Resumo da solução

Migração segura do SAP para a nuvem e modernização de aplicativos com o Zscaler Private Access (ZPA)

As empresas estão adotando a transformação digital para colher os benefícios de melhor desempenho, redução de custos e complexidade operacional. Para clientes da SAP, a transformação digital também é impulsionada pelo fim do suporte ao SAP ERP Central Component (SAP ECC) 6.0, um sistema de planejamento de recursos empresariais local. Isso não é surpreendente, pois a Gartner estima que até 2025, 95% das novas cargas de trabalho digitais serão implantadas nativamente na nuvem. No entanto, a experiência do usuário final não é uma prioridade durante processo de migração do SAP S/4HANA, permanecendo lenta, complicada ou arriscada.

A tecnologia legada continua colocando os usuários na rede e gera uma complexidade que retarda a migração para a nuvem, dificultando o retorno do investimento na nuvem pelas empresas. Simplificando, as arquiteturas de castelo e fosso e rede em estrela não podem ser dimensionadas ou proporcionar uma experiência de usuário rápida e contínua.

Apresentamos o Zscaler Private Access (ZPA)

Para acelerar as migrações do SAP S/4HANA para a nuvem e garantir a experiência do usuário e a produtividade durante todo o processo de transformação, as organizações podem aproveitar o Zscaler Private Access (ZPA) para obter experiências contínuas e consistentes, modernização de aplicativos sem esforço e segurança baseada em aplicativos. Com mais de 150 pontos de presença pareados com os maiores provedores de nuvem do mundo, clientes como a Kubota, uma fabricante de máquinas agrícolas, podem escalar e expandir rapidamente as operações, afirmando: "Na próxima vez que adicionarmos um depósito, não haverá necessidade de esperar semanas e gastar milhares de dólares em rede para conectar aos nossos sistemas SAP ERP para gerenciamento de estoque... estaremos prontos e funcionando em qualquer lugar desde o primeiro dia."

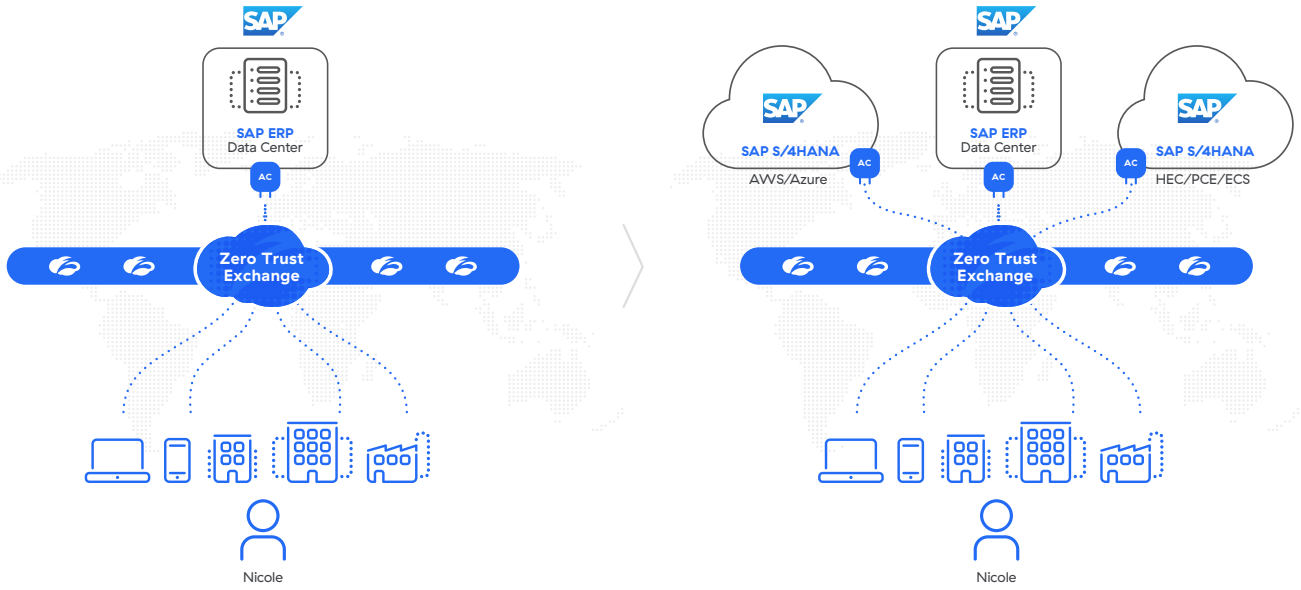
Atuando como uma camada de abstração entre o usuário e o aplicativo, o mecanismo de política global único do ZPA aplica princípios de zero trust em todos os dispositivos, locais e aplicativos. Os usuários se conectam da mesma forma aos aplicativos executados no data center e na nuvem e de qualquer dispositivo ou local. A localização do aplicativo pode ser alterada por meio de uma simples mudança de política, do data center para a nuvem pública ou de VPC para VPC, conectando os usuários com segurança diretamente aos aplicativos privados e com uma experiência de usuário superior.

Benefícios do Zscaler Private Access (ZPA):

- Acelere a migração de aplicativos SAP e a adoção da nuvem
- Ofereça controle granular do acesso do usuário aos aplicativos SAP
- Gerencie ativamente o acesso a cargas de trabalho antes e depois da migração
- Ofereça visibilidade de ponta a ponta do aplicativo SAP e melhore a experiência do usuário

> "Na próxima vez que adicionarmos um armazém, não haverá necessidade de esperar semanas e gastar milhares de dólares em rede. Estaremos prontos e funcionando em qualquer lugar desde o primeiro dia com nossos scanners RF conectados por 4G usando o Zscaler Client Connector para conectar-se ao gerenciamento de estoque dos nossos sistemas SAP ERP."
>
> **Jonathon Bonnici**
> Gerente de entrega de serviços de TI, Kubota Austrália

Como funciona o Zscaler Private Access

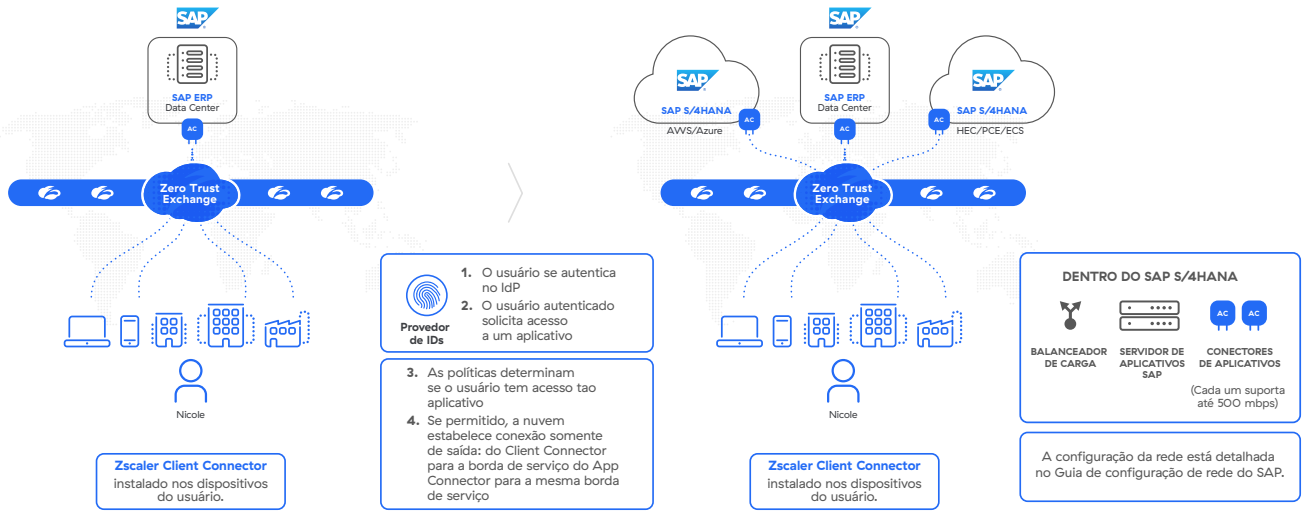


Componentes do ZPA/SAP

- 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) garante 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 dos seus usuários, co-localizado com os provedores de nuvem e aplicativos que eles acessam, como Microsoft 365 e AWS. Ela garante a rota mais curta entre os usuários e seus destinos, proporcionando 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 sejam seguros e estejam 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 aplicativo.
- 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. Existem 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 vários canais de comunicação chamados Microtúneis.

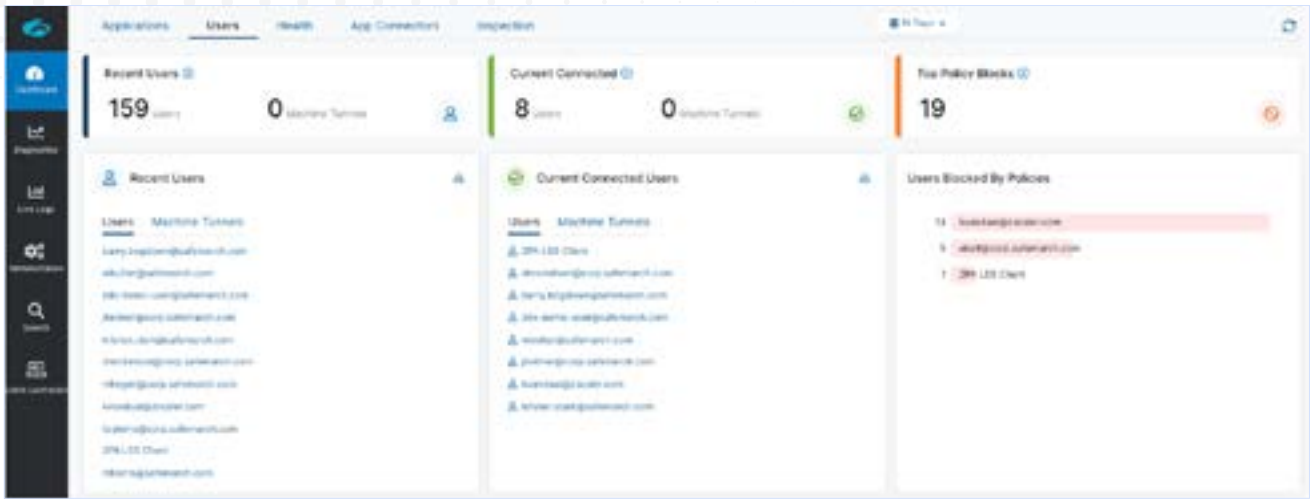
- Um Microtunnel (M–Tunnel) é um canal de comunicação de ponta a ponta criado entre o Zscaler Client Connector e um aplicativo interno por meio de um ZPA Public Service Edge ou ZPA Private Service Edge e um App Connector mediante demanda.
- Os servidores hospedam aplicativos disponibilizados para o ZPA e podem estar localizados em data centers corporativos ou em nuvens públicas virtuais.
- Grupos de servidores são uma coleção de servidores. Cada segmento de aplicativos deve ser mapeado para um grupo de servidores.
- Servidores de aplicativos SAP são servidores que hospedam aplicativos SAP.

Design do ZPA e do SAP



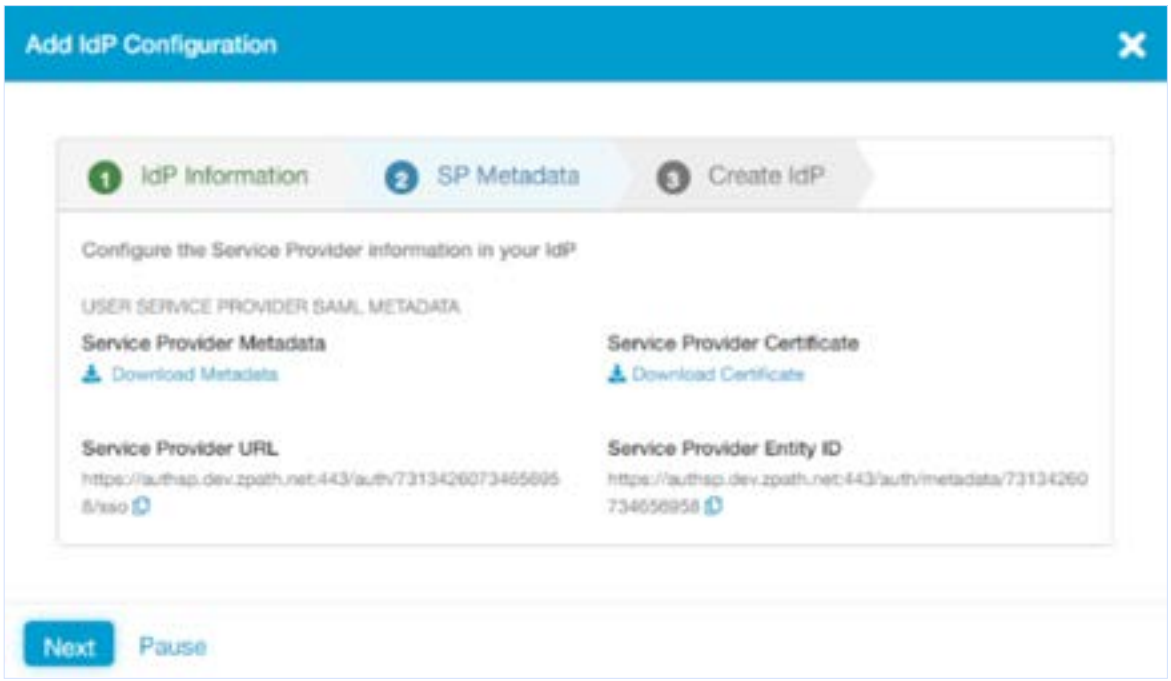
Por exemplo, a ACME atualmente hospeda seu sistema SAP ERP em um data center local na sede da empresa. A empresa está em processo de modernização de rede e aplicativos com planos de migrar todos os aplicativos SAP da empresa para o S/4HANA na AWS e no Azure. Felizmente, a ACME está aproveitando o ZPA, que faz parte da Zscaler Zero Trust Exchange (ZTE), no início de sua jornada de transformação, reduzindo o atrito ao longo do processo para garantir uma experiência simples e perfeita.

Quando Nicole, uma funcionária da ACME, solicita acesso a um aplicativo SAP hospedado no data center local, ela precisa se autenticar com o provedor de identidade (IdP) da ACME. Após a autenticação, a ZTE avalia a solicitação de Nicole em relação à política existente. Se Nicole tiver permissão para acessar o aplicativo determinado pela identidade e pelo contexto, a ZTE 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 ZTE. Simultaneamente, a ZTE iniciará um Z–Tunnel de dentro para fora do Client Connector no dispositivo de Nicole de volta para a ZTE. A ZTE então unirá os Z–Tunnels e formará um M–Tunnel, um canal de comunicação de ponta a ponta entre Nicole e o aplicativo, dentro dele. Esse mesmo processo acontece quando a ACME migra seus aplicativos SAP para a nuvem. A ACME simplesmente duplica os aplicativos do data center local para a nuvem. Quando estiver pronta, a ACME simplesmente remove os aplicativos do data center local. Agora, quando Nicole acessa seus aplicativos SAP, ela é automaticamente roteada para os aplicativos na nuvem.



Introdução à migração para a nuvem e modernização de aplicativos

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

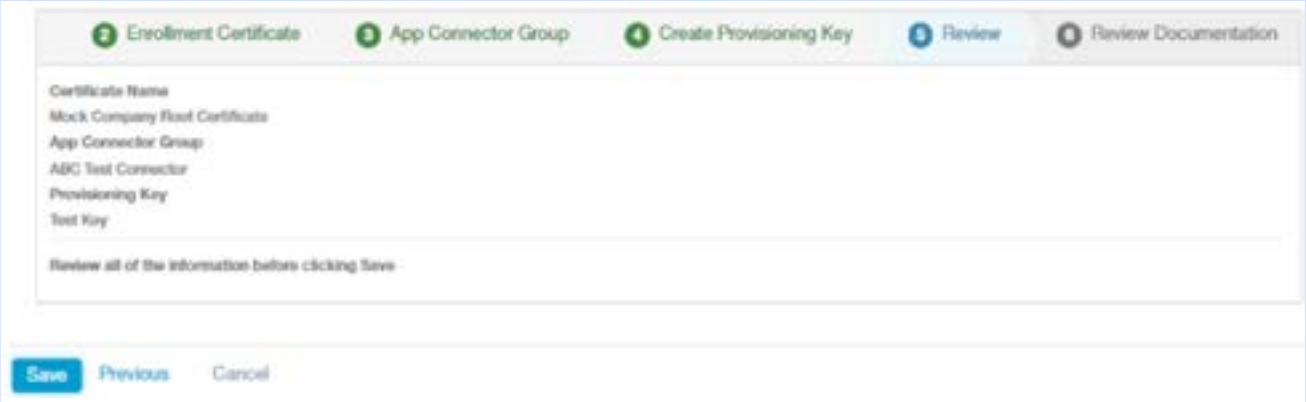


O ZPA aproveita as identidades de usuários do Provedor de Identidade (IdP) existente de uma organização e pode ser configurado para oferecer suporte a uma ou várias soluções de IdP. O ZPA oferece suporte ao logon único (SSO) via SAML para que seus usuários remotos possam acessar aplicativos corporativos 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: configurar App Connectors e grupos de 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 são organizados em grupos de App Connectors. Cada App Connector pertence a um grupo de App Connector específico e cada grupo de App Connector é associado a pelo menos um grupo de servidores para atender a qualquer aplicativo. 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.

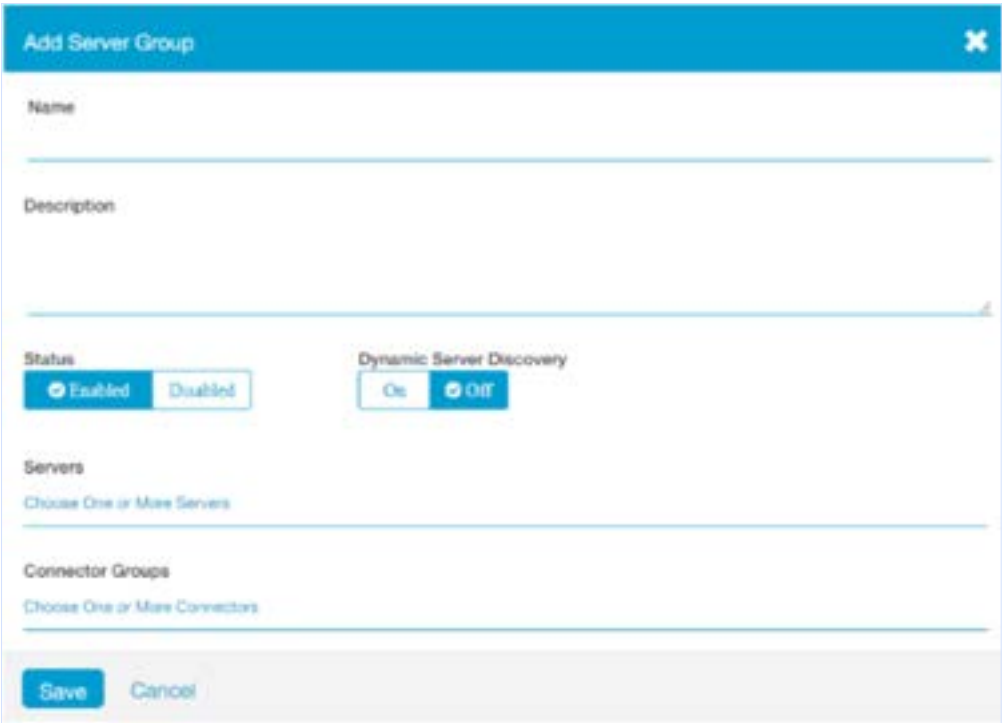
A configuração padrão do App Connector consiste em duas etapas principais:

1. Adicione um App Connector por meio do portal de administração do ZPA.
2. Implante os App Connectors na plataforma compatível de sua escolha.
3. Para migração para a nuvem, os App Connectors precisarão ser associados ao grupo de servidores do data center local e ao grupo de servidores da nuvem.

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 servidores e grupos de servidores



Você deve configurar servidores que hospedam os aplicativos que deseja disponibilizar para o ZPA, estejam eles no seu data center corporativo ou em uma nuvem pública virtual (VPC).

Existem dois métodos principais para configuração do servidor:

- **Defina explicitamente servidores e grupos de servidores:** Você pode definir explicitamente cada servidor que hospeda um ou mais aplicativos. Para cada servidor, você fornece um nome, bem como um endereço IP ou um nome de domínio totalmente qualificado (FQDN). Então, você pode organizar manualmente esses servidores em grupos de servidores.
- **Habilite a descoberta dinâmica de servidor:** em vez de definir explicitamente cada servidor, você pode habilitar a descoberta dinâmica de servidor para que o ZPA possa descobrir os servidores apropriados para seus aplicativos conforme os usuários os solicitam. Para esse método, você só precisa criar um grupo de servidores vazio que tenha a descoberta dinâmica de servidor habilitada.

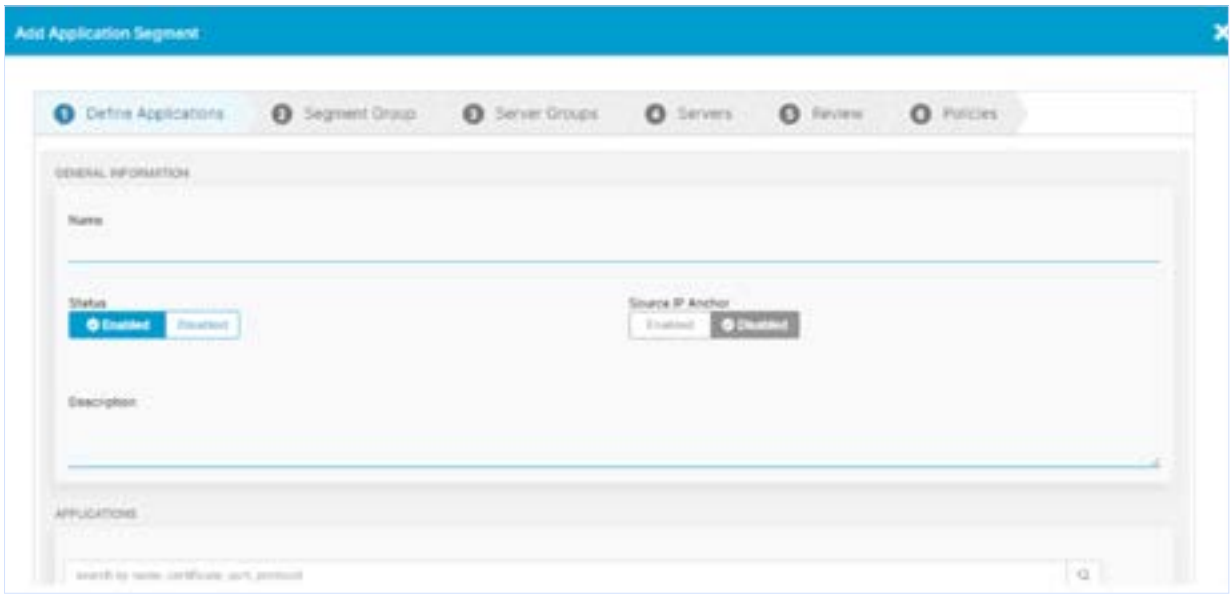
Cada segmento de aplicativo será associado a um servidor e grupo de servidores. Se a descoberta dinâmica de servidor estiver habilitada, quando o aplicativo for migrado para a nuvem, o ZPA registrará automaticamente a alteração e encaminhará os clientes para o aplicativo na nuvem. Se a descoberta dinâmica de servidor não estiver habilitada, o administrador do ZPA precisará alterar manualmente o servidor e o grupo de servidores associados ao aplicativo que agora reside na nuvem.

Etapa 4: 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 5: 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.

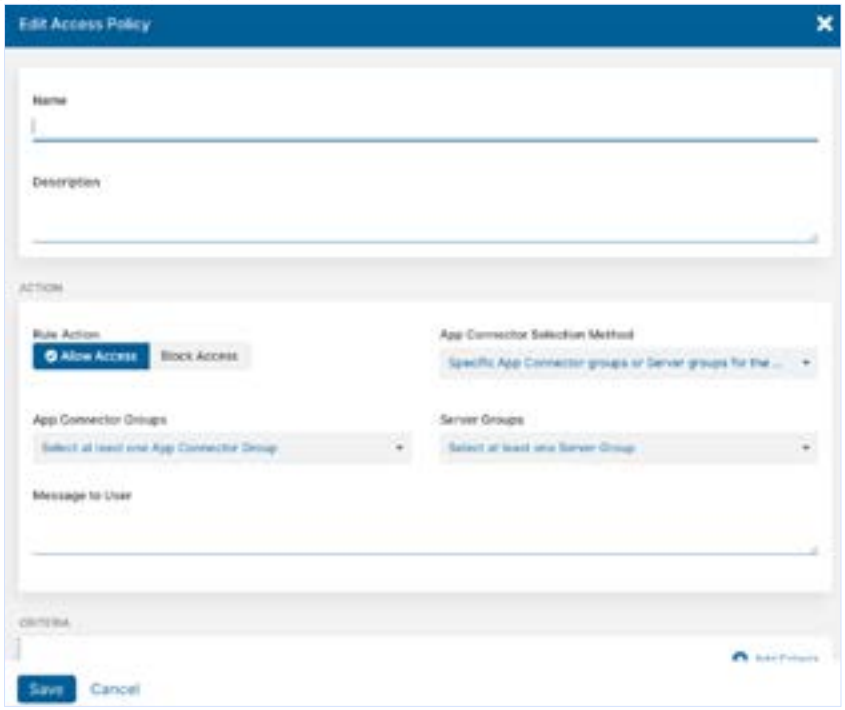
A Zscaler recomenda as seguintes práticas para configurar segmentos de aplicativos SAP:

- 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.

Etapa 6 (opcional): migração de aplicativos via política



Durante migrações típicas para a nuvem, não há alterações de política adicionais necessárias para concluir a migração do acesso do usuário do aplicativo legado para o aplicativo na nuvem. Em alguns casos, as organizações podem não querer migrar todos os usuários de uma vez para os aplicativos na nuvem. Por exemplo, eles podem querer testar os aplicativos na nuvem com um pequeno grupo de usuários antes de migrar todos os usuários. Nesse cenário, as organizações podem usar uma abordagem baseada em políticas para migração para a nuvem.

1. No portal de administração do ZPA, crie uma política para os usuários que acessarão os aplicativos na nuvem e selecione a opção “Grupos de App Connectors específicos ou grupos de servidores”.
2. Em seguida, selecione o grupo de App Connectors para os aplicativos hospedados na nuvem.
3. Repita esse processo para os usuários que acessarão os aplicativos no data center. Certifique-se de selecionar o grupo de App Connectors para os aplicativos no data center local.
4. Quando estiver pronto, migre o restante dos usuários para a nuvem atualizando a política com os grupos de App Connectors associados à nuvem.

Recursos

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

> “O ZPA nos dá flexibilidade para encerrar usuários onde for necessário, para que possamos executar o SAP em uma região na AWS, mas fazer failover para outra região e fazer com que esses usuários se conectem perfeitamente por meio de uma mudança de política. O ZPA permite que os usuários acessem aplicativos legados, bem como nosso novo ambiente SAP na nuvem.”
>
> **Growmark**

zscaler™ | Experience your world, secured.™

Sobre a Zscaler
A Zscaler (NASDAQ: ZS) acelera a transformação digital para que seus clientes possam ter mais agilidade, eficiência, resiliência e segurança. A solução Zscaler Zero Trust Exchange protege milhares de clientes contra ataques cibernéticos e perda de dados, conectando com segurança usuários, dispositivos e aplicativos em qualquer local. Distribuída em mais de 150 data centers globalmente, a Zero Trust Exchange baseada em SASE é a maior plataforma integrada de segurança na nuvem do mundo. Saiba mais em **zscaler.com/br** ou siga-nos no Twitter **@zscaler**.

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