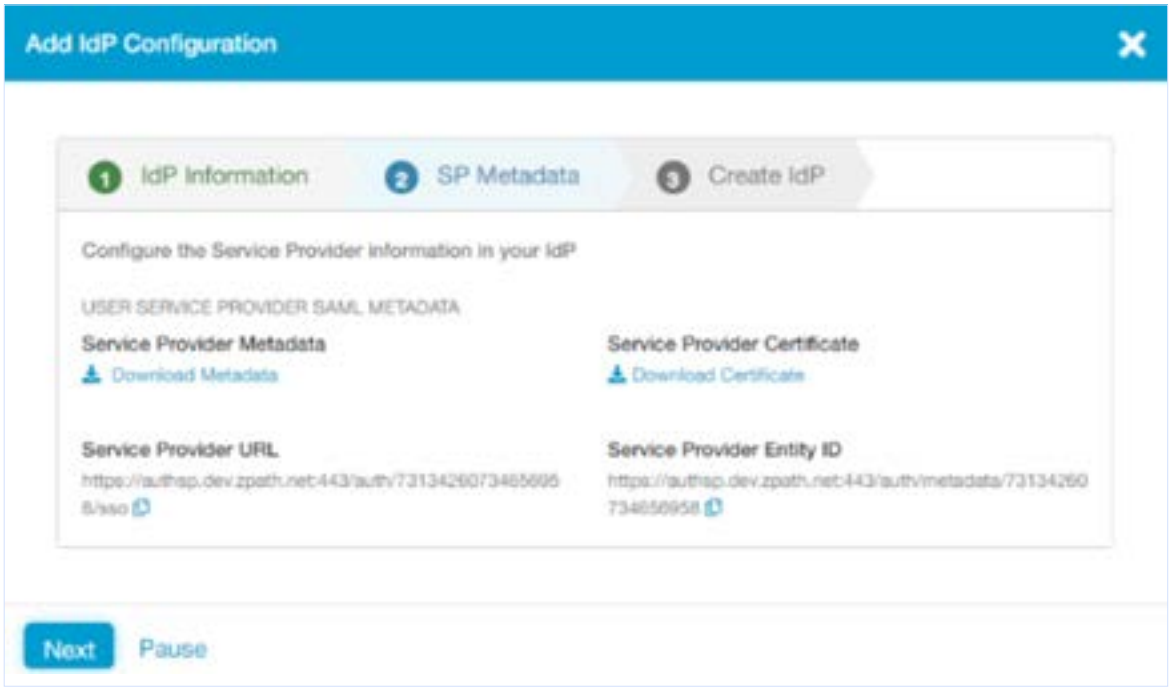


> “É fundamental oferecer aos nossos funcionários um ambiente de trabalho seguro e altamente disponível, garantindo-lhes acesso seguro a aplicativos na nuvem, como SAP, e à internet o tempo todo, ao mesmo tempo em que reduzimos nossa exposição.”
>
> **Schmitz Cargobull**

Introdução ao ZPA e SAP

Para obter etapas detalhadas sobre como configurar o ZPA, consulte help.zscaler.com/zpa.

Etapa 1: configurar autenticação de logon único (SSO) e IDP

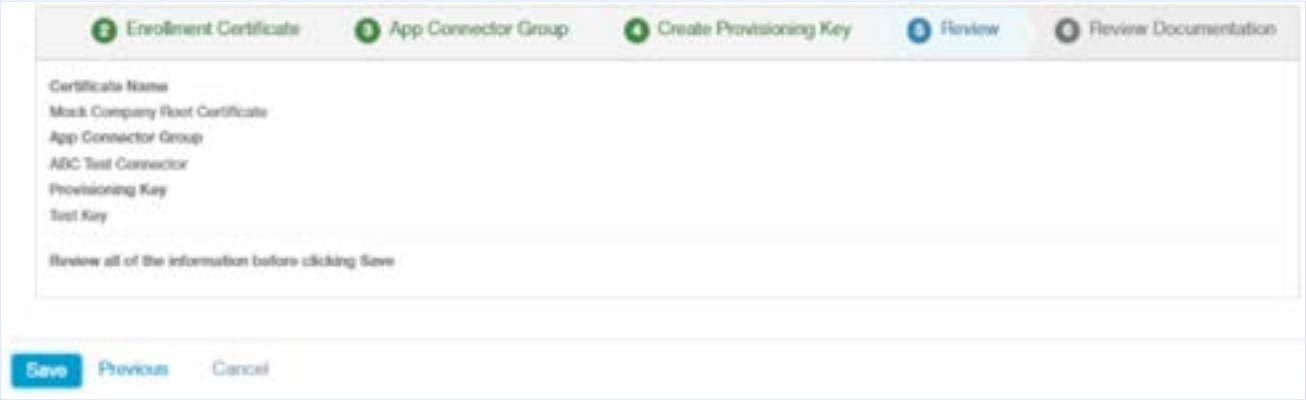


O ZPA aproveita as identidades de usuários do Provedor de Identidade (IdP) existente de uma organização e pode ser configurado para oferecer suporte a uma ou várias soluções de IdP. O ZPA é compatível com logon único (SSO) via SAML para que seus usuários remotos possam acessar aplicativos corporativos sem precisar fazer login separadamente no ZPA.

Para que os usuários acessem seus aplicativos via ZPA, eles devem primeiro se autenticar no Zscaler Client Connector usando qualquer provedor de identidade (IdP) compatível com SAML 2.0 usando o modelo iniciado pelo provedor de serviços (iniciado pelo SP). O SSO do usuário do ZPA é iniciado pelo SP, mas o SSO do administrador do ZPA pode ser iniciado pelo SP ou pelo IdP.

1. Configure seu IdP e especifique o ZPA como SP. Antes de adicionar uma configuração de IdP usando o portal de administração do ZPA, você precisa ter o IdP em vigor para sua organização.
2. Adicione uma configuração de IDP por meio do portal de administração do ZPA.

Etapa 2: implantar App Connectors



Os App Connectors fornecem uma interface autenticada segura entre os aplicativos SAP e a nuvem do ZPA. Os App Connectors geralmente são implantados em pares para oferecer alta disponibilidade, e são normalmente implantados adjacentes ao servidor de aplicativos SAP. Os App Connectors podem ser implantados de várias formas. A Zscaler distribui uma imagem de máquina virtual (VM) padrão para implantação em data centers corporativos, ambientes de nuvem local privada, como VMware, ou ambientes de nuvem pública, como Amazon Web Services (AWS) EC2. Além disso, a Zscaler fornece pacotes que podem ser instalados em distribuições Linux compatíveis.

A configuração padrão do App Connector consiste em duas etapas principais:

1. Adicione um App Connector por meio do portal de administração do ZPA.
2. Implante os App Connectors na plataforma compatível de sua escolha.

No entanto, configurar os App Connectors para SAP HEC/PCE requer etapas especiais:

1. O cliente SAP solicita o Zscaler Endpoint Service ao seu representante de conta SAP ou gerente de entrega ao cliente.
2. A SAP instala App Connectors de alta disponibilidade no SAP HEC/PCE em nome do cliente.
3. O cliente fornece à SAP a licença do ZPA para aplicar aos App Connectors.

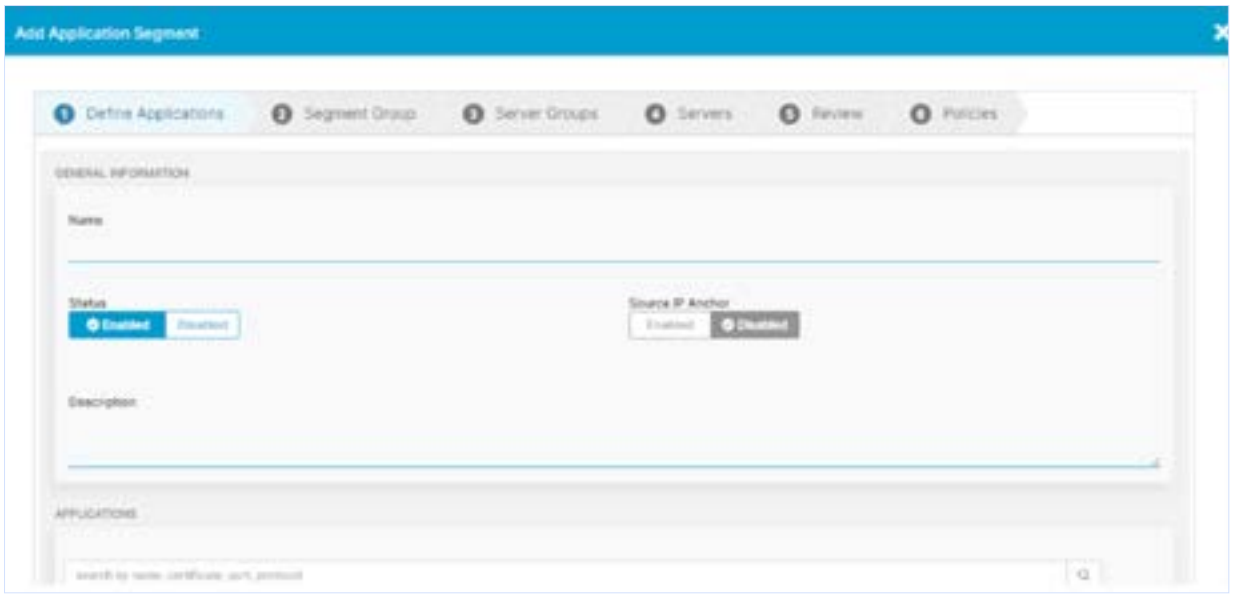
Etapa 3: configurar o Client Connector

O Zscaler Client Connector é um aplicativo leve que fica nos terminais dos usuários (laptops e dispositivos móveis gerenciados pela empresa, dispositivos pessoais, dispositivos portáteis, entre outros) e aplica políticas de segurança e controles de acesso independentemente do dispositivo, local ou aplicativo. O aplicativo Zscaler Client Connector encaminha o tráfego para o ponto de presença da Zscaler Cloud mais próximo, onde o tráfego é roteado para aplicativos SAP por meio da Zero Trust Exchange.

1. Conclua os requisitos do sistema e as tarefas pré-requisitos:
   - Configure as configurações de segurança e acesso apropriadas no portal de administração do ZPA.
   - A autenticação baseada em SAML deve ser configurada e os usuários provisionados. Você não pode usar o portal do Zscaler Client Connector como um IdP para o serviço do ZPA.
   - Certifique-se de que o Zscaler Client Connector processe corretamente o tráfego para o ZPA.
2. Configure as definições de administração para o Zscaler Client Connector. A política de uso aceitável, as configurações de atualização, as políticas de encaminhamento, o acesso do usuário ao suporte e logs e as configurações de falha de abertura são todas configuráveis.
3. Configure os perfis do Client Connector. No portal do Zscaler Client Connector, você pode configurar perfis de aplicativos adicionando regras de política a cada perfil. Você pode selecionar a ordem de precedência entre as regras, bem como a quem cada regra se aplica (ou seja, a todos os usuários ou a diferentes grupos de usuários). Quando um usuário registra o aplicativo no serviço da Zscaler, o aplicativo leva em consideração a ordem de precedência e a identidade do usuário para baixar um perfil de aplicativo com a regra de política apropriada.

4. Baixe o Zscaler Client Connector da loja Client Connector
5. Personalize o Client Connector com opções do instalador. Você pode configurar um arquivo instalador do Zscaler Client Connector com opções de instalação que permitem remover etapas do processo de registro do usuário (por exemplo, permitindo que os usuários ignorem a página de registro ou o prompt de seleção de nuvem no Zscaler Client Connector).
6. Implante o Client Connector. Você pode instalar o Zscaler Client Connector manualmente em dispositivos individuais ou usar o mecanismo de gerenciamento de dispositivos da sua organização para implantar o Zscaler Client Connector nos dispositivos dos seus usuários.

Etapa 4: adicionar segmentos de aplicativos



Um segmento de aplicativos é uma coleção de instâncias de aplicativos. Os aplicativos são descobertos automaticamente e podem ser agrupados automaticamente com base em critérios de correspondência. Um segmento de aplicativos pode estar ancorado a um ou mais hosts ou segmentos de host. Segmentos de aplicativos são usados para acomodar políticas que incluem ou abrangem vários outros segmentos.

A Zscaler recomenda as seguintes práticas para configurar segmentos de aplicativos SAP:

- Crie um único segmento de aplicativos para todos os aplicativos SAP. Isso permitirá que o serviço ZPA faça o balanceamento de carga das solicitações dos usuários para esses aplicativos. Entretanto, se a segmentação for necessária, crie vários segmentos de aplicativos para os aplicativos SAP.
- Crie segmentos de aplicativos para aplicativos SAP usando FQDNs. Se o cliente SAP não conseguir resolver o FQDN do host, ele tentará se conectar ao endereço IP. Embora o serviço seja compatível com endereços IP, é mais seguro que modelos zero trust se conectem com FQDNs.

- Se o nome do host SAP não for um FQDN, um domínio de pesquisa DNS será necessário. Se o cliente não tiver um sufixo de pesquisa, ele não poderá preencher o FQDN para se conectar ao SAP. O cliente retornará ao endereço IP fornecido pelo servidor de mensagens SAP, o que pode não ser desejável ou roteável pelo serviço ZPA.
- Use o rastreamento do Wireshark ou as configurações do SAP para identificar os endereços IP de todos os servidores SAP e crie um segmento de aplicativos que inclua apenas esses endereços IP e as portas TCP apropriadas. Não anuncie todo o intervalo de sub-rede (por exemplo, 192.168.1.0/24).
- Se houver uma lista de controle de acesso (ACL) configurada no servidor de mensagens SAP ou no servidor de aplicativos, adicione os endereços IP do App Connector a ela. Como o serviço ZPA executa um NAT de origem para o cliente, todo o tráfego é visto do endereço IP do App Connector. Para o grupo App Connector associado aos segmentos de aplicativos, o ZPA balanceará a carga das solicitações do usuário entre os App Connectors neste grupo App Connector. Por isso, é recomendável que os endereços IP de todos os App Connectors no grupo App Connector sejam adicionados à ACL.

Para oferecer suporte a aplicativos SAP no ZPA, você precisa configurar segmentos de aplicativos e domínios de pesquisa de DNS.

1. Adicione um segmento de aplicativos por meio do portal de administração do ZPA.
   - Na janela Adicionar aplicativo, em Definir aplicativos. Insira um nome de domínio totalmente qualificado (FQDN) que corresponda aos aplicativos SAP. Embora seja possível inserir um endereço IP, a Zscaler recomenda que você use FQDNs sempre que possível, pois é mais seguro. Se o cliente não tiver um sufixo de pesquisa, ele não poderá preencher o FQDN para se conectar ao SAP. O cliente retornará ao endereço IP fornecido pelo SAP Message Server.
   - Para garantir o acesso ao Zscaler Client Connector, certifique-se de inserir os intervalos de portas TCP para o aplicativo.
2. Adicione um domínio de pesquisa de DNS. Para o SAP, você pode configurar domínios de pesquisa de DNS para FQDNs no portal de administração do ZPA. Isso permite que o cliente SAP anexe o sufixo de pesquisa e crie o FQDN. No entanto, você também pode configurar o SAP para fornecer um FQDN em vez de um nome curto. Isso elimina a necessidade de configurar um domínio de pesquisa de DNS.

Recursos

Políticas do ZPA
ZPA: suporte a aplicativos SAP
RISE com nuvem SAP S/4HANA, edição privada e SAP ERP, PCE

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