Resumen de la solución

Acceso a SAP seguro para la cadena de suministro y terceros con Zscaler Private Access (ZPA)

Las empresas globales con operaciones en la cadena de suministro y activos de OT e IIoT necesitan que los usuarios externos, como contratistas y socios, dispongan de un acceso ágil y conectado a las aplicaciones internas de gestión empresarial de SAP. Para maximizar el tiempo de actividad de producción y evitar interrupciones debido a fallas en los equipos y procesos, las organizaciones deben considerar un enfoque de acceso de usuario moderno que proporcione:

1. Acceso remoto seguro y sin agentes a los usuarios de la cadena de suministro que accedan a SAP Suite a través de un navegador web desde dispositivos no confiables o no gestionados, por ejemplo: BYOD, contratistas, trabajadores de fábrica, etc.
2. Reducción de los riesgos de exposición a ataques de la superficie de la aplicación SAP al otorgar acceso a la cadena de suministro a las aplicaciones empresariales, es decir, que los usuarios se conecten directamente a la aplicación SAP sin exponer otras aplicaciones ni la red corporativa.
3. Garantía de que las políticas de acceso global se aplican de manera uniforme, manteniendo la visibilidad del usuario y limitando los permisos de acceso excesivos.

Sin embargo, el riesgo de ampliar el acceso a terceros es significativo y las cadenas de suministro son blancos fáciles para ransomware y otros ataques sofisticados. Cuando se producen interrupciones, por pequeñas que sean, producen efectos dominó que pueden afectar a la economía mundial. Para mitigar los riesgos, las empresas han confiado en las VPN para acceder a las aplicaciones SAP ERP necesarias. Sin embargo, en muchos casos, implementar un cliente de acceso remoto no es posible o requiere infraestructura de TI adicional. Además, es posible que los socios no dispongan de los privilegios necesarios a nivel de dispositivo para instalar dichos clientes o que simplemente no estén dispuestos a hacerlo.

Presentamos Zscaler Private Access (ZPA)

Cuando el acceso a SAP es crucial para las operaciones de la cadena de suministro, el acceso al navegador (Browser Access) sin agente le permite aprovechar un navegador web para la autenticación de usuarios y el acceso a las aplicaciones a través de Zscaler Private Access (ZPA), sin necesidad de que los usuarios se conecten a VPN de sitio a sitio o instalen Zscaler Client Connector en sus dispositivos. Esto es pertinente para usuarios externos, como contratistas y socios, cuya organización de TI no permite clientes externos o cuyo sistema BYOD (traiga su propio dispositivo) no puede admitir clientes.

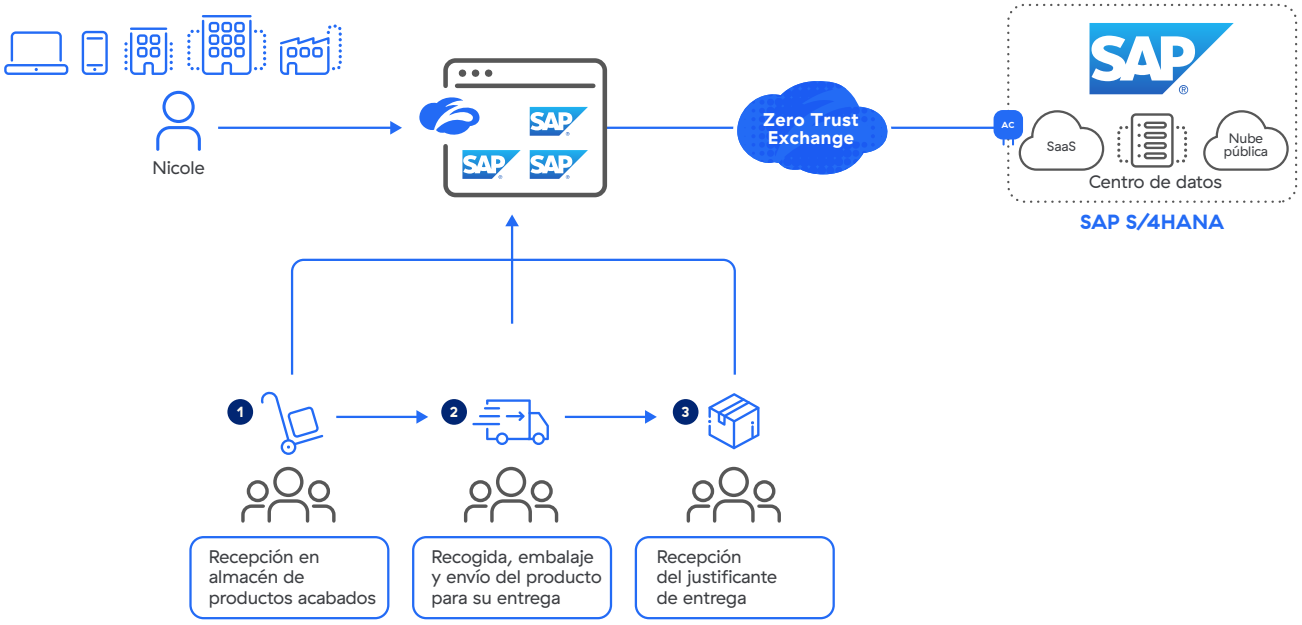
Para muchos clientes como **Schmitz Cargobull**, un fabricante innovador, acceder a las aplicaciones SAP internas mediante VPN ya no era factible tras múltiples errores de acceso que ponían en peligro operaciones confidenciales de la cadena de suministro. Tras aprovechar ZPA para el acceso seguro a SAP ERP, Michael Schöller, responsable de infraestructuras, señaló que **"los empleados y terceros pueden acceder de manera segura y confiable a los sistemas SAP sin exponer toda la red"**. Cuando las políticas Zero Trust se aplican por defecto en todos los dispositivos, ubicaciones y aplicaciones, los colaboradores nunca entran en la red y la aplicación nunca queda expuesta a Internet. Al limitar el uso no autorizado, los usuarios son más productivos y las organizaciones están a salvo de movimientos laterales injustificados. Los administradores de ZPA pueden recurrir al servicio para obtener visibilidad en tiempo real de la actividad de los usuarios, identificar a los usuarios que acceden a las aplicaciones a través del navegador y descubrir aplicaciones hasta ahora desconocidas.

Ventajas de Zscaler para SAP

- **Proteja el acceso de usuarios y dispositivos sin agentes a SAP:** Nunca coloque usuarios externos o herramientas de la cadena de suministro en su red corporativa, reduciendo la exposición a riesgos y movimientos laterales.
- **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.
- **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 continuos de ZDX.
- **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 SAP S/4HANA.
- **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.

Cómo funciona el acceso sin agente de ZPA

Diseño de la cadena de suministro de ZPA/SAP



Cifra 1: Empleados y usuarios externos de la cadena de suministro que acceden a aplicaciones de SAP con ZPA Browser Access

Componentes de ZPA/SAP

- Los App Connectors proporcionan una interfaz segura autenticada entre los servidores de aplicaciones de una organización y la nube ZPA.
- La plataforma Zero Trust Exchange de Zscaler (ZTE) permite conexiones rápidas y seguras y permite que sus empleados trabajen desde cualquier lugar utilizando Internet como red corporativa. Zero Trust Exchange consta de 150 centros de datos en todo el mundo, lo que garantiza que el servicio esté cerca de sus usuarios, ubicado junto a los proveedores de la nube y las aplicaciones a las que acceden, como Microsoft 365 y AWS. Garantiza la ruta más corta entre sus usuarios y sus destinos, lo que proporciona una seguridad integral y una experiencia de usuario increíble.
- Los portales de usuario con Browser Access brindan a los usuarios y dispositivos acceso sin agentes a aplicaciones autorizadas para los empleados o socios de una 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.

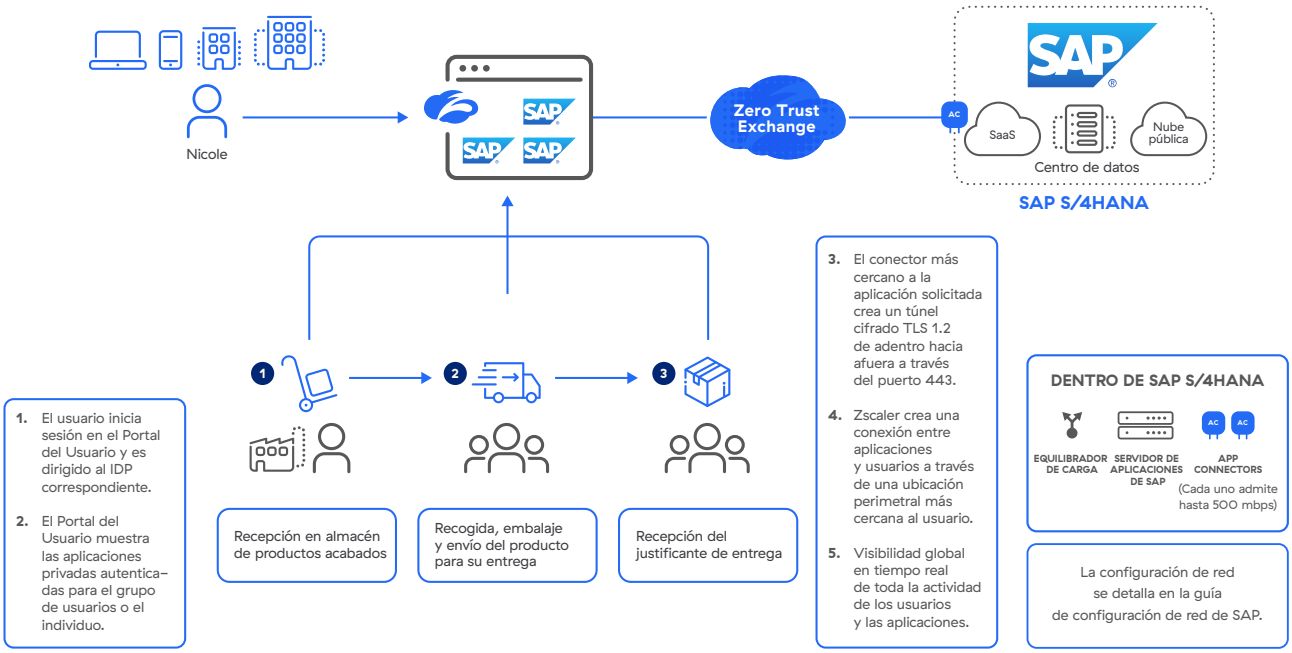
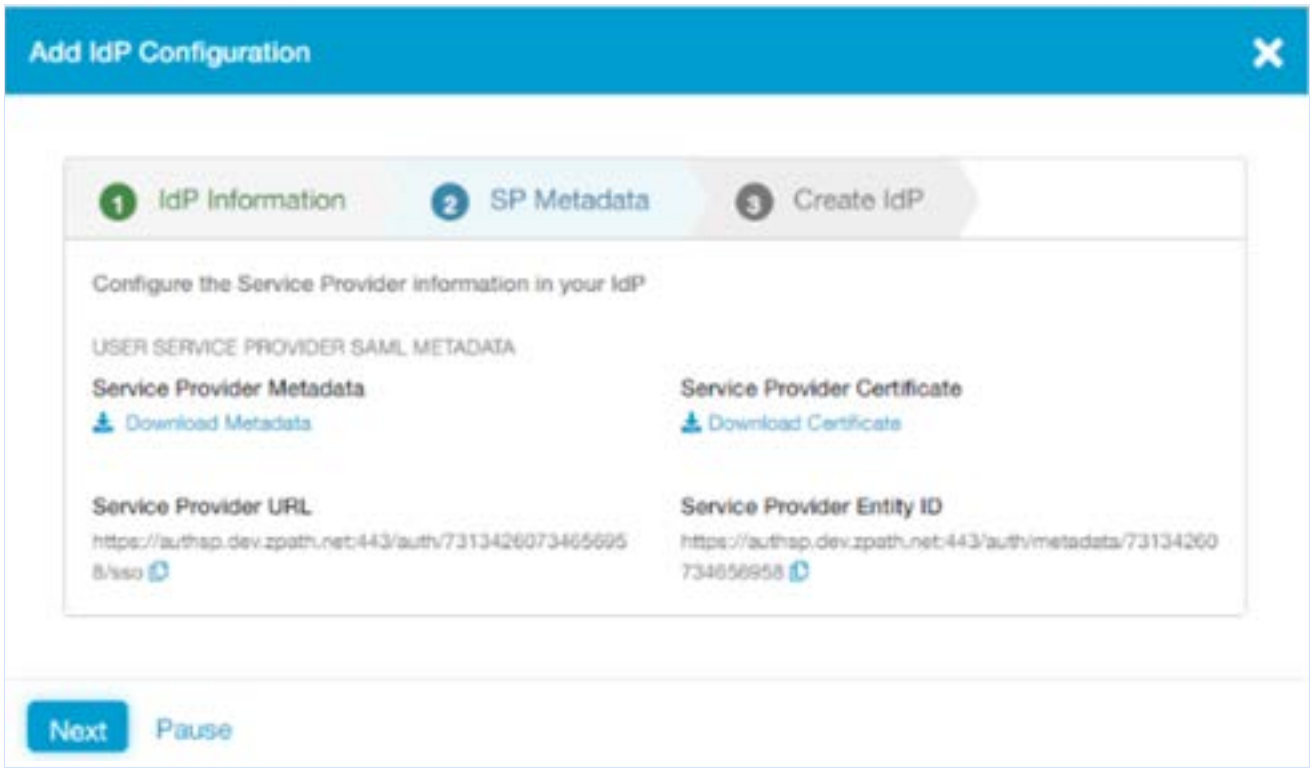


Figura 2: Empleados y usuarios externos de la cadena de suministro que acceden a las aplicaciones SAP con ZPA Browser Access (detalles adicionales)

Las figuras 1 y 2 muestran una implementación de ZPA para un entorno SAP híbrido. Nicole es una empleada de ACME que tiene que hacer un seguimiento de los productos a medida que avanzan por la cadena de suministro. Paul es un empleado en un almacén que almacena productos de ACME antes de enviarlos a los clientes. Cuando Paul recibe un envío, alerta a ACME y a Nicole a través de un portal de ZPA Browser Access. Paul accede al portal de usuarios de ACME en su table y es redirigido a su proveedor de identidad (IDP). Después de que Paul se autentique, el portal de usuario mostrará las aplicaciones apropiadas para Paul. Paul selecciona la aplicación SAP que necesita y, tras bambalinas, el App Connector más cercano a la aplicación SAP solicitada crea un Z–Tunnel, una conexión TLS cifrada, a la nube de Zscaler. Luego, la nube de Zscaler une la conexión desde el portal del usuario a la aplicación SAP. Paul ahora tiene acceso y puede actualizar a ACME y Nicole sobre las ubicaciones de sus productos. Es importante tener en cuenta que Paul no necesita un dispositivo ACME específico, el dispositivo no tiene agente y puede no estar administrado o no ser confiable, y solo necesita un navegador web para acceder al puerto de ZPA Browser Access para conectarse a las aplicaciones SAP.

Introducción a ZPA Agentless Access para SAP

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



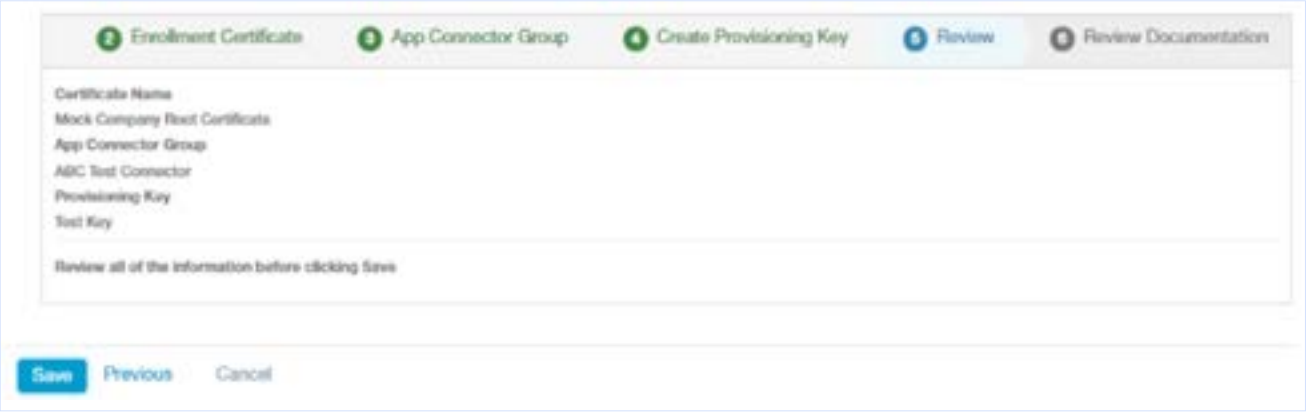
ZPA aprovecha las identidades de los usuarios del proveedor de identidad (IdP) existente de una organización y puede configurarse para admitir una o varias soluciones de IdP. ZPA admite el inicio de sesión único (SSO) a través de SAML para que sus usuarios remotos puedan acceder a las aplicaciones empresariales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

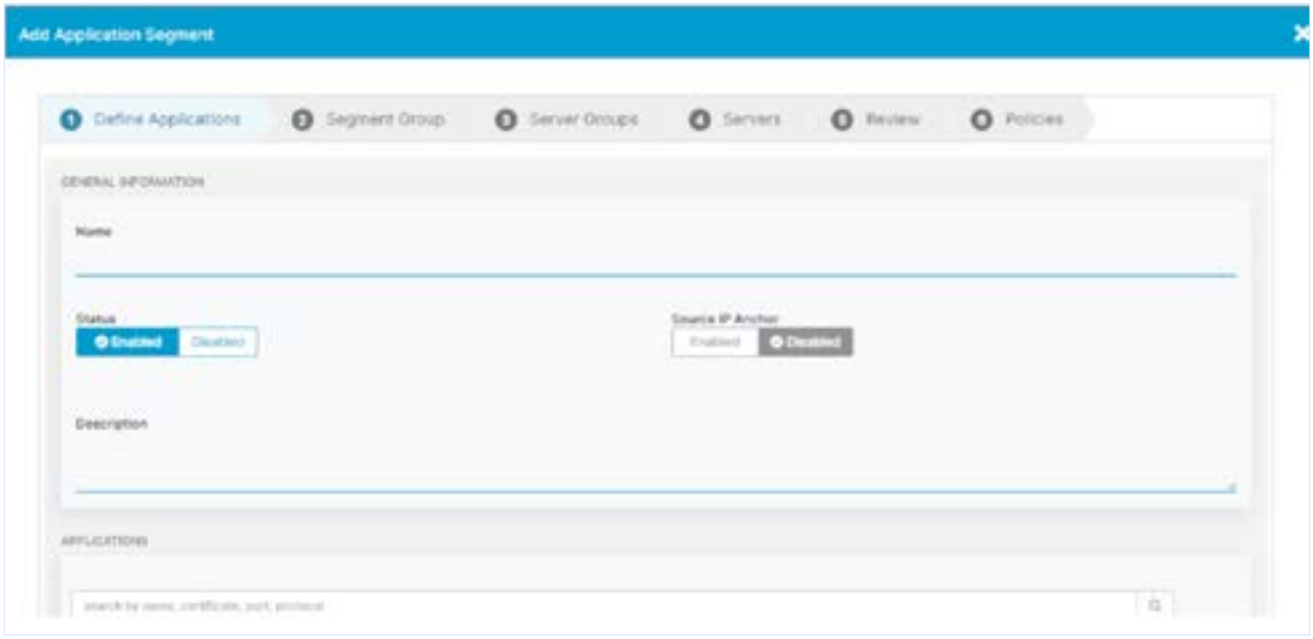
La configuración del App Connector estándar consta de dos pasos principales:

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

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 los segmentos de aplicación para Browser Access



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:

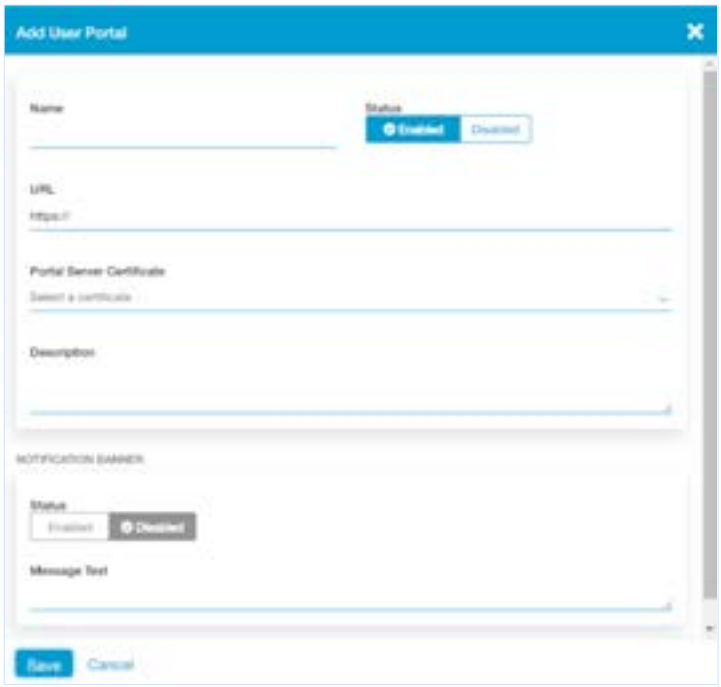
- Cree un único segmento de aplicación para todas las aplicaciones de SAP. Esto permitirá que el servicio ZPA equilibre la carga de las solicitudes de los usuarios para estas aplicaciones. Sin embargo, si se requiere segmentación, cree múltiples segmentos de aplicación para las aplicaciones SAP.
- Cree 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.
   - 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.
   - Seleccione Access Browser para habilitar el Segmento de Aplicación para Access Browser.
2. Navegue hasta la página de Acceso al Navegador en el Portal de Administración de la ZPA y expanda el Segmento de Aplicación que acaba de configurar para el Acceso al Navegador. Copie el nombre canónico (CNAME).
3. Agregue la información CNAME que acaba de copiar a su DNS público y compruebe que el FQDN del portal de usuario se resuelva en el registro.
4. 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 4. Configure el portal de Browser Access



1. Configure un portal de Acceso al Navegador a través del Portal de administración de ZPA. Al agregar un nuevo portal, se le pedirá que agregue el nombre del portal, la URL, el certificado del servidor del portal, una descripción, así como la opción de agregar un recuadro de visualización para los usuarios.

2. En la página Portales de Usuario del portal de administración de ZPA, expanda la fila para ver los detalles del portal dentro de la tabla y, a continuación, haga clic en el ícono Copiar situado junto al nombre canónico (CNAME). Necesitará este registro CNAME para su DNS público.

3. Agregue la información CNAME que acaba de copiar a su DNS público y compruebe que el FQDN del portal de usuario se resuelva en el registro.

4. A continuación, agregue los enlaces del portal, que son los enlaces de las Aplicaciones habilitadas para Browser Access que se mostrarán en el Portal de Usuario de Browser Access.

5. Navegue a la página Enlaces del Portal en el Portal de Administración de ZPA. Desde aquí, puede configurar el nombre, el protocolo (HTTPs/HTTP), la descripción y el icono/imagen de cada aplicación que se mostrará en el portal.

Recursos

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

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