Resumen de la solución

Migración segura a la nube de SAP y modernización de aplicaciones con Zscaler Private Access (ZPA)

Las empresas están adoptando la transformación digital para aprovechar los beneficios de un mejor rendimiento, menores costos y menor complejidad operativa. Para los clientes de SAP, la transformación digital también se ve impulsada por el fin del soporte para SAP ERP Central Component (SAP ECC) 6.0, un sistema de planificación de recursos empresariales local. Esto no es sorprendente, ya que Gartner® estima que para 2025, el 95 % de las nuevas cargas de trabajo digitales se implementarán de manera nativa en la nube. Sin embargo, la experiencia del usuario final es una ocurrencia tardía durante el proceso de migración a SAP S/4HANA, que sigue siendo lento, complicado o riesgoso.

La tecnología heredada sigue colocando usuarios en la red y genera una complejidad que ralentiza la migración a la nube, lo que dificulta que las empresas rentabilicen su inversión en la nube. En pocas palabras, las arquitecturas de castle-and-moat y hub-and-spoke no pueden escalar ni ofrecer una experiencia de usuario rápida y sin fisuras.

Presentamos Zscaler Private Access (ZPA)

Para acelerar las migraciones a la nube de SAP S/4HANA y garantizar la experiencia del usuario y la productividad durante todo el proceso de transformación, las organizaciones pueden aprovechar Zscaler Private Access (ZPA) para obtener experiencias fluidas y uniformes, una modernización de las aplicaciones sin esfuerzo y una seguridad basada en las aplicaciones. Con más de 150 puntos de presencia interconectados con los mayores proveedores de nube del mundo, clientes como Kubota, un fabricante de maquinaria agrícola, pueden escalar y ampliar rápidamente sus operaciones, y afirman: «La próxima vez que agregamos un almacén, no hay necesidad de esperar semanas y gastar miles de dólares en redes para conectarnos a nuestros sistemas SAP ERP para la gestión de inventarios... estamos en marcha en cualquier lugar desde el primer día".

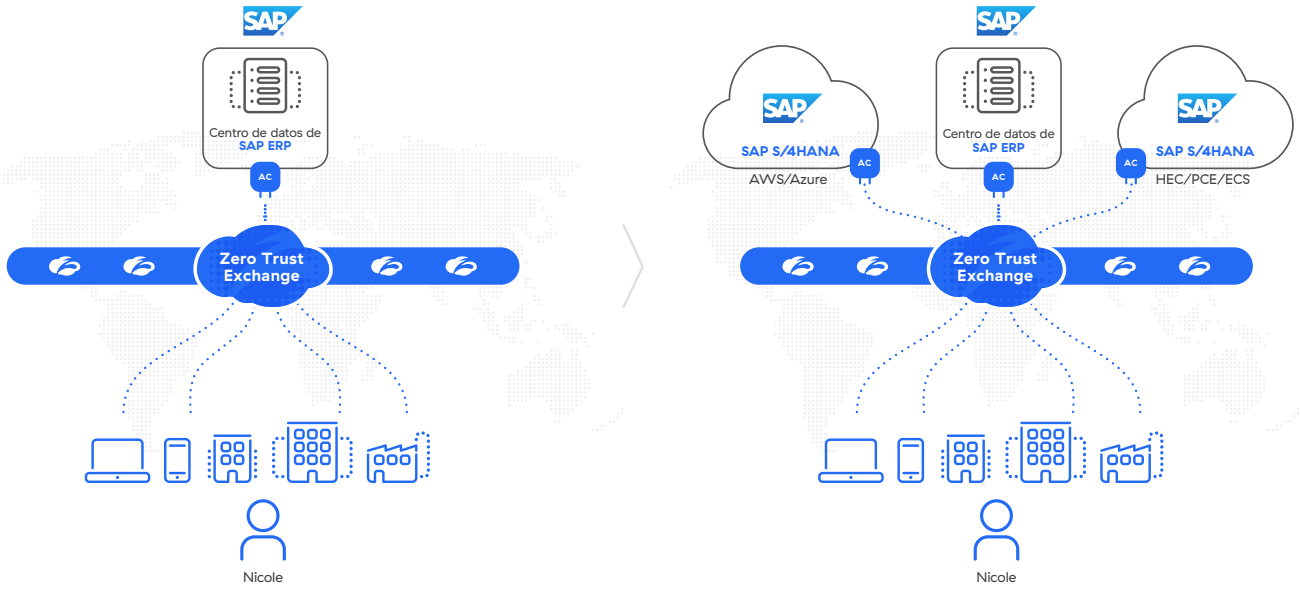
Actuando como una capa de abstracción entre el usuario y la aplicación, el motor de políticas único y global de ZPA aplica los principios Zero Trust en todos los dispositivos, ubicaciones y aplicaciones. Los usuarios se conectan del mismo modo a las aplicaciones que se ejecutan en el centro de datos que a las que están en la nube y desde cualquier dispositivo o ubicación. La ubicación de la aplicación puede cambiarse mediante un simple cambio de política, de centro de datos a nube pública o de VPC a VPC, conectando de manera segura a los usuarios directamente a las aplicaciones privadas y con una experiencia de usuario superior.

Ventajas de Zscaler Private Access (ZPA):

- Acelere la migración de aplicaciones SAP y la adopción de la nube
- Habilite el control granular del acceso de los usuarios a las aplicaciones de SAP Suite
- Gestione activamente el acceso a la carga de trabajo antes y después de la migración
- Ofrezca visibilidad de aplicaciones SAP de extremo a extremo y una mejor experiencia de usuario

> "La próxima vez que agreguemos un almacén, no hay necesidad de esperar semanas y gastar miles de dólares en la creación de redes, estamos en funcionamiento en cualquier lugar desde el primer día con nuestros escáneres RF conectados a 4G utilizando el Zscaler Client Connector para conectar con nuestros sistemas SAP ERP de gestión de inventario."
>
> **Jonathon Bonnici** Director de prestación de servicios de TI, Kubota Australia

Cómo funciona Zscaler Private Access

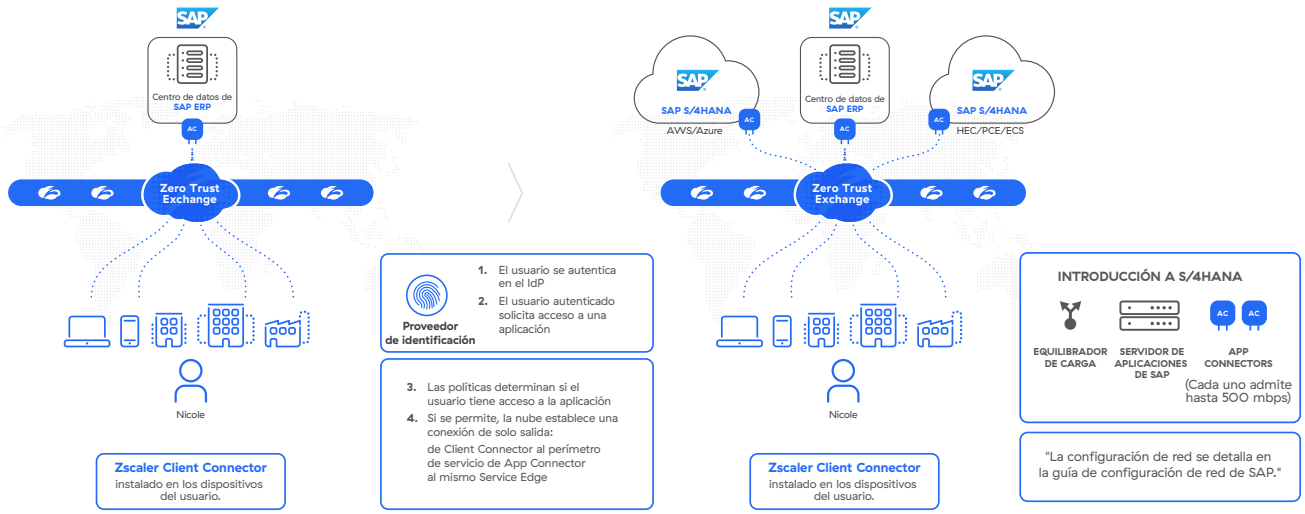


Componentes de ZPA/SAP

- 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 facilita las conexiones rápidas y seguras y permite a sus empleados trabajar desde cualquier lugar, utilizando Internet como red corporativa. El Zero Trust Exchange consta de 150 centros de datos en todo el mundo, lo que garantiza que el servicio esté cerca de sus usuarios, coubicado con 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, brindando 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 en ZPA controlan cómo 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 llevar en su interior múltiples canales de comunicación llamados microtúneles.

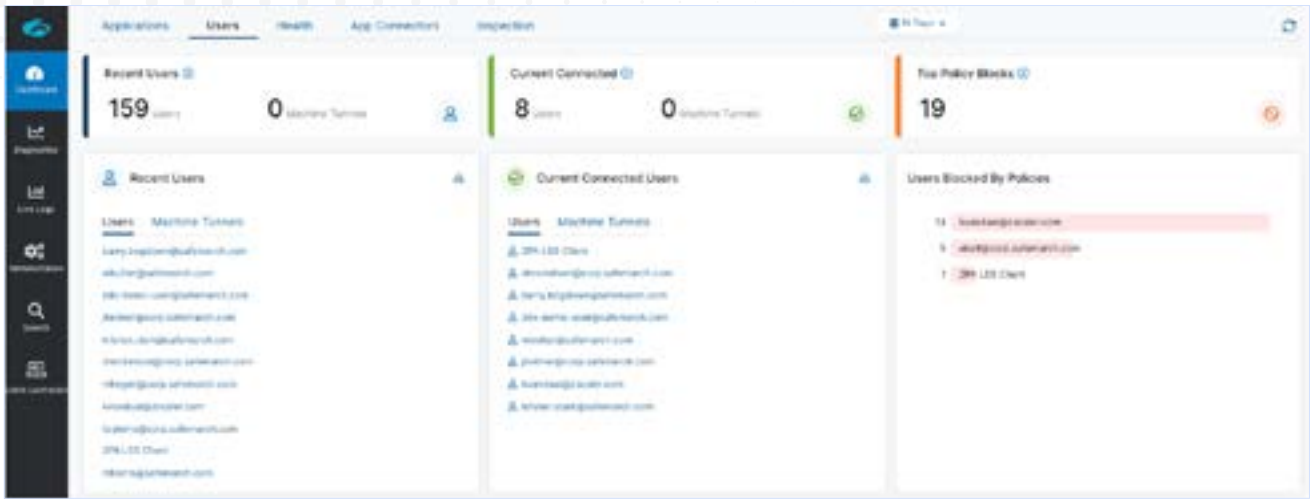
- Un microtúnel (M–Tunnel) es un canal de comunicación de extremo a extremo creado entre Zscaler Client Connector y una aplicación interna a través de un ZPA Public Service Edge, o un ZPA Private Service Edge y un App Connector a demanda.
- Los servidores alojan aplicaciones disponibles para ZPA, los servidores pueden estar ubicados en centros de datos empresariales o en nubes públicas virtuales.
- Los grupos de servidores son una colección de servidores. Cada segmento de aplicación debe asignarse a un grupo de servidores.
- Los servidores de aplicaciones SAP son servidores que alojan aplicaciones SAP.

Diseño de ZPA y SAP



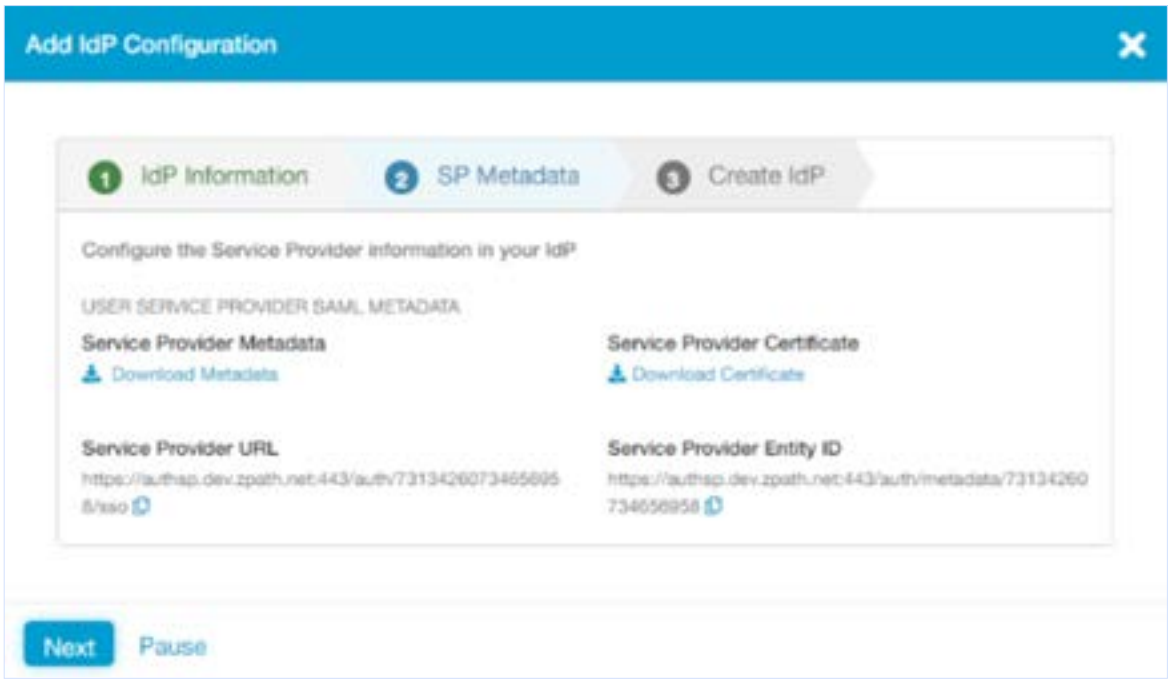
Por ejemplo, ACME actualmente aloja su sistema SAP ERP en un centro de datos local en la sede de la empresa. La empresa está en proceso de modernización de la red y las aplicaciones con planes para migrar todas las aplicaciones SAP de la empresa a S/4HANA en AWS y Azure. Afortunadamente, ACME está utilizando ZPA, una parte de Zscaler Zero Trust Exchange (ZTE), al inicio de su proceso de transformación, reduciendo la fricción en todo el proceso para garantizar una experiencia sencilla y fluida.

Cuando Nicole, una empleada de ACME, solicita acceso a una aplicación SAP alojada en el centro de datos local, se le pide que se autentique con el proveedor de identidades (IdP) de ACME. Tras la autenticación, el ZTE evalúa la solicitud de Nicole con respecto a la política existente. Si Nicole tiene permiso para acceder a la aplicación determinada por la identidad y el contexto, el ZTE 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 al ZTE. En paralelo, el ZTE iniciará un Z–Tunnel de dentro hacia fuera desde el conector del cliente en el dispositivo de Nicole de vuelta al ZTE. A continuación, el ZTE unirá los Z–Tunnels y formará un M–Tunnel, un canal de comunicación de extremo a extremo entre Nicole y la aplicación, en su interior. Este mismo proceso se produce cuando ACME migra sus aplicaciones SAP a la nube. ACME simplemente duplica las aplicaciones del centro de datos local a la nube. Cuando está listo, ACME simplemente elimina las aplicaciones del centro de datos local. Ahora, cuando Nicole quiere acceder a sus aplicaciones SAP, es dirigida automáticamente a las aplicaciones en la nube.



Introducción a la migración a la nube y la modernización de aplicaciones

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

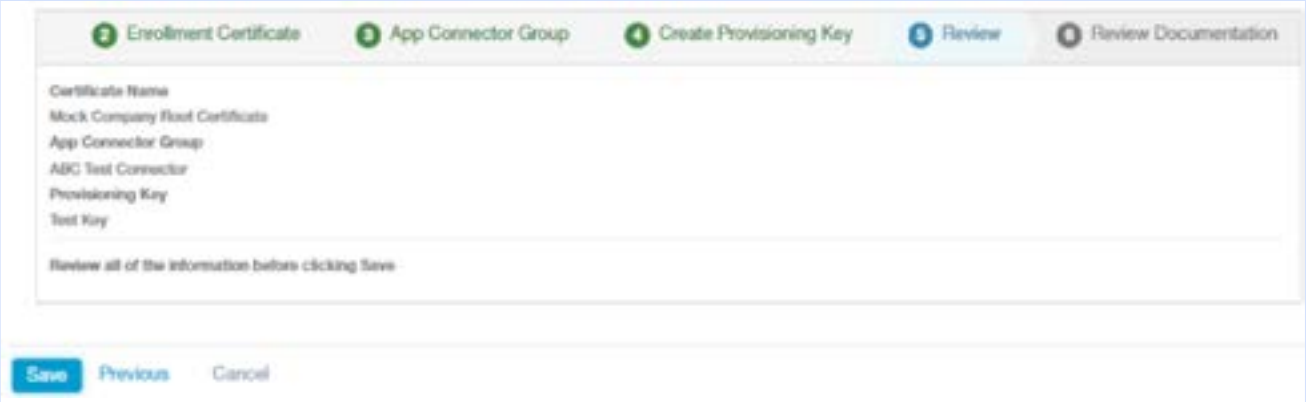


ZPA aprovecha las identidades de los usuarios del proveedor de identidad (IdP) existente de una organización y puede configurarse para admitir una o varias soluciones de IdP. ZPA admite el inicio de sesión único (SSO) a través de SAML para que sus usuarios remotos puedan acceder a las aplicaciones empresariales 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 con 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. Configurar los App Connectors y los grupos de App Connector



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 organizan además en grupos de App Connector. Cada App Connector pertenece a un grupo App Connector específico y cada grupo App Connector está asociado con al menos un grupo de servidores para servir a cualquier aplicación. Los App Connectors se pueden implementar de varias formas. 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.

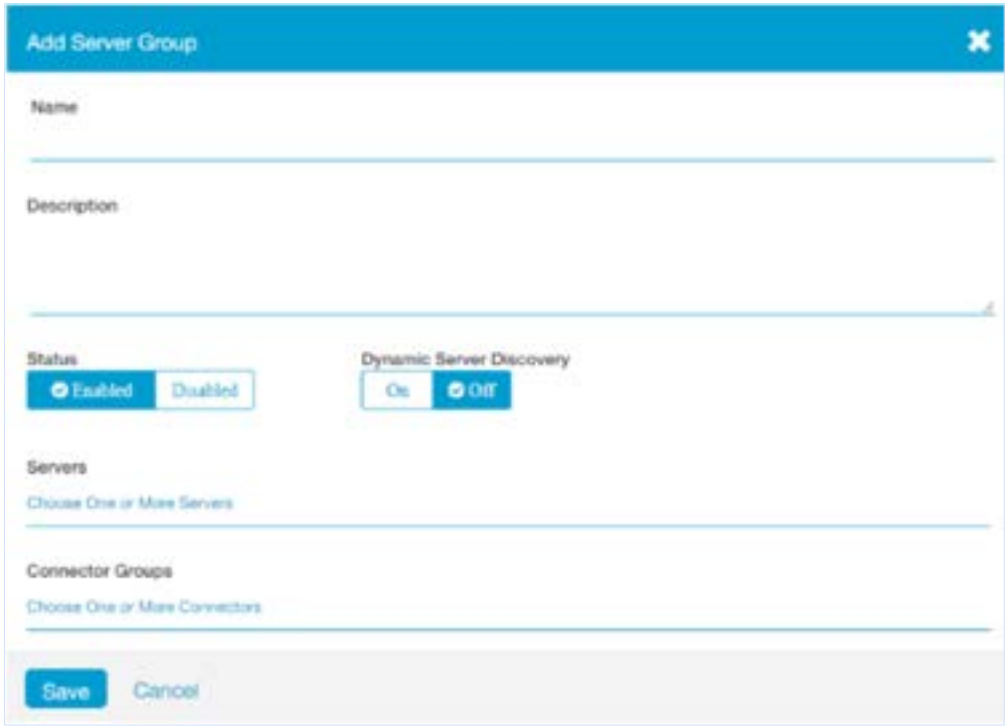
La configuración del App Connector estándar consta de dos pasos principales:

1. Agregue un App Connector a través del Portal de administración de ZPA.
2. Implemente los App Connectors en la plataforma compatible de su preferencia.
3. Para la migración a la nube, los App Connectors deberán asociarse al grupo de servidores del centro de datos local y al grupo de servidores de la nube.

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 servidores y grupos de servidores



Debe configurar los servidores que alojan las aplicaciones que desea poner a disposición de la ZPA, tanto si los servidores se encuentran en el centro de datos de su empresa como en una nube pública virtual (VPC).

Hay dos métodos principales para la configuración del servidor:

- **Defina explícitamente los servidores y los grupos de servidores:** Puede definir explícitamente cada servidor que aloje una o varias aplicaciones. Para cada servidor, debe proporcionar un nombre, así como una dirección IP o un nombre de dominio completo (FQDN). A continuación, puede organizar manualmente esos servidores en grupos de servidores.
- **Habilite la detección dinámica de servidores:** En lugar de definir explícitamente cada servidor, puede habilitar la detección dinámica de servidores para que ZPA pueda detectar los servidores apropiados para sus aplicaciones a medida que los usuarios los soliciten. Con este método, solo necesita crear un grupo de servidores vacío que tenga activada la detección dinámica de servidores.

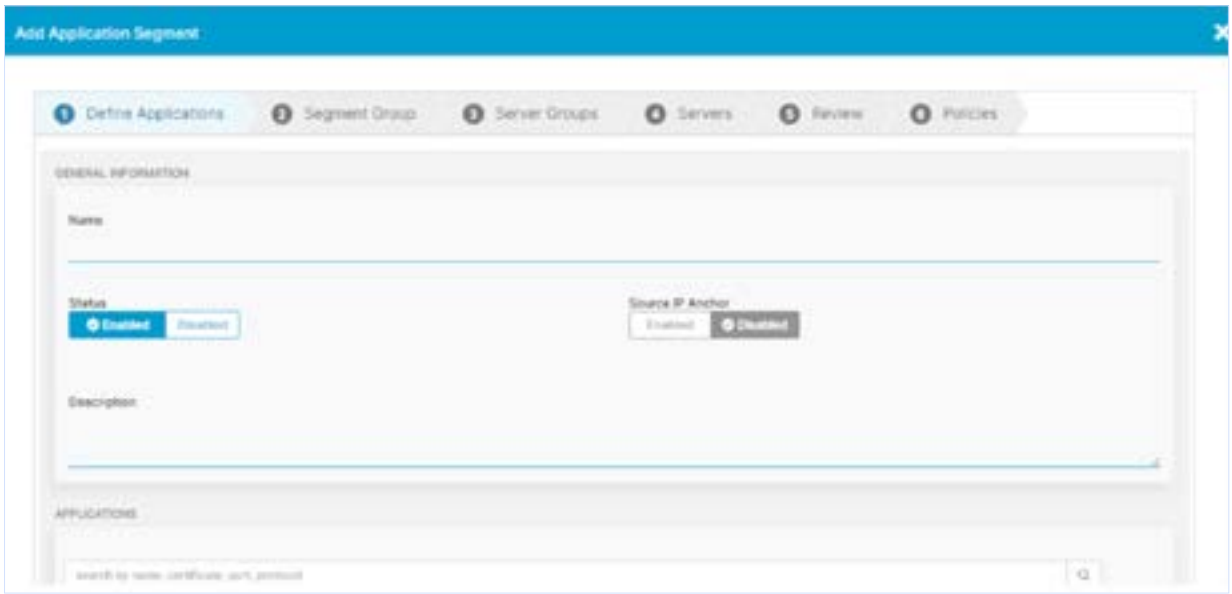
Cada segmento de aplicación estará asociado a un servidor y a un grupo de servidores. Si se activa la detección dinámica de servidores, cuando la aplicación se migre a la nube, ZPA registrará automáticamente el cambio y dirigirá a los clientes a la aplicación en la nube. Si la detección dinámica de servidores no está activada, el administrador de la ZPA tendrá que cambiar manualmente el servidor y el grupo de servidores asociados a la aplicación que ahora reside en la nube.

Paso 4. 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 5. 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.

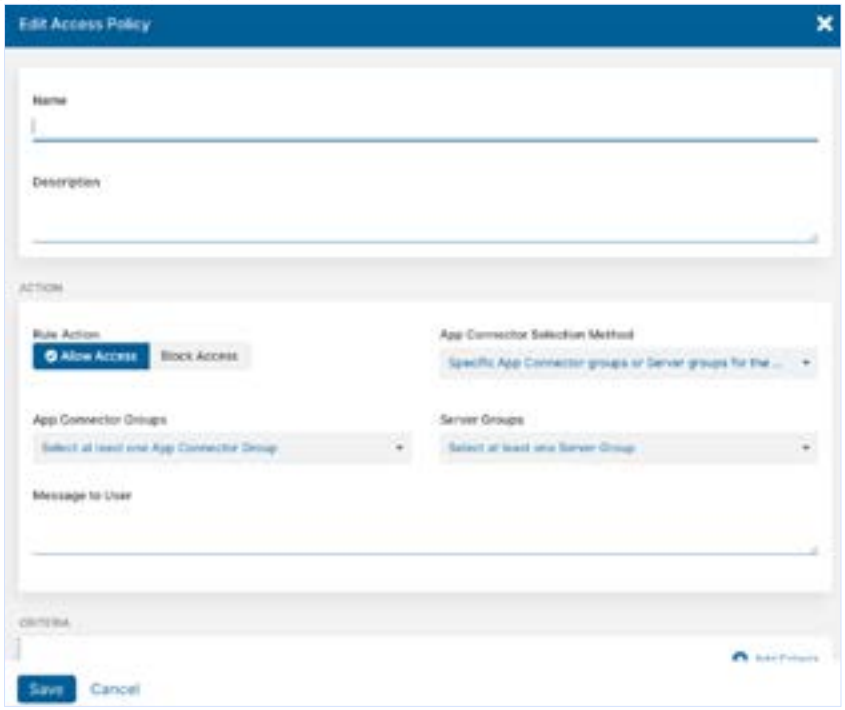
Zscaler recomienda las siguientes prácticas recomendadas para configurar segmentos de aplicaciones de SAP:

- 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 Admin.
   - 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.

Paso 6. (Opcional) – Migración de aplicaciones mediante políticas



Durante las migraciones típicas a la nube no se requieren cambios adicionales en las políticas para completar la migración del acceso de los usuarios de la aplicación heredada a la aplicación en la nube. En algunos casos, es posible que las organizaciones no deseen migrar a todos los usuarios a la vez a las aplicaciones en la nube. Por ejemplo, es posible que quieran probar las aplicaciones en la nube con un grupo pequeño de usuarios antes de migrar a todos los usuarios. En este escenario, las organizaciones pueden utilizar un enfoque basado en políticas para la migración a la nube.

1. En el portal ZPA Admin, cree una política para los usuarios que accederán a las aplicaciones en la nube y seleccione la opción “Grupos específicos de App Connector o grupos de servidores”.
2. A continuación, seleccione el grupo de App Connector para las aplicaciones alojadas en la nube.
3. Repita este proceso para los usuarios que accederán a las aplicaciones en el centro de datos. Asegúrese de seleccionar el grupo de App Connector para las aplicaciones del centro de datos local.
4. Cuando esté listo, migre el resto de los usuarios a la nube actualizando la política con los grupos de App Connector asociados con la nube.

Recursos

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

> “ZPA nos ofrece flexibilidad para dar de baja a los usuarios donde necesitemos, de modo que podamos ejecutar SAP en una región en AWS, pero conmutar por error a otra región y hacer que esos usuarios se conecten sin problemas mediante un cambio de política. ZPA permite a los usuarios acceder a aplicaciones heredadas, así como a nuestro nuevo entorno SAP en la nube”.
>
> **Growmark**

zscaler™ | Experience your world, secured.™

Acerca de Zscaler
Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resilientes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de ciberataques y pérdida de datos al conectar de manera segura usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SASE es la plataforma de seguridad en la nube en línea más grande del mundo. Obtenga más información en **zscaler.com/mx** o síganos en Twitter **@zscaler**.

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