Resumen de la solución

Acceso remoto seguro y confiable para SAP con Zscaler Private Access (ZPA)

Dado que el 98 % de las 100 marcas más valoradas confían en SAP, 85 de las cuales son clientes de SAP S/4HANA y cada día hay más empresas que migran cargas de trabajo, es fundamental proporcionar un acceso remoto confiable y seguro a las aplicaciones SAP críticas para la actividad. Además, a medida que el trabajo híbrido se convierte en la nueva norma y los usuarios acceden a SAP desde cualquier lugar, en cualquier dispositivo y desde cualquier ubicación, el perímetro virtual se ha ampliado más allá de la red hasta llegar a los usuarios, los dispositivos y las aplicaciones. Sin embargo, las organizaciones continúan dependiendo de tecnologías tradicionales centradas en la red, como VPN y firewalls, para controlar el acceso a las aplicaciones. Estos enfoques tradicionales son ineficaces en el mundo que le da prioridad a la nube y al móvil, creando cuellos de botella en el rendimiento y aumentando los riesgos de seguridad.

En su lugar, su empresa puede aprovechar un enfoque Zero Trust que se base en la identidad y el comportamiento para verificar a los usuarios y las máquinas en tiempo real, y restrinja los datos y el acceso basándose en privilegios mínimos. De hecho, Gartner® afirma que para 2025, al menos el 70 % de las nuevas implementaciones de acceso remoto se realizarán predominantemente mediante el acceso a redes Zero Trust (ZTNA).

Presentamos Zscaler Private Access (ZPA)

Zscaler Private Access (ZPA) es la plataforma ZTNA más implementada del mundo, con más de 150 puntos de presencia alimentados por energía 100 % renovable en todo el mundo y en colaboración con los mayores proveedores de nube del mundo, que proporciona una conectividad segura y directa a las aplicaciones privadas. Los usuarios que acceden a las aplicaciones de SAP que se ejecutan en las instalaciones o en la nube pública nunca entran en la red, lo que hace que las aplicaciones sean invisibles para Internet y los usuarios no autorizados o los atacantes. Las direcciones IP nunca se exponen utilizando conexiones de "adentro hacia afuera", y las aplicaciones se segmentan para que los usuarios solo puedan acceder a una aplicación específica, limitando el movimiento lateral.

Cuando el acceso remoto se simplifica, la conectividad y la disponibilidad mejoran. Para clientes como Growmark, una cooperativa de suministros agrícolas, la ZPA permitió la continuidad y la resiliencia empresarial al permitir que el 98 % de su personal siguiera realizando eficazmente su trabajo desde casa. Eric Fisher, director de TI de Growmark, señaló que con ZPA para SAP, "estamos logrando una mejor huella de seguridad, mejor visibilidad y cumplimos mejor con las normativas".

Beneficios de Zscaler para SAP

- **Ofrezca una experiencia de usuario SAP superior:** aumente la productividad de su fuerza de trabajo híbrida y resuelva de manera proactiva los problemas de experiencia del usuario con la visibilidad y la supervisión continua de ZDX.
- **Extienda Zero Trust a las aplicaciones, las cargas de trabajo y el IoT:** Aproveche un único motor de políticas global para ofrecer un acceso rápido y directo a aplicaciones SAP privadas, cargas de trabajo y dispositivos OT/IIoT.
- **Reduzca la complejidad y los costos operativos:** sin hardware ni software que administrar, las implementaciones de acceso a la red Zero Trust (ZTNA) en la nube eliminan la sobrecarga de infraestructura.
- **Mitigue el riesgo de una violación de datos:** haga que las aplicaciones SAP sean invisibles para usuarios no autorizados y aplique el acceso con privilegios mínimos, minimizando la superficie de ataque de las aplicaciones en SAP S/4HANA.

> "Con ZPA para SAP, estamos consiguiendo una mejor huella de seguridad, una mejor visibilidad y cumplimos más las normativas. "Podemos permitir que nuestros usuarios trabajen desde cualquier lugar: una victoria para todos".
>
> **Eric Fisher**
> Director de TI, Growmark

Cómo funciona Zscaler Private Access

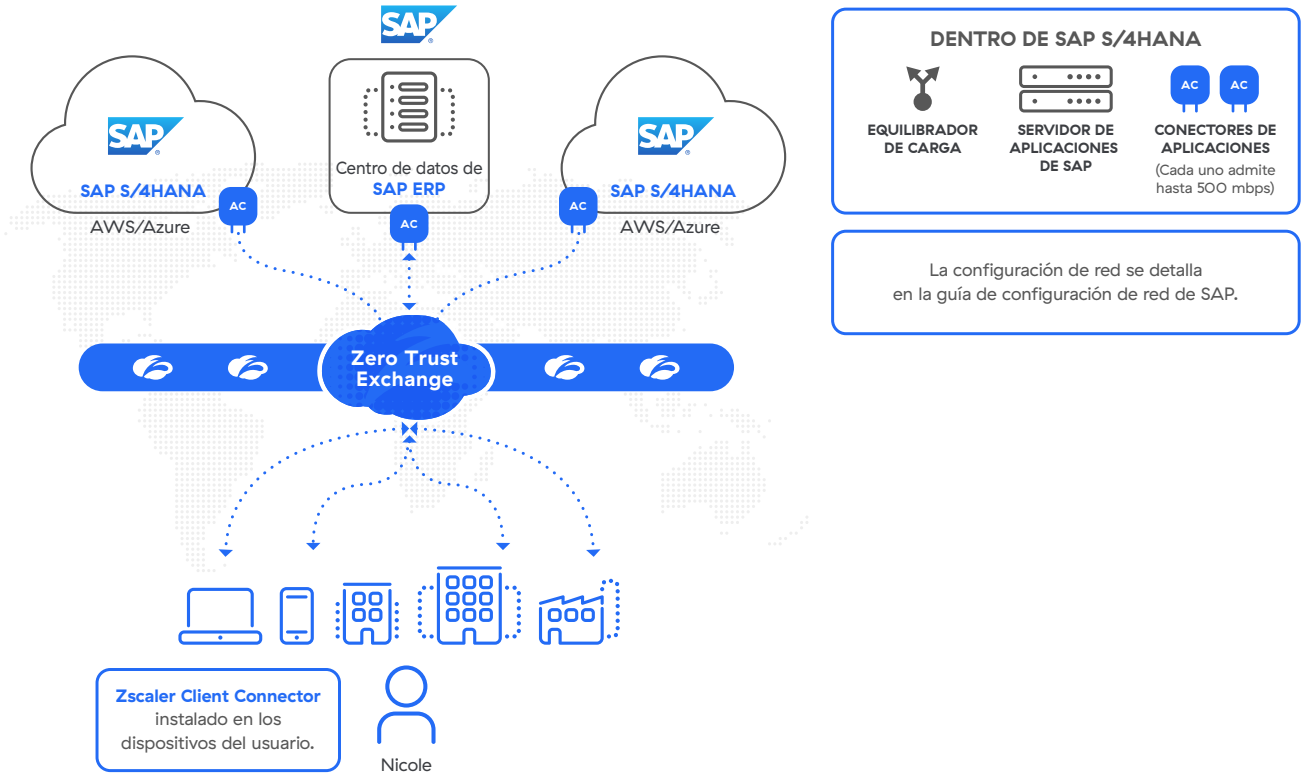


Figura 1: Acceso confiable y seguro de los usuarios a las aplicaciones SAP en S/4HANA con ZPA

ZPA y SAP pueden configurarse fácilmente comprendiendo estos componentes comunes, los pasos de configuración y siguiendo las mejores prácticas de SAP.

Componentes ZPA/SAP

- **Los App Connectors** proporcionan una interfaz segura autenticada entre los servidores de aplicaciones de las organizaciones y la nube ZPA.
- **La plataforma Zscaler Zero Trust Exchange (ZTE)** permite conexiones rápidas y seguras y permite a sus empleados trabajar desde cualquier lugar utilizando internet como red corporativa. La Zero Trust Exchange consta de 150 centros de datos en todo el mundo, lo que garantiza que el servicio esté cerca de sus usuarios, situado junto a los proveedores de la nube y las aplicaciones a las que acceden, como Microsoft 365 y AWS. Garantiza el camino más corto entre sus usuarios y sus destinos, proporcionando una seguridad integral y una experiencia de usuario increíble.
- **Zscaler Client Connector** es una aplicación que se instala en su dispositivo para garantizar que su tráfico de Internet y el acceso a las aplicaciones internas de su organización sean seguros y cumplan con las políticas de su organización.
- **Las aplicaciones** son un nombre de dominio completo (FQDN), un nombre de dominio local o una dirección IP que se define en un conjunto estándar de puertos. Las aplicaciones deben definirse dentro de un segmento de aplicación.
- **El segmento de aplicación** es una agrupación de aplicaciones definidas, según el tipo de acceso o los privilegios del usuario.

- **Las políticas** de ZPA controlan el modo en que los usuarios acceden a las aplicaciones. Antes de que un usuario pueda acceder a una aplicación, se debe definir una política. Existen muchos tipos de políticas. Consulte nuestro enlace de recursos para obtener más información sobre los tipos de políticas.
- **Un túnel de Zscaler (Z–Tunnel)**es una conexión punto a punto autenticada mutuamente y cifrada mediante TLS entre el Zscaler Client Connector y un Public Service Edge administrado por Zscaler, o entre un App Connector y un ZPA Private Service Edge administrado por una organización. Un Z–Tunnel no contiene ningún dato de IP directo. Además, el Z–Tunnel puede transportar en su interior múltiples canales de comunicación denominados microtúneles.
- **Un microtúnel (M–Tunnel)** es un canal de comunicación de extremo a extremo creado entre Zscaler Client Connector y una aplicación interna a través de un ZPA Public Service Edge, o un ZPA Private Service Edge y un App Connector a demanda.
- **Los servidores de aplicaciones SAP** son servidores que alojan aplicaciones SAP.

Cómo proteger el acceso remoto de los usuarios a SAP S/4HANA con ZPA

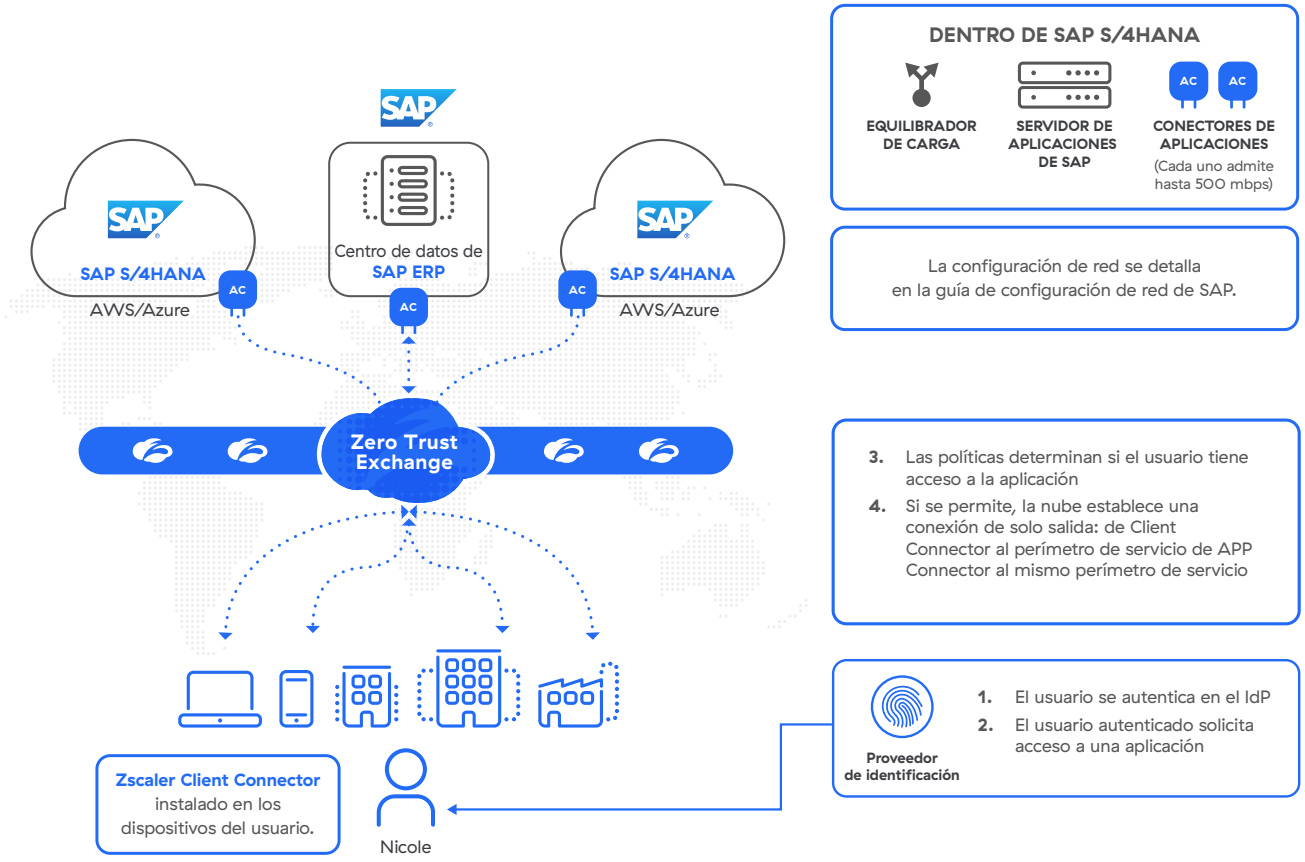
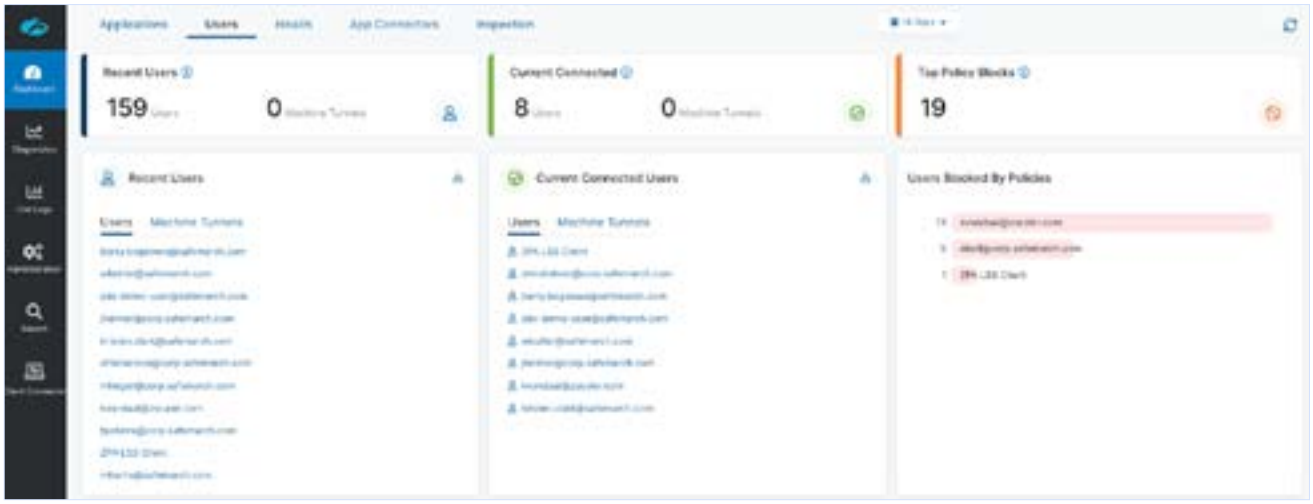


Figura 2: Acceso confiable y seguro de los usuarios a las aplicaciones SAP en S/4HANA con ZPA (detalles adicionales)

Las figuras 1 y 2 muestran una implementación de ZPA para un entorno SAP híbrido. Nicole es una empleada de ACME que necesita acceder a una aplicación SAP. Nicole puede estar en cualquier lugar: en la sede de la empresa, en su casa, fuera de ella, en una fábrica de la empresa o en una cafetería de la ciudad.

Cuando Nicole solicita por primera vez acceso a una aplicación SAP, se le solicita que se autentique con el IDP de su organización. Tras la autenticación, Zscaler Cloud evalúa la solicitud de Nicole con respecto a la política existente. Si se permite a Nicole acceder a la aplicación, el Zero Trust Exchange se pondrá en contacto con el App Connector más cercano a la aplicación, que establecerá un Z–Tunnel de adentro hacia afuera, una conexión TLS cifrada, desde la aplicación hasta el Zero Trust Exchange. Al mismo tiempo, Zscaler Cloud iniciará un túnel Z de adentro hacia afuera desde el Client Connector en el dispositivo de Nicole hasta Zscaler Cloud. Luego, Zscaler Cloud unirá los Z–Tunnels y formará un M–Tunnel en su interior, un canal de comunicación de extremo a extremo entre Nicole y la aplicación. Nicole ahora tiene acceso seguro a la aplicación SAP con la mejor experiencia de usuario posible al aprovechar la conexión más rápida desde uno de los más de 150 puntos de presencia globales de Zscaler.

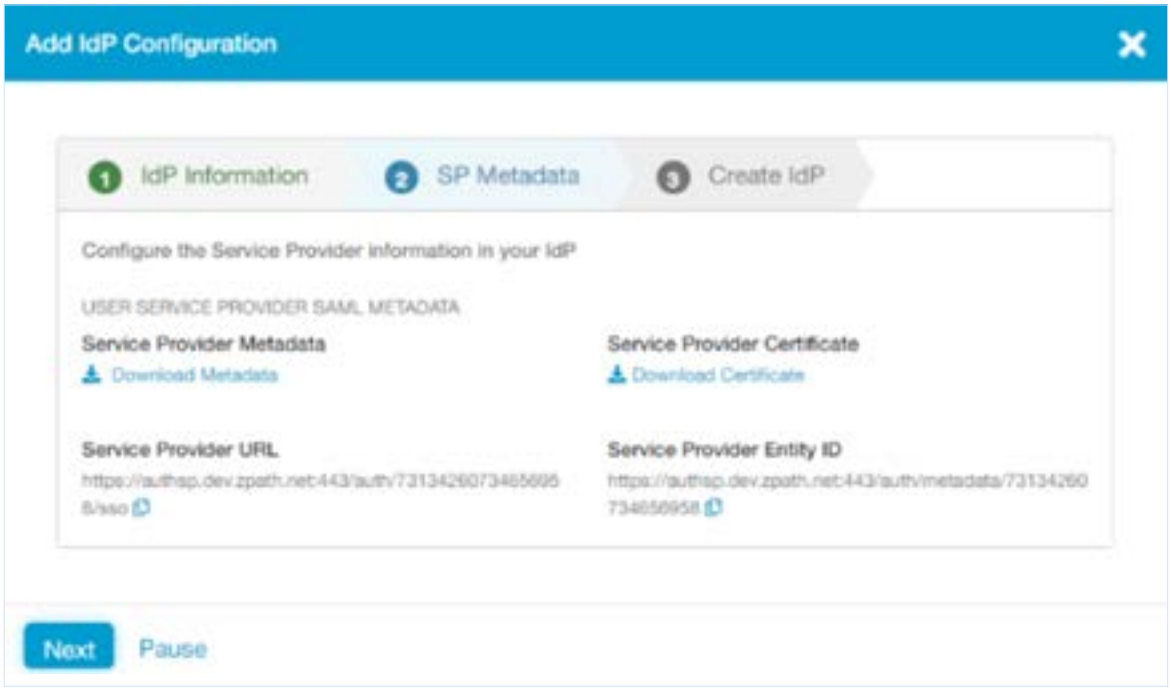


> “Es fundamental proporcionar a nuestros empleados un entorno de trabajo seguro y de alta disponibilidad garantizándoles en todo momento un acceso seguro a las aplicaciones en la nube, como SAP, y a Internet, al tiempo que reducimos nuestra exposición”.
>
> **Schmitz Cargobull**

Introducción a ZPA y SAP

Para conocer los pasos detallados sobre cómo configurar ZPA, consulte help.zscaler.com/zpa.

Paso 1: Configure la autenticación de inicio de sesión único (SSO) y el IDP

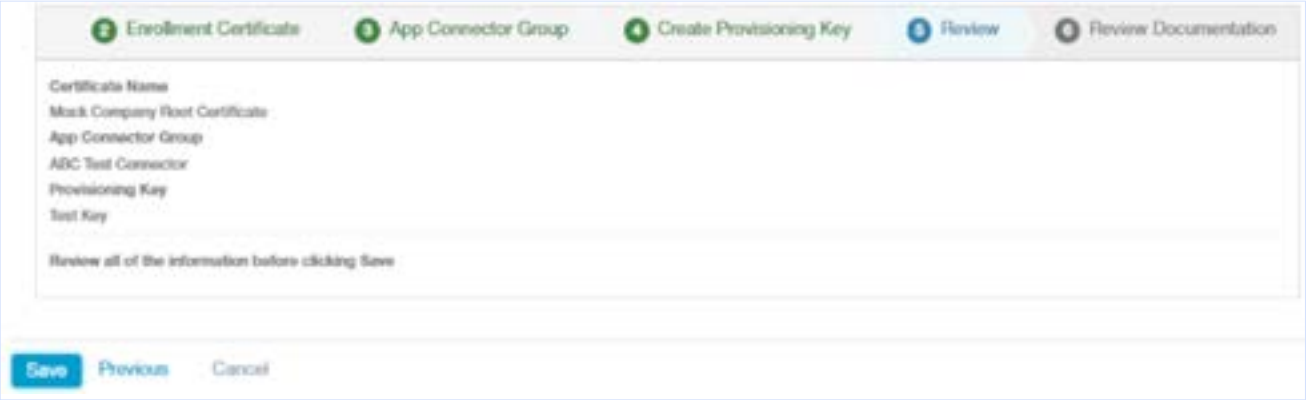


ZPA aprovecha las identidades de los usuarios del proveedor de identidad (IdP) existente de una organización y puede configurarse para admitir una o varias soluciones de IdP. ZPA admite el inicio de sesión único (SSO) a través de SAML para que sus usuarios remotos puedan acceder a las aplicaciones empresariales sin tener que iniciar sesión por separado en ZPA.

Para que los usuarios puedan acceder a sus aplicaciones a través de ZPA, primero deben autenticarse en Zscaler Client Connector utilizando cualquier proveedor de identidad (IdP) compatible con SAML 2.0 mediante el modelo iniciado por el proveedor de servicios (SP). El SSO del usuario de ZPA lo inicia el SP, pero el SSO del administrador de ZPA puede iniciarlo el SP o el IdP.

1. Configure su IdP y especifique ZPA como SP. Antes de que pueda agregar una configuración de IdP utilizando el Portal de administración de ZPA, debe tener el IdP en funcionamiento para su organización.
2. Agregue una configuración de IDP a través del Portal de administración de ZPA.

Paso 2. Implemente App Connectors



Los App Connectors proporcionan la interfaz autenticada segura entre las aplicaciones SAP y la nube ZPA. Por lo general, los App Connectors se implementan por parejas para garantizar una alta disponibilidad y, normalmente, se implementan junto al servidor de aplicaciones SAP. Los App Connectors se pueden implementar de varias maneras. Zscaler distribuye una imagen de máquina virtual (VM) estándar para su implementación en centros de datos empresariales, entornos de nube privada local, como VMware, o entornos de nube pública, como Amazon Web Services (AWS) EC2. Además, Zscaler proporciona paquetes que pueden instalarse en las distribuciones de Linux compatibles.

La configuración del App Connector estándar consta de dos pasos principales:

1. Agregue un App Connector a través del Portal de administración de ZPA.
2. Implemente los App Connectors en la plataforma compatible que elija.

Sin embargo, configurar App Connectors para SAP HEC/PCE requiere pasos especiales:

1. El cliente de SAP solicita el servicio Zscaler Endpoint a su representante de cuenta de SAP o al gerente de entrega al cliente.
2. SAP instala App Connectors de alta disponibilidad en SAP HEC/PCE en nombre del cliente.
3. El cliente proporciona a SAP la licencia ZPA para aplicarla a los App Connectors.

Paso 3. Configure el Client Connector

Zscaler Client Connector es una aplicación ligera que se sitúa en los puntos finales de los usuarios (laptops y dispositivos móviles gestionados por la empresa, BYOD, dispositivos de bolsillo y más) y aplica políticas de seguridad y controles de acceso independientemente del dispositivo, la ubicación o la aplicación. La aplicación Zscaler Client Connector reenvía el tráfico al punto de presencia Zscaler Cloud más cercano, donde el tráfico se enruta a las aplicaciones SAP a través del Zero Trust Exchange.

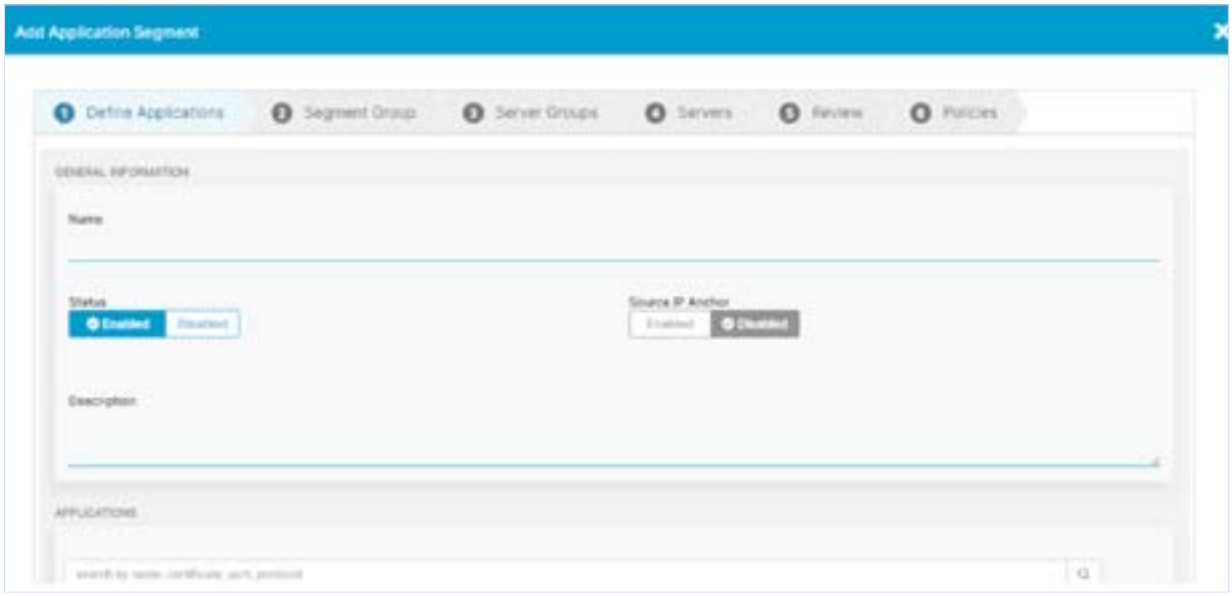
1. Complete los requisitos del sistema y las tareas previas:
   - Configure los ajustes de seguridad y acceso adecuados en el Portal de administración de ZPA.
   - Se debe configurar la autenticación basada en SAML y aprovisionar usuarios. No puede utilizar el Portal del Zscaler Client Connector como IdP para el servicio ZPA.
   - Asegúrese de que Zscaler Client Connector procese correctamente el tráfico para ZPA.
2. Configure los ajustes de administración para Zscaler Client Connector. La política de uso aceptable, los ajustes de actualización, las políticas de reenvío, el acceso de los usuarios al soporte y al registro y los ajustes de falla de apertura son configurables.
3. Configure los perfiles del Client Connector En el portal Zscaler Client Connector, puede configurar perfiles de aplicaciones agregando reglas de políticas a cada perfil. Puede seleccionar el orden de prioridad entre las reglas, así como a quién se aplica cada regla (es decir, a todos los usuarios o a diferentes grupos de usuarios). Cuando un usuario inscribe la aplicación en el servicio Zscaler, este tiene en cuenta el orden de prioridad y la identidad del usuario para descargar un perfil de aplicación con la regla de política adecuada.

4. Descargue Zscaler Client Connector desde la tienda Client Connector

5. Personalice el Client Connector con las opciones del instalador. Puede configurar un archivo de instalación de Zscaler Client Connector con opciones de instalación que le permitan eliminar pasos del proceso de inscripción de usuarios (por ejemplo, permitiendo a los usuarios omitir la página de inscripción o el aviso de selección de nube en Zscaler Client Connector).

6. Implemente Client Connector. Puede instalar Zscaler Client Connector manualmente en dispositivos individuales o utilizar el mecanismo de gestión de dispositivos de su organización para implementar Zscaler Client Connector en los dispositivos de sus usuarios.

Paso 4. Agregue segmentos de aplicaciones



Un segmento de aplicación es una colección de instancias de aplicación. Las solicitudes se autodetectan y pueden agruparse automáticamente en función de criterios coincidentes. Un segmento de aplicación se puede anclar a uno o más hosts o segmentos de host. Los segmentos de aplicación se utilizan para alojar políticas que incluyen o abarcan otros segmentos múltiples.

Zscaler recomienda las siguientes prácticas recomendadas para configurar segmentos de aplicaciones de SAP:

- Cree un único segmento de aplicación para todas las aplicaciones de SAP. Esto permitirá que el servicio ZPA equilibre la carga de las solicitudes de los usuarios para estas aplicaciones. Sin embargo, si se requiere segmentación, cree múltiples segmentos de aplicación para las aplicaciones SAP.
- Cree segmentos de aplicación para aplicaciones SAP utilizando FQDN. Si el cliente SAP no puede resolver el FQDN del host, intentará conectarse a la dirección IP. Si bien el servicio admite direcciones IP, es más seguro para los modelos Zero Trust conectarse con FQDN.

- Si el nombre de host de SAP no es un FQDN, se requiere un dominio de búsqueda DNS. Si el cliente no tiene sufijo de búsqueda, no puede completar el FQDN para conectarse a SAP. El cliente recurrirá a la dirección IP proporcionada por el servidor de mensajes SAP, que podría no ser deseable o enrutable a través del servicio ZPA.
- Utilice el seguimiento de Wireshark o las configuraciones de SAP para identificar las direcciones IP de todos los servidores SAP y crear un segmento de aplicación que incluya solo estas direcciones IP y los puertos TCP adecuados. No anuncie todo el rango de subredes (por ejemplo, 192.168.1.0/24).
- Si hay una lista de control de acceso (ACL) configurada en el servidor de mensajes de SAP o en el servidor de aplicaciones, agréguele las direcciones IP del App Connector. Dado que el servicio ZPA realiza un NAT de origen para el cliente, todo el tráfico se ve desde la dirección IP del App Connector. Para el grupo de App Connector asociado con los segmentos de aplicación, ZPA equilibrará la carga de las peticiones de los usuarios a través de los App Connectors en este grupo de App Connector. Debido a esto, se recomienda que las direcciones IP de todos los App Connectors del grupo App Connector se agreguen a la ACL.

Para admitir aplicaciones SAP en ZPA es necesario configurar segmentos de aplicación y dominios de búsqueda DNS.

1. Agregue un segmento de aplicación a través del portal ZPA Amin.
   - En la ventana Agregar aplicación, en Definir aplicaciones. Introduzca un nombre de dominio completo (FQDN) que corresponda a las aplicaciones de SAP. Aunque es posible introducir una dirección IP, Zscaler recomienda utilizar FQDN siempre que sea posible, ya que es más seguro. Si el cliente no tiene sufijo de búsqueda, no puede completar el FQDN para conectarse a SAP. El cliente volverá a la dirección IP proporcionada por el servidor de mensajes SAP.
   - Para garantizar el acceso al Zscaler Client Connector asegúrese de introducir los rangos de puertos TCP para la aplicación.
2. Agregue un dominio de búsqueda DNS. Para SAP, puede configurar dominios de búsqueda de DNS para FQDN dentro del Portal de administración de ZPA. Esto permite al cliente SAP agregar el sufijo de búsqueda y construir el FQDN. Sin embargo, también puede configurar SAP para proporcionar un FQDN en lugar de un nombre corto. Al hacer esto se elimina la necesidad de configurar un dominio de búsqueda DNS.

Recursos

Políticas de ZPA
ZPA: Soporte de aplicaciones SAP RISE con SAP S/4HANA Cloud, edición privada y SAP ERP, PCE

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