**Configuración de subsistemas**

**NOTA:** El procedimiento detallado se creó el 04 de junio del 2021. Debe consultarse las referencias detalladas en cada sección para confirmar si existen cambios en el procedimiento.

**Referencia:**

<https://www.ibm.com/docs/en/api-connect/10.0.1.x?topic=configuring-managing-your-server-environment>

**Configurar y administrar su entorno de servidor**

Configure y gestione los servidores que componen su nube local de IBM® API Connect utilizando la interfaz de usuario de Cloud Manager.

La interfaz de usuario de Cloud Manager es la parte de IBM API Connect que permite a un administrador de la nube definir y gestionar la nube local de API Connect.

Puede utilizar Cloud Manager para definir la nube API Connect realizando las siguientes tareas:

* Cree organizaciones de proveedores e invite a los usuarios a actuar como propietarios
* Crear y administrar roles de usuario y valores predeterminados de roles
* Crear zonas de disponibilidad para servicios
* Registre los servidores relevantes que proporcionarán los servicios de Gateway, Analytics y Portal.
* Asocie un servicio Analytics con un gateway para habilitar informes para eventos de API
* Configure los recursos para la autenticación de usuarios, la seguridad TLS y los proveedores de OAuth y haga que los recursos sean visibles para todas las organizaciones de proveedores o para algunas de ellas.
* Conéctese a un servidor de correo SMTP existente y edite plantillas para correos electrónicos generados por el sistema
* Establecer el servicio gateway predeterminado para catálogos

1. **Lista de verificación de la configuración de Cloud Manager**

Un resumen, con enlaces, de las tareas de configuración inicial clave que debe completar en la interfaz de usuario de Cloud Manager después de instalar y desplegar IBM® API Connect, y otras tareas complementarias.

**Tareas iniciales claves:**

|  |  |
| --- | --- |
| **Task** | **Description** |
| Log in to the Cloud Manager user interface | Se proporciona una cuenta de usuario de administrador predeterminada para que comience sus tareas de configuración. |
| Configure an email server for notifications | El servidor de correo electrónico envía invitaciones de registro y otros correos electrónicos impulsados por eventos. Debe configurar el servidor de correo electrónico antes de agregar organizaciones de proveedores o registrar un servicio de Portal. |
| Specify your email server as the notification server | Seleccione el servidor de correo electrónico que se utilizará como servidor de notificaciones y configure el nombre del remitente y la dirección de correo electrónico que se incluirán en los correos electrónicos. |
| Register a Gateway service | Un Gateway service representa un grupo de servidores gateway que alojan API publicadas y proporcionan los endpoints de API que utilizan las aplicaciones cliente. Los gateway ejecutan invocaciones de API proxy para sistemas backend y hacen cumplir las políticas de API, incluida client identification, security and rate limiting. |
| Register an Analytics service | El Analytics service recopila datos de eventos de API del Gateway service. |
| Associate the Analytics service with a Gateway service | Debe asociar un Analytics service con cada uno de los Gateway services de los que desea recopilar datos de eventos de API. |
| Register a Portal service | El Portal service proporciona un portal para desarrolladores que utilizan los desarrolladores de aplicaciones para descubrir las APIs y los consumidores incorporados. |
| Create a provider organization | Para que los desarrolladores puedan publicar APIs y para que los API managers puedan administrar el ciclo de vida de las API, deben ser miembros de una organización proveedora. Debe crear al menos una organización proveedora especificando el propietario, quien podrá agregar más miembros. |

**Otras tareas complementarias:**

|  |  |
| --- | --- |
| **Task** | **Description** |
| Configure authentication and security | API Connect proporciona de manera predeterminada registro de usuarios locales, pero puede configurar su propio registro de usuarios, de varios tipos, para la interfaz de usuario y el API Access control. También puede configurar perfiles TLS para proteger la transmisión de datos a través de HTTPS y OAuth providers para proteger el acceso de aplicaciones o sitios web de terceros a las APIs. |
| Create an Availability Zone | Una zona de disponibilidad (Availability Zone) es un conjunto lógico o físico de data centers que contienen uno o más servicios API Connect. Las zonas de disponibilidad proporcionan redundancia y conmutación por error en caso de problemas de red. Se proporciona una zona de disponibilidad predeterminada cuando instala API Connect, pero puede agregar más zonas de disponibilidad para reflejar la topología de su centro de datos. |
| Administer members and roles | Puede agregar más usuarios como miembros de administración de la organización y controlar sus permisos asignando roles predefinidos. También puede crear sus propios roles personalizados. |
| Monitor your API Connect cloud | API Connect genera eventos para permitirle monitorear el estado de su nube. |

1. **Acceder a la interfaz de usuario de Cloud Manager**

Cómo navegar e iniciar sesión en la interfaz de usuario de Cloud Manager.

**Antes de comenzar:**

Para abrir la interfaz de usuario de Cloud Manager, ingrese la URL del endpoint <cloud-admin-ui> que se ingresó durante la instalación, seguido de /admin (***https://<cloud-admin-ui>/admin***). El endpoint <cloud-admin-ui> se configura en el subsistema Management mediante el siguiente comando: apicup subsys set mgmt cloud-admin-ui <endpoint>.

La primera vez que acceda a la interfaz de usuario de Cloud Manager, ingrese **admin** como nombre de usuario y **7iron-hide** como contraseña. Se le solicitará que cambie la contraseña y la dirección de correo electrónico del administrador de la nube.

**Importante:** La primera vez que acceda a la consola en la nube, debe, por razones de seguridad, ingresar una nueva contraseña y su dirección de correo electrónico. Si olvida su contraseña y solicita un **restablecimiento de contraseña**, el correo electrónico de notificación se envía a esta dirección de correo electrónico. El correo electrónico es enviado por el servidor de correo electrónico que está configurado en la sección **Notifications** de la **cloud Settings**.

1. **Activando su cuenta de usuario de Cloud Manager**

Si ha sido invitado a ser administrador de su nube API Connect, debe activar su cuenta mediante el enlace de activación que le envió otro administrador. Luego puede acceder a la interfaz de usuario de Cloud Manager.

**Procedimiento:**

* 1. Complete los siguientes pasos para activar su cuenta de Cloud Manager:

**Si el proveedor de identidad usa LDAP:**

Se envía un correo electrónico de invitación con un enlace de activación. Haga clic en el enlace de activación o péguelo en un navegador para iniciar sesión directamente con sus credenciales de usuario LDAP. Tras la autenticación, el registro de usuario de API Connect se actualiza desde el proveedor de identidad backend.

**Si el proveedor de identidad utiliza un registro local:**

Se envía un correo electrónico de invitación con un enlace de activación. Haga clic en el enlace de activación o péguelo en un navegador. El enlace de activación lo lleva a una página de registro donde ingresa su nombre, apellido y contraseña. Las contraseñas deben tener un mínimo de 8 caracteres y contener caracteres de al menos tres de las cuatro categorías siguientes:

* Letras mayúsculas
* Letras minúsculas
* Números
* Caracteres especiales (por ejemplo: ! # $ %)

**Nota:**

La dirección de correo electrónico que ingrese en la página de registro debe coincidir con la dirección de correo electrónico a la que se envió el correo electrónico de invitación; de lo contrario, la activación de la cuenta fallará.

Si anteriormente tenía una cuenta que fue eliminada y está siendo invitado nuevamente, debe reactivar su cuenta usando la opción Iniciar sesión (Sign In) en la página, no usando la opción Registrarse (Sign Up) para completar el formulario de registro; intentar volver a registrarse fallará.

**Si el proveedor de identidad utiliza una URL de autenticación:**

Se envía un correo electrónico de invitación con un enlace de activación. Haga clic en el enlace de activación o péguelo en un navegador. El enlace de activación lo lleva a una página de registro donde ingresa sus credenciales, que luego se convierten en su nombre de usuario y contraseña. Tras la autenticación, el registro de usuario de API Connect se actualiza desde el proveedor de identidad backend.

Si hay varios **user registries** disponibles para su selección en la página de registro, asegúrese de que esté seleccionado el registro correcto para su cuenta de Cloud Manager. Es posible que deba preguntarle a su administrador qué **user registry** es apropiado para su cuenta.

Para obtener información sobre cómo configurar los **user registries** y ponerlos a disposición para el inicio de sesión de Cloud Manager, consulte [User registries overview](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.cmc.doc/capic_cmc_registries_concepts.html)  y  [Selecting user registries for Cloud Manager and API Manager](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.cmc.doc/task_cmc_set_userReg.html" \o "Select the user registries to authenticate users for Cloud Manager and API Manager.).

* 1. Haga clic en **Sign up** para completar su registro, luego haga clic en **Sign in** para abrir la página de inicio de sesión de Cloud Manager.

Ha creado su cuenta de administrador de API Connect!!

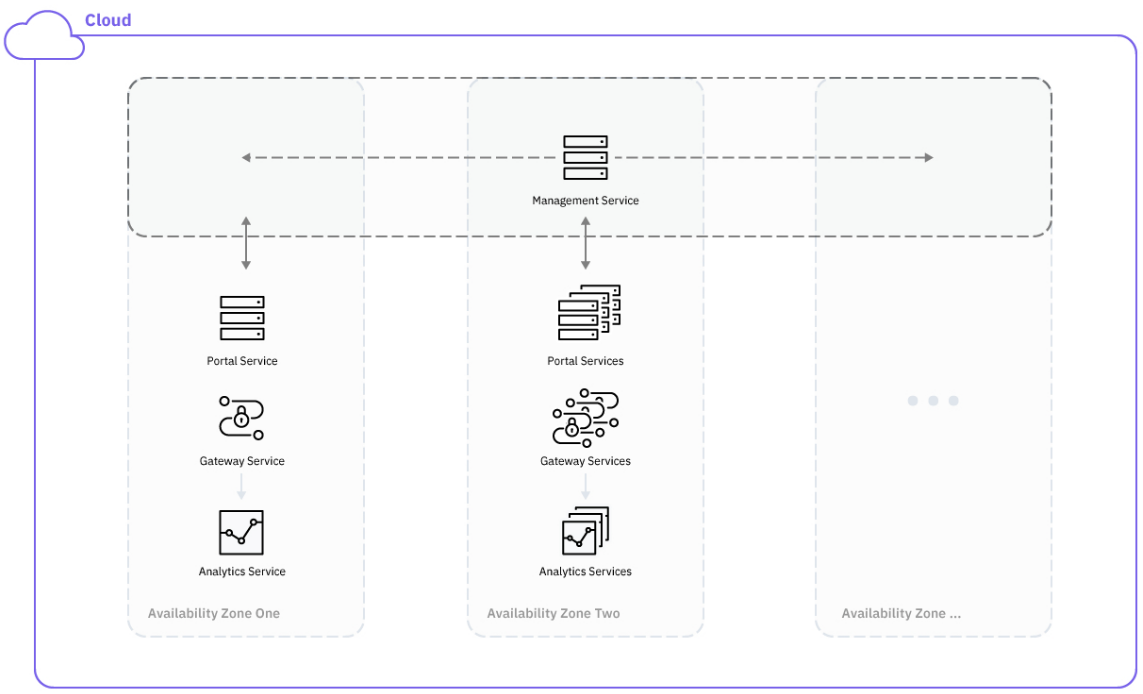
1. **Definición de la topología de Cloud Manager**

Para definir su nube local de API Connect, defina las zonas de disponibilidad y registre los servicios dentro de esas zonas para crear, promover y realizar un seguimiento de las API de forma segura. El procedimiento de instalación proporciona la configuración inicial de una zona de disponibilidad que contiene el Management Service.

**Acerca de esta tarea**

La topología de Cloud Manager consta de zonas de disponibilidad que contienen los servicios API Connect (management, gateway, analytics and portal services). Las zonas de disponibilidad pueden contener uno o más Gateway Services, Analytics Service y Portal Services, pero hay un solo Management Service que abarca todas las zonas de disponibilidad. Al configurar sus zonas de disponibilidad y servicios, la práctica recomendada es que los Gateway, Analytics y Portal Services no se comuniquen entre las zonas de disponibilidad. Solo el servicio de administración puede atravesar las zonas de disponibilidad.

El siguiente diagrama ilustra la topología de los servicios y las zonas de disponibilidad en una red de API Connect:



Se requiere uno de los siguientes roles para registrar y administrar servicios:

* Administrator
* Topology Administrator
* Owner
* Un rol personalizado con el permiso “Topology:Manage”

Las siguientes son las tareas involucradas en la definición de la topología de API Connect:

* Cree una o más zonas de disponibilidad.
* Registre uno o más Gateway, Analytics, and Portal services en cada zona de disponibilidad.
* Asociar un Analytics service con cada Gateway service.
* Establecer la visibilidad de los servicios

Hay dos tipos de escenarios de implementación:

1. Implementación basada en dispositivos utilizando archivos OVA en máquinas virtuales

2. Implementación basada en contenedores con clústeres de Docker y Kubernetes

La configuración del servicio de administración será diferente según el escenario de implementación. Para ambos, la utilidad de instalación agrega un Management Service a la zona de disponibilidad predeterminada.

Una vez que se define la nube y se ha configurado un servidor de correo electrónico, invita a otros usuarios a acceder al API Management para crear API. Exponga estas API a la comunidad de desarrolladores a través de la interfaz de usuario del Developer Portal.

Para definir la nube de API Connect, complete las siguientes tareas:

* 1. **Configuración del Management service**

Un Management Service se configura en la zona de disponibilidad predeterminada mediante el script de instalación. Para una implementación basada en Appliance de máquinas virtuales, se pueden configurar Management services adicionales mediante el archivo OVA. Para una implementación basada en contenedores, solo se configura un Management service para la nube.

**Antes de que empieces:**

Debes completar las siguientes tareas:

* Ejecute el programa de instalación **Install Assist** para configurar la zona de disponibilidad predeterminada que contiene el Management service. Consulte [Installing API Connect into a Kubernetes environment](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.install.doc/tapic_install_Kubernetes_overview.html) y [Deploying the Management OVA file](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.install.doc/overview_installing_mgmtvm_apimgmt.html#overview_installing_mgmtvm_mgmt).

**Acerca de esta tarea**

El Management service se agrega a su nube mediante el script de instalación. Se agregará a la zona de disponibilidad predeterminada. No puede agregar ni configurar Management services mediante la interfaz de usuario de Cloud Manager.

El Management service se maneja de manera diferente según la opción de implementación:

* **Implementación basada en Appliance:** los servicios de API Connect se implementan en máquinas virtuales mediante un archivo de configuración OVA. Se pueden implementar varios Management services, pero cada zona de disponibilidad solo puede tener un servicio de administración.
* **Implementación basada en contenedores:** los servicios se implementan en contenedores Docker y se administran en clústeres de Kubernetes. Se implementa un Management service para toda la nube mediante el script de instalación.

Con esto, tendrá configurado uno o más servicios de administración.

* 1. **Crear una Availability Zone**

Una zona de disponibilidad es un conjunto lógico o físico de centros de datos que contienen uno o más servicios API Connect. Las zonas de disponibilidad proporcionan redundancia y conmutación por error en caso de problemas de red. La zona de disponibilidad predeterminada se crea durante la instalación; incluye un Management service.

**Antes de que empieces:**

Debes completar la siguiente tarea:

Ejecute **Install Assist** para configurar la zona de disponibilidad predeterminada que contiene el Management service. Consulte  [Installing API Connect into a Kubernetes environment](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.install.doc/tapic_install_Kubernetes_overview.html) o [Deploying the Management OVA file](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.install.doc/overview_installing_mgmtvm_apimgmt.html#overview_installing_mgmtvm_mgmt).

**Acerca de esta tarea:**

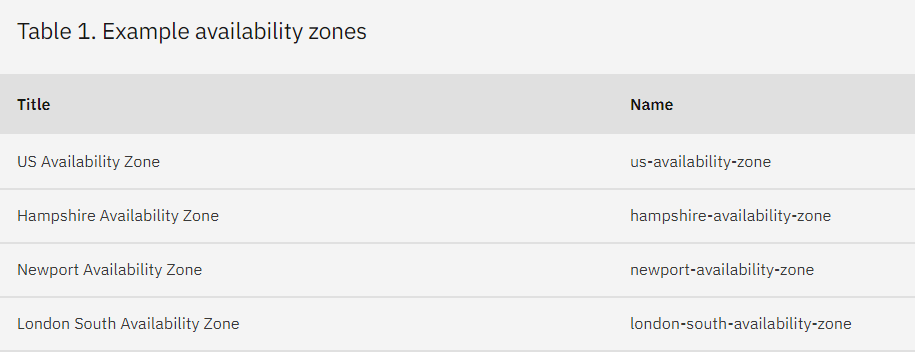
Las zonas de disponibilidad organizan las operaciones de API Connect según las necesidades de su negocio. Las zonas de disponibilidad son conjuntos de centros de datos lógicos o físicos que contienen uno o más servicios de API Connect. Varias zonas de disponibilidad en su nube proporcionan redundancia y conmutación por error en caso de problemas de red. Las zonas de disponibilidad se pueden organizar por región, para la separación global o para la separación física o lógica de los centros de datos.

La zona de disponibilidad predeterminada se crea durante el proceso de instalación. Contiene el Management service que fue configurado por Install Assist. Registre uno o más servicios Portal, Analytics y Gateway en las zonas de disponibilidad para configurar la topología de la nube de API Connect.

**Nota:**

Para implementaciones basadas en Appliance, se pueden agregar Managememt services adicionales (uno por zona de disponibilidad) mediante el script de instalación. Sin embargo, para las implementaciones basadas en contenedores que usan Docker y Kubernetes, solo se permite un Management service. No se pueden agregar Management services adicionales si está utilizando una implementación basada en contenedores.

Cuando crea una zona de disponibilidad, debe proporcionar un título descriptivo; se genera automáticamente un nombre para identificación interna. Por ejemplo:



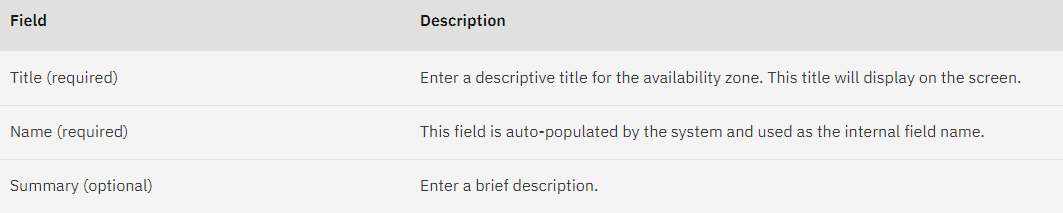
Se requiere uno de los siguientes roles para agregar y administrar zonas de disponibilidad:

* Administrator
* Topology Administrator
* Owner
* Un rol personalizado con el permiso “Topology:Manage”

**Procedimiento:**

Siga estos pasos para agregar una o más zonas de disponibilidad adicionales a su nube local:

* 1. En Cloud Manager, haga click en Topology**Topology**.
  2. Verá las Zonas de disponibilidad actuales configuradas en su nube. La zona de disponibilidad predeterminada se crea mediante el script de instalación e incluye el Management service. Para agregar otra zona de disponibilidad, elija **Create Availability Zone**.
  3. Ingrese los siguientes valores:
  4. Haga click en **Create** para completar la operación.



La zona de disponibilidad se agregará en la página **Services**. Ahora puede agregar servicios Gateway, Analytics y Portal a la zona de disponibilidad.

* 1. **Registro de un Gateway service:**

Se requiere un Gateway service para manejar el tráfico entrante (incoming traffic) de las API.

**Antes de que empieces:**

Antes de registrar un Gateway service en Cloud Manager, el Gateway service de DataPower® API Connect debe instalarse como un subsistema en su clúster de Kubernetes o habilitarse en el Appliance DataPower. Para un entorno de Kubernetes, consulte  [DataPower Gateway subsystem on Kubernetes](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.install.doc/tapic_v10_install_kubernetes_gwy.html). Para Appliance, consulte [Configuring API Connect Gateway Service](https://www.ibm.com/support/knowledgecenter/en/SS9H2Y_10.0/com.ibm.dp.doc/apicgws_configuring.html) para obtener más información.

También complete la siguiente tarea: [Configuring the Management service](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.cmc.doc/create_node_mgmt_1.html)

**Acerca de esta tarea:**

Un Gateway service representa un grupo de servidores de gateway que alojan API publicadas y proporcionan los API endpoint que utilizan las aplicaciones cliente. Los gateway ejecutan invocaciones de API proxy para sistemas backend y hacen cumplir las políticas de API, incluidas client identification, security and rate limiting.

Se requiere uno de los siguientes roles para registrar y administrar los Gateway services:

* Administrator
* Topology Administrator
* Owner
* Un rol personalizado con el permiso “Topology:Manage”

**Nota:**

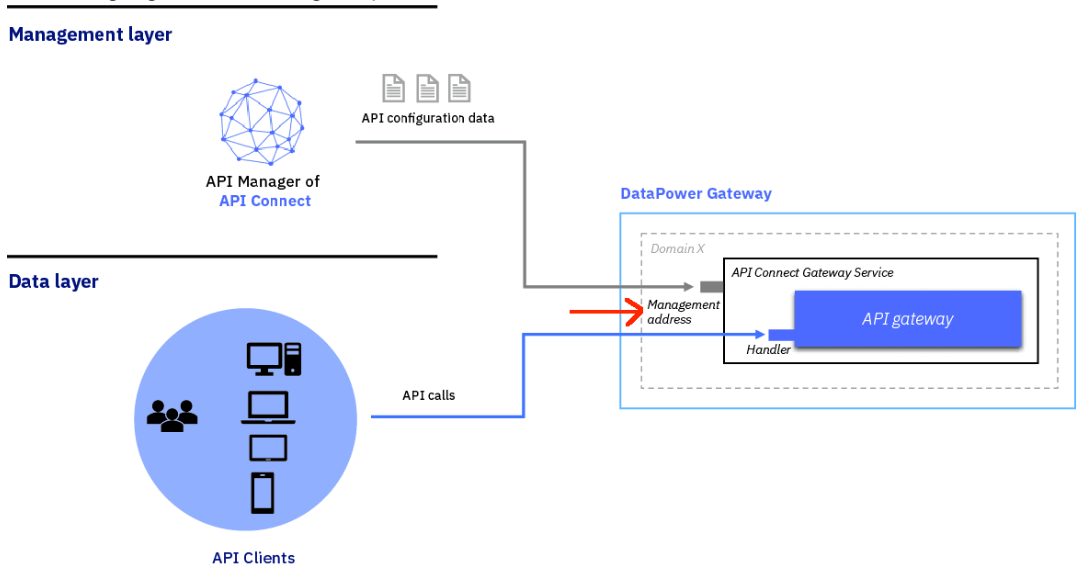
También puede registrar y administrar los Gateway services utilizando el **developer toolkit CLI**; para obtener más información, consulte [apic gateway-services](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.cliref.doc/apic_gateway-services.html).

**Procedimiento:**

1. En Cloud Manager, haga click en Topology**Topology**.
2. En la zona de disponibilidad que contendrá el Gateway service, seleccione **Register Service**.
3. En la página Configure Service, seleccione **DataPower Gateway** como tipo de servicio. Seleccione el tipo de Gateway que desea crear, ya sea DataPower Gateway (compatible con v5) o DataPower API Gateway. Para obtener una descripción de los tipos de gateway, consulte  [API Connect gateway types](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.overview.doc/rapic_gateway_types.html).
4. Ingrese los valores para configurar el servicio Gateway. Deberá obtener los endpoint de su configuración de implementación. Para un entorno de Kubernetes, los endpoint se configuran mediante los siguientes valores en el archivo CR (custom resource/recurso personalizado). Para un Appliance, el endpoint se configura en DataPower.

|  |  |
| --- | --- |
| **Field** | **Description** |
| Title (required) | Ingrese un título descriptivo para el gateway service. Este título se mostrará en la pantalla. |
| Name (required) | El sistema rellena automáticamente este campo y se utiliza como nombre de campo interno. |
| Summary (optional) | Ingrese una breve descripción. |
| **Management endpoint on the gateway service:**  Endpoint (required) | Ingrese al endpoint del servicio API Connect Gateway.   * Para un entorno de Kubernetes, el Management Endpoint es el endpoint creado en el CR (custom resource). Consulte [DataPower Gateway subsystem on Kubernetes](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.install.doc/tapic_v10_install_kubernetes_gwy.html) para obtener más información. * Para un Appliance, el Management Endpoint es la *Management address* del servicio API Connect Gateway que se muestra en el diagrama [gateway service connection diagram](https://www.ibm.com/docs/es/api-connect/10.0.1.x?topic=topology-registering-gateway-service#config_gateway__gw_service_conn_diag) (se muestra más abajo). Para un gateway, esto toma el formato ***http://<ip-address-for-gateway>:3000***. Para múltiples gateways, sería ***address:port*** del balanceador de carga |
| **Management endpoint on the gateway service:**  TLS client profile (required) | Especifique el perfil de cliente TLS que se utilizará cuando se contacte con el gateway a través del Management Endpoint.  **Nota:** El valor predeterminado es **Gateway management client TLS client profile:1.0.0**. Si está utilizando un DataPower Gateway en una implementación de Kubernetes, con TLS mutuo habilitado, utilice esta configuración. Para cualquier otro gateway, si el gateway no está configurado con las credenciales TLS correctas, el registro del gateway fallará con esta configuración. Para evitar fallas en el registro, seleccione **Default TLS client profile:1.0.0** o su propio perfil de cliente TLS personalizado. Para obtener información sobre cómo configurar un perfil de cliente TLS personalizado, consulte [Creating a TLS Client Profile](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.cmc.doc/ssl_client.html). |
| **API invocation endpoint:**  API endpoint base (required) | Ingrese la parte base de la URL que se asigna a la parte base de la URL para el tráfico API entrante. Es un FQDN público con rutas adicionales que son específicas de sus llamadas a la API. Por ejemplo: https://api.mycompany.com |
| **API invocation endpoint:**  Server Name Indication (SNI) - Host name | Para soportar Server Name Indication (SNI) en el API Endpoint Base. Se requiere el nombre de host predeterminado '\*' para permitir todos los hosts. Ingrese otros nombres de host según sea necesario. Se admite el formato de comodín. La capacidad SNI le permite servir varios nombres de host TLS seguros a través del mismo servicio gateway, utilizando la misma dirección IP y puerto, sin necesidad de que utilicen el mismo perfil TLS.  **Nota:** Para permitir requests de clientes que no admiten SNI, debe incluir un valor de nombre de host de '\*'. |
| **API invocation endpoint:**  Server Name Indication (SNI) - TLS server profile | El perfil del servidor TLS que admite el hostname especificado para SNI. |
| OAuth shared secret (optional) | Para los sitios que usan proveedores nativos de OAuth, ingrese el **shared secret** que usarán todas las llamadas API que atraviesan el gateway.  **Nota:** El shared secret especificado debe tener 64 caracteres (64 bytes) de longitud, con el prefijo 0x y debe constar solo de caracteres hexadecimales. Por ejemplo: 0xa354282f227c10250511ae9c9e8c7ed9f4f1bd0d7c04cb6d5bd178f8c62296e3 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

El siguiente diagrama ilustra la conexión del servicio gateway:



1. Cuando haya terminado, haga clic en **Save**. El servicio Gateway se agrega a la zona de disponibilidad adecuada para su nube.
   1. **Registro de un Analytics service:**

Configure al menos un servicio de análisis en su nube local de API Connect. El servicio de análisis siempre está asociado con un servicio gateway, del cual recopila datos de eventos de API.

**Antes de que empieces:**

Debes completar las siguientes tareas: [Creating an Availability Zone](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.cmc.doc/az_create.html) y [Registering a gateway service](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.cmc.doc/config_gateway.html)

**Acerca de esta tarea:**

El Analytics service recopila datos de eventos de API del servicio gateway. En Cloud Manager, configure el analytics service y luego lo asocia con una o más gateway. Puede tener varios gateways asociados con un solo analytics service, pero cada gateway se puede asociar con un solo analytics service. Con el analytics service, puede filtrar, ordenar y agregar los datos de eventos de la API y ver los resultados en un Dashboard.

Se requiere uno de los siguientes roles para registrar y administrar los servicios de Analytics:

* Administrator
* Topology Administrator
* Owner
* Un rol personalizado con el permiso “Topology:Manage”

**Procedimiento:**

Complete los siguientes pasos para configurar el Analytics service en su nube:

1. En Cloud Manager, haga click en Topology**Topology**.
2. En la zona de disponibilidad que contendrá el Analytics service, seleccione **Register Services > Analytics**.
3. Ingrese los valores para configurar el Analytics service:

|  |  |
| --- | --- |
| **Field** | **Description** |
| Title (required) | Ingrese un título descriptivo para el Analytics service. Este título se mostrará en la pantalla. |
| Name (required) | El sistema rellena automáticamente este campo y se utiliza como nombre de campo interno. |
| Summary (optional) | Ingrese una breve descripción. |
| **Management endpoint on the analytics service:** Endpoint (required) | Ingrese el nombre de dominio completo (fully-qualified domain name) para el Analytics client endpoint que definió durante la instalación.  **Nota:** Si inhabilitó el almacenamiento interno para Analytics, proporcione el ingestion endpoint en su lugar.   * En una implementación de Kubernetes, el client endpoint (o ingestion endpoint) se define en el CR con la variable $STACK\_HOST. Para obtener más información, consulte [Creating the Analytics CR](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.install.doc/analytics_install_create_cr_k8s.html). * En una implementación de VMware, el client endpoint (o ingestión endpoint) se define con un comando **apicup** durante la instalación. Para obtener más información, consulte [Deploying the Analytics subsystem](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.install.doc/overview_installing_analytics_ova.html). |
| TLS client profile (required) | Seleccione el **TLS Client Profile** que se utilizará para comunicarse con el Analytics service. El Client Profile se aplica al endpoint que especificó en la fila anterior. |
| Advanced analytics configuration (available when editing an analytics service) | Configure parámetros avanzados en Kibana. |

1. Haga click en **Save** para completar la operación. Con esto el Analytics service se agrega a la configuración de su nube.
   1. **Registro de un Portal service:**

Defina uno o más servicios de portal en su nube local de API Connect..

**Antes de que empieces:**

Debes completar las siguientes tareas:

* [Creating an Availability Zone](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.cmc.doc/az_create.html)
* [Registering a gateway service](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.cmc.doc/config_gateway.html)
* [Configuring an email server for notifications](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.cmc.doc/config_emailserver.html)
* [Setting up notifications](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.cmc.doc/task_cmc_config_notifications.html)

**Acerca de esta tarea:**

Cada zona de disponibilidad contiene uno o más Portal services. El Portal service proporciona un portal para desarrolladores que utilizan los desarrolladores de aplicaciones para descubrir las API y los consumidores incorporados. Se debe configurar un servidor de correo electrónico y establecerlo como servidor de correo electrónico para la nube antes de registrar un Portal service.

Se requiere uno de los siguientes roles para registrar y administrar los servicios de Analytics:

* Administrator
* Topology Administrator
* Owner
* Un rol personalizado con el permiso “Topology:Manage”

**Procedimiento:**

Complete los siguientes pasos para configurar el Portal service en su nube:

1. En Cloud Manager, haga click en Topology**Topology**.
2. En la zona de disponibilidad que contendrá el Portal service, seleccione **Register Services > Portal**.
3. Ingrese los valores para configurar el Portal service:

|  |  |
| --- | --- |
| **Field** | **Description** |
| Title (required) | Ingrese un título descriptivo para el Portal service. Este título se mostrará en la pantalla. |
| Name (required) | El sistema rellena automáticamente este campo y se utiliza como nombre de campo interno. |
| Summary (optional) | Ingrese una breve descripción. |
| **Management endpoint on the portal service:** Endpoint (required) | Ingrese la dirección IP, el hostname completo (fully-qualified host name), el service o ingress name. Se utiliza para la comunicación con API Manager.   * En una implementación de Kubernetes, el endpoint se define en el CR mediante **api.portal.$STACK\_HOST**. Consulte [Developer Portal subsystem on Kubernetes](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.install.doc/tapic_v10_install_kubernetes_portal.html). * Si se configura durante la instalación en un entorno VMware, es el valor de **apicup subsys set portal portal-admin**. |
| **Management endpoint on the portal service:**  TLS client profile (optional) | Seleccione el TLS client profile que se utilizará para comunicarse con el Portal service. El perfil se aplica al ingestión endpoint. |
| Portal website URL (required) | La URL que se utilizará para el acceso público al portal.   * En una implementación de Kubernetes, el endpoint se define en el CR por **portal.$STACK\_HOST**. Consulte [Developer Portal subsystem on Kubernetes](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.install.doc/tapic_v10_install_kubernetes_portal.html). * Si se configura durante la instalación en un entorno VMware, es el valor de **apicup subsys set portal portal-www <portal>.<hostname>.<domainname>**.   Se pueden configurar varios endpoint portal-www, como se describe aquí en estos temas:   * [Defining multiple portal endpoints for a Kubernetes environment](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.install.doc/tapic_multi_urls_portal.html) * [Defining multiple portal endpoints for a VMware environment](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.install.doc/tapic_multi_urls_portal_vm.html) |

1. Cuando haya terminado, haga clic en **Save**. El Portal service está configurado en su nube y se puede utilizar para publicar API.
   1. **Asociación de un Analytics service con un Gateway service:**

Para recopilar datos sobre el uso de su API y otras estadísticas, debe asociar un Analytics service con cada gateway service. Puede asociar varios Gateway services con un Analytics service, pero cada gateway se puede asociar con un solo Analytics service.

**Antes de que empieces:**

Debes completar las siguientes tareas:

* Ejecute Install Assist para configurar la zona de disponibilidad predeterminada que contiene el Management service.
* Registre un Gateway service y un Analytics service.

**Acerca de esta tarea:**

Cada Gateway service está asociado con un Analytics service. Cada Gateway service se puede asociar con un solo analytics service (una relación uno-uno), sin embargo, cada analytics service se puede asociar con uno o más gateway services (una relación uno-muchos). El analytics service asociado recopila datos de eventos de API del Gateway service.

Para asociar un analytics service con un gateway, primero debe configurar al menos un analytics service y un Gateway service.

Se requiere uno de los siguientes roles para asociar un analytics service con un analytics service:

* Administrator
* Topology Administrator
* Owner
* Un rol personalizado con el permiso “Topology:Manage”

**Procedimiento:**

Complete los siguientes pasos para configurar el Portal service en su nube:

1. En Cloud Manager, haga click en Topology**Topology**.
2. En la sección de la zona de disponibilidad en la que desea trabajar, ubique el gateway service que requiere un analytics service en la columna **SERVICE**.
3. Busque la columna **ASSOCIATED ANALYTICS SERVICE**.
4. Si se ha configurado un servicio Analytics, el Associate Analytics service link está habilitado para cada servicio Gateway. Haga clic en **Associate Analytics Service** en la misma fila que el servicio gateway que requiere un servicio Analytics.
5. En **Associate Analytics Service**, verá el nombre del servicio Gateway y una lista de los servicios Analytics que se han configurado en su nube.
6. Seleccione el servicio Analytics para asociarlo con el servicio Gateway agregando una marca de verificación, luego haga clic en **Associate**.
7. Para eliminar el servicio Analytics asociado, seleccione **Unassociate analytics service** en el menú de acciones. Tenga en cuenta que cuando no hay un servicio Analytics asociado con un servicio gateway, toda la recopilación de análisis (analytics collection) se deshabilitará y no habrá datos en los dashboard de API Manager ni en los sistemas de terceros que haya configurado.

El Analytics service está asociado con un servicio gateway y recopilará datos de eventos de API para ese gateway.

* 1. **Establecer visibilidad para un servicio:**

La configuración de visibilidad determina qué organizaciones proveedoras pueden acceder a un servicio.

**Antes de que empieces:**

Debes completar las siguientes tareas:

* Ejecute Install Assist para configurar la zona de disponibilidad predeterminada que contiene el Management service
* Cree zonas de disponibilidad adicionales si es necesario, consulte [Creating an Availability Zone](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.cmc.doc/az_create.html)
* Registre al menos un servicio gateway, consulte [Registering a gateway service](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.cmc.doc/config_gateway.html)
* Registrar otros servicios

**Acerca de esta tarea:**

La configuración de visibilidad controla qué organizaciones proveedoras pueden utilizar un servicio. La configuración de visibilidad predeterminada es **Public**.

Se requiere uno de los siguientes roles para configurar la visibilidad de los servicios:

* Administrator
* Topology Administrator
* Owner
* Un rol personalizado con el permiso “Topology:Manage”

**Procedimiento:**

Siga estos pasos para configurar la visibilidad de los servicios en su nube local:

1. En Cloud Manager, haga click en Topology**Topology**.
2. En la lista de Servicios, elija **Set visibility** en el menú **actions** junto al nombre del servicio que requiere la configuración de visibilidad.
3. Seleccione la configuración de visibilidad para el servicio. Las opciones son:

* **Private**: el servicio no es visible y no puede ser utilizado por ninguna organización proveedora.
* **Public**: el servicio es visible y puede ser utilizado por todas las organizaciones proveedoras.
* **Custom**: el servicio solo es visible para las organizaciones proveedoras designadas por usted.

1. Para la visibilidad **Custom**, seleccione las organizaciones proveedoras que podrán utilizar el servicio.
2. Haga clic en **Make visible** para completar la operación.

Para **Private**, el servicio no puede ser utilizado por ninguna organización proveedora. Para **Public**, el servicio puede ser utilizado por todas las organizaciones proveedoras. Para **Custom**, el servicio puede ser utilizado por las organizaciones proveedoras que usted designe.

1. **Configurar un servidor de correo electrónico para notificaciones**

Conéctese a un servidor de correo electrónico en su nube local de API Connect. El servidor de correo electrónico envía invitaciones de registro y otros correos electrónicos impulsados por eventos. Debe configurar el servidor de correo electrónico antes de agregar cualquier organización proveedora o registrar un Portal Service. De lo contrario, el propietario de la organización no recibirá el correo electrónico con los detalles que requiere para acceder al API Managemet.

**Antes de empezar:**

Debe completar las tareas en la siguiente sección: [Defining your Cloud Manager topology](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.cmc.doc/api_create.html#api_create)

**Acerca de esta tarea:**

Esta tarea puede ser completada por usuarios a quienes se les asigna uno de los siguientes roles:

* Cloud Owner (Propietario de la nube)
* Cloud Administrator (Administrador de la nube)
* Topology Administrator (Administrador de topología)
* Custom role with Settings:Manage permission (Rol personalizado con configuración: administrar permisos)

El servidor de correo electrónico envía correos electrónicos de invitación con enlaces de activación y otros mensajes del sistema. Se puede configurar más de un servidor de correo electrónico en Cloud Manager, pero solo se puede seleccionar un servidor de correo electrónico como servidor activo para enviar notificaciones a la vez. Para obtener instrucciones sobre cómo seleccionar el servidor de correo electrónico activo y ver una lista de los mensajes de correo electrónico que se envían, consulte [Setting up notifications](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.cmc.doc/task_cmc_config_notifications.html).

**Nota:**

Si no selecciona un servidor de correo electrónico para enviar correos electrónicos de notificación, un usuario no podrá restablecer su contraseña desde las páginas de inicio de sesión de Cloud Manager o API Manager.

**Procedimiento:**

Para configurar uno o más servidores de correo electrónico para usarlos en las notificaciones por correo electrónico en Cloud Manager, complete los siguientes pasos:

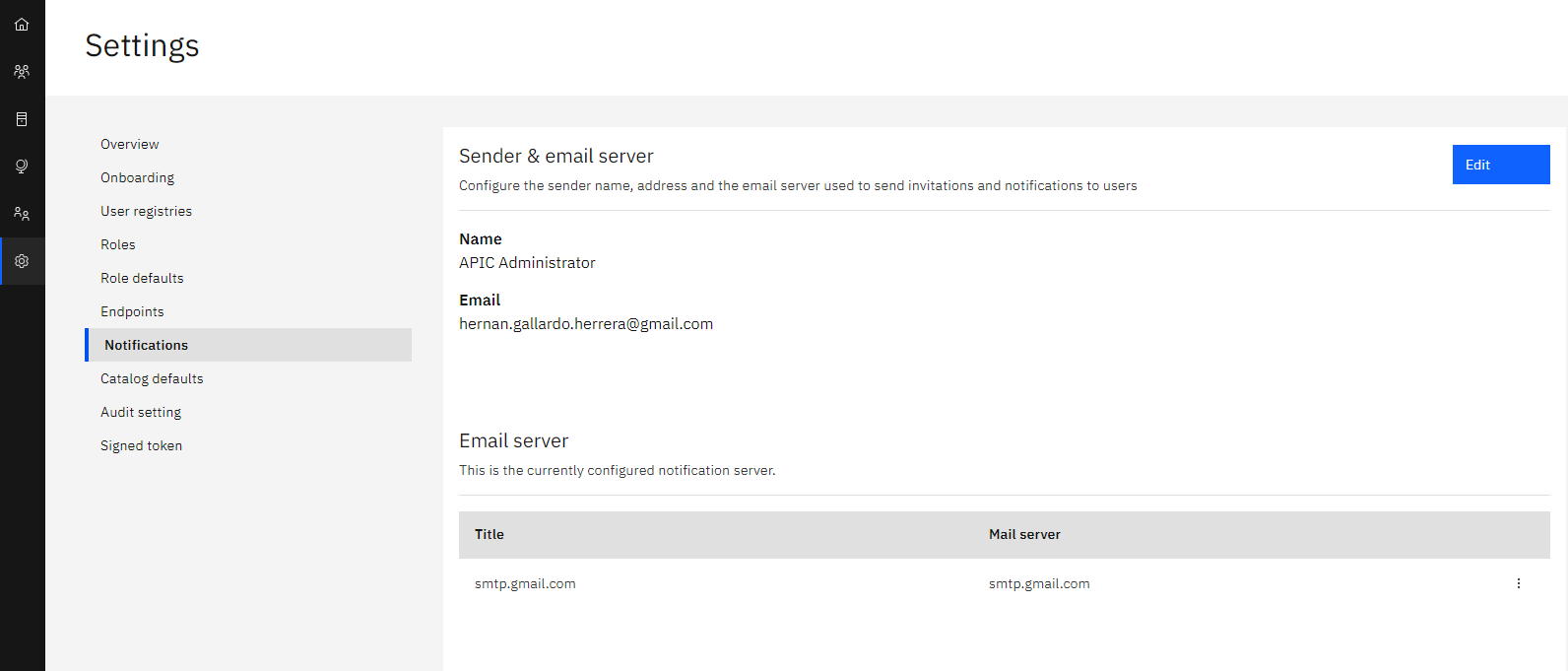
* 1. En Cloud Manager, haga click en Resources**Resources**
  2. Elija **Notifications**.
  3. Ingrese los valores para configurar el servidor de correo electrónico.

|  |  |
| --- | --- |
| **Field** | **Description** |
| Title (required) | Ingrese un título descriptivo para la zona de disponibilidad. Este título se mostrará en la pantalla. |
| Name (required) | El sistema rellena automáticamente este campo y se utiliza como nombre de campo interno. |
| Address (required) | Dirección IP del servidor de correo electrónico |
| Port (required) | Puerto en el que se ejecuta el servidor de correo electrónico |
| Authenticate User | Introduzca un nombre de usuario para utilizarlo para la autorización con el servidor SMTP. El nombre de usuario es obligatorio si el servidor SMTP requiere autenticación. |
| Authenticate Password | Ingrese la contraseña para el usuario autenticado. Esta contraseña se utiliza para la autorización con el servidor SMTP. La contraseña es necesaria si el servidor SMTP requiere autenticación. |
| TLS Client Profile (optional) | Seleccione un perfil de cliente TLS opcional que se utilizará para comunicarse con el servidor de correo electrónico si se selecciona la opción Conexión segura (Secure Connection). |
| Secure Connection | Seleccione esta opción para especificar que se utiliza seguridad TLS. Se aplican las siguientes condiciones:   * Si esta opción no está seleccionada, la seguridad TLS no se usa incluso si el servidor de correo electrónico está configurado para usar el protocolo STARTTLS. * Si se selecciona esta opción y se selecciona un perfil de cliente TLS, se utiliza ese perfil y se respeta la configuración del protocolo STARTTLS en el servidor de correo electrónico. * Si se selecciona esta opción y no se selecciona ningún perfil de cliente TLS, se utiliza el perfil de cliente TLS predeterminado y se respeta la configuración del protocolo STARTTLS en el servidor de correo electrónico. |

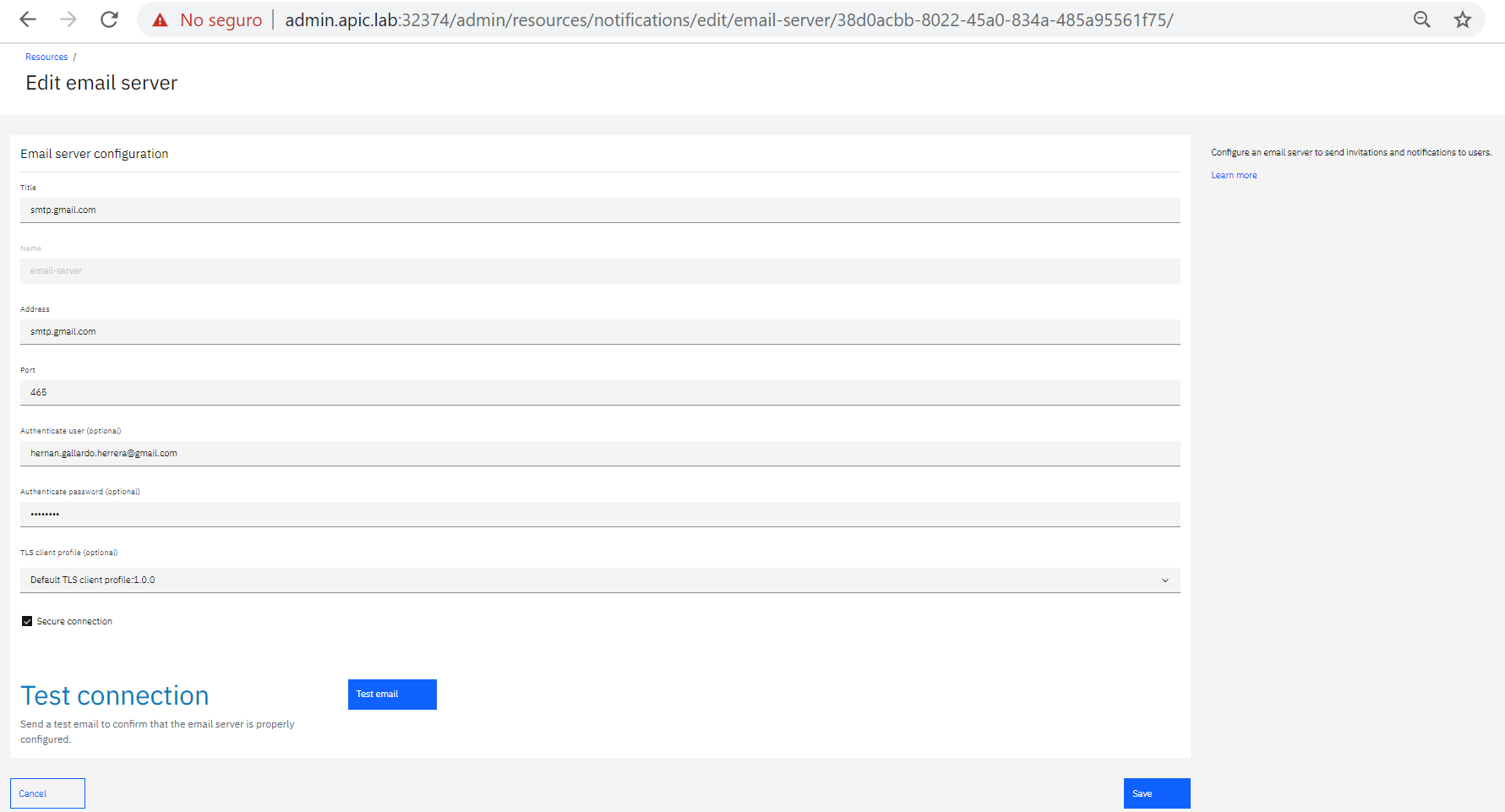
* 1. Puede enviar un correo electrónico de prueba para confirmar que el servidor de correo electrónico está configurado correctamente. Haga clic en **Test email** en el panel **Test Connection** para abrir una ventana de diálogo. Ingrese una o más direcciones de correo electrónico válidas en el campo **Recipients**. Separe varios destinatarios con comas. Haga clic en **Send test email**. Compruebe que los destinatarios hayan recibido el correo electrónico de prueba.
  2. Si el correo electrónico de prueba tiene éxito, haga clic en **Save** para guardar la configuración del servidor de correo electrónico. Si la prueba no tiene éxito, verifique los valores de configuración y actualización según sea necesario.

**Nota:**

Para enviar correos electrónicos, debe seleccionar un servidor de correo electrónico como su servidor activo en **Settings > Notifications**, además de agregar el email como se aprecia en la siguiente imagen:



**OBS:** Para realizar pruebas con el servidor de correo de Google, active <https://myaccount.google.com/lesssecureapps> si está APAGADO, para habilitar menos aplicaciones seguras (link: <https://www.it-swarm-es.com/es/node.js/recibo-un-error-error-inicio-de-sesion-no-valido-535-5.7.8-nombre-de-usuario-y-contrasena-no-aceptados.-cuando-intento-enviar-un-correo-con-el-modulo-nodemailer-desde-node-js/806503797/>). Con esto comienza a funcionar el envío de notificaciones. La configuración para este ejemplo es la siguiente:



1. **Configurar notificaciones**

Seleccione un servidor de correo electrónico y configure la información "sent from" (enviado desde) para las notificaciones.

**Acerca de esta tarea**

En **Settings > Notifications**, seleccione el servidor de correo electrónico que desea usar como servidor activo para enviar correos electrónicos de notificación en **Resources > Notifications**. Se requiere un servidor de correo electrónico activo para enviar notificaciones por correo electrónico. Se puede configurar más de un servidor de correo electrónico en Cloud Manager, pero solo se puede seleccionar un servidor de correo electrónico para enviar notificaciones a la vez. El servidor de correo electrónico debe estar configurado y seleccionado para recibir notificaciones antes de agregar un **Portal Service** a su nube.

También configure la información del remitente (**sender**) para que se incluya en todos los correos electrónicos y, opcionalmente, edite el texto estándar para las plantillas de correo electrónico.

Se requiere uno de los siguientes roles para agregar roles para seleccionar el servidor de correo electrónico, ingresar la información del remitente y editar las plantillas de correo electrónico:

* Administrador
* Dueño
* Un rol personalizado con la configuración de la nube: administrar permisos

**Nota:**

Si no selecciona un servidor de correo electrónico para enviar correos electrónicos de notificación, el usuario no podrá restablecer su contraseña desde las páginas de inicio de sesión de Cloud Manager o API Manager.

**Procedimiento:**

* 1. En Cloud Manager, haga clic en Settings **Settings**.
  2. En la lista de navegación **Settings**, haga clic en **Notifications**.
  3. Para configurar el servidor de correo electrónico activo:
* Haga clic en **Edit** en la sección **Sender & Email Server**.
* Seleccione un servidor de correo electrónico en la lista; Se muestra una marca de verificación junto al servidor seleccionado actualmente.
* Clic en **Save**.
  1. Para eliminar un servidor de correo electrónico de la lista, haga clic en el menú **options** junto al nombre del servidor y seleccione **Delete**.
  2. Para cambiar el nombre del remitente y la dirección de correo electrónico de las notificaciones:
* Haga clic en **Edit** en la sección **Sender & Email Server**.
* Complete el nombre y la dirección de correo electrónico desde donde se enviarán las notificaciones.
* Clic en **Save**.
  1. Para obtener una vista previa y editar las plantillas de correo electrónico de notificación, consulte [Customizing email notification templates](https://www.ibm.com/docs/es/SSMNED_v10/com.ibm.apic.cmc.doc/task_cmc_email_templates.html" \o "API Connect includes a set of email templates for invitations and other notification emails. You can preview the templates and customize the text if required.).